

Advanced Computer Network
Professor Dr. Neminath Hubballi
Department of Computer Science Engineering
Indian Institute of Technology, Indore

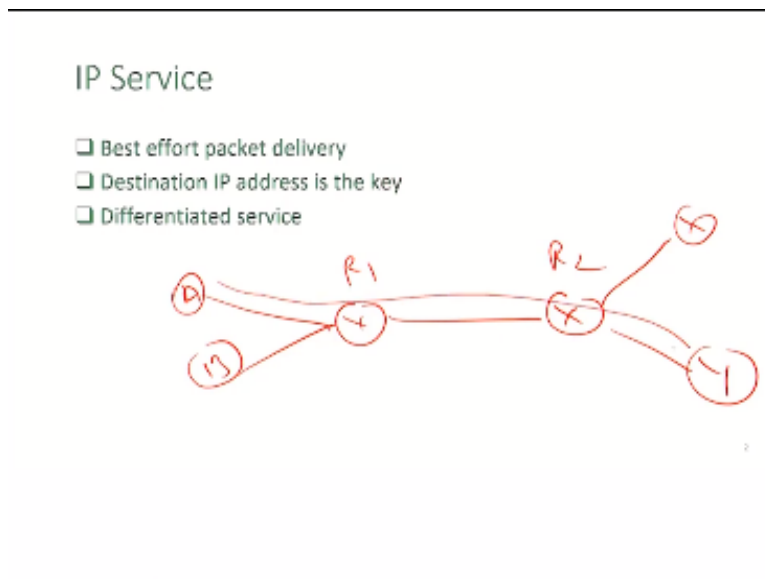
Lecture 9
Packet Classification – Part 1

Welcome back in today's lecture, we will talk about another topic called Packet Classification. And before we actually move into the content, of course so, let us take a look at what exactly did we discuss in the previous classes.

We said that the primary job of the router or any router in the internet or network is to route the packets given a packet from any source to the network; it needs to forward that to the corresponding destination.

And every router all along the path needs to do this decision of where to forward that packet. That is the forwarding decision and we see that there are millions of packets coming per second, the routers need to have the ability to forward those many number of the packets.

(Refer Slide Time: 1:12)



So, the internet or the routers, whatever the functionality that we discussed with a bunch of algorithms to provide that facility to do the lookup operation, all of that was the best effort to packet delivery meaning the network will do or every router will try to do its best to deliver the

packet to the correct destination. So, that is how the internet routers have been designed to work and it is not always guaranteed that we know very well.

And in order to do the forwarding decisions, routers consult the routing tables or the forwarding table or FIB information and they pick up the destination IP address from the header field of the packet and then do a lookup operation and forward that packet. Although routing or forwarding is the fundamental job of a router, that is not the only thing the routers are supposed to do or at least they are doing.

So, in addition to the forwarding decisions or constructing the routing tables, routers also do lot of other jobs. So, one of the other primary jobs any router on the internet does is something called as differentiated service.

What it means is if let us say there are two people, let us say A is here and B is here. These are two computers and I got a router R1 and there is a second router R2. They are connected and A and B are connected to this router R1 and there are two other computers, X and Y, which are connected to router R2.

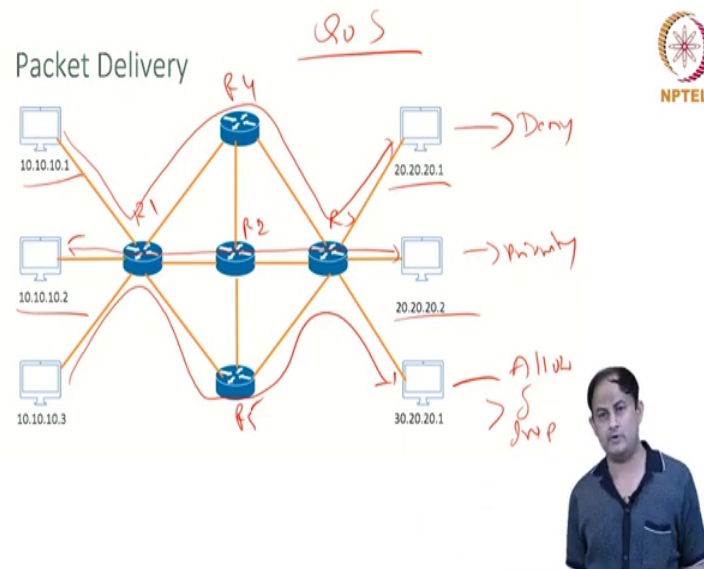
Differentiated service refers to, every time A and Y talk to each other you provide a priority-based service to these two endpoints A and Y will have priority in communication. While B and X or B and A will have a different priority assigned to them. This means I can define in the network or I can tell my routers in the network to do a kind of differentiation.

Based on who is talking to whom, what kind of protocol is being used, whether they are directly connected to the same router, or based on so many other parameters, you can actually decide to do this differentiation.

So, that is been usually practiced, and the routers which are out there in the network at least in today's network, understand how to do this differentiation and that also means that you need a mechanism to tell the routers how to do this differentiation. So, how do I specify, how do I tell my router that, for example, R1 needs to understand who A is? let us say A and Y are talking. When they are talking, so what to do when B and X are talking? What to do when A and B are talking? This kind of specific understanding is required. So, packet classification is all about doing this kind of differentiation using some mechanism.

We will try to understand in this lecture how we actually think about it. What is the mechanism? What are the algorithms? What is the operation we need to implement inside the router to facilitate this kind of differentiated operation that is the agenda.

(Refer Slide time: 4:52)



So, let us try to understand the big picture with this diagram what we see in this is a bunch of routers let me name them R1 and R2, R3, and maybe this one as R4 and this as R5. And you can see a bunch of computers connected to this. So, it is not only when A and B are talking to each other or A and X, and Y are talking to each other; you need to provide priority there are a bunch of other things that you can tell your routers to do. So, when 10.10.10.2 communicate with 20.20.20.2, you may want this to be given some priority over the other one, which is one thing.

Or when 10.10.10.1 talks to 20.20.20.1, whether he starts or he starts, I do not want to allow this communication to happen, I might tell my routers in the network that you deny this communication. So, all of the routers have something called Access Control Mechanism or Access Control List. You can use that to specify who is not allowed to talk to whom.

And suppose maybe when 10.10.10.3 talks to 30.20.20.1, and you allow this transmission to happen, but if the rate is greater than some quantity, let us say δ , you drop the packets. Up to δ

you allow but beyond the δ , you do not allow it. So, when this communication happens, when he is talking maybe he is taking this direct route, and then they are talking. So, now R1 R2 R3 need to be aware that when 10.10.10.1 is talking to 20.20.20.1, we do not want to allow them. Maybe this is actually going through R1, R4, and then R3 like this.

So, now a different set of routers, R1, R4, and R3 need to be aware of what communication is not allowed. And now, if 10.10.10.3 is talking to 30.20.20.1 this is going to a different set of the routers. Now R1, R5, and R3 need to be aware of this kind of communication.

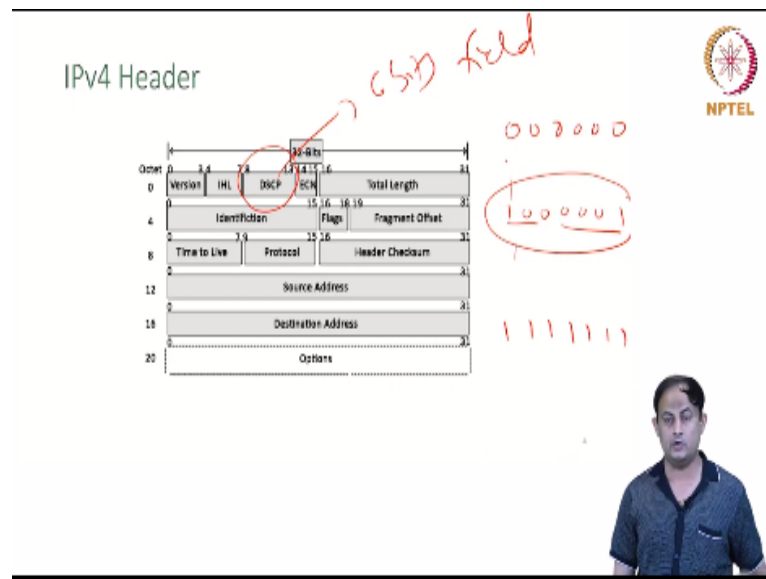
And then it is allowed but only up to a certain threshold of δ . δ may be packets per second or bytes per second, whatever parameter you want to use; using that, you need to remember what is the rate at which these two computers are communicating with each other. So, these are the kind of the stuff that we want to do.

So, this kind of differentiation is not new; even earlier also in networks, people used to do this so we call or study under generic technology called the quality of service. For a variety of reasons, why do we want to give priority to two sets of people? Why do we want to allow or deny traffic from two computers? there may be a variety of reasons. These two computers are running an audio-video communication in real time if you suppress their traffic, then the utility of the end applications might come down if you experience a jerk in the audio communication, then that is not a useful conversation.

Or there might be other reasons or we know that X and Y people connected to the internet are just running some useless application may, be playing an online game or something. Although this is a hypothetical example, no offense to people who use the internet for playing games.

But it is possible as a network service provider, I may decide what is useful, what is not useful when to curtail or drop the communication, when to provide priority to the end users, or maybe just because these two end users are subscribed to higher bandwidth they are paying more money, then you want to provide more bandwidth to them.

(Refer Slide Time: 9:34)



Now the question is, how do we actually tell this to the routers? How do the routers understand what needs to be done with this particular packet? So one of this is a picture of the IP version 4 header. So, there is a field in the IP version 4 header called the differentiated service or DSCP.

So, this is six bits field, and depending upon the value set inside these 6 bits, bit numbers 8 to 13. 6-bit field and the remaining two bits of that particular byte from 8 to 15 indicate the ECN.

ECN stands for Explicit Congestion Control. So, these six bits can be all 0s or all 1s, so 2^6 possibilities; using the values that you set, let us say my higher order bits are 100 and then this is 0001, and using this, what is the meaning? What kind of priority do you need to give to this particular packet I can tell the router.

This is one way of letting the router know what to do with a particular packet. But this is historically used by the internet service providers to tell the router, okay, this particular packet is going with the DSCP field set to this particular combination of the bits. Using that, the router will understand what priority needs to be given to this particular packet.

But over a period of time, this has become an inadequate mechanism to let the router know what to do with the particular packet; we want to do a much more sophisticated differentiation of the service. So, how do we actually do or engineer this kind of facility in the router, that is the question we will try to answer.

What kind of data structure, algorithms, and mechanism that we want to implement? In a nutshell, differentiated service requirements what is the quality of service requirements that I want to achieve in my network can be summarized in these particular points.

(Refer Slide Time: 12:05)

The slide is titled "Practical QoS Requirements" and features the NPTEL logo in the top right corner. On the left, there is a list of four requirements, each preceded by a checkbox:

- ☐ Admission control — Allow/Deny
- ☐ Resource reservation
- ☐ Per flow queuing
- ☐ Fair scheduling

To the right of the list is a hand-drawn network diagram in red ink. It shows three routers labeled R1, R2, and R3 connected in a line. R1 is connected to a source node S, and R3 is connected to a destination node D. Below the routers, there are two sets of rectangular boxes representing queues. The top set has three boxes labeled R1, R2, and R3, with arrows pointing from the routers to these boxes. The bottom set has two boxes labeled R1 and R2, with arrows pointing from the routers to these boxes. The diagram illustrates the concept of per-flow queuing and fair scheduling.

One thing that I can do is, given a particular packet or some particular node X is transmitting, I want to do the admission control. What it means is, I either allow this particular packet from this particular node or I deny it.

And this allow or deny can be dynamic, meaning it can be conditioned on how much of the traffic historically X has transmitted. So, whether in the last one minute so many number of the bytes have been transmitted from that particular node or it is less than X, or what is that?

So, it could be a combination of that, at a particular point of time, I may decide as a router whether to admit this traffic from this particular node or not and at this moment, I might deny it and subsequently, I might allow it. So, that fine-grained control I want to build inside the router

that is called as admission control at the time when the packet is originating from the sender itself.

And the second thing I want to provide some kind of prioritized services, let us go back to the same example A and B are connected to this router R1, R2, R3 and maybe I have two computers here X and Y, when A and Y talks to each other this is the path, this is the path taken.

So, I want to ensure that R1 reserves some amount of the resources when I say resources, it could be the memory, it could be other computation power, or whatever is there. So, I want to reserve the bandwidth. So, let us say all of them have got uniform bandwidth, may be 10 units of the bandwidth, might be Mbps, Gbps, or whatever, you want a fraction of that out of 10, maybe one unit of the bandwidth is reserved between router R1 and R2.

And another unit of the resource is reserved from the R2 to R3 and so forth. So, one unit of bandwidth all along the path, whether it is Mbps or Gbps. So, let us say Mbps, one Mbps bandwidth is reserved exclusively for the communication between A and Y. Now the router needs to be aware that this bandwidth has been reserved for so and so purpose. Whatever might be the end use cases, but I want to do this.

So, if you want to do this, how do I do this? And the third thing that I can do is, from the previous discussion, every router has got a queue. Every time a packet, let us say, the queue of this router R1 looks something like this every time he sends a packet, the packet would come from that on this particular link and it will come and sit in this queue.

And let us say B and X are also talking the B's packet will also reach R1. So, maybe his packets will also come and sit here and so, forth; depending upon the rate at which A and B are transmitting, the packets will come and accumulate inside this queue and then you need to do the lookup operation and then forward these packets.

So, now instead of having one common queue for all the flows or all the communications that are flowing through this particular router R1, what I can do is I can have two different queues, one for the communication involving these packets and the second one for the communications that involve the host B.

So, all the packets originating from A will come and sit in this queue and all the packets originating from node B will come and sit in this queue. Now, if I want to have differentiated service, I can give certain priority; maybe A's and Y have got priority in communication I can tell that this is the highest priority queue, and the second one is the lower priority queue.

So, when I am going to pick up packets from this particular input queue and then do an inspection route lookup and forwarding, I will say that first, you pick up the packets from the higher product queue and then do the lookup and do the forwarding. If there are no packets inside the higher priority queue, then I go to the lower priority queue and pick up the packets, and then forward.

So, it is not necessary that you have only 2 queues, but you can have as many numbers of queues as you want, and I can order them this is the highest priority, this is the next higher priority, this is the next higher priority, and so forth.

Depending upon how many numbers of priorities or differentiated services I want to provide, I can have multiple numbers of queues and then appropriately pick up the packets for the lookup operation and forward. And at the same time, if I do this so, let us say that I always look for the packets in the higher priority queue, and if there are none, then you come to the next highest priority queue and the next one, and so forth.

Then what can happen is, in this case, you will assume there are only 2 queues at this moment, if A and Y constantly pump packets to the network and the router R1, the Queue reserved for the communication involving A would always be full, i.e., there will always be packets.

So, then the other people, B and X, will, although they want to communicate, will not get any resources, or their packets will not be scheduled for transmission or for the lookup. Now we do not want that to happen. so indefinitely, B and X need not wait in the network although I want to give, I give some priority to A and Y, but, at the same time, I do not want B and X to suffer indefinitely.

That brings us to the question of how I actually differentiate. How do I become fair to all the users? Although A and Y got the priority, I do not want B and X to suffer either. So this is called

fair scheduling I will do the priority but not at the expense of the other ongoing communications or other people who are involved or dependent on the resources in the network.

So, that is the practical condition, want to do prioritized-based look-up and forwarding but at the same time, I do not want others to suffer. How do I actually do this?

(Refer Slide Time: 19:16)

The slide is titled "IP Flows" and features the NPTEL logo in the top right corner. It contains two bullet points: "Flows are specified by rules" and "Classifier: A collection of rules". Handwritten in red ink, there is a table with two columns: "Source IP" and "Destination IP", with a third column for "Action". The first row shows "10.10.1.1" as the source IP, "20.20.1.1" as the destination IP, and "allow" as the action. Below the table, a diagram shows a circle labeled "M" connected by a line to a circle labeled "X", with a small box labeled "IP" above the line.

Source IP	Destination IP	Action
10.10.1.1	20.20.1.1	allow

Diagram: (M) — IP — (X)

So, you need to tell the routers something using the flows whenever two endpoints communicate with each other; the series of packets that are exchanged are called the flows.

And these flows are evaluated using a set of rules that we call the classifier. So, the classifier is a collection of the rules so, for example, I might have a bunch of fields maybe I will use the source IP address and then the destination IP address; let us say whenever the computer 10.10.1.1 is sending to another computer 20.20.1.1, you allow this communication to happen so this is an example of the rule, a rule written with two fields one is the source IP address, and the second one is the destination IP address and then what action needs to be taken when this combination is matched is in the action field.

So, I have a bunch of fields to look for, and then at the end of this, if the rules are these conditions are met, then certain action you want to take, whether you allow, whether you deny, whether you prioritize whatever you want to do, you tell that.

So, a collection of such kinds of rules is called the classifier. Now, you can imagine these fields that I have mentioned are coming from the header portion of the packet I got an incoming packet, so let us say A is the computer, and there is a packet and inside the packet contains two things one is the header and the second portion is the payload or the actual content. So, whatever the fields that I have mentioned here, the rules are written using the fields of the header, so now we can think of that is not only the network header although these two field source and destination IP address are coming from the network header, there are other fields as well. So, other headers as well, the TCP header, the link layer header, whatever it is.



So, although in purely technical terms, the routing or the forwarding decision should not depend on the other fields, practically, the fields of the other headers are also used. So, I can write a set of rules using a combination of these header fields so that an incoming packet arriving at the router, you pick up the header portion, the bits corresponding to the header, and then you extract the required fields from that header and against a bunch of rules written inside the router you match it and then you take the corresponding action.

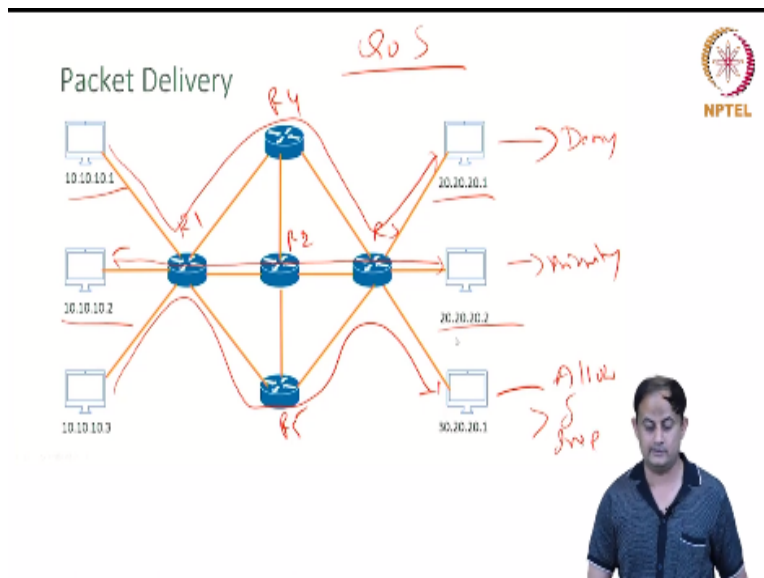
(Refer Slide Time: 22:10)

Classifier Rules for Router-3

1 2 3 4 5

S. No	Src	Dest	Protocol	SPort	DPort	Action
R1	10.10/16	20.20/16	TCP	5000	181	Deny
R2	30.30.30.30	20.20/16	TCP	80	80	Forward to Port II
R3	10.10.10.1	10.10.10.2	UDP	*	*	Forward to Port II with Priority
R4	20.20.20.1	20.20.20.1	TCP	1000	25	Drop if Rate is > 10 Mbps





Here is an example of how the classifier rules might look like; there are four rules in this table this is a classifier. So, the classifier is usually denoted with the capital letter C and it is a collection of these rules. So, here, in this case, rule R1, R2, R3, and R4, and five fields are used here these are also called the dimensions D1 is one field, D2 is the second field, D3, D4, and D5.

So, the first rule says whenever the source IP address is 10.10/16, this is the /16 address. Any computer which is sharing this common prefix 10.10 and going to the destination 20.20 again the prefix format /16 address for the entire series of 2^{16} combinations at the source and 2^{16} combinations on the destination field. If the protocol of the communication between these two, any two entities falling under this series, is TCP and the source port is actually 5000 and the destination port is 181, you should not allow this communication to happen.

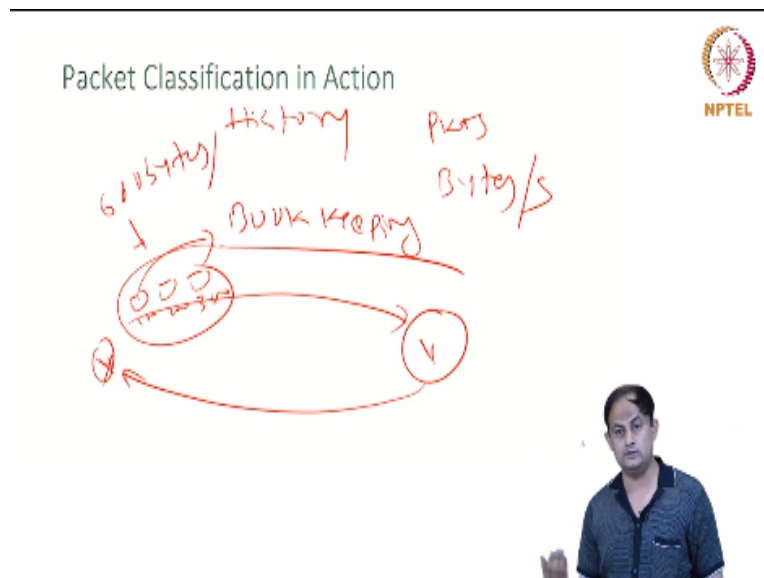
The second rule says if the source address is the entire 30.30.30.30 and the destination IP address is the class 16 address going to 20.20. The protocol field is TCP and the source port can be anything I do not mind * indicates the wildcard entry, but the destination port number is 80, then you forward it to port number 3; this is the classifier for router number 3 in this diagram.

So, it will not only have one rule but a bunch of rules. Similarly, R3 says that when a 10.10.10.1 is communicating with 10.10.10.2, if the protocol is UDP and it does not matter what the source and destination IP address, you forward it to port number 2 with a certain priority, that is what it says, and similarly, R4.

You can think of whether D1, D2, D3, D4, and D5 are the only Dimensions that I can have. No, not necessarily I can have as many numbers of dimensions or fields as I want to have in a nutshell; what I am trying to say is using a combination of the header fields, you can write some rules by looking at those rules the router can dynamically decide what to do with this particular packet.

So, these collections of rules is called a classifier. When a classifier is there inside the router and it is inspecting the packet header and doing this lookup operation, taking that action, that process is called the classification and, precisely, packet classification. Now, the packet classification in action, how do we actually do this?

(Refer Slide Time: 25:40)



Classifier Rules for Router-3

NPTEL

S. No	SIP	DIP	Protocol	SPort	DPort	Action
R1	10.10/16	20.20/16	TCP	5000	181	Deny
R2	30.30.30.30	20.20/16	TCP	*	80	Forward to Port II
R3	10.10.10.1	10.10.10.2	UDP	*	*	Forward to Port II with Priority
R4	20.20.20.1	20.20.20.2	TCP	1000	25	Drop if Rate is > 10 Mbps

So, you can look into this particular set of rules, and rule number R4 says that drop the packets if the rate is greater than 10 Mbps, but up to 10 Mbps, it is okay, so 20.20.20.1 is connected to or talking to 20.20.20.2

Now, if these two communications exceed this threshold limit of bandwidth utilization of 10 Mbps then you actually drop the packet. But, in order to facilitate this, you need to remember the history information, i.e., how many packets have been transmitted? How many number of the bytes have been transmitted?

That history can be measured in terms of the packets or they can be measured in terms of the number of bytes or it could be any other metric. So, bytes per second, packets per second, byte, packets per minute, bytes per minute, and so forth. Or I can even go to the granularity that if X and Y are talking to each other, how many packets have gone in the forward direction from X to Y?

And how many numbers of packets have gone from Y to X? I can specify if the threshold number of the transmissions in the forward direction is greater than some δ , you drop it, if the utilization in the reverse direction is so and so forth, you do this action, so all kinds of the combinations are possible.

So, in order to do this till date action, you need to remember the history that requires something called the bookkeeping work, i.e., every time a packet goes from X to Y, how many numbers of

bytes have been transmitted, you need to tell this. If my granularity is byte per second, at what time, how many numbers of bytes have been transmitted in what packet?

So, the second packet, third packet, so let us say 100 have gone here, 200 in this packet, 300 in this packet, and if these three packets are gone in one second, then the total aggregate number of the transmission is 600 bytes, and in the last one minute. So, using that, I want to make the decision whether the third or fourth packet that is coming from the same source going to the same destination should be allowed or not allowed or should be sent with priority, not sent with priority, whatever action I want to take. So, in a nutshell, what I am trying to say is that decisions are made using a set of rules. Each rule may require some kind of bookkeeping work to be done by the router and it is not only one router but all the routers in the network need to have one classifier, and every router need to do the bookkeeping work.

So, now you can see, we said that large millions of packets are coming, the router needs to do a quick lookup now we are bringing another thing which is saying I not only want to do the lookup operation but also I want to do some kind of differentiation in the forwarding itself that requires bookkeeping work for every two combinations of the computers and the protocols and other fields whatever is there engaging in the conversation. That is actually a lot of work and now the question is how do we actually routers actually implement this kind of feature and what kind of things that you want to implement?