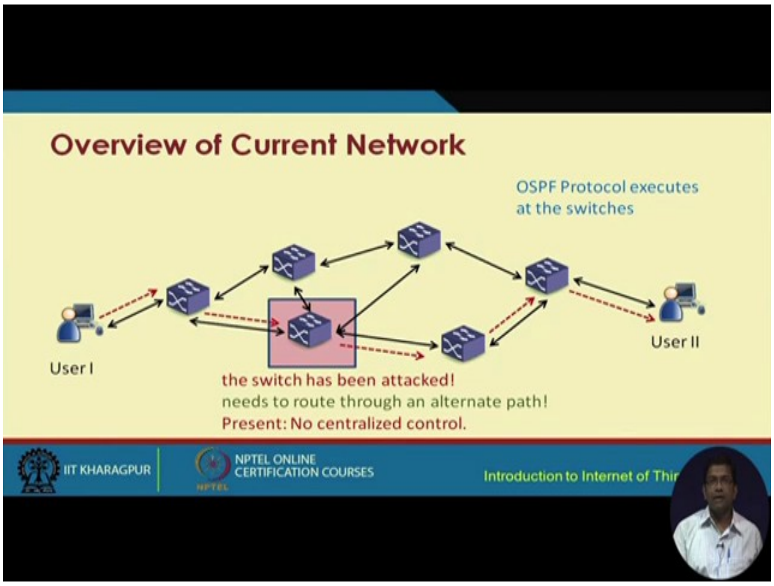
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 33
Software – Defined Networking – Part – I

We are going to discuss a very important technology the software defined networking in short it is called as SDN and it is a very important technology which has lot of potential for use in internet of things for making IoT efficient. So, we will discuss about the basics of SDN first what software defined networking is and some of the basic concepts that surrounds SDN and thereafter in another lecture we are going to discuss about how SDN can be used for in the context of IoT to make IoT efficient.

So, when we talk about SDN it is about transforming or restructuring the existing network infrastructure and that can be done in an efficient manner. So, how that can be done is what we are going to discuss now.

(Refer Slide Time: 01:22)



So, if we look at the current day networks this is what happens. So, we have users different users connected to the network enjoying network services and this can be any network you know we are talking about SDN in a general network a wired network let us say a very simplified wired network.

Now, let us say that the topology of the network is something like this. So, this is the topology of the network. So, what we have are different L3 switches like this and maybe the data has to be sent from user 1 to user 2 and back. So, the data can be sent in different ways different you know. So, these are the routes through which the data can traverse from the user the data can traverse maybe one of the possible routes is like this to the user 2.

Another possible route is may be like this and another possibility is like this and there are few other possibilities also for the data to be sent from user one to user 2. So, we have multiple different routes and the data or the packet basically traverses through multiple switches L3 switches and this is how it looks like. So, before I proceed further I would like to mention that in this particular lecture and let; that means, lecture on SDN and SDN IoT.

I am going to use the terms switch and router interchangeably. So, when I mention about switch and basically talking about the L3 or the layer 3 switch and. So, L3 switch and router these terms are going to be used interchangeably in the SDN lecture. So, let me just you know let us look at the slide once again. So, what we have is a scenario like this and then let us say for switching or routing the protocol that is used is the OSPF protocol.

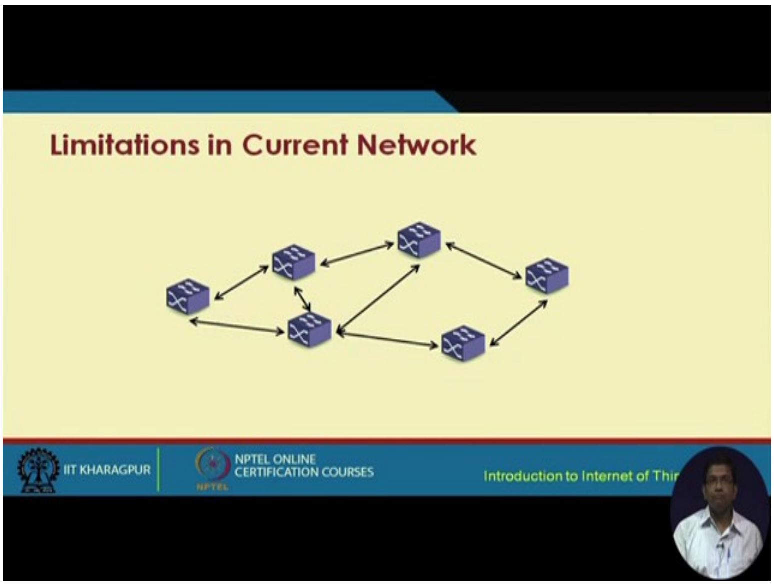
So, what essential happens is every switch is going to every switch over here it is going to implement OSPF. So, it executes OSPF and so when the data is sent you know the OSPF PF protocol is going to the packet is sent the OSPF protocol is going to route the packet through these corresponding switches depending on which route the OSPF protocol finds to be the best.

So, what essentially happens is every switch basically knows how it has to send the packet based on the routing table that it has. So, it does not have a global view of the network as a whole now let us say that a particular switch the one that is shown in this particular figure this one let us say that it becomes down for one reason or another maybe because it has been attacked. So, let us say that it has been attacked and the switch is down.

So, then traditionally what has to happen is a new route or an alternate route has to be found for the packets to be sent from the source to the destination node and because there is no centralized control. So, you know this becomes a difficult task. So, what happens is at present the technology the routing technology is such that there is no centralized control over the network.

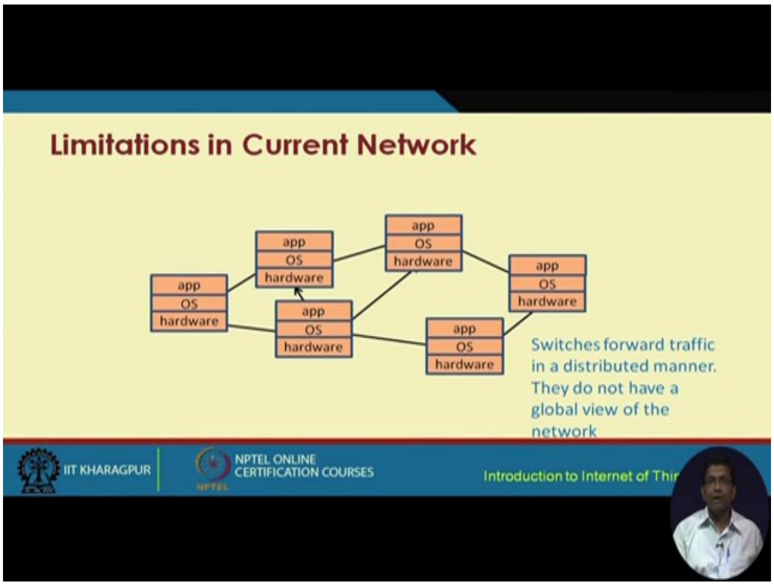
So, if one switch becomes down the other switches can; will become affected and there is no centralized way that we can address this particular problem. So, there are different ways to read out you know found find routes depending on the protocols you know what are the alternate route. So, on, but there is no centralized solution there is no centralized entity that can take care of it.

(Refer Slide Time: 05:53)



So, these are the limitations of the existing network and if we look at this network you know. So, what we see over here is just a snapshot of a very simple network consisting of different switches.

(Refer Slide Time: 06:13)

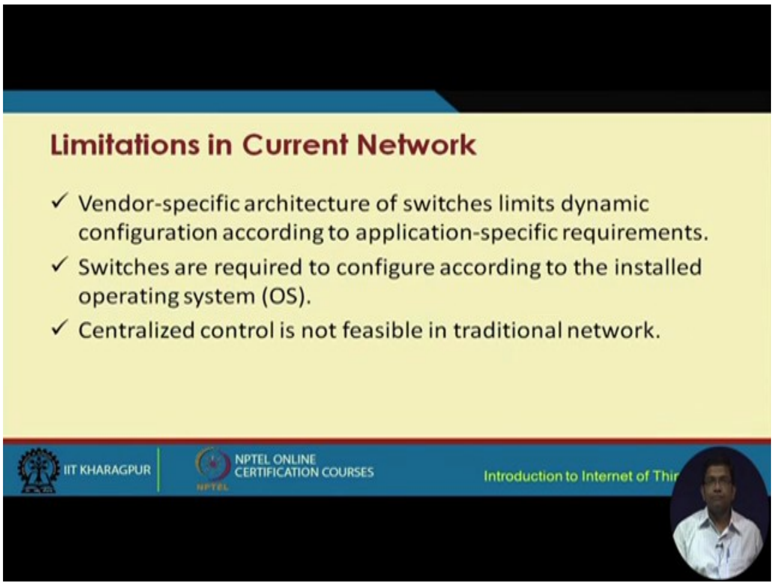


And each of these switches they run these different layers we have a hardware then we have the operating system and we have the applications that are running on top.

So, essentially a very skeletal view of the stack that is run on each of these switches is hardware OS and app and that is basically applicable to all these switches that are there in the network. So, each of these switches is running these 3 different layers. Now these switches they forward the traffic in a distributed manner and they do not have the global view of the network this is what I was mentioning in the previous slide as well.

So, each of these switches they do not have the global view they route the traffic they forward the traffic in a distributed fashion they just know locally what you know what has to be done.

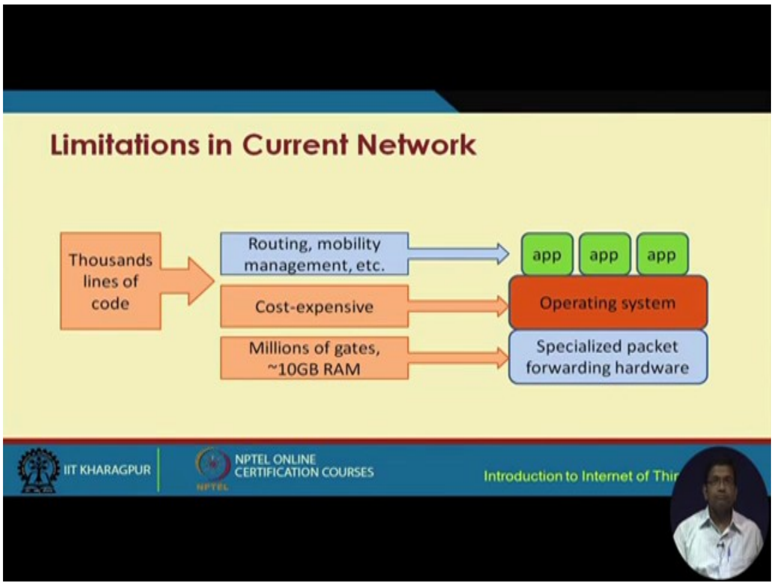
(Refer Slide Time: 07:08)



So, if we now summarize the present network has different limitations; limitations which are for example, the architecture of these switches are vendor specific and correspondingly you know if we have to do any dynamic configuration based on the application specific requirements that we cannot do very easily. So, that cannot be done in a dynamic way dynamic configuration cannot be done.

Switches are required to configure according to the installed operating system in each of these stacks. So, each of these switches they run their different operating system and they have to be this way they have to be configured according to that particular operating system and there is no centralized control that is feasible in these networks there is no centralize controller.

(Refer Slide Time: 08:03)

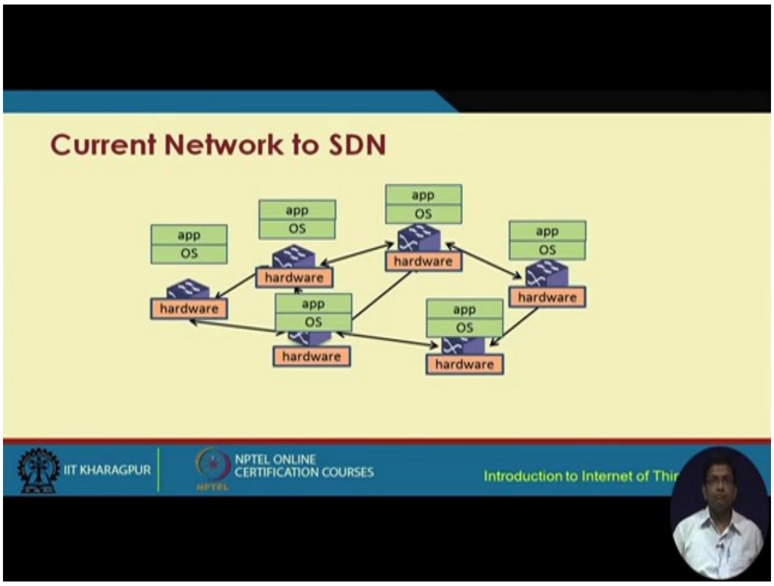


So, if we look at another view point of these current networks. So, we have each of these switches running thousands of lines of code they have each switch has millions of gates logic gates that are implemented requiring more than 10 GB of ram they are cost expensive each switch is cost expensive and they run different you know applications for example, routing, mobility, management, etcetera.

So, here basically you know. So, we are not talking about you know when we mention about applications we are talking about the different application functionality and not simply the applications that we used to refer to in a OSI model. So, here we are talking about applications in general. So, like the general network applications like routing, mobility, management, etcetera.

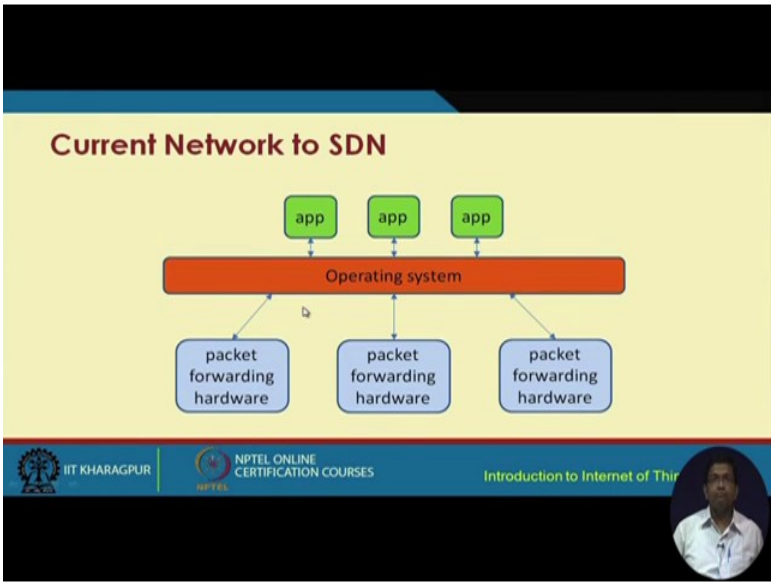
So, this is the challenge with these networks. So, each of these you know networks you know these each of these switches in this networks the have specialized packet forwarding hardware they have their own operating system and they run their own different applications with respect to routing mobility management and so on and so forth.

(Refer Slide Time: 09:21)



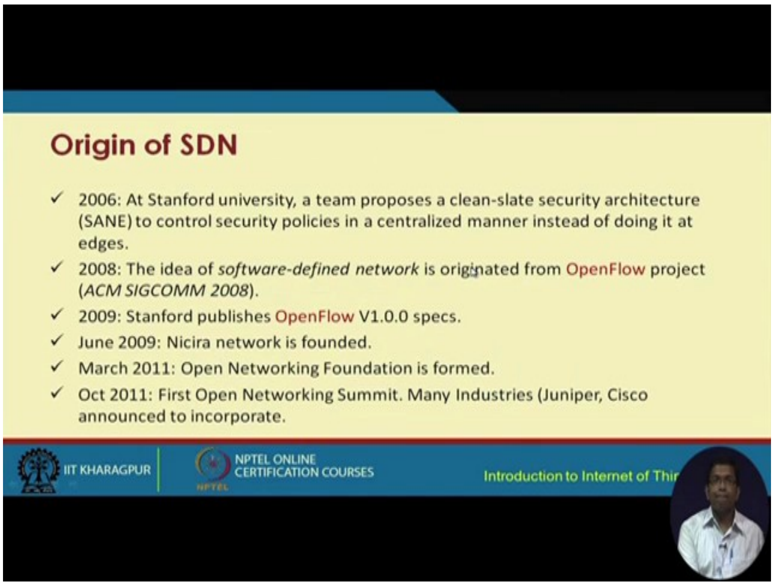
Now, what is required is to make these networks efficient by trying to overcome these challenges or the limitations that we have just gone through. So, the whole idea in SDN is to take care of the limitations by separating the application and operating system from the hardware. So, earlier in the earlier view what we had seen is the app OS and hardware were hold or were all put together in each of these switches and here what we are doing is we are separating the application and operating system from the hardware in each of these switches. So, hardware is separated out from the app and the OS.

(Refer Slide Time: 10:10)



So, what we will have is the packet forwarding is going to be packet forwarding is going to be separated out from the OS and applications.

(Refer Slide Time: 10:23)

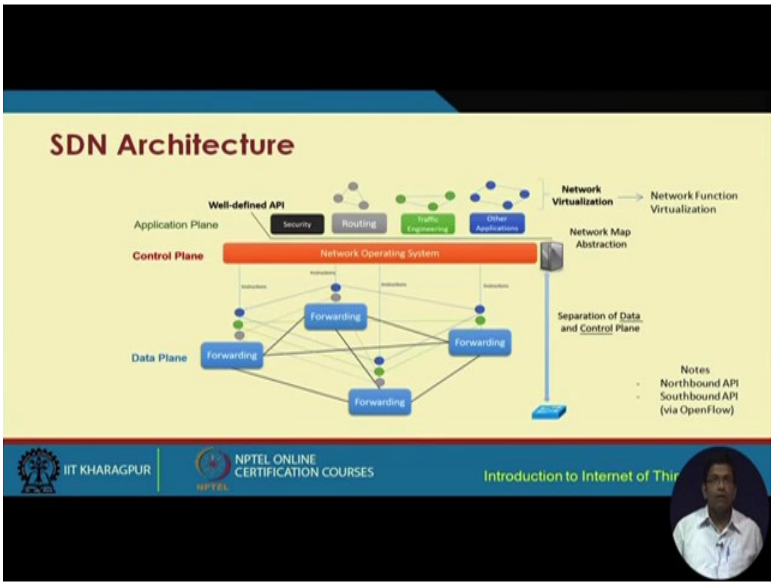


So, before we look any further into SDN. So, let us try to look at the history the brief history about the genesis of SDN. So, in the year 2006 a Stanford University team proposed a clean slate security architecture which was termed as SANE to control the security policies in a centralized manner instead of doing it at each of these edges; that means each of these switches.

In 2008 the idea of software defined network was originated with the open flow project and that was published in the very popular ACM SIGCOMM paper in 2008; in 2009 Stanford basically published the open flow version one specifications and June 2009; the Nicira network company was founded in March 2011 the open network foundation was formed and in October 2011 the first open networking summit and many industries for example, all these routing router companies like Juniper, Cisco etcetera they basically announced that they want to incorporate SDN into their switches.

So, basically it the whole concept of the SDN technology goes back to only a few years back; that means, in 2006. So, it is not a very old thing it is very new and we will see that how what are the different features of SDN further in the next few slides we are going to look at what are the different features of SDN open flow is sort of like a de facto protocol or and architecture that is used for SDN. So, both of these are not the same, but open flow basically follows you know open flow is used for SDN.

(Refer Slide Time: 12:16)



So, let us now look at this particular architecture. So, what we have you know let us say that each we have different switches which perform forwarding individually. So, that is the data plane and then we have the control plane which has the network operating system and then the application plane performing functionalities like security, routing, traffic engineering and different other applications.

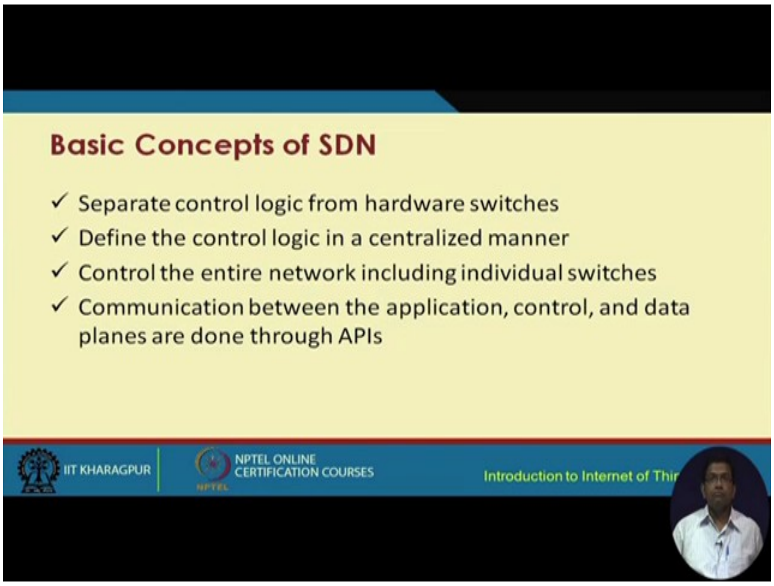
So, the whole idea behind SDN and this SDN architecture as a whole is to separate the data plane from the control plane or rather the control plane from the data plane. So, you see that the control plane has been separated in SDN this control plane has been separated in SDN from this data plane which takes care of things like forwarding. So, this is made possible they the concept of SDN is made possible through the process of network function virtualization NFV.

So, this network function virtualization. So, what happens if these different network functions for examples you know security, routing, etcetera, etcetera, these have been these have been you know these are performed on a virtualized networks. So, this network function virtualization basically gives a logical view of the network and based on that these functions are performed.

So, one more concept I should mention over here before we proceed further is. So, we have 3 different planes in SDN in the you know in the SDN architecture we have the data plane, control plane and application plane and we have also seen that the data plane and the control plane are basically decoupled in SDN.

Now, we have the concept of northbound API and southbound API. So, the northbound API is between the control plane and the application plane. So, this particular interface is known as the northbound API in SDN and this particular interface between this forwarding; that means the data plane and the control plane this is known as the southbound API and the current protocol supporting this southbound API is the open flow protocol.

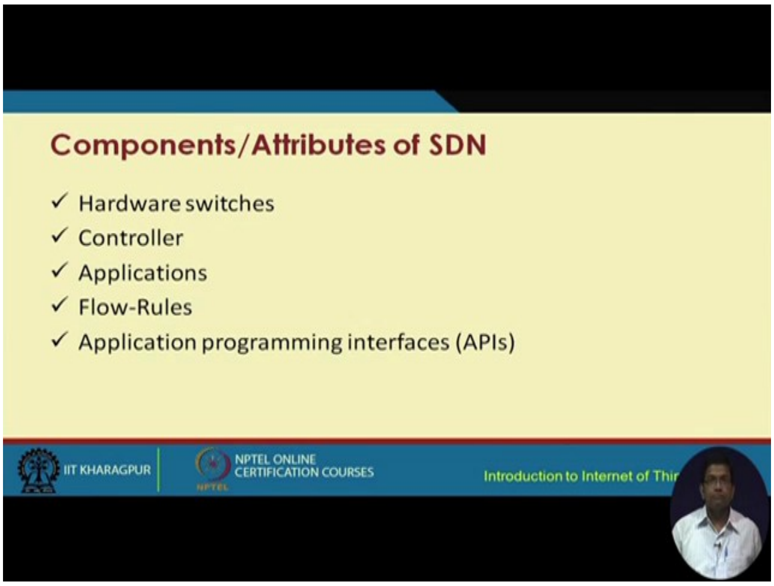
(Refer Slide Time: 14:45)



So, now let us summarize some of these basic concepts of SDN the whole idea is to separate the control logic from the hardware switches to define the control logic in a centralized manner. So, the everyday all this control functions are going to be centralized because this control plane has been separated out and is centralized. So, you know. So, this is how this SDN is going to work. So, the control logic is going to be centralized and is separated from the data logic, the data plane.

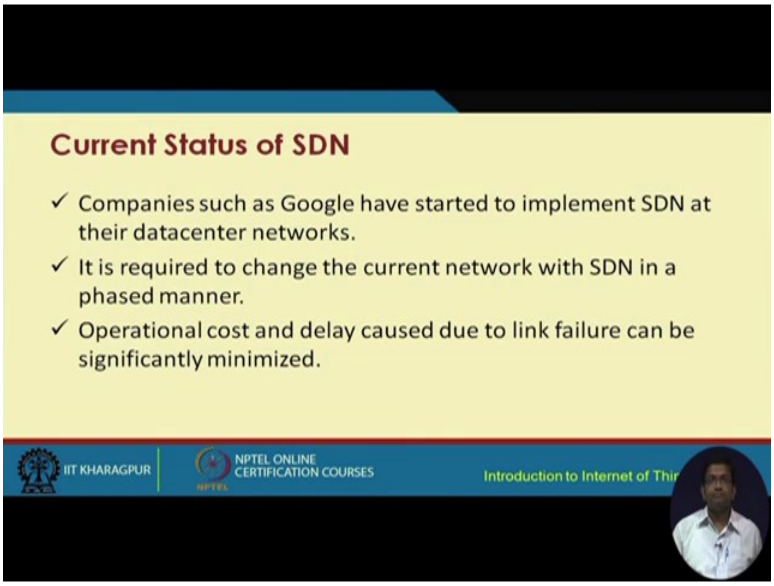
Control in the other concept of SDN is to control the inter network including the individual switches in a centralized manner and the communication between the application the control and the data planes are done through different APIs northbound APIs southbound API.

(Refer Slide Time: 15:38)



So, we have different components or attributes of SDN we have hardware switches we have controller applications flow rules and different application programming interfaces or the API these are the different components of SDN.

(Refer Slide Time: 15:59)



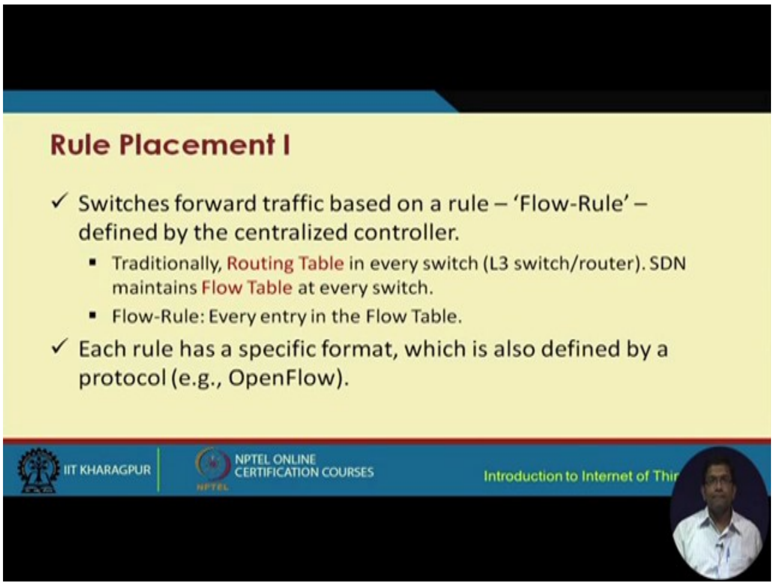
Now the current status of SDN are companies big big companies joined companies like SDN who have their own data centers they have started to implement SDN in their own data centre networks SDN it is required to change the current network with SDN in a phase manner you know it is not like you know we can go and we can change the existing network we can transform the existing switches to support SDN it is not. So, simple you know I has to be architected the hardware have to support the software have to support and so on.

So, these has to be done in a very progressive manner in a very phased manner you know step by step it has to be done operation cost and delay that are caused due to link failure can be significantly minimized using SDN.

(Refer Slide Time: 16:47)

Now, let us come to 2 main challenges when we want to implement SDN in any network. So, these are the rule placement problem and the controller placement problem. So, these are the 2 main problems to be taken care of fundamentally when we talk about SDN.

(Refer Slide Time: 17:08)

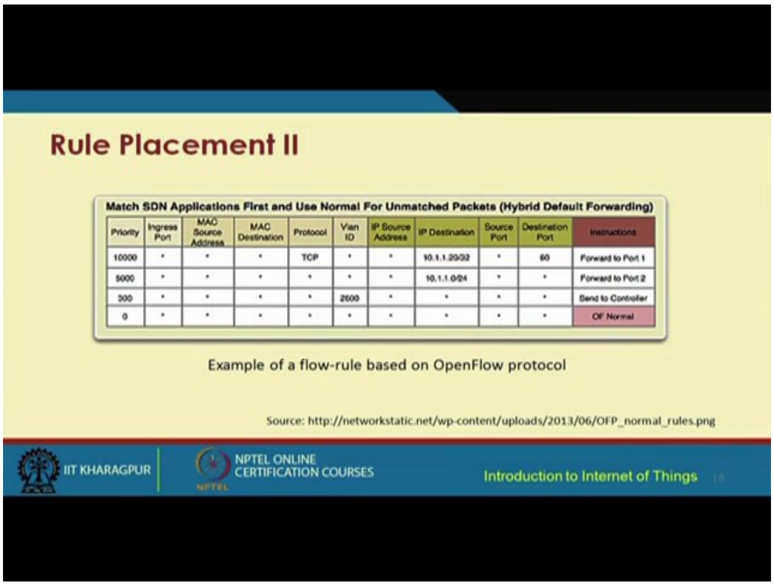


So, with respect to rule placement what happens is here we are talking about flow tables instead of routing tables in the concept of SDN. So, these flow tables. So, basically what happens is this flow tables have different flow rules which are implemented in the same way as traditionally these routing tables have their routing table entries you know different entries in the routing table very synonymously analogously we have flow rules implemented in this flow table.

So, these switches basically in the network they forward the traffic based on this flow rules and this flow rules are basically defined by the centralized controller and this controller as we can recall does not exist in each of these individual switches controller is centralized you know it is separated out typically implemented you know the controller side implemented as the server.

So, from a server this controller is implemented and these controllers basically takes care of this flow rules defining the flow rules based on which the strings of packets that are coming to each of the switches this flow rules are going to determine what is going to be done with the streams of packets that are arriving at the switches. So, we are going to talk about that you know in further detail in a short while.

(Refer Slide Time: 18:47)

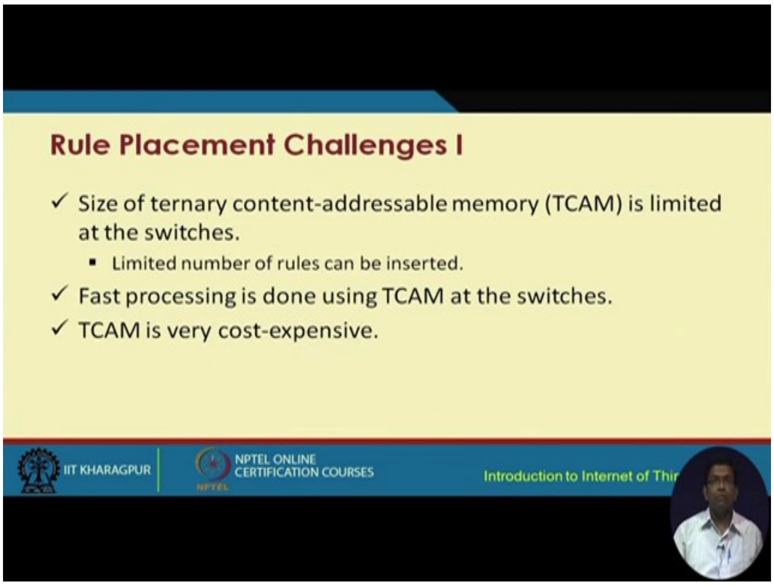


So, each rule has a specific format and that is defined by a particular protocol and currently we are talking about open flow which is sort of like a defacto protocol that is used for implementing SDN. So, you have the rule placement issue. So, you know here what we see over here in this slide is an example of a flow rule that is based on the open flow protocol. So, you know essentially what we see over here is if a packet arrives then it will check the priority if the priority matches maybe in a star means that you know it is it does not require any match.

So, you know if the values of the packet corresponding to this particular fields are different it does not matter, but the protocol has to be TCP and if the IP destination is this and the destination port is this then the instruction; that means, the action that has to be taken is to forward to the particular port. So, here it is forward to port one like this the other flow rules are given over here.

So, for different priority and these things can be anything if the IP destination is this and the; you know the source port and the destination port can be anything then forward to port 2 and so on and so forth for the other entries. So, these are the different flow rules and these fields basically you know we have to remember one thing. So, these fields are fixed this particular fields in open flow these are fixed no one cannot go and change this field and if one changes then we have a different protocol. So, in open flow this field cannot be changed.

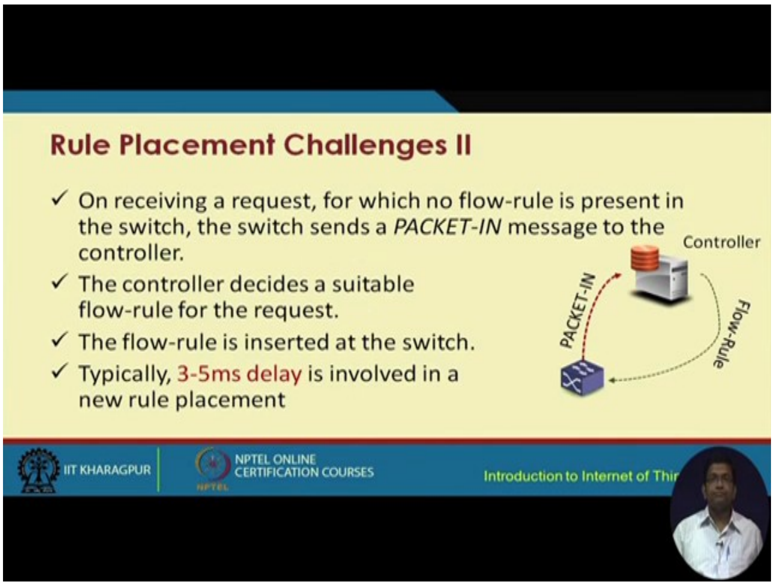
(Refer Slide Time: 20:41)



So, this you know. So, when we place these rules they are placed in the open flow table the flow tables and this flow tables are basically stored in the switches the size of their you know the size of these flow tables are such that they have to be stored in a specialized memory which are known as a TCAM memory ternary content addressable memory and these memories are very limited in size and so, that only a limited number of rules can be inserted in this flow tables. And so, basically the flow tables are residing in these TCAM memories and these TCAM memories are very fast; that means, fast processing can be done that is why the specialized memories are required.

We cannot use any other memories that is at normally available in the switches and other computing hardware and we have to use this TCAM memory at the switches and this TCAM memory they are very expensive as well they are very expensive. So, you cannot you know very easily you cannot scale up we cannot you know get as much memory as we want because of the cost for prohibitiveness.

(Refer Slide Time: 22:01)

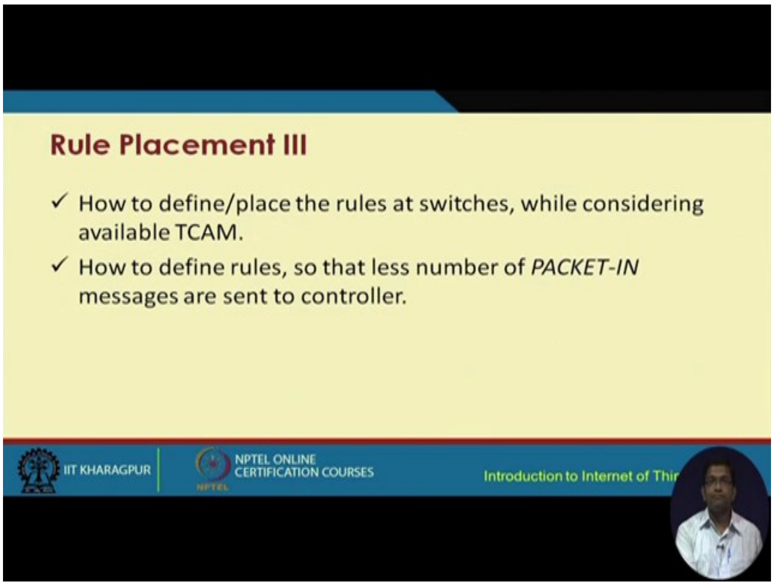


So, on receiving a particular request for which no flow rule is present in the switch, what happens is the switch basically sends a packet which is called the PACKET-IN. So, we have this switch; switch receives a request and it checks its flow table if there is no flow rule that is present in this particular switch in that particular table the switch sends the packet in message to the controller.

Now, this controller besides a suitable flow rule for this particular request and this flow rule is then communicated back to the switch and then this flow rule is going to be inserted in that portable in the switch and typically there is a delay of 3 to 5 milliseconds involved in the new rule placements. So, whenever there is a new rule that has to be placed in the switch which is which is not already existing in the portable in the switch.

This entire communication with controller; controller deciding and sending back the flow rule this takes about 3 to 5 milliseconds delay.

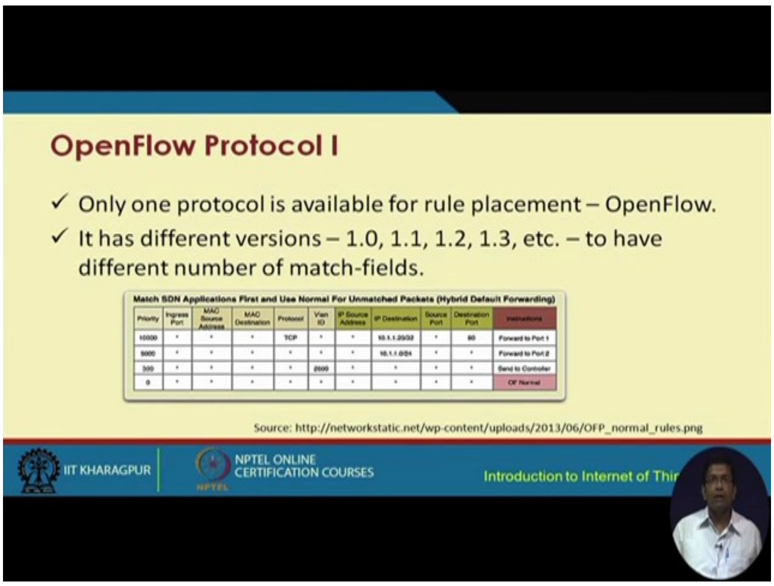
(Refer Slide Time: 23:17)



So, one of the challenges is how to define or place the rules at the switches while considering the available TCAM I already mentioned to you that TCAM is very small in size and it is very expensive it is not very easy to skill scale up.

So, how do we define one of the problems is to define or place the rules at the switches the other problem is how to define the rules. So, that less number of packet in messages are sent to the controller and these are challenges that people the researchers are working on at present defining solutions to these specific problems.

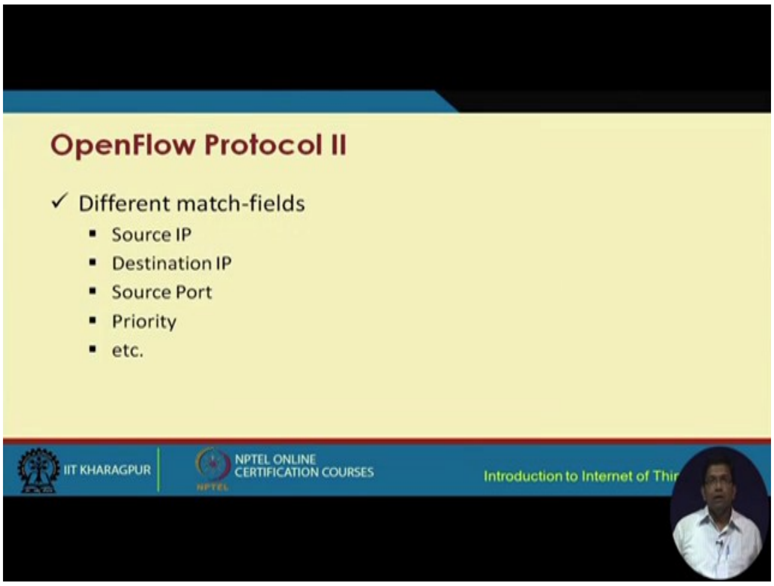
(Refer Slide Time: 23:56)



So, in the open flow protocol rule placement is done it is one of the vital things only one protocol is available for this rule placement which is the open flow protocol.

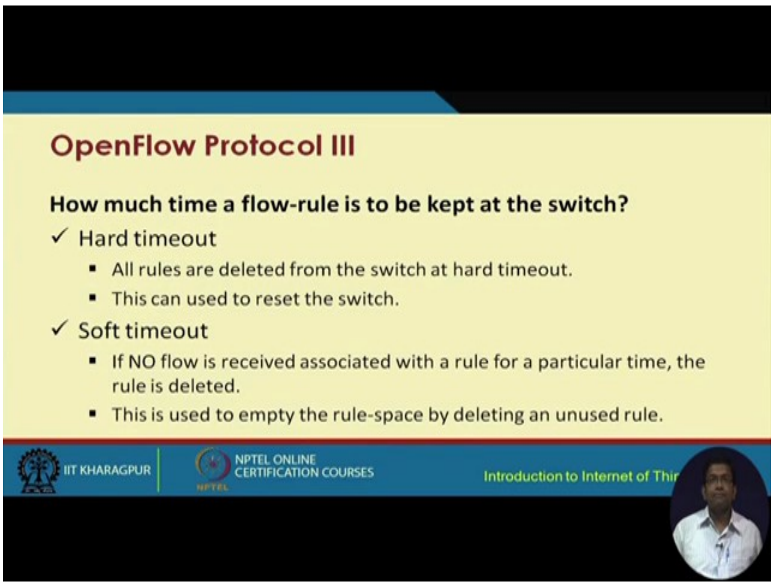
And it has different versions 1.0 1.1 1.2 1.3 open flow has different versions and they have different number of matching fields, but in a particular version of open flow this fields are going to be fixed.

(Refer Slide Time: 24:30).



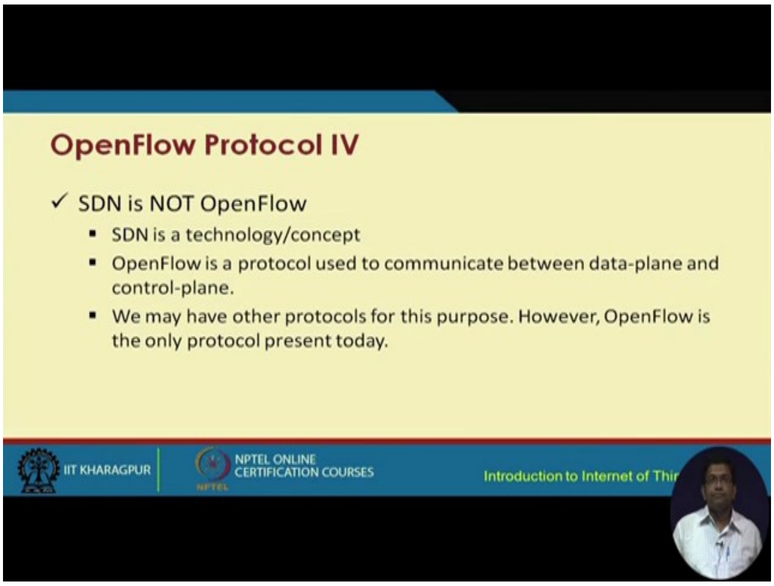
So, there are different matching fields source IP, destination IP source port priority etcetera in a particular version of open flow and that these fields are fixed as I already mentioned.

(Refer Slide Time: 24:45)



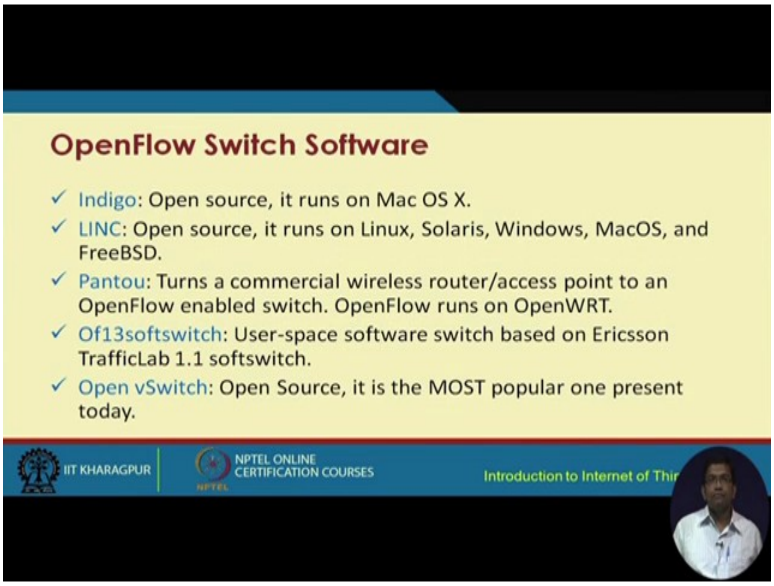
So, one of the issues is that for how long a particular flow rule that is generated is to be kept in the switch for this there are 2 times time outs that are defined one is known as the hard time out the other one is known as the soft time out. So, all the rules are deleted from the switch at a particular hard time in the hard time out methodology this can be done by resetting the switch for example and in the soft time out methodology if no flow is received associated with a particular rule for a timeout interval of time then this particular rule is deleted. So, this is the soft time out.

(Refer Slide Time: 25:37)



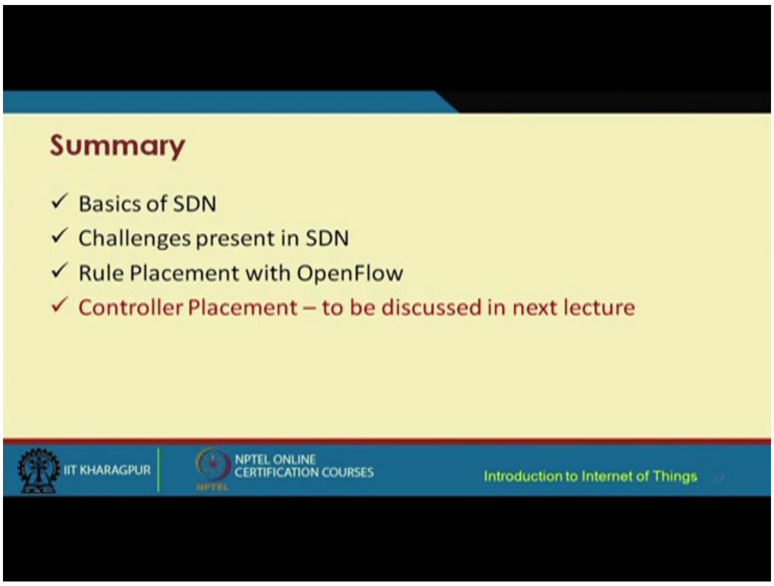
So, we have to remember one thing that I was also briefly mentioning at the outset of this lecture is that SDN and open flow are not one and the same SDN is a technology or a concept, open flow is a protocol that is used to communicate between the data plane and control plane. So, they are distinct and we have to understand and remember this particular difference between these 2.

(Refer Slide Time: 26:05)



Now, these open flow switches are implemented in sorry open flow is implemented in different switches there are different software that have to be that are associated to with open flow implementation. Here is a list of these different software I am not going to go through them most of them are open source and they run on different platforms, different ways for example, linux solaris windows etcetera, etcetera, Indigo, Linc, Pantou open vSwitch these are some of the popular open flow switch software that are available currently to support open flow.

(Refer Slide Time: 26:44)



So, to summarize we have gone through the basics of SDN we have understood the architecture for SDN. We have also understood that in SDN the whole idea is to separate the control plane from the data plane and there is a centralized controller which is typically implemented in a server that takes care of the control logic that has to be implemented while any flow in any flow is received at each of these different switches of the routers.

So, the rule placement is an important problem that we have talked about and there are different issues with the rule placement and another very important problem is the controller placement problem and this is what we are going to discuss in the next part, the second part of the SDN lecture.

Thank you.