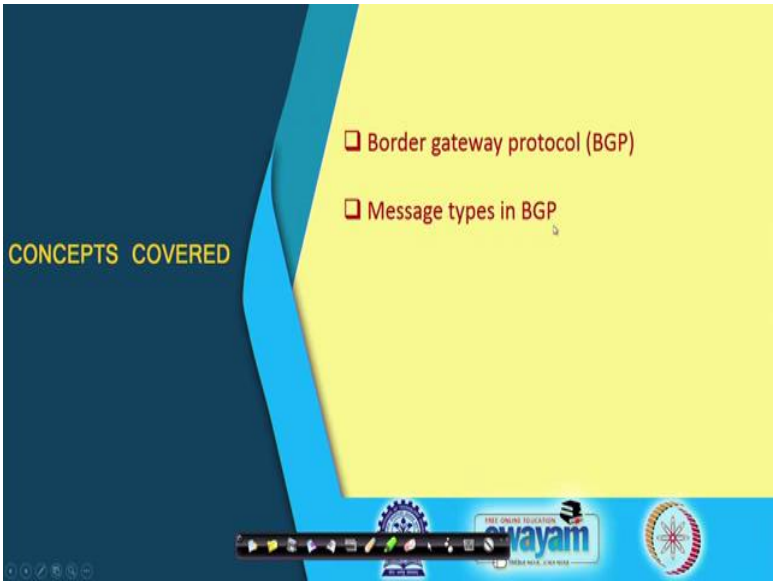
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 13
Routing Protocols (Part III)

In this lecture, we continue with our discussion on Routing Protocols. If you recall in the last lecture, we discussed the two interior routing protocols namely the RIP and OSPF and in this lecture, we shall be talking about the exterior routing protocol that is most widely used in the internet with the help of TCP/IP that is BGP.

(Refer Slide Time: 00:48)

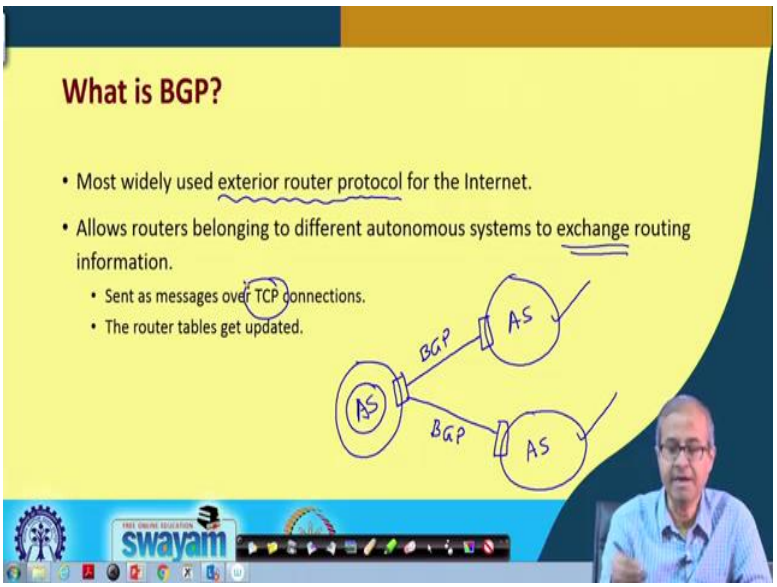


So, the topic of today's discussion is Border Gateway Protocol and some of the message types in BGP. I shall also show you some very overall high level example that how BGP works, just to give you a conceptual idea ok.

(Refer Slide Time: 01:03)

So, talking about the Border Gateway Protocol, BGP, well as you can understand from the name we are talking about something called border. You see for every country, border is an interface with some other country right; similarly in a network when you say a border, border gateway it means; it is like a router which is often called a gateway which connects this network to the outside world to other networks, to other you can say router ok.

(Refer Slide Time: 01:39)



So, let us see what BGP exactly is. Now, as I said BGP is the most widely used exterior router protocol. Now, exterior and interior, I explained the distinction earlier. Let us say

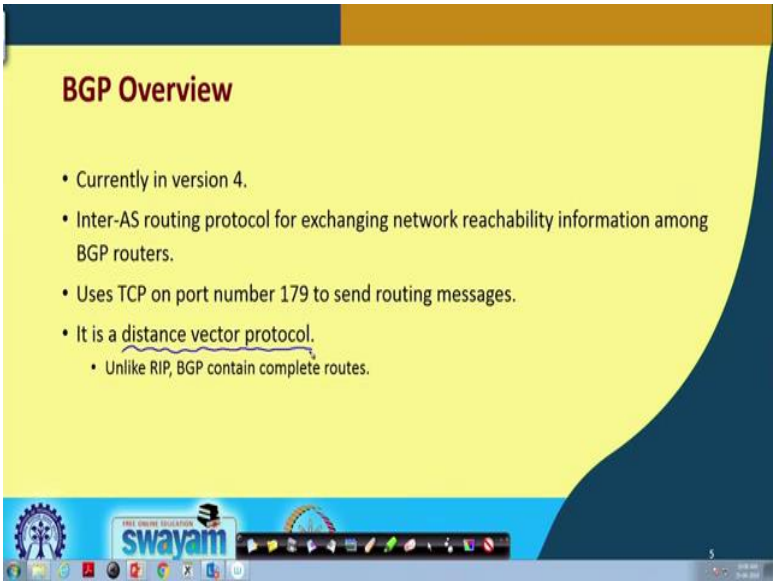
when you have several autonomous system. Suppose, these are all autonomous systems, which consists of networks and routers. So, you can have one router here, one router here and may be one router here, these are exterior routers or these are border routers.

These border routers can connect with each other depending on means how you want to connect, they are going to be multiple ways of connection and it is over this links that connect the border routers you have this BGP protocol running. So, you will also have BGP here, but inside the autonomous systems will be having some of the interior router protocols running ok.

Now, what is the role of BGP? BGP allows these routers to exchange routing information. Like for example; the router sitting in this particular autonomous system does not know what is the network status of the other two networks, other two autonomous systems. So, once the other router sends some information to this particular router; so we will have some information about the other place, how the network situation is; what are the available routes and so on.

So, that the local routing tables can be updated accordingly, right. And these all BGP messages which are transmitted, they are sent over TCP connections and based on that as I said the routing tables of the routers, they get updated.

(Refer Slide Time: 03:50)

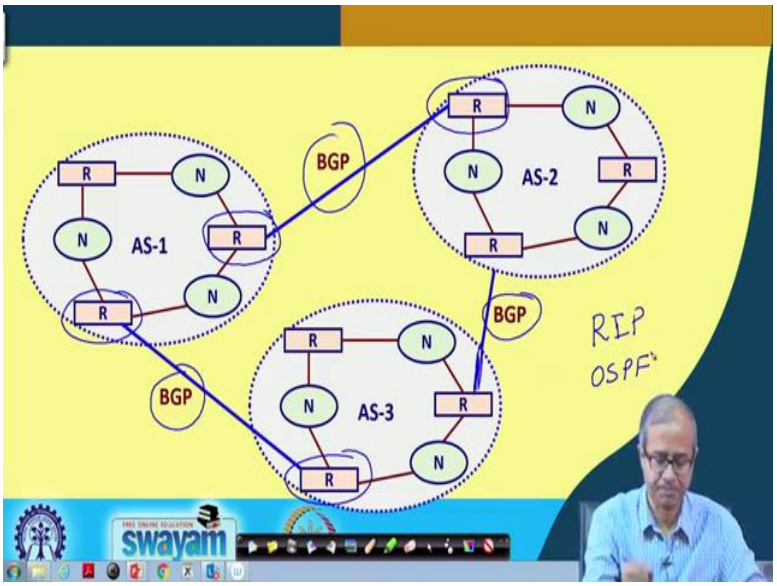


Now, BGP comes in various versions. Presently version 4 is most common and as I said, it is used to communicate between routers, which are across autonomous systems, which we say inter-AS routing right. Inter-AS means across two different autonomous systems and as I said for exchange of the messages, it uses TCP with well known port number 179.

So, 179 number is reserved for BGP packet transmission. And similar to RIP which we talked about, here also we use a version of distance vector protocol; meaning every router will be sending some information to the other router over this exterior links, telling about the distances with other networks and other places. Now, there is one difference; in RIP which was an interior protocol here, this distances referred to distance between routers, within the autonomous systems.

But here since, we are talking about other networks which may be outside this autonomous system also; so here there is an option of specifying complete routes, not just the next hop. Suppose, I want to go from x to y what is the paths to be followed, what is the sequence of routers I should follow, that also can be additionally specified in BGP ok, so that if you want, you can have source routing facilities implemented, if of course, your router supports that.

(Refer Slide Time: 05:50)

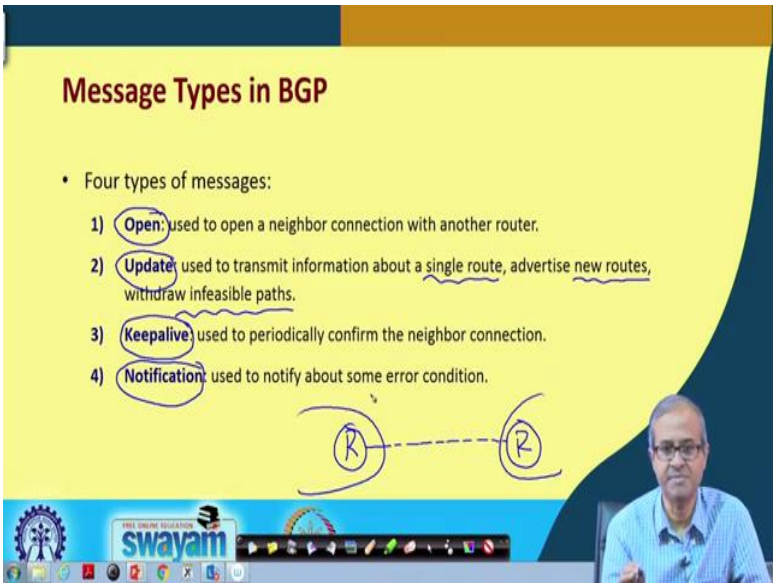


Now, here we have a pictorial view of what we have said. You see that there are three autonomous systems as you can see. There are three AS-1, 2 and 3 and these blue links which connect some of the routers they run the BGP protocol. So, these blue links will be

connecting with this router ok. So, you see these will be the boundary routers or boundary gateways. They will be connecting with the routers of the other networks right. So, it is between these routers that this BGP protocol will be running.

Now, in contrast, inside a network wherever there are routers also for updating information with respect to a particular autonomous system; they will be using the interior protocols. Typically, RIP was used earlier, but as I said now the most commonly used is OSPF. Of course there is a version of BGP, called internal BGP that can also be used as an interior routing protocol.

(Refer Slide Time: 07:11)



So, let us talk about the different message types that are there in BGP. BGP is somewhat similar to what we talked about in OSPF; because in OSPF also, routers where trying to maintain some neighborhood connections and through those neighborhood connections they were either sending hello packets to tell the other person that well I am alive or they were sending some kind of route update packets, some kind of link state advertisement through which state of the link which are changing are sent, so that all the routers can update the information in the routing tables.

Here, there are somewhat similar commands available in BGP and also there is a message type called open. Well, open says well if I have one router here in one autonomous system and another router here in another autonomous system, this open message can start or initiate a neighborhood connection between the two routers. So, when this router comes

up, it can send an open message, so that this BGP link between the two routers will get established.

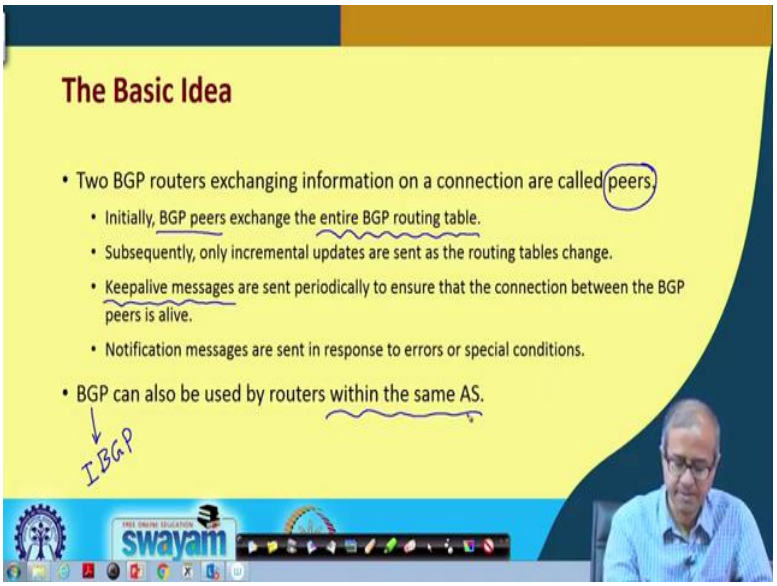
Now both the routers will know well, now we can expect to send and receive BGP messages and responses over this connection which has been established. This update as the name implies, it sends information about changing routes. So, they can transmit various kinds of information like about a single route, the route changes, some link goes down, some link comes up. So, the route can change that information might be sent.

Some new routes which are created maybe a new link is established, some new router connections have been established. So, some new routes will come up that kind of information are also shared and of course, some of the paths which may become infeasible.

Because some of the links are too slow or maybe some link has gone down that information can also be sent using these update messages and just like hello message in OSPF here in BGP, there is a message called keep alive. Keep alive message sent between the neighbors will maintain that connection alive. Well if you do not say keep alive for a certain amount of time, the neighborhood connection will be automatically terminated.

It means that one of the two parties is not interested in exchanging BGP messages anymore, ok and in case of some error conditions happening in the network; some notification messages maybe sent again using this BGP protocol. So, these are broadly the various messages I am not going into the details. For details you can refer to a number of materials which are available. I am just giving you the overall idea ok. These are the four message types supported by BGP.

(Refer Slide Time: 10:38)



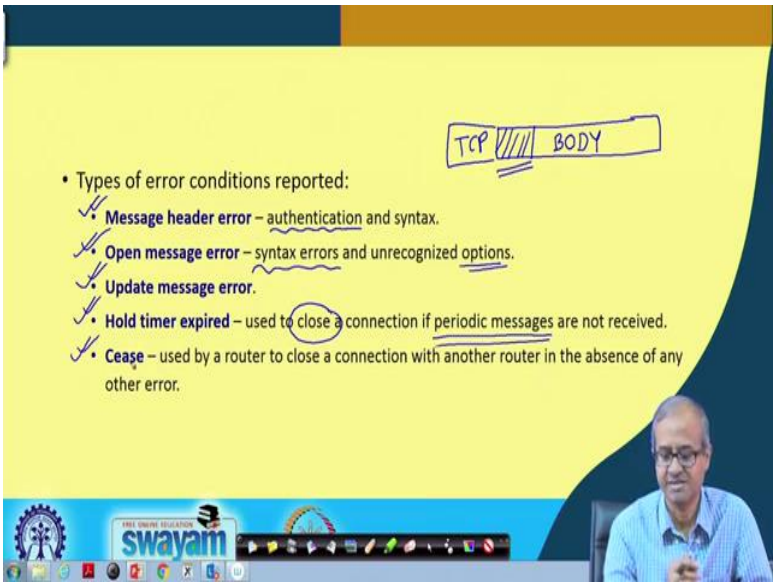
Now, the two end routers through which BGP establish a connections and exchange messages, these are called peers or peer routers or peer gateways. So, these peers are the one which participate in sending and receiving BGP messages right.

So, initially when everything starts up at the very beginning, the BGP peers will exchange entire routing table with the neighbors. Initially when the network comes up. Suppose, I am one of the peers, I will send my entire routing table information that I have to my neighbors. Similarly I will be receiving similar information from the others, so that all of the routers can update their routing table, with the latest information that is available right.

But after this initial exchange of the entire routing table, subsequently I shall not be sending the entire table anymore. I shall only sending information about the changes, some new routes are getting added, some existing routes are getting modified information like that ok and of course, I can mention this keep alive messages are important. They are sent periodically, so that both the parties know that well the link is alive and the routers are up and running. Notification messages also I mentioned, they are sent in response to some error conditions.

As I mentioned that there is a version of BGP called internal BGP or in sometimes in short you call IBGP that can also be used by routers to update their information within the same autonomous system also, just as a substitute of OSPF let us say, fine.

(Refer Slide Time: 12:47)



Now, this notification message as I said is used to sense and receive some error conditions. So, what kind of error conditions? Some of these are mentioned here. You see, suppose I have a BGP packet coming ok, BGP packet is a TCP packet. So, there will be some header and there will be the body of the packet message. Now, the first thing is that there can be some error in the header, like this is the BGP header right, now on top of the BGP header, TCP will be including its own header to make it a TCP packet.

So, it may so happen that there is some erroneous information in the header part, some of the fields which are invalid. So, something might happen during transit, some bits might become changed, 0 may become 1, 1 may become 0. So, if there is some error in the header, so either in the syntax, some invalid values are there or there is an authentication option. Also I mentioned some of the packets might get encrypted.

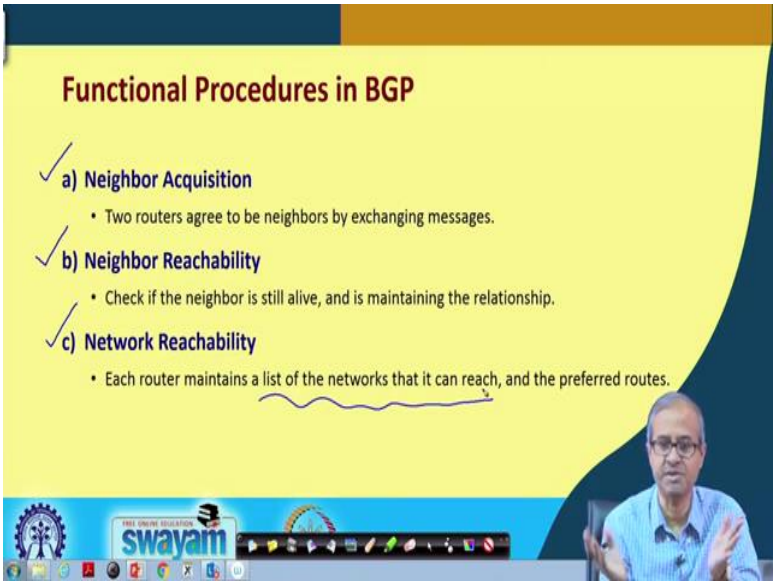
So, if the encryption is somewhere wrong, so that the receiving end cannot decrypt it, they will be reported as message header errors. Similarly, there can be open message errors, where there is some syntax error in the body of the message, some options you have specified which are not one of the valid options. This can again happen due to network errors during transmission right.

Similarly, when the routing table changes are being transmitted through the update messages, there can be some error in those messages also, somewhere some corruption may happen, so that the receiver is unable to understand what it means.

Hold timer expired means the keep alive messages are used to inform that the link is up, the connection is running. There is a timer which is set every time a keep alive message is reached. After that if the timer expires, it means that the periodic messages are not coming. So, now I can close the connection, maybe the other side is not responding. Sometimes, due to some reason, you can forcibly terminate a connection. Let us say due to some reason, your network is being brought down due to maintenance and other things, you are forcibly terminating connection with the other peers.

So, there you send a cease error message to your neighbors saying that well I am requesting to terminate or cease the connection right, but there is no other error as such I am wanting to close the connection.

(Refer Slide Time: 15:59)

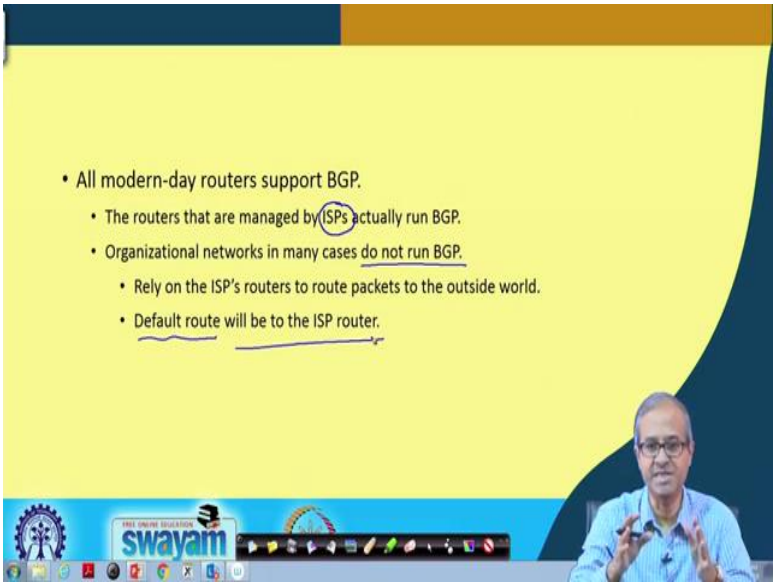


Broadly speaking, there are three functional procedures that are there in the BGP which is achieved through BGP messages. One is of course, neighbor acquisition, I had said. Initially a neighbor connection can be set up and can be maintained through keep alive messages.

Neighbor reachability; periodically we check for the receipt of the keep alive messages, if it is not coming, it may mean that the neighbor is not reachable anymore, there is some network problem and network which this is neighbor reachability.

Network reachability means you see BGP, in BGP we maintain information about other networks; because of some link failure somewhere, maybe one of those networks has become unreachable, I cannot connect to that network. So, that is a list which the router maintains. It is a list of networks that it can reach and also the ones which it cannot reach. The list of network which it can reach means those networks are reachable and the networks, which are not there in the list will mean they are not reachable or I do not have information about them as of now ok.

(Refer Slide Time: 17:25)



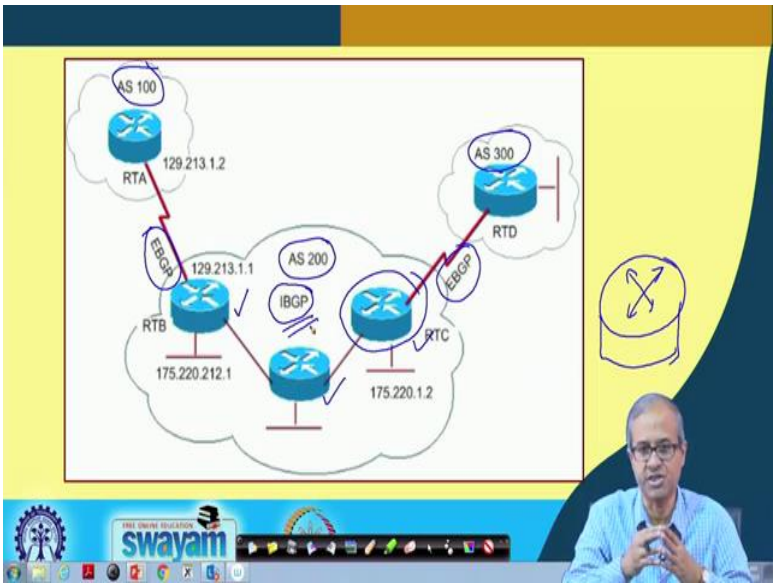
Now, the point you note is that all modern day routers particularly the ones you are using in the border or the gateway, they support BGP, but whether or not to implement BGP and run BGP that is dependent on the decision of the organization. Well if you decide to run BGP on your router; that means, you are putting some extra responsibility on yourself. Mean you are not relying on a, it means other routers to provide you correct information. It is also your responsibility to maintain the information correctly, so that packet routing takes place ok.

So, the internet service provider, from where you typically get the network connections, the routers which has, which are managed by ISP, they invariably run BGP. So, when you make a connection with an ISP; so you may also choose to run BGP or you can rely on the BGP router at the ISP's side. That is of course, your choice. This is what I am saying, organizational networks in many cases that do not run BGP, because it may be so, that the

network administrators which are there, they are not competent enough to maintain the routers, to initialize the routers, so that they run BGP in the correct way.

So, in that case they can rely on the ISP's router right. So, the default route for packets will be to the ISP's router. So, whatever packet comes will be sending it to the ISP's router and the ISP's router will decide where to route. But if your network is running BGP, then you can also maintain a comprehensive routing table, where the packets that are coming for going somewhere else, you can decide where to send. But in the previous case you are sending only to the ISP's router.

(Refer Slide Time: 19:29)

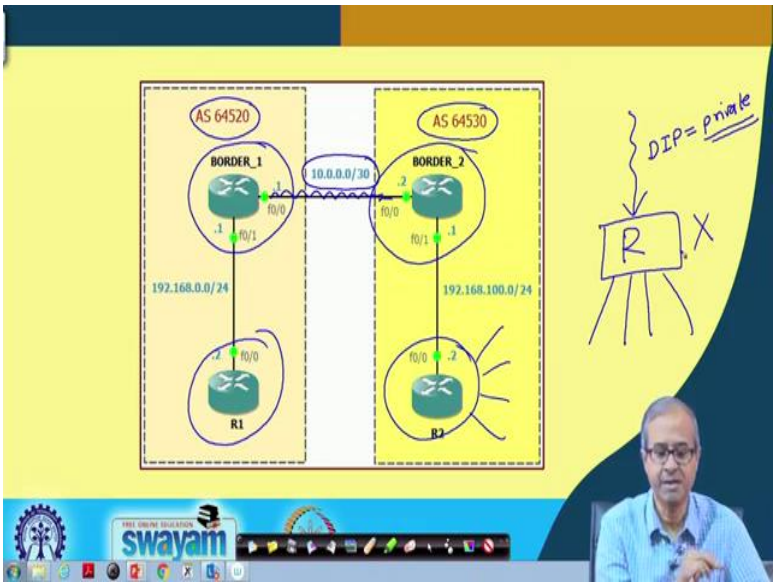


So, here I am just showing you a couple of examples. The first thing is that the routers that I talked about; this is an alternate symbol of a router. This is how you represent a router like this.

So, here you are seeing that there are several routers and there are some autonomous systems. This is autonomous system number 200. Let us say this is let us say100 and this is let us say 300. So, there are boundary routers which are running exterior BGP, which is the conventional BGP, which is supposed to be used as exterior routing protocol. But as I said if you choose to use, even inside of this autonomous system, these three routers which are using, which are there, they can choose to use internal BGP, IBGP.

So, in that case you can use the variation of the same protocol BGP, both inside and also outside the network. So, you really have a choice today. Inside the network in the autonomous system you can either use IBGP or you can use OSPF both options are available.

(Refer Slide Time: 20:57)



And here, in this diagram if you see, here again there are two autonomous systems with some numbers are given, arbitrary numbers, autonomous system numbers and as I said the routers that connect to other autonomous systems, they are called border routers or border gate, as you see here some routers are designated as borders; border 1, border 2.

But there can be other routers which are inside the autonomous system, which are meant to connect sub networks or networks inside that autonomous system, they are not connecting with the outside world. So, let us say here this connection between, this connection is a point to point link right, this link is not shared by anyone else. So, here if you want, you may choose to use a private IP network. So, recall I mentioned anything that starts with 10, is regarded as a private class A network.

So, here we are using this private class A network 10 to maintain this dedicated connection between two routers. You see only when there is a question of routing, you cannot use the private, this IP address. So, like you see, you recall when you discussed IP addresses, we said that some IP addresses are meant to be private. What is meant by private? Suppose I have a router and a packet arrives for routing, there may be multiple outgoing links.

Suppose, you see that the destination IP address, let us say DIP is an address which is one of the private addresses belong to one of the private networks.

So, if your destination address belongs to a private network, then this router will simply discard this packet, it will not forward it ok. But you see in this case, in this example, we are talking about a dedicated link between two routers, it can be a leased line. So, here there is no concept of routing in between. So, here if you want, you can use such private networks also. So, with this we come to this; we come to the end of this lecture where we give you some very overall idea as to how the border gateway protocol, BGP works as an exterior routing protocol.

Now, with this our general discussion on routing protocol ends. Of course, in the next lecture, we shall be talking about something which is quite related and similar. We shall be talking about a new IP version, IP version 6 which is becoming very important in the present day context.

Thank you.