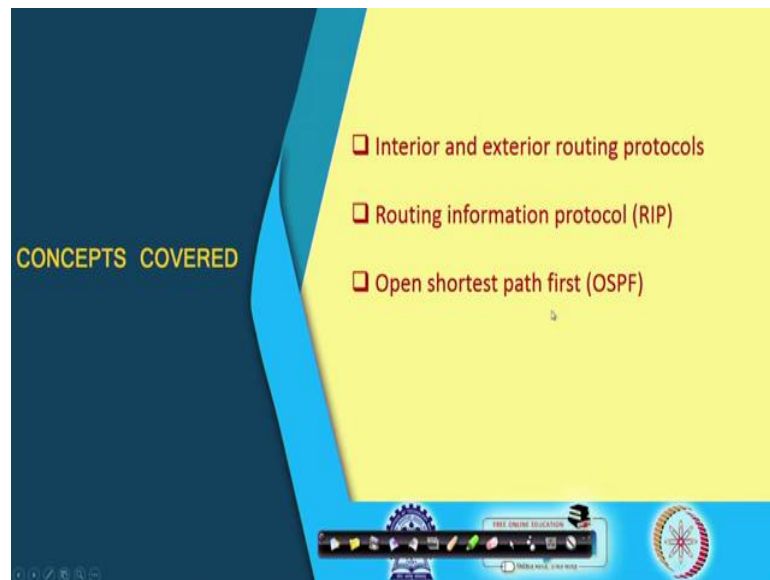


Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 12
Routing Protocols (Part II)

Let us continue with our the discussion on Routing Protocols which we had initiated during the last lecture. In the last lecture, we talked about routing tables, the way packets get delivered and some typical fields or entries that are present in the routing table. So, we continue with the discussion. The topic of this lecture is Routing Protocol Part II.

(Refer Slide Time: 00:41)



In this lecture, we shall be first distinguishing between two different kinds of routing protocols called interior and exterior and specifically, we shall be briefly looking at two different practical routing protocols; one is called Routing Information Protocol or RIP, other is Open Shortest Path First or OSPF.

(Refer Slide Time: 01:13)

Routing Protocols

- Two broad classes of protocols are used in the Internet:
 - Interior**
 - Routing Information Protocol (RIP) ✓
 - Open Shortest Path First (OSPF) ✓
 - Exterior**
 - Border Gateway Protocol (BGP)

The diagram illustrates two distinct groups of routers, each enclosed in a hand-drawn circle. A dashed line connects a router in the top circle to a router in the bottom circle, representing communication between different administrative domains. The bottom circle contains three routers connected in a triangle. A video feed of a man is visible in the bottom right corner of the slide.

Let us see. First as I have said we would be distinguishing between two different classes of routing protocols; one is called interior, one is called exterior. You see by the very name interior, exterior, you can understand, we are talking about some kind of a boundary that whether we are inside the boundary or outside the boundary ok.

Now, interior means see these protocols are used for routers to communicate among themselves. Multiple routers they communicate using these protocols for updating their routing tables. So, we saw in the previous lecture that there is a field in the routing table which indicates some flags that whether a route was added or was modified through redirection.

So, these protocols help in this redirection and can automatically make updations in the routing table entries right. Now, interior protocols for which examples are RIP and OSPF, there the idea is that the routers that are talking among themselves for updating their routing tables, they are all inside some kind of a boundary ok. They are all inside, that is why they are called interior and exterior means well let us say there is another boundary.

There is some other router there and one of these routers can talk to that other router in that other boundary and update routing information, share routing information accordingly. These are called exterior routing protocols and border gateway protocol is one very important example of that.

(Refer Slide Time: 03:21)

Autonomous Systems (AS)

- What is an AS?
 - A set of routers and networks managed by a single organization.
 - The routers within the AS exchange information using a common routing protocol.
 - The AS graph is connected (in the absence of failure).
- Every autonomous system is assigned a unique **AS number**.
- Routing protocols within an AS and across different AS's can be different.
 - Interior versus Exterior.

Now, that boundary I was talking about, that boundary technically is known as an autonomous system ok. Autonomous system is that imaginary boundary which I am, I have just mentioned, so, that imaginary boundary, an autonomous system or in short AS, this is an AS and how do we define an AS? AS is loosely defined as inside this, there can be multiple routers, there can be many routers, there can be many hosts, many networks also, there can be multiple networks not a single network ok, multiple networks and obviously, there are large number of computers, hosts.

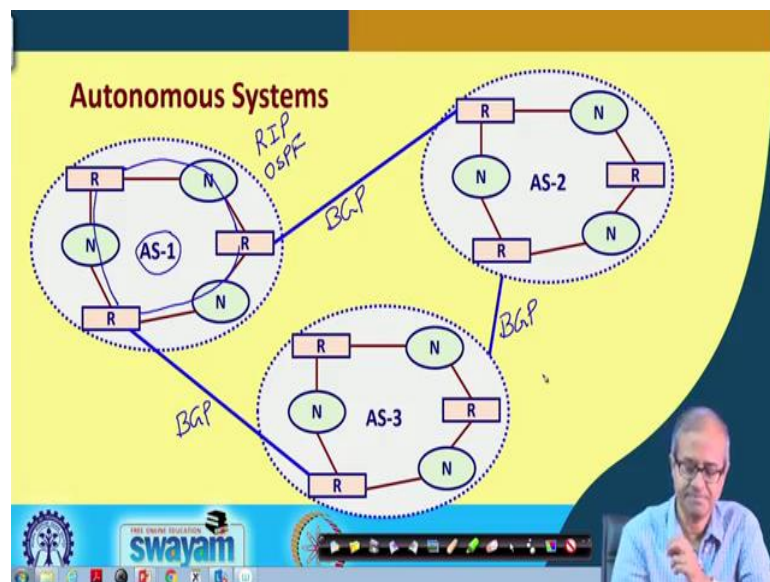
Now, if all of them are managed by a single organization, then we can define it as an AS. Many organizations may have different sections or departments, there can be multiple networks connected together, but they are all managed by a single entity or organization. So, if the organization wants they can define their organization as an autonomous system or AS. There is a procedure you can get a unique autonomous system number for your network and all autonomous systems in the world, their number, numbering is unique; no two autonomous systems have the same number ok.

Now, inside this autonomous system, the routers within the autonomous system, they can exchange information using some common routing protocol. Because there inside the organization, you are following the same rules, same protocols and AS graph means graph is what, some nodes connected by some edges. So, in some means in a network graph, we have seen some examples. The nodes are the hosts, routers and networks; edges are their

interconnections. So, if the graph is connected which of course it has to be, because if there is no path between 2 nodes, then you really cannot reach there. The graph is disconnected, but if there is some failure, some link failure; then, your graph might get disconnected ok.

But normally, the AS graph is connected and as I had said every autonomous system, if you register with a central authority, you will be assigned a unique AS number and routing protocols between routers belonging to the same AS will be following interior routing protocols and across different AS's, they will be following exterior routing protocols. This is the difference.

(Refer Slide Time: 06:35)



Now, here I am showing a picture, where there are three autonomous systems, I am showing those numbers are 1, 2 and 3. Now, as you can see in each autonomous system, there are several routers, there are several networks. Of course, there are computers. I have not shown the computers here and there are links which connect routers to the networks. So, the router which have there inside, you can see that there are multiple connection for AS-1 for example, this router is connected to this router via this network. This router has a connection to this router via this network and this router has a connection here.

Now, these routers can exchange information and keep their routing table updated using interior protocols which I said, there are two main examples RIP and OSPF. But when you talk about routers which belong to different autonomous systems which are shown by these blue lines, here we use some external or exterior routing protocol like BGP ok. This is how

these interior and the exterior protocols work and this is how their scopes are defined all right.

(Refer Slide Time: 08:13)

• Which class of protocols to use?

- Use interior router protocols to exchange information between routers within an AS.
 - ❖ RIP or OSPF.
- Use exterior routing protocol to pass exchange routing information between routers in different AS's.
 - ❖ BGP.

The slide features a yellow background with a blue header and footer. The footer includes the Swayam logo and a video player interface. A small inset video shows a man speaking.

This already I have mentioned, I am just repeating once more that which class of protocol you need to use for a particular scenario. Well, for routers within an autonomous system, inside the autonomous system, you use interior routing protocols RIP or OSPF and to exchange routing information between routers in different autonomous systems, you use exterior routing protocol like BGP. This is what we use.

(Refer Slide Time: 08:49)

Routing Information Protocol (RIP)

- It is an interior routing protocol.
- Routers within an autonomous system exchange messages.
 - Distance vector routing using hop count.
 - Table entries updated using values received from neighbors.
 - Maintain timers to detect failed links.
 - Used in first generation ARPANET.

The slide features a yellow background with a blue header and footer. The footer includes the Swayam logo and a video player interface. A small inset video shows a man speaking. A network diagram is drawn on the slide, showing a sequence of routers R1, R2, R3, and R4 connected in a line. R1 and R4 are connected by a dashed line. To the right, a separate network is enclosed in a circle and labeled 'AS', containing two routers connected by a dashed line.

Now, let us briefly look at these routing protocols one by one. First, we talked about this RIP, Routing Information Protocol. Now, I mentioned already, it is an interior routing protocol meant to be used inside an autonomous system. If this is an autonomous system, routers that are present inside this AS, they will be using RIP to exchange information for updating the routing tables. Now, you may ask why this exchange is required because they are anyway belonging to the same organization.

But you see, consider an organization where there can be two departments, two different networks. There is one router sitting here; one router sitting there. The other router will know much better about the status of the other network whether some link is down or everything is alright or not. But when I am sitting in this network, I want to send a packet to one of the computers in the other network, I do not know what is the status in the other network; which path is this best; which path is required to be followed. So, the other network can give me some information about the current state of the network.

Current state; what is the links that are currently down; what are the links that are currently congested; various information like that. So, I can update my routing table so that I can choose the best route to follow to reach that host ok, all right. Now, in RIP the way the routing tables are updated, there is a very standard method called distance vector routing. Well, I am not going into the detail of these methods. These methods are given in significant detail in any standard textbook on computer networks, you can see through them if you are interested. Distance vector routing basically says, every router will have some information about how far the other routers are from myself.

Like for example, I have a router here; there can be other routers like this. Let us say, this is router 1, router 2, router 3 and router 4. Let us suppose the connections are like this, router 1 will have the information that router 4 is 3 hops away from me ok, but suppose a new link gets established between R1 and R4, so that 3 will get updated to 1. Now, R1 and R4 are directly connected. Similarly, if one of the links go down, these values will change ok. Distance vector routing sends the distances to all routers whatever information I have to all the other routers and everyone collects all the information they receive and in a consolidated way, they update their routing tables.

This is what is done here and some timers are used to detect link failures. If some packet you are sending, you are not getting acknowledgement within certain amount of time, then

you may assume that the link has failed; link is not working. This was used in older networks, but presently this RIP is very rarely used because RIP has some drawbacks.

(Refer Slide Time: 12:41)

Problems with RIP

- Slow convergence for larger networks.
- If a network becomes inaccessible, it may take a long time for all other routing tables to know this.
 - After a number of message transfers.
 - A drawback of routing table updation using distance vectors.
- Routing loops may take a long time to be detected.
 - Counting to infinity problem.
- Too much bandwidth consumed by routing updates.

The diagram shows a network topology with routers R0, R1, R2, R3, and P4. R0 is connected to R1 with a hop count of 5. R1 is connected to R2 with a hop count of 3. R2 is connected to R3 with a hop count of 1. R3 is connected to P4 with a hop count of 0. There is a handwritten 'X' over the link between R1 and R2, indicating a failure. The slide is part of a video lecture, as evidenced by the 'swayam' logo and a video feed of a presenter in the bottom right corner.

Some of the drawback is that the way the routing tables are updated using distance vectors, see once distance vectors are shared, something will change. That change again will be shared that will again trigger some more change. So, this leads to something called convergence in the routing table which at times is very slow.

Suppose a link fails, again a link goes up. So, how quickly can the routers respond to these changes and update their routing table. This RIP is not very good at that. It can take a lot of packet exchanges to update all the routing table to reflect the correct status. So, broadly speaking I am just mentioned here if a network becomes inaccessible due to a link failure, some link has failed; it may take a long time for all other routing tables to know about this.

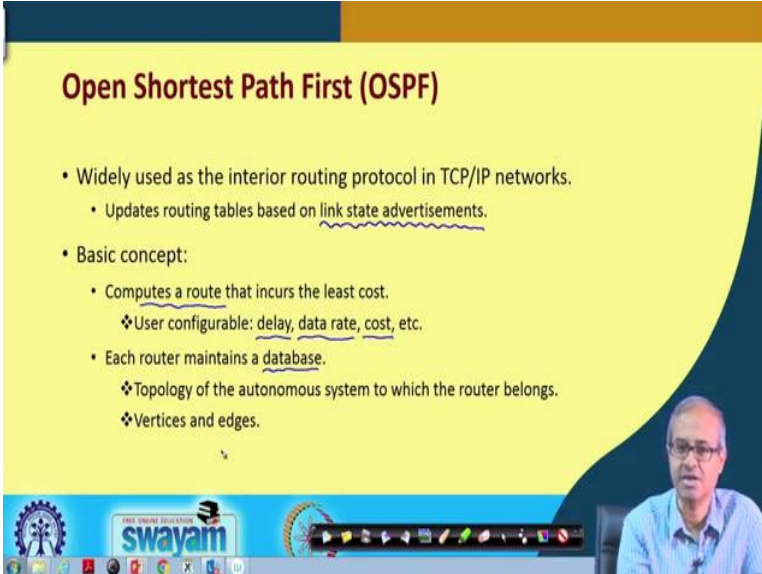
Because you see I am giving a very small example. Let us say R1 is there, R2 is there, R3 is there and let us say R4 is there. R1, R2 this is the connection. Now, let us say I am thinking about the distance to R4. Well, R1 knows that R4 is 3 hops away; R2 knows R4 is 3 hops away; R3 knows R4 is 1 hop away and R4 is R4, it is already R4, 0 hop.

Now, suppose this link has failed and let us say there is another router here, let us say R0 which initially was 4 hops away, this was 2 ok. Now this link has failed. So, you see now

R1 has no path to R4, the network has become disconnected; but R0 will tell R1 that well R4 is 4 distance away from me and because this is 1 hop.

So, R1 will update this to 5; 4 plus 1. But actually there is no path. So, in this way this 5, then 6, then 7, it will go up slowly, this is sometimes called counting to infinity; counting to infinity problem and this becomes very slow and too much bandwidth gets consumed due to the routing updates. This is some drawback here; some of the drawbacks.

(Refer Slide Time: 15:33)



Open Shortest Path First (OSPF)

- Widely used as the interior routing protocol in TCP/IP networks.
 - Updates routing tables based on link state advertisements.
- Basic concept:
 - Computes a route that incurs the least cost.
 - ❖ User configurable: delay, data rate, cost, etc.
 - Each router maintains a database.
 - ❖ Topology of the autonomous system to which the router belongs.
 - ❖ Vertices and edges.

The slide is part of a video lecture, as evidenced by the 'swayam' logo and a small video inset of a man speaking in the bottom right corner.

Now, this OSPF, Open Shortest Path First, this is more widely used as the interior routing protocol. Let us see some of the features of OSPF. Now, in TCP/IP networks, this is most widely used as I said and it relies on something called link state advertisements.

Well, here distance vectors are not shared like how far R1 is from me, R2 is from me, R3 is from me, nothing like that, but status of the links, some link what is the current delay from myself. It sends or shares the link delays, if a link is down, it tells the link is down. But in the earlier case that information was never sent ok. Basic concept is that the OSPF tries to compute a route again dynamically based on some least cost algorithm ok.

The notion of cost again can be configured how, means how do we define cost. Is it minimum delay; is it minimum cost or is it with respect to the data rate of the links you are following ok; how are you defining? So, each router will be maintaining the information about the current state of the network, of the autonomous system that we are

calling as the database. The topology of the autonomous system is stored in the database, how the graph looks like as per the information available with the router right and this graph will contain obviously, vertices and edges; networks and routers and how they are connected.

(Refer Slide Time: 17:33)

- Two types of vertices:
 - a) Router
 - b) Network
- Two types of (weighted) edges:
 - a) Two routers connected to each other by direct point-to-point link.
 - b) A router is directly connected to a network.
- A router calculates the least-cost path to all destination networks.
 - Using Dijkstra's algorithm.
 - Only the next hop to the destination is used in the forwarding process.

Vertices are routers and networks. Talking about edges, there are two types of edges and every edge will be assigned a weight like for example, there are two nodes, they are connected and this edge will be having some weight, let us say 5 or something. This is called weight, now there can be two kinds of edges; one is an edge between two routers.

This can be a router, this can be a router; both can be routers. Directly two routers are connected by a point to point link; well, I mean such when does it have happen? Suppose, I have an organizational network, where there is a router and there is another network, this is my internet service provider from where I have got my internet connection, it can be BSNL, Airtel whatever.

They have a router and from this router to router there is a direct, point to point connection. This is the first kind of link. The second kind of link may be, the router may be connected to an internal network like I have a network here, this router is connected to this network. There is a second kind of edge or link now in this OSPF method, each router will try to calculate the least cost path to all destination networks that is available in its own database.

It has a set of networks in its database, it tries to compute the shortest path to all the networks and it uses a very well known algorithm Dijkstra's algorithm.

Dijkstra's algorithm is a algorithm that computes shortest path between pair of nodes in a graph ok. And once this is done, the routing tables are updated, during the packet forwarding only the next hop information is stored in a router.

(Refer Slide Time: 19:37)

- Two types of vertices:
 - a) Router
 - b) Network
- Two types of (weighted) edges:
 - a) Two routers connected to each other by direct point-to-point link.
 - b) A router is directly connected to a network.
- A router calculates the least-cost path to all destination networks.
 - Using Dijkstra's algorithm.
 - Only the next hop to the destination is used in the forwarding process.

Suppose I am a router; I am a router and I have received an incoming packet. My routing table will only tell that where to forward it next which is the next router I have to send it to. Well, it will not tell you that what is the sequence of routers I have to follow, no, only the next router. Let the next router decide after that what to do ok. Here the packet forwarding will happen on a next hop basis. It only sends to the next router and the next router will again decide after that.

(Refer Slide Time: 20:19)

- In the steady state
 - All routers know the same network topology.
 - "Hello" packets sent every 10 seconds (configurable) to neighbors.
 - Link State Advertisement (LSA) flooded initially from each router.
 - Absence of "Hello" packet for 40 seconds indicate failure of neighbor.
 - ❖ Causes LSA to be flooded again.
 - LSAs re-flooded every 30 minutes anyway.

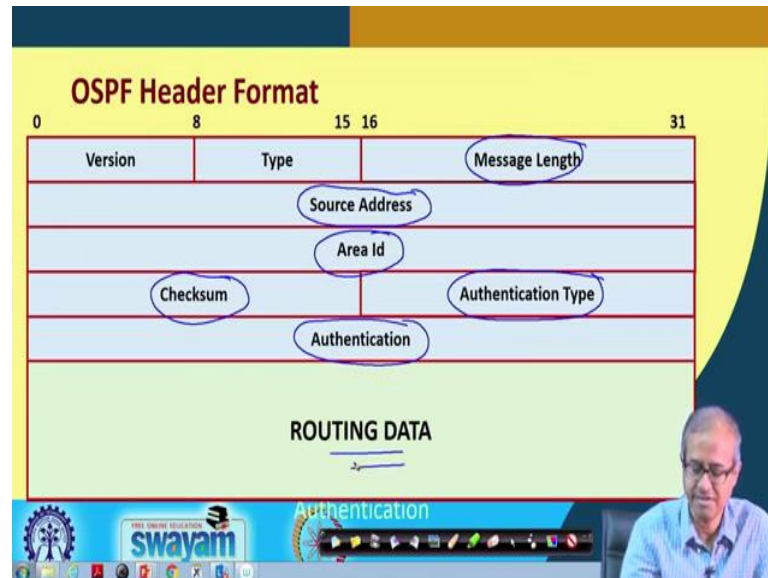
So, in the steady state after the link states are exchanged and all the routers have computed the network topology, the distances, shortest paths. So, all routers will be having the same network topology, finally after the shortest paths are all computed and calculated ok. There are a few other things; each router will be sending some dummy packets called "Hello" packets to all its neighbours just telling that well I am alive, I am still active so that other routers can know that well that the other person has sent me a "Hello" packet, that other fellow is fine, it working at present.

So, every 10 seconds or so, that time can be configured, such "Hello" packets are sent to neighbours and there is another kind of a packet which is more elaborate, Link State Advertisement or LSA. It will send information about the status of all the links. Suppose, I am a router, I have four links connected to me. Well, I will tell everybody that the current status of these four links are this. This link is down and the other three link, the status is this; current delay is this. This delay is 3, this delay I am finding 2, this delay I am finding 5; some units ok. Now, absence of "Hello" packet for certain time for 40 seconds or so.

This may lead the router to take a decision or a conclusion that well that link is currently down, that other router has failed ok. So, once such a failure is detected, this link state advertisement is initiated again. Again, this new state is forwarded because now one router has detected that one link has failed, let the others also know and anyway every 30 minutes

or so, link state advertisements are re-flooded or resent by default, but once somebody detects a failure, it will be sent forcefully.

(Refer Slide Time: 22:43)



This shows the OSPF header format, what are the fields in the header. Well, I am not going into too much detail. There is a OSPF version number as you can see. The first 7 bit contains the version number; the second 7 bit contains the type of the packet, what kind of OSPF message it is carrying. The length of the message 16 bits, source address, from where it is coming. Area, here this is a concept of a area, well I am not going to detail again. Well, inside an autonomous system, there is a concept of a zone, or an area, you can identify an area and each area can be given some id or an address.

So, this area id will contain the id of that particular area and this header information, there will be a checksum for error correction. There will also be an authentication type, because you see these packets are very crucial, depending on these packets, the routing table will get updated. Well, if someone maliciously sends a wrong link state advertisement, then all the routing table might get updated in the wrong way and packet might follow some circular loops and never get forwarded to the right direction.

That is why some authentication, authentication means I must be sure that the link state advertisement is coming from the right person, right router and some authentication information and of course, the actual link state advertisement or whatever you are sending,

they actual routing data, link states etc. ok. So, these are the information which is carried as part of a OSPF packet.

(Refer Slide Time: 24:35)

OSPF Packets

- Packet types :
 1. **Hello** (check if neighbor is up)
 2. **Database Description** (synchronize database at beginning)
 3. **Link State Request** (request specific LSA)
 4. **Link State Update** (LSAs flooded)
 5. **Link State Acknowledgement** (flooded LSAs are explicitly ack-ed – reliable flooding)
- Authentication type:
 - Cleartext
 - Encrypted (MD5 Hash, others possible)

The slide is part of a video lecture, as evidenced by the speaker's video feed in the bottom right corner and the 'swayam' logo in the bottom left. The slide has a yellow background with a blue header and footer.

Now, packet types here I am summarizing the different types of packets; some of them I have already mentioned. There is the “Hello” packet I have already mentioned. It actually says that whether a neighbour is up and running or not. Database description, this is used at the beginning. Just initially when the network is up, database description packet is sent to synchronize the database of all the routers.

Link state request; some router might due to some reason it might have lost its routing table. It might specifically request link state information from some other router. This is called link state request and that link state advertisement is this link state update, that is actually the link state information which a router sends to the some other router and link state acknowledgement means once some router receives a link state advertisement, it will send back an acknowledgement that well I have received it correctly, so that other routers know that what I have sent was received correctly by everyone else right and regarding authentication type I said the simplest case may be clear text.

Everyone can see what is going or you can encrypt it, so that if someone wants to hack my network and make changes in my routing table by altering these packets, it will be difficult to do so ok. These are the options which are available.

So, with this I come to the end of this lecture where I have very briefly talked about the Interior Routing Protocols, RIP and OSPF. In the next lecture, I shall be talking about the exterior routing protocol BGP which as I have already mentioned is used to update or share routing information across autonomous systems which becomes much more crucial for routing data packets over longer distances.

Thank you.