

Computer Networks and Internet Protocol
Prof. Soumya Kanti Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 53
Connecting LANs, VLAN

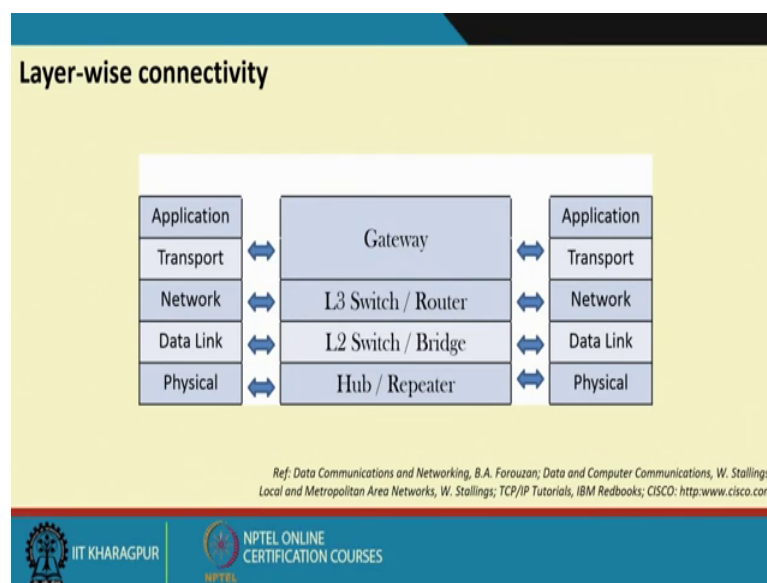
Hello, so we will be continuing our discussion on data link layer on this course on Computer Networks and Internet. Today we will be talking something on connecting LANs and a concept called virtual LAN or VLAN this is keeping that other technologies in place, we will try to see that how LANs can be connected whether the what are the issues into this connection of the LANs etcetera right.

As we understand that in our modern day labs or modern day offices etcetera. There are several networks right or what we have talking about layer 2 networks right they need to be connected right. And in not only that lot of if you look at the today's applications or today's operations of any organization, any section, any division, any department. They are primarily dependent on applications which runs over networks right.

So, it become it is becoming a what we say that it is becoming a necessity to keep this network always up. In doing so the network administrator loves to have a multiple connection into the connecting network right. So that means, between two LAN there can there should be more than one connection. So, that if connection is tiered off fail for some reasons, or other the other connection popup and start executing. Indeed doing so there may be lot of other issues right. So, even there are redundant connection how to manage them etcetera. So, connecting LAN in a appropriate fashion or in a seamless fail proof way is a challenge.

So, we will see that a basic consideration that what how do you connect LANs and type of things today's lecture. And also see a concept call virtual LAN right in the thought it is not only a layer 2 phenomena, it requires for routing layer 3 type of thing that we will see that three level routing activity. But we see that it also helps in handling the things. Another concern of over in case of layer 2 is it is in the same broad cast domain though the collision domains are divided, but still they are in the same broad cast domain, so that dividing the broad cast domain into different things. So, that it gives better manageability better security of the traffic and all those things that will try to see in this lecture.

(Refer Slide Time: 02:59)



So, if we come to the basic slides, or basic philosophy of layer wise connectivity, or peer to peer connectivity. So, what we will see that in the physical layer is hub and repeater which are primarily signal regenerator at layer 2 or data link layer. We have layer 2 switches or bridges which bridges LANs etcetera LAN.

And we have also seen that MAC layer protocols and other things. Layer 3 is a primarily that network activity one of the major part is or activity is routing. And then at the other layer there are primarily application to application connectivity, or in transport layer it gives a liable and reliable are this is a that what we mostly say that there are gateway connections between the two applications.

And as it indicates it is there can be multiple hub within the things and it goes on like peer to peer. And also we understand that intermediate devices can open the packet up to the layer it is enabled. So, if it is a hub or repeater it is it can see that layer 1 where as if it is a switch or bridge it can switch about layer 2 and so and so forth right.

And further we understand that your any upper layer phenomena or any upper layer device can have all the lower layer capabilities like a layer 2 bridge or switch can also have a signal repeating capability, or repeater capability. Like layer 3 switch has a definitely a switching capability and also a repeating capability right.

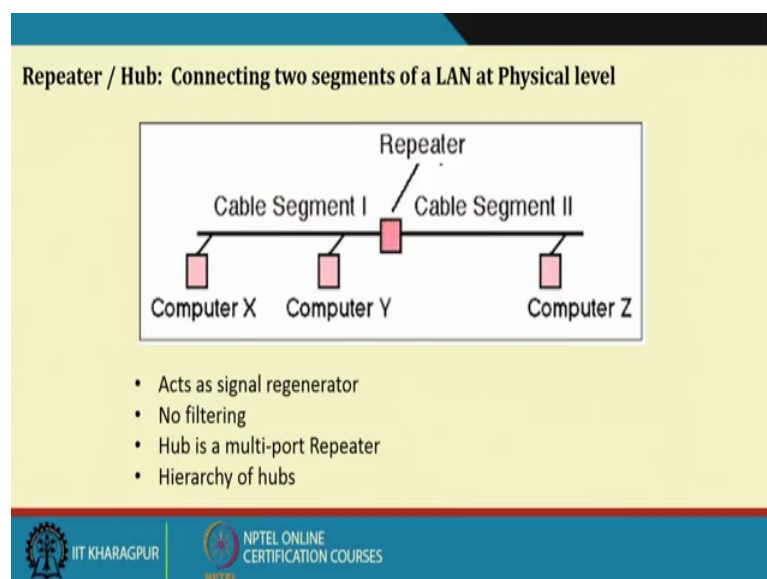
So, hub a higher in the layer you have the capabilities doing the things. Then why not by the something which is a layer 7 11? One of the major constraint is the cost right here, we have a huge cost on the if you go up in the ladder right.

So, you may not require that much cost to be invested. Secondly, more is the capability more is your processing time right, so that is why the cost is higher and not only that you need to process. Like so you may not want to have so much thing or you need to plan accordingly where you require layer 2, layer 3, layer 4. All upper layer capability switches right.

So, these are different consideration which has a separate way of system administration and management per say which need to look at that what are the things there. Other aspects what we look at is the scalability right the network should be scalable right. So, today I may have 10 systems, tomorrow I have 15 systems. So, I that most of your networking infrastructure are somewhat it is in the backbone and changing them now and then is very costly affair right. Costly affair in terms of monitor items, costly affair in terms of other configuration power etcetera.

So, when you increase the things there should be able to scalable; scalable to a definitely to a range type of things. So, those things has to be kept in mind when we design a things and this different type of things we are what we are discussing may help in able to do a better management of the things.

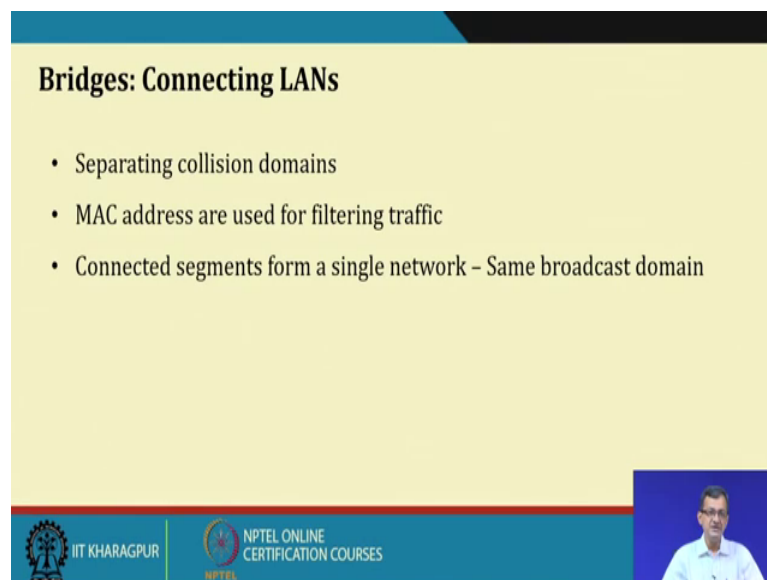
(Refer Slide Time: 06:21)



So, if we look at the repeater or hub its act as a signal regenerators, so I can have a 1 segment, 2 segment, and there is a repeater in between regenerates the things. But never the less it is in the same broadcast and collision domain as it is in layered 1. And so connecting more will in you will have a problem of more what we say more crunch on the bandwidth. Because if there are more collision that more repetition of the things etcetera right.

So, it has does not have any filtering per say because whether it understand layer 3 IP, or layer 2 MAC right. And I can have hierarchy of hub a hub a say couple of hubs below the level and couple of so, it is I can hierarchy of hub. And again it save a lot of bandwidth side.

(Refer Slide Time: 07:13)



Bridges: Connecting LANs

- Separating collision domains
- MAC address are used for filtering traffic
- Connected segments form a single network - Same broadcast domain

The slide features a yellow background with a blue header and footer. The footer contains the IIT Kharagpur logo and the NPTEL Online Certification Courses logo. A small video inset of a speaker is visible in the bottom right corner.

So bridges on the other end is a layer 2 phenomenon which connects LAN separates collision domain. So, bridge typically a LAN is in a different collision domain. But same broadcast domain or bridges also separate the collision domain even if they are in the same collision domain when I bridge them with layer 2 switch they are in the different collision domain.

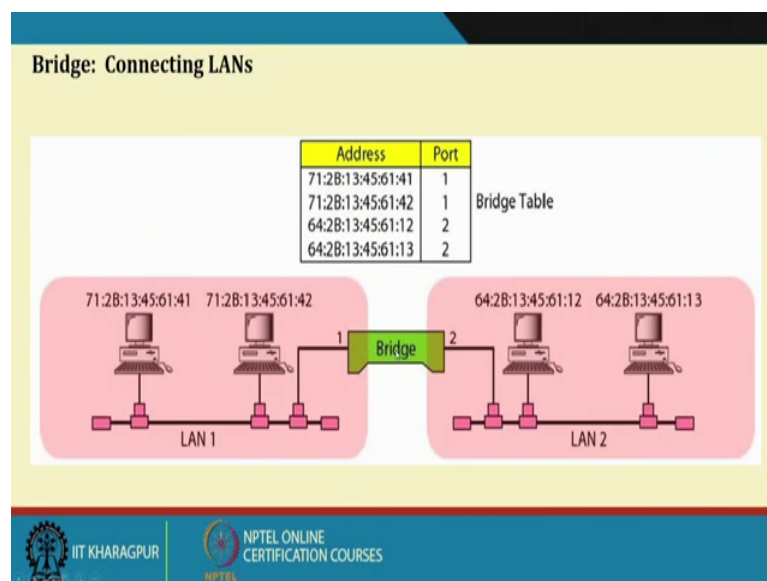
So that means, I have say file 5 LAN network, or 10 network connect with a bridge, or say two LAN network connect with a bridge. Usually bridge bridges are typically to port when it is multiport bridge we say a layer 2 switch right. So, this is convention there is

nothing harm in talking that number of connection in the bridge, but this is the way or showing domain the bridges.

So, they use MAC layer, MAC address for filtering traffic connecting segments form a single network same broadcast domain. So once it is connected it is becomes a single network. So, I we have a bridge network which is a single network; that means, in the same broad cast domain, but different collision domain right. So, that is none of the aspect of the thing and it can filter based on the MAC address, so that is the another property of bridging.

So, like here what we see that there are in one LAN there are two systems with this MAC addresses. And the other LAN there are the two systems and there is a mapping things that or which MAC address is connected to which port, which MAC address is connected to which port and these are the mapping things right.

(Refer Slide Time: 08:53)

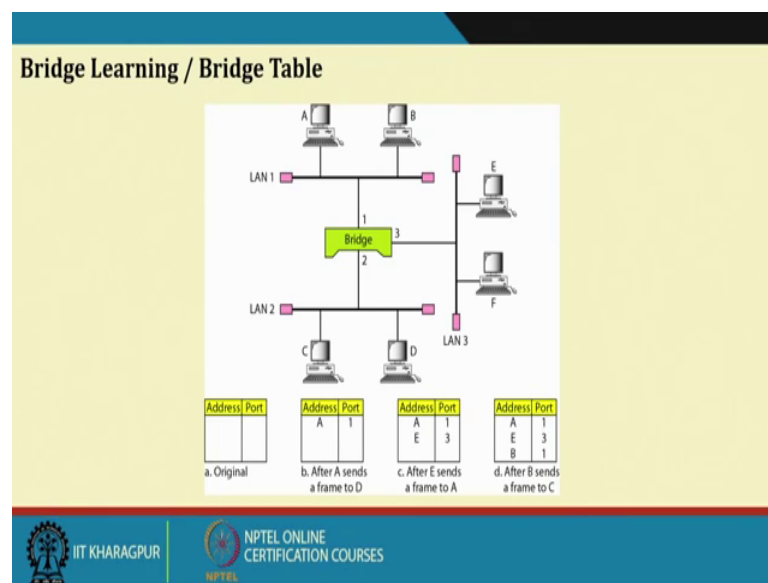


So, if you see that in the port 1, so that the bridge has a 2 ports, port 1, these two machines are connected port 2 machines are connected port 2 machines are connected, and here is the bridge table. So, what to from there what we see that bridge initially does not know who is connected 1, where once the data trans start transmitting the bridge start learning this once it is learn then it is not that the port thing.

So, if a request comes from this particular thing it knows that it need to be host to port to port 1 it not to the port 2. If this is a multiport bridge or a layer 2 switch there can be a more bigger diagram a bigger table, but never the less I can forward the data into the appropriate table right.

So, this is this way it able to learn and have divide collision domain and type of things right. So, what we see it is a still in the same broad cast domain, but two different collision domain right.

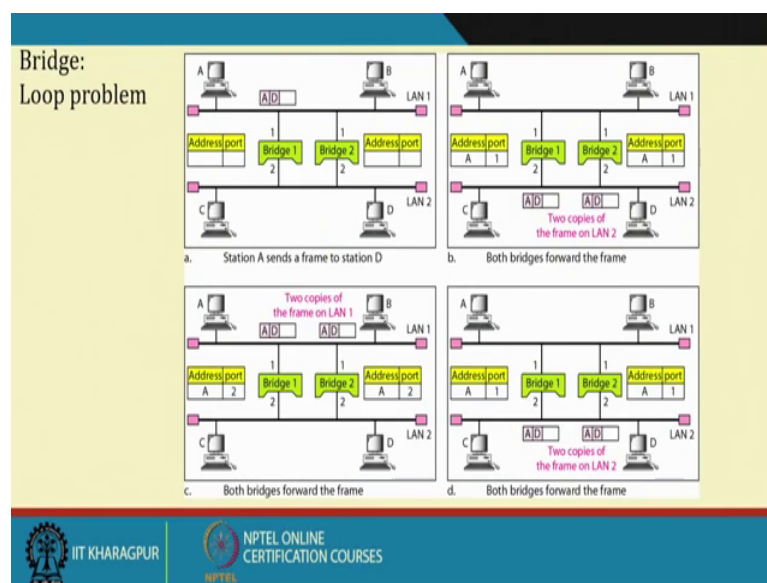
(Refer Slide Time: 09:53)



So, I can have bridge or layer 2 switch with multiple connections and as we attaining that it is it will learn that initially when A sends to D. So, that it learns that A is connected to 1 and then typically C after E sends to frame A; it learns that E is in 3 and so and so forth.

So, while communication goes on B bridge goes on learning and the bridge table goes on populating populated. So, once the bridge table is populated than it basically now it is easier to the forward packet. And it basically works gives a better performance in terms of bandwidth; that means, the collision domain etcetera are broken into different things.

(Refer Slide Time: 10:43)



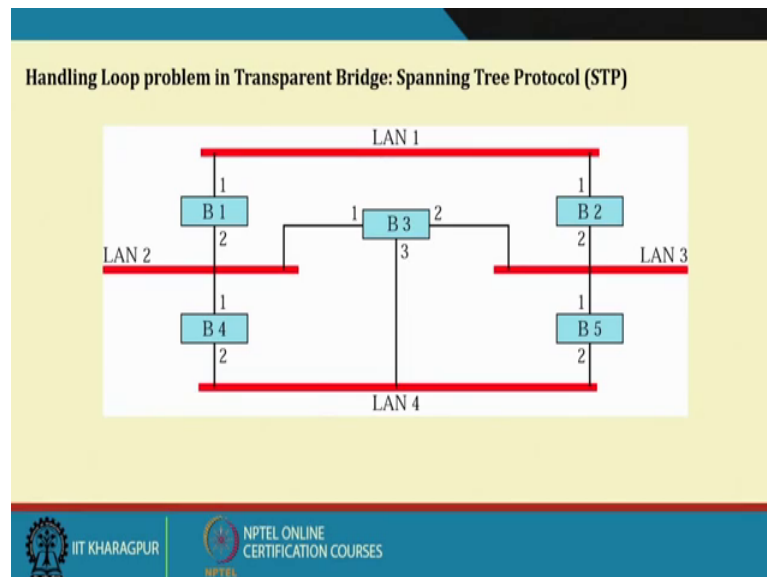
So, there is a problem in bridge like, so as we are mentioning initially that given a network the it is it is sometimes user able, and sometime making it some sort of fel proof or having multiple connection between the network. So, I have say connected I have a say cache section, or a administrative section and a account section and then I have lot of communication. So, if there is a communication break the things may have become problematic. So, what we do? We have multiple connection between these two LANs right.

In doing so whether we are end up in a some problem right here in this a typical case it is shown that A is sending to D a message and it is it learns that A is connected to port 1, and bridge 1 and 2 does not have any connection to those are all transparent bridges and it also LANs that this is A is at 1 port 1, and then this message is broadcasted and the when this gets that message. So, it gets the message A from bridge 2 as a from the at port 2 and then it converted to the port 1.

A is connected to port 2, and go on doing this in a circular fashion. As if you remember as the as our basic Ethernet, Ethernet frame does not have any TT a lot time lever where the timeout will be happening that is so to say. So that means, it goes on learning it goes on in a loop, and that creates a problem in the whole bridging thing. So, there so one of the one of the major challenge when we have this out of a bridge network all layer 2 switch network is how to handle this loops right. There should not be any loop into the

things otherwise it will not only take away all the bandwidth, it also creates a problem of communicating between any source to destination.

(Refer Slide Time: 12:55)



So, that is why you need to deploy some mechanisms. So one of the popular mechanisms which is being deployed is the STP, or spanning tree protocol right. So, handling loop problem in transparent bridge right, so spanning tree protocol. So, in this case if you see LAN 1 is connected to LAN 2 one connection. LAN 1 is connected to LAN 3; 1 connection and so and so forth.

In other sense from LAN 1 to LAN 2 there are several ways I can connect this through this I can connect this through this I can connect this through this right. So, there are multiple way how we can connect LAN 1 and LAN 2 right, so two LANs right. So, and in doing so we end up in that loop problem right if we allow this it will end up in a problem.

So, what we need to do is to handle of this. In order to handle this what we need to do is to look have a mechanism, or spanning tree protocol, that means I need to generate a cycle free all loops free connectivity, or if you consider as a graph this one a loop free graph into the thing.

(Refer Slide Time: 14:11)

Applying STP for Loop avoidance

1. Every bridge has an *unique ID*. Select the bridge with smallest ID. This is the **root bridge**.
2. Mark one port of each bridge (except root bridge) as the **root port**. Root port is the port with least-cost path from the bridge to the root bridge (marked with 1 star).
3. For each LAN, choose a **designated bridge**. A designated bridge has the least-cost path between the LAN and root bridge (the arrows). Mark the corresponding port that connects the LAN to its designated bridge the **designated port** (two stars).
4. Mark the root port and designated port as **forwarding ports**, the others as **blocking ports** (every port with 1 or 2 stars keep, ports with no stars drop).
5. *There is only one path between any two bridges.*

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, how this spanning tree can be implemented out here or how do I do that? So, in incidentally every B has a unique ID. Let me say every B layer to see has a unique ID; that means, B 1, B 2, B 3, B 4 let it be the unique IDs, so the select the bridge with the smallest ID as the root bridge. So, what we select here that the bridge means smallest ID than in this case B 1 as the root bridge. So, that I have a bridge tree, so the root bridge is the bridge with the smallest ID, mark one port in it bridge except the root bridge as the root port right. So, the root port is the port with least cost path from the bridge to the root bridge.

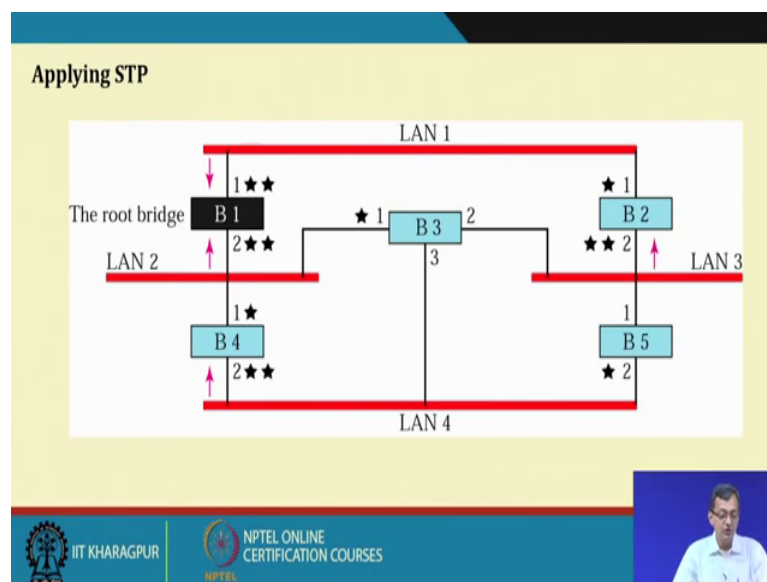
So, every bridge will have a root port which has the path to the root bridge as a least cost path right. Now least cost may be a consideration from the system administrator whatever organisation or whatever organization thinks it may be the minimum distance minimum hop to the path, or it may be the congestion free bandwidth driven etcetera. So, that is the least cost path between the any root any note to the any bridge to the root bridge and that particular interface is marked as a star right, or say one star.

For each LAN choose a designated bridge. So, for now on the for the LAN we need to choose a designated bridge the designated bridge as the least cost path between the LAN and the root bridge right. So, that is the designated bridge as the least path between the LAN and root bridge. Root bridge the arrows mark the corresponding port and connects the LAN to its designated bridge the using the designated port right.

So, the mark the corresponding port that connects the LAN to its designated bridge as designated port right with a two star. So; that means, designated that LAN to the designated bridge is the through this term. Now mark the root port and the designated port as the forwarding port.

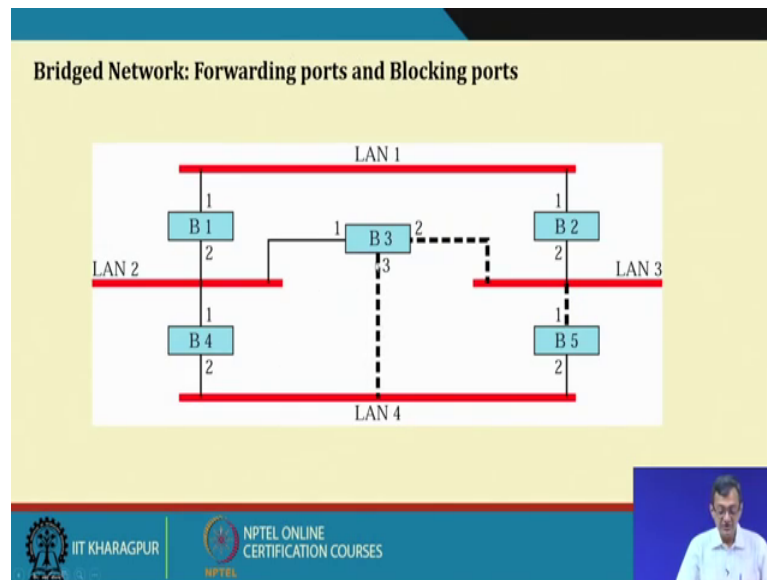
Now we are coming to that that mark the root port and designated port the forwarding port rest are blocking ports right the or every port with one on start are kept ports with no star are dropped right. So, this is the thing or our basic objectives is or the final goal is to have there is only one path between any two bridge, so other are in block stage and there are only one path between any two bridge.

(Refer Slide Time: 16:51)



Now looking applying STP, if we see so this is my root bridge and accordingly we connected by 2 star or 1 star which is from this every bridge. And there are so these are all marked as forwarding where as this fellow, this fellow and this fellow are marked as blocking.

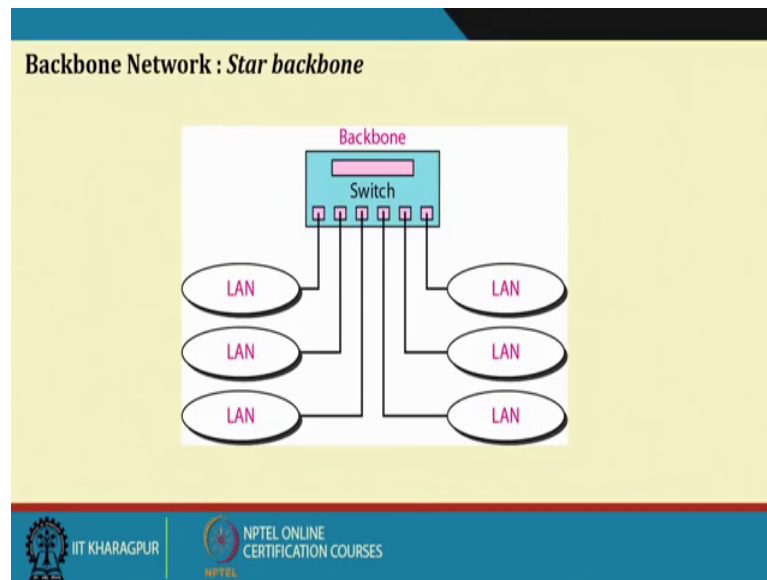
(Refer Slide Time: 17:19)



So, if you if you see so this not having star, this also not having star, this also not having star, so these are having blocking. Now you see for every LAN there is only one connectivity to this other LAN like LAN 1 and LAN 2 through B 1; LAN 1 and LAN 3 to B 2; LAN 4 to LAN 2 or LAN 2 to LAN 4 by B 4. So, this is the only these are the only connectivity; that means, every LAN has one connection, one connectivity or one path to this any other LAN.

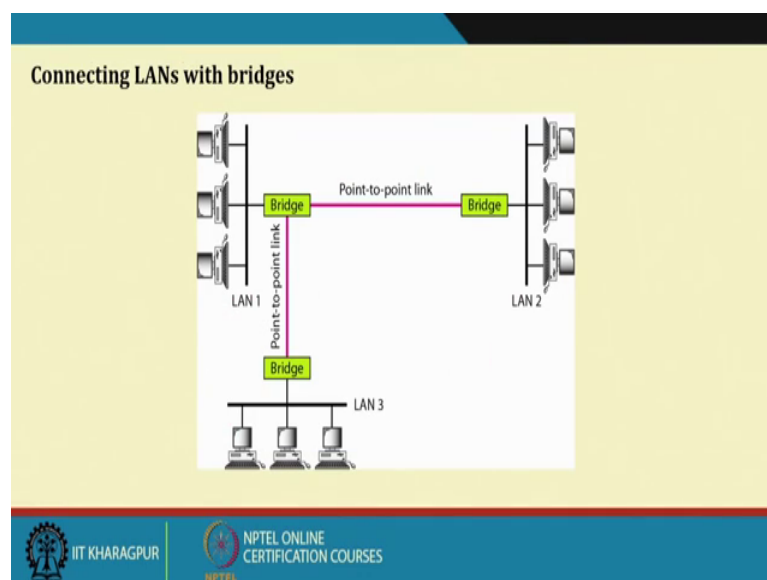
So, this STP, or this spanning tree protocol ensures that right. Again if you look at the spanning tree protocol is not done that new it is well studied, but it is a application of this things becomes much interesting. Now with this now I can allow a redundant connectivity right. So, if the connectivity goes off then I can have a option of switching to another connectivity to do that. So, the connections will be one is forwarding's mode, another in the blocking mode.

(Refer Slide Time: 18:33)



Now if you look at the backbone networks. So, there are different variety of back bone network, one very popular backbone switch is that multiport switch. So, in this case 6 LAN a typically multiport switch ranges form say 8 to 16 to 48, even higher than that right. So, these are the ports which are there in the multi port switch and reacts as a back bone with a star connection.

(Refer Slide Time: 19:01)



So, we can have a bridge connection; that means, there are 2 LAN's, 3 LANs connected with bridge and point to point or point there several point to point links between

connecting between the bridges. So, these are this is also possible at the back bone that how it correct to the thing.

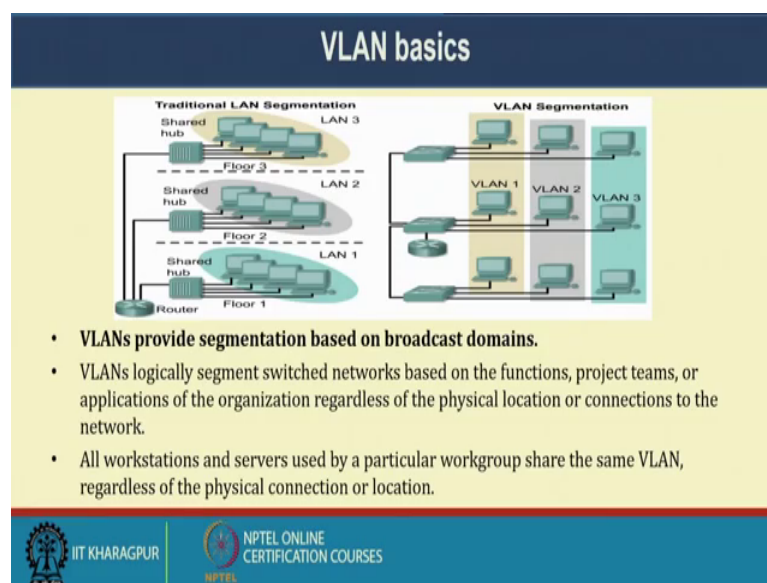
Now so what we have seen till now? We have we have looked into a bridge network. So, there are these are several LAN segments, LAN segments and we have layer 2 bridges or layer 2 switches which connect this LAN right. Also the one interesting thing is that as they are may be redounded connection any source, and between 2 LAN; that means, more than one connection. So, at a time one of the connections will be made active right. Otherwise there will a problem loop or what we say bridge loop right.

So, that this is a bridge network there can be loop which is which is extremely difficult to handle. But; however, if we have this sort of things like your STP spanning tree protocol and so and so forth. So, then we can we are what we can see that is able to handle the things. Next thing what we thought that will sit discuss in this context is the virtual LAN. What does it mean? I whatever we are discussing so far is the physical LAN that is the an end is there network etcetera is there. Now what is my requirement like say I want to make a I have a generic lab and I want to make say into different segments to work on the lab this say some of the data and maybe having sharing the same problem etcetera right.

So, that may be a section say in the lab there is a section call maybe a one part of the students are working on assignment on networking. So, there is a network group there is a computer architecture nobody sits in chaos group. So, there may be a data science group and type of things right. So, I have different groups nevertheless they are connected in the same layer 2 switch, or bridge layer to so; that means, the same broadcast domain right.

So, what I want to do? I want to segregate them into different groups right. So, whether there is a possibility to create a virtual LAN within the LAN right, so the LAN is there in the layer 2 LAN along with the virtual LAN right. So, this is a serious means and practical requirement for organisations having different departments, layer accounting, sales, purchase and sort of thing. They are companies like these they are will be are will be very convenient to have this thing. So, this will I case up like that one.

(Refer Slide Time: 22:01)



So, as we are discussing we can have this layer hub, or switch for different floor and then a router to route the things. Why router is required? We will come to that. Here also you see there may be three buildings right three separate building where there is a department for say account department, or section for say maintenance and type of things right.

So, the location of this one and location of this one is maybe different like one maybe building 1, another maybe building 3 and but what I require that all administration should be one in one LAN. So, that their communication are faster if there is a security enhancement is required instead of doing it across the board, I can do it only for that particular things and there may be several requirement, rather they share the only broadcast.

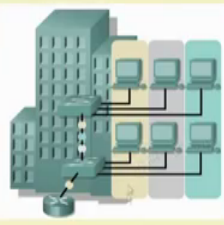
In another sense there are in the separate collision domain now you want to do it in a separate broad cast domain. One interesting thing you can see that it is from the same layer 2 switch it is coming up one going to this VLAN 1, another is some other VLANs or something right. So, this you know this is what the basic of VLAN is. So, it provides a segmentation based on broad cast domain; broad cast domain. VLAN's logically segments switch network based on the function project teams or application of the organisation regardless of the physical location and connection to the network, so that is the requirement of the switch network a VLAN network right.

So, now so all work station server used by a particular group share the same VLAN ID and physically connected to the location, so this is my objective. So, hope those are new to the VLAN concept and get it. So, I have different I want to segregate say administration systems and etcetera accounts etcetera sales.

And then the administration department or the people working for the administration of systems in the administration department may be across several physical locations. But I want to bring them in suppurate VLAN and that the within the layer 2 this things are coming up here right.



(Refer Slide Time: 24:19)

VLAN basics



- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

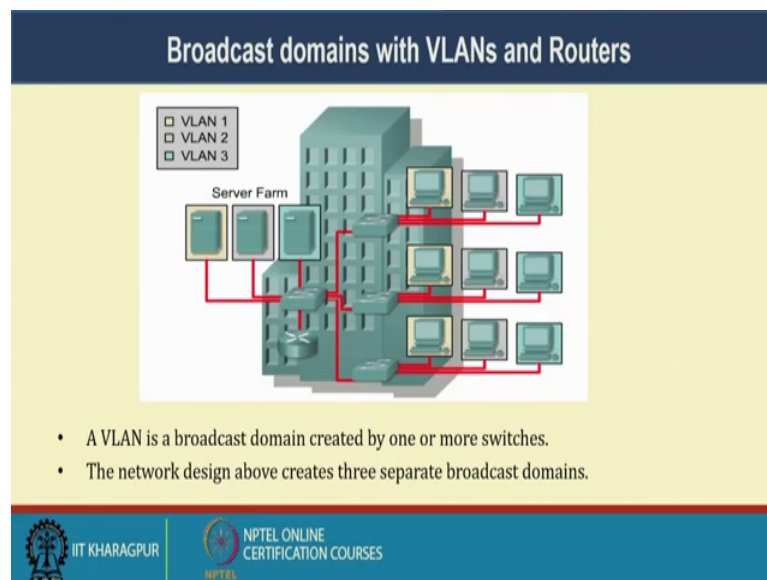
 IIT KHARAGPUR |  NPTEL ONLINE CERTIFICATION COURSES

So, VLANs are created to provide segmentation service traditionally provided by physical routers in the LAN configuration. If you look at the LAN in the physical routers, this segregate those things right in the in the routing, every interface as a separate LAN with a separate broadcast, and collision domain right.

So, VLANs address, address, scalability, security network management as we are discussing routers in VLAN topology provides broadcast filtering, security, traffic through etcetera. Switches may not bridge any traffic between VLANs, as would valid integrity of the VLAN things right. So that means, a switch where if a switch of a 8 port can 4 port can be VLAN 1.

And other 4 port can be VLAN 2, but they will not route the traffic because they do not have the routing capability. You require a layer 3, or layer 3 switch or router to do that that what exactly here also we are showing that this is a router which allows this VLAN 1, VLAN 2 and VLAN 3; 3 VLANs to be can be routed things.

(Refer Slide Time: 25:23)



Similarly same thing that I can have this different VLANs and the server from switch off particular this may be, but they are in the same layer 2 switches, these three VLANs, three machines indifferent VLAN etcetera. So, VLAN is a broadcast domain created by one or more switches. The network design above create three different broadcast domain, so this is having this colour is one broadcast, this is one broadcast domain right.

(Refer Slide Time: 25:47)

Broadcast domains with VLANs and routers

1) Without VLANs

Without VLANs, each group is on a different IP network and on a different switch.

Using VLANs, Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch.

What are the broadcast domains in each?

One link per VLAN or a single VLAN Trunk

2) With VLANs

So, without VLAN you see I have this switches for one engineering marketing sales like this, another switch and etcetera and then connecting. But with VLAN I can have a dual switch and have all this segments right. So, this may be in the same floor on the same particular floor and then, but I can have this type of things right. So, without VLANs each group on the different IP networks and so and so forth.

(Refer Slide Time: 26:15)

VLAN operation

Configuring VLANs	Description
Statically	<p>Network administrators configure port-by-port.</p> <p>Each Port is associated with a specific VLAN.</p> <p>The network administrator is responsible for keying in the mappings between the ports and VLANs.</p>
Dynamically	<p>The ports are able to dynamically work out their VLAN configuration.</p> <p>Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).</p>

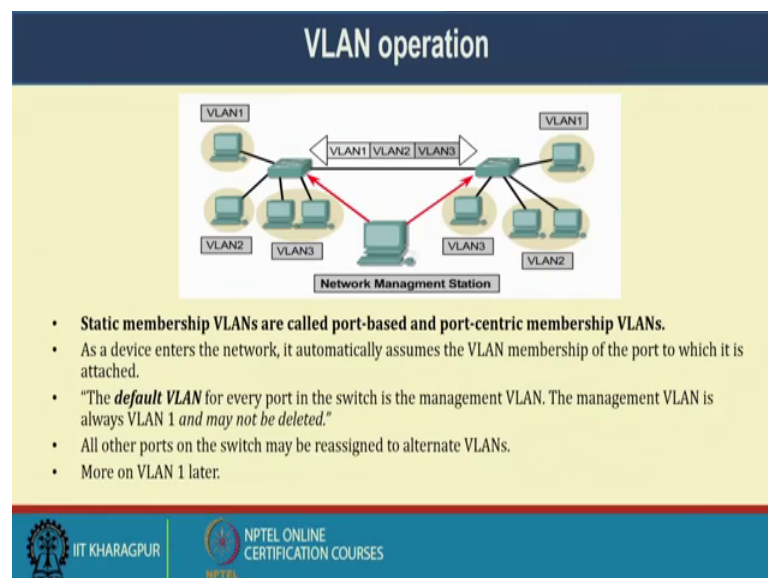
- Each switch port can be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

So, VLANs can be done statically that is port by port each port has a shares that dynamic. Otherwise dynamically; that means, I need to have done a applications at the

MAC address use a software base of the MAC address to VLAN mapping etcetera, so that MAC can be. So, each switch port can be assign different VLANs ports assigned same VLANs say on the same broadcast domain, port that do not belong to a VLAN do not receive this broad cast.

So, that if that port belong all the port belonging to the VLAN in the same broad cast domain. So, what we are trying to look at the different switches? We define the ports and these ports are a designated with the VLANs right I say that 1 to 4 is in this switch is the VLAN 3, another switch also 1 to 4, and the etcetera etcetera those are the things.

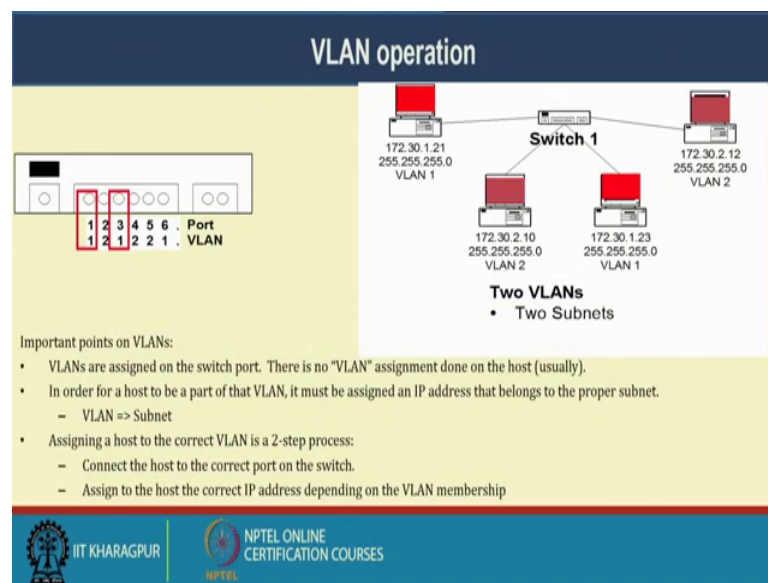
(Refer Slide Time: 27:05)



So, I need to only connect to the things right and if you look at the operations static membership VLANs are called port based and port centric member see VLANs right. As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached.

So, once you connected it is attached, it is the default VLAN for every port in the switch is the management VLAN. Management VLAN is always VLAN 1, and may not be deleted right, or because you can basically destroy the VLAN, or delete the VLAN etcetera, all other ports in the switch may be reassigned in alternate VLANs.

(Refer Slide Time: 27:43)



So, important on VLANs; VLANs are assigned on switch port there is no assignment done on the host that is usually not done. In order to host be a part of the VLANs it must assigned in IP address that belongs to the proper subject that is important. So not only that port where it is connected, but also IP address which is at the proper subnet is required, or in other sense if VLAN drives that in sub netting type of things right somewhat equivalent.

Assigning a host to the VLAN 2 is a two step process right, connect the host to the correct port of the switch. So, I need to connect that and assign the host of the correct IP address depending on the VLAN membership. So, it should be in the same proper subnet of the IP that is also important. So, not only the physical port of the things also that IP address which is important. So, this is the thing.

(Refer Slide Time: 28:37)

VLAN operation

- Dynamic membership VLANs are created through network management software.
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network, it queries a database within the switch for a VLAN membership.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So as we have seen, so there can be a VLAN with the taking VLAN 1, 2, 3 the packet moves and there is that can be transferred across this different switches. So, dynamic membership VLANs are created to network management software. It requires a suppurate software, dynamic VLAN allows membership based on MAC address of the device connected to the switch. As a device enter the network it queries the database and the switch for the VLAN membership right. So, once in the network it can enquiry on the things.

(Refer Slide Time: 29:11)

Benefits of VLANs

All systems attached to the same port must be in the same VLAN

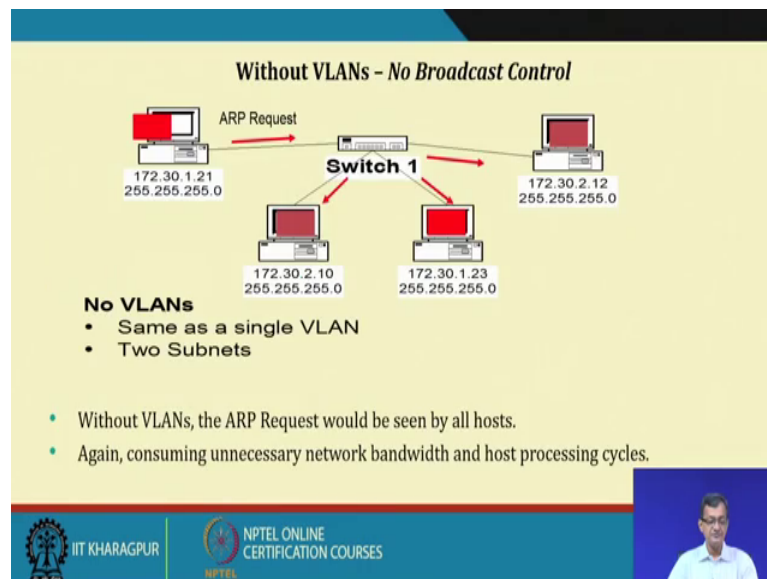
If a hub is connected to VLAN port on a switch, all devices on that hub must belong to the same VLAN.

- Key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.
- Helps an administrator:
 - Easily move workstations on the LAN.
 - Easily add workstations to the LAN.
 - Easily change the LAN configuration.
 - Easily control network traffic.
 - Improve security.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

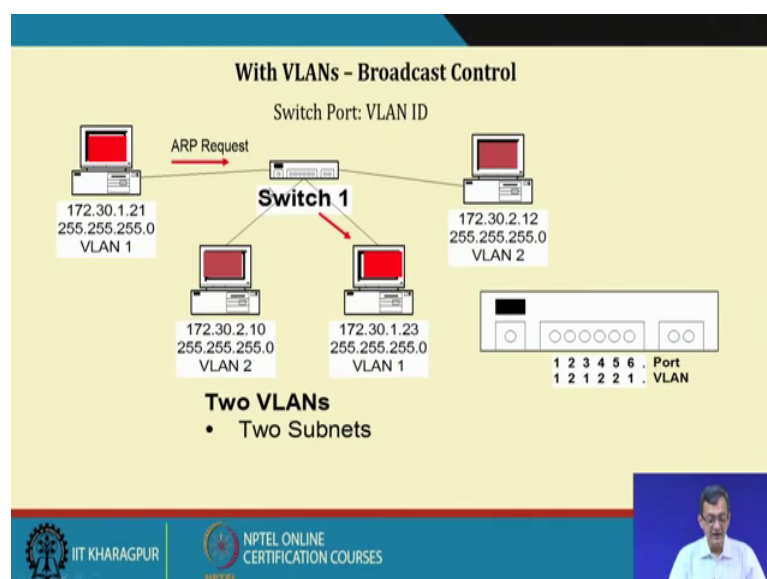
So, there are several benefits. So, key benefit is that a permit the network administrator to organize LAN logically instead of physically. So, it may be distributed in different physiological we can arrange that. Easily move workstation on the LAN, easily at workstation on the LAN, easily change VLAN configuration, easily control network traffic and improve security. So, there are several advantages of using VLANs.

(Refer Slide Time: 29:41)



So, if you see that broadcast domain without VLAN, that appear ARP request goes to the every machine.

(Refer Slide Time: 29:51)



And with VLAN it goes to that only those machines which are the member of the VLAN right. So, that is the broadcast is control here no broad cast will pursing.

(Refer Slide Time: 30:03)

VLAN Types

Approaches Can Vary Performance

VLAN Types	Description
Port-based	<ul style="list-style-type: none"> Most common configuration method. Ports assigned individually, in groups, in rows, or across 2 or more switches. Simple to use. Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	<ul style="list-style-type: none"> Rarely implemented today. Each address must be entered into the switch and configured individually. Users find it useful. Difficult to administer, troubleshoot and manage.
Protocol Based	<ul style="list-style-type: none"> Configured like MAC addresses, but instead uses a logical or IP address. No longer common because of DHCP.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, what are the different types of VLAN? The most popular and use type is the port based VLAN right. And there are other types like MAC address rarely implemented today. Each address must be entering the switch and configured individually and there is a protocol based configured like MAC address by instead is a logical, or IP address it is not so common these days. So, the predominant is the port based.

(Refer Slide Time: 30:31)

VLAN Tagging

- VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.
 - Trunk link:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- This header information designates the VLAN membership of each packet.
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the destination node (Switch) the VLAN ID is removed from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a **trunk link** or **VLAN trunking**.

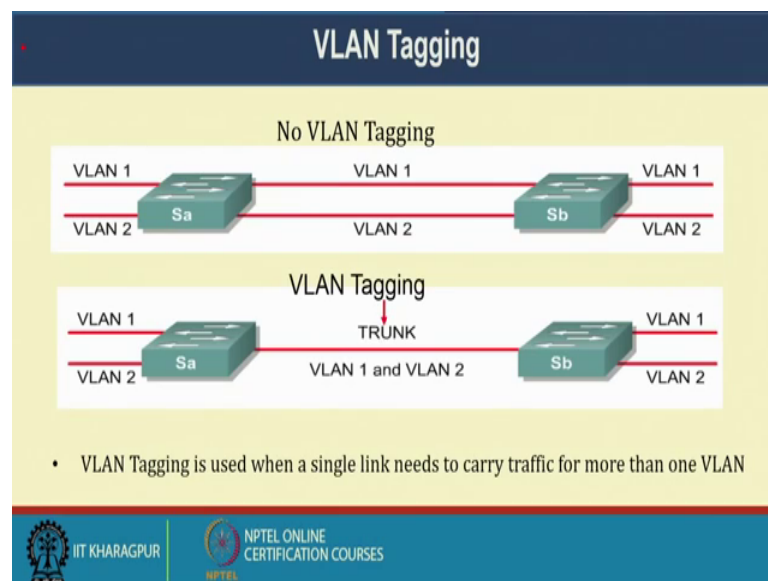
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, VLAN tagging as the traffic moves or the layer to frame move so there is the VLAN tagging that tag with the VLAN number which is read and stepped up the other end to read that actual content. Another interesting is that if the switch cannot segregate the VLAN, there are possibility there are thing it can still trunk the thing across the switch because there may be switch large network and go on doing that. So, it goes on trunking the things.

So, the VLAN tagging is used when the link needs to carry the traffic for more than one VLAN right. So, when only one VLAN is fine, but if you have more than one VLAN then I need to have a tagging. So, trunk link as the packets are received by the switch from one any attached end device a unit packet identifier is added for the each of the header.

The header information designate the VLAN membership of each packet right, the packet is then forwarded to the appropriate switch, or router based on the VLAN identifier and MAC address right. Upon reaching the destination nodes switch VLAN ID is removed from the packet by the adjacent switch and forward to the attached device. So, at the end point it is tip top and put the thing right. So, this is VLAN link and VLAN trunking is there.

(Refer Slide Time: 31:49)




So, with no VLAN we have multiple link, where with a VLAN trunk we can have a single line to have the both the VLAN with the VLAN tagging.

(Refer Slide Time: 32:05)

VLANs Types

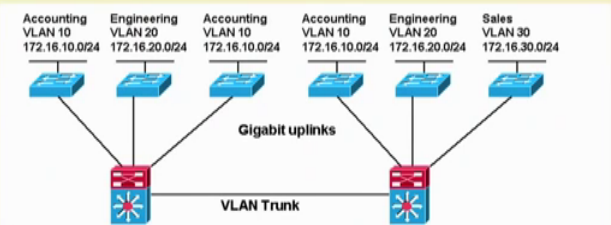
- End-to-End or Campus-wide VLANs
- Geographic or Local VLANs



And finally, there can be two types of VLAN one is end to end campus wide VLAN. Another is geographical location based VLAN.

(Refer Slide Time: 32:13)

End-to-End or Campus-wide VLANs





Gigabit uplinks

VLAN Trunk

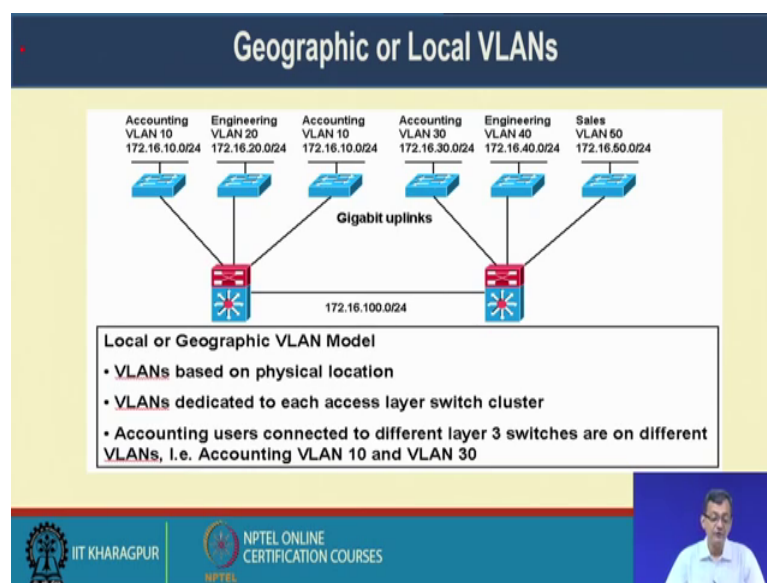
Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, i.e. Accounting VLAN 10, can be anywhere in the network



First one is most on based on functionality like here that accounting, here also VLAN 10 here also VLAN 10 engineering and so and so forth. So, it is a based on thing VLAN everywhere model. So, you can have that the function based.

(Refer Slide Time: 32:29)



The other one is more of a location based here the accounting is VLAN 10, but whereas this location is defined the accounting is VLAN 30. So, it is location based on the physical location of the system VLAN dedicated to each access layer of the switch and accounting switch are different in different VLANs. For example, there can be even in the same location these are two accounting things on the VLAN. So, what we will see that VLAN allows us to better manageability have a some sort of the I mean allows us to have deferent broad cast domain within the within at the layer 2 level.

But one thing need to be kept in mind this at four port of a particular switch is VLAN 1, other port is VLAN 3. Then if you want to send the packet from this one of the port 1, 2, 3, 4 is VLAN 1; 4, 5, 6, 7, 8 is VLAN say 3; then a port 2 wants to communicates to port 7. Then I require a layer 3 device or routing router to route this packet from the things. Because they are in separate broadcast and collision domain right both broad cast domain and they are in separate network needs a router thing. But never the less it allows us a in a better manageability right. So, with this let us conclude today's lecture on connecting LANs and VLANs we will be continuing our discussion on this networking topic in subsequent classes.

Thank you.