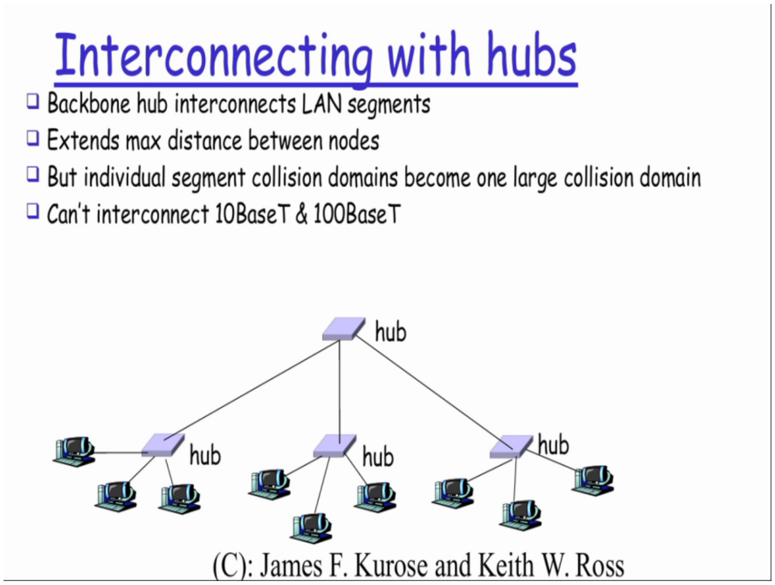
Information Security 3
Sri M J Shankar Raman,
Consultant Department of Computer Science and Engineering,
Indian Institute of Technology Madras
Module 51
Network Devices

So in this module we will basically try to look at some of the very very commonly used network devices for us to understand what they are used for where are they typically placed, what kind of functionality into the exhibit in case we are basically looking at something like a network topology where all these devices would be typically present.

(Refer Slide Time: 00:32)



Interconnecting with hubs

- ❑ Backbone hub interconnects LAN segments
- ❑ Extends max distance between nodes
- ❑ But individual segment collision domains become one large collision domain
- ❑ Can't interconnect 10BaseT & 100BaseT

(C): James F. Kurose and Keith W. Ross

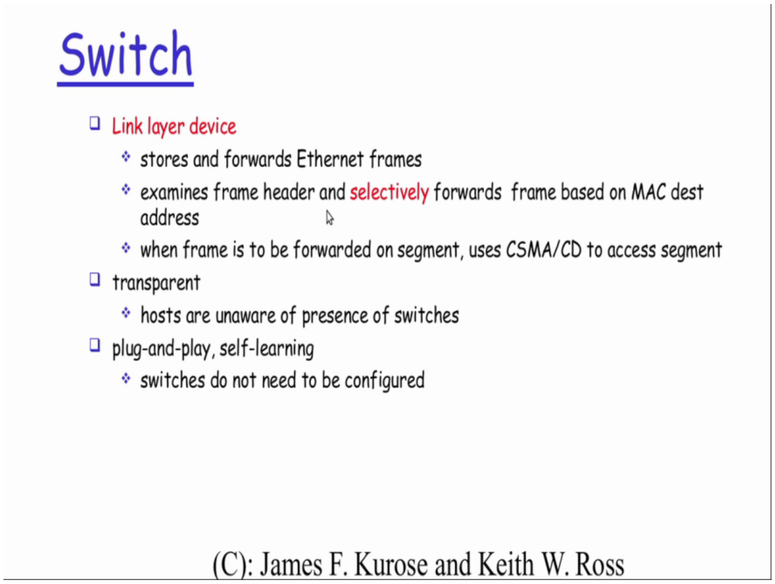
So one of the very very low level device is what is refer to as an hub which is basically interconnecting the different kind of LAN segments, so LAN is your local area network which tries to extend whatever is a maximum distance otherwise that would be possible to be connected between two different nodes or systems.

So in case of a hub you would have typically what is refer to as individual segment collision domain instead of actually having one very large collision domain, so what do we exactly mean by collision domain is that when I have a set of systems connected to a hub the the traffic that is actually originating from one of this systems is will be getting collided only with the traffic of on any other two any any of the other systems that is actually connected to the same hub device, right?

So in that way a traffic originating from this device is not going to impact the traffic that is actually part of this particular collision domain. So by trying to restrict the collision domain to a very small segment of my entire network what we essentially try to achieve is that we try to improve the overall bandwidth that you would typically be getting for my entire network because unnecessarily the traffic that is originating from this particular system and which is destined for this particular system do not need to go on to any of these domains and thereby having the traffic from this particular system to this particular system getting affected with a collision from the traffic of this particular system, right?

So in this case I would basically be able to restrict the amount of packets and the bits that is actually needing to be going on from one particular system to another system individually so that I tend to have a much higher bandwidth utilization of my entire network. So one flip of this entire thing is that if I really have a devices that are of different bandwidths so let say a a 10mbps network or a 100 mbps network, I wouldn't be able to sort of interconnect those kind of devices together when I actually make use of this hub device.

(Refer Slide Time: 02:42)



Switch

- Link layer device
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC dest address
  - when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of switches
- plug-and-play, self-learning
  - switches do not need to be configured

(C): James F. Kurose and Keith W. Ross

So coming down to the next kind of a device that we typically make use of is what is refer to as a switch, switch is basically a link layer device so a link layer device as we have seen in the previous module is something that is actually operating at level 2 just above my physical layer right.

So what is the main functionality of this particular device is it tries to store and forward the Ethernet frame, it will basically wait till the entire frame is received by the device that is one way of operation of this particular device and then once it has the entire Ethernet frame then it goes higher and tries to forward it to the next device that it has to reach to,

So as part of this the device would also be examining the frame header so we looked at what is a frame header when we were discussing about encapsulation and de capsulation in our last module and the frame header is an header that is actually getting added as part of the link layer and which will typically contain all the metadata that has to be there for the link layer to be effectively working, so looking at the frame header it will exactly know what is the destination address to which this particular frame has to be sent to, right?

So the destination address here is refer to as the MAC destination address, so we would heard about something called as an MAC address for every system and every port that we are operating on, so essentially the MAC address will be looked at by the switch device and selectively it will forward the frame depending on what the destination MAC address is and the and the lastly when the frame is to be forwarded on a segment it uses something called as a CSMA/CD to access the particular segments.

So what is CSMA/CD carrier sense multiple access collision detection, so CS here stands for carrier sense MA stands for multiple access, CD stands for collision detection, so now what exactly CSMA/CD so on a shared bus medium if I really need to have multiple systems connected on that shared bus medium like my Ethernet trying to send packets across from one mission to another mission which is on the same media, I need to ensure that the packets from two different systems do not get collided on that shared medium at the same time because when it gets collided it is effectively not going to be getting successfully transmitted and received by the the destination node whichever that particular frame was destine to be, right?

So what this particular CSMA/CD actually tries to do is that first it tries to sensed whether the carrier is basically free right so there should not be any other node that is actually transmitting on the same shared medium so the first the carrier will be sensed to be whether it is free or not as soon as it is free if it detects that it is free and there is no bites flowing across on that medium then this particular node which actually has some frames to be transmitted will start the transmission right.

Now the problem is even though it is sensing for the carrier to be free there is a possibility that more than one node at the same time could have detected that the carrier is free and starting to do the transmission at the same time so that is basically what that ma stands for so multiple access, now when multiple nodes are basically going to be sensing that the carrier is free at the same instant of time and start the transmission then what is going to happen is that there is going to be a collision.

And this particular mechanism puts across a MAC way by which I will be able to detect that the collision has actually happened on the transmission and immediately stop the transmission so that there could be another node that could possibly sense the trans carrier is free and then do the transmission because of moment a collision has been detected as part of my frame transfer there is really no use in continuing to transfer the remaining part of the frame.

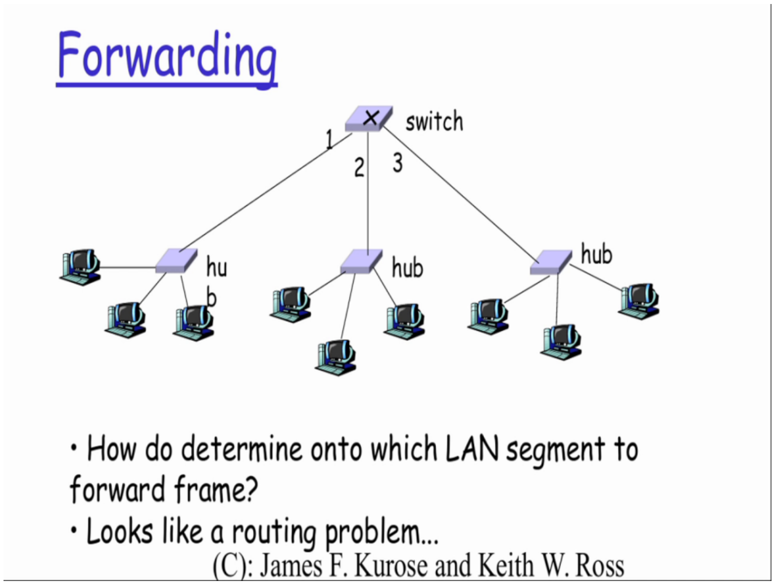
So I may I might as well stop my transmission thereby insuring that the the carrier becomes free for some other node in my system to basically start transmitting the data so this is essentially how the CSMA/CD works we just talked about very briefly just to give you an idea about what this mechanism is all about and based on this CSMA/CD I will basically try to send across the frame one from one system to another system.

then the next thing that switches is its basically its completely transparent in the sense that the host systems are not really aware that they are basically connected with the destination systems so a source system is not aware of how many switches are there if it all there are any switches when they are basically connected to the another system they are really completely transparent to the presence or the absence of the switches in the path from the source system to the destination system.

then thirdly and very importantly it basically supports plug and play whereby it basically sorts of does a self learning right on where each of the end systems are connected on which port because a switch device is basically a device which has multiple ports like it could be of 8 ports or 16 ports or whatever and on each port you basically connect a system.

So the moment you power up the switch there is a self learning mechanism that will happen over a very short period of time by which the switch itself automatically will sort of discover which system is actually connected on which of it ports and thereby it doesn't need to be done any kind of a separate configuration explicitly for a switch to start functioning normally.

(Refer Slide Time: 08:23)



Forwarding

- How do determine onto which LAN segment to forward frame?
- Looks like a routing problem...

(C): James F. Kurose and Keith W. Ross

So how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right. So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right.

So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right. So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right.

So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right. So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right.

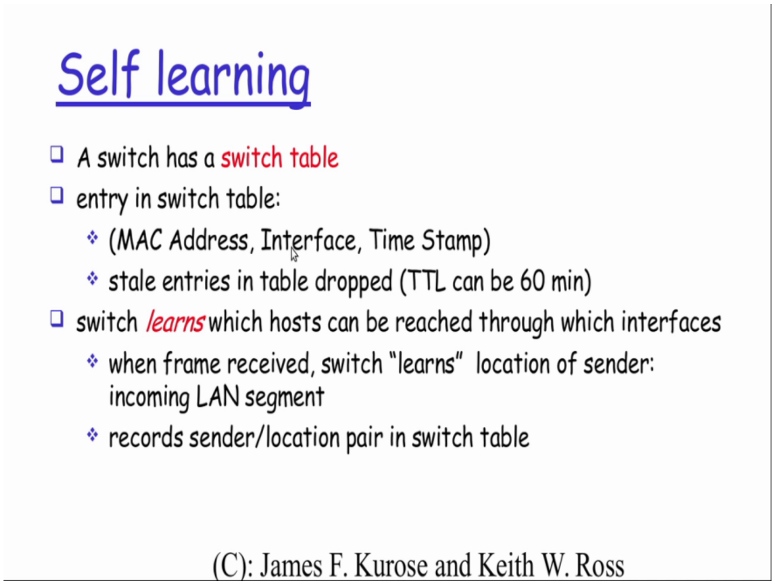
So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right. So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right.

So that is basically the problem that we are referring to for a switch to start functioning normally, so how does a switch know the moment of frame arrives on what particular port it has to be sending the frame to so that it has to reach the final destination right.

So that is basically the problem that we are referring to here as forwarding because the core functionality or the responsibility of a switch device if layer 2 that is my data link layer will be to basically forward the frame which is actually received from one port so it has to forward a frame which is actually received on port 1, so on port 1 it could have actually received a frame either from this system or this system or this system and for the port on the frame that is actually coming on port 1 might have to be either forwarded on port 2 or on port 3, right?

So how is this switch going to a node whether it has to be forwarded on port 2 or port 3, so that is basically what is a problem that the switch device actually tries to solve.

(Refer Slide Time: 09:23)



Self learning

- A switch has a switch table
- entry in switch table:
  - (MAC Address, Interface, Time Stamp)
  - stale entries in table dropped (TTL can be 60 min)
- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table

(C): James F. Kurose and Keith W. Ross

So how does this forwarding actually work so the whole concept of forwarding is basically using something called as a switch table, right? So a switch internally has a switch table and each entry in a switch table so the moment we say switch table you can hypothetically imagine yourself to be the table to be a sort of an array where I will have each entry in that particular table will contain the MAC address the interface and the time stamp, right?

Now this time stamp is basically the amount of time that this particular entry is valid so beyond that particular point in time I am going to consider this particular entry as not valid so and then I will again be doing what is called as a rediscovery right,

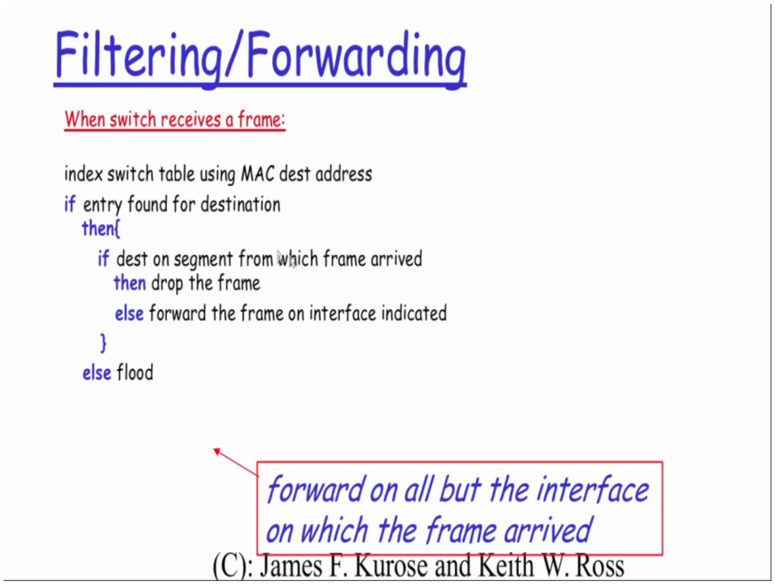
So we will just see the subsequent slide on how this entry gets updated but for every entry that I have in my switch table there is a corresponding time stamp of which basically talks about the validity duration of that and after that particular time stamp is elapsed, I am going to consider that entry as a stale entry and all stale entries in the table will be automatically dropped.

So one possible value of the TTL value the TTL here stands for time to live can be 60 minutes right, so how does a switch learn and built this table so switch learn which host can be reach through which interfaces, so when a frame is received right.

Switch learns a location of the sender based on the incoming LAN segment because the frame is actually come on one particular port with a particular source MAC address it indirectly means that this particular MAC address is connected on this particular port right,

So now the switch will basically add an entry saying that the source MAC address is this much and the corresponding interface is particular segment and the time stamp duration so this this entry will now be getting added into the switch table and it will basically know subsequently after this that if it all there is another frame that is actually coming in with the destination MAC address as the newly added MAC address in this particular entry the switch has to basically take that frame and then dump it down to the corresponding interface number right.

(Refer Slide Time: 11:40)



Filtering/Forwarding

When switch receives a frame:

```
index switch table using MAC dest address
if entry found for destination
  then{
    if dest on segment from which frame arrived
      then drop the frame
      else forward the frame on interface indicated
    }
  else flood
```

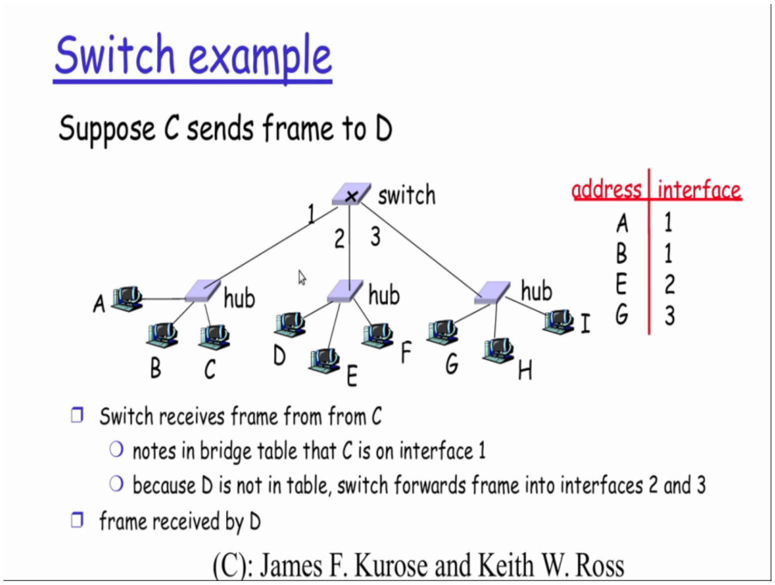
forward on all but the interface on which the frame arrived

(C): James F. Kurose and Keith W. Ross

So this is basically what happens so when the switch is basically receiving a frame so the I will index a switch table using a destination MAC address if I find an entry for the destination then if the destination of the segment from which is arrived its basically the same and which the frame has arrived and I find that the destination is also on the same segment.

I simply drop the frame or else the frame the switch will be forwarding the frame on all interfaces indicated except the one on which it has actually arrived right. So it basically goes through this looping mechanism to determine on what all interfaces it has to basically sent the incoming frame, so the purpose of it to reach the final destination is actually met.

(Refer Slide Time: 12:27)



Switch example

Suppose C sends frame to D

address	interface
A	1
B	1
E	2
G	3

- ❒ Switch receives frame from from C
  - ○ notes in bridge table that C is on interface 1
  - ○ because D is not in table, switch forwards frame into interfaces 2 and 3
- ❒ frame received by D

(C): James F. Kurose and Keith W. Ross

So this particular example we will see how the logic is working so let say I'll have a switch with three interfaces 1 2 3 so my current switch table is something like this, so I am just not showing you the time to live field here because for the building on the switch table that is not something which is important because the default value is of that particular validity duration is going to be built up so in this particular case for this switch table.

I have four entries in my switch table so the entry corresponding to address A it says interface 1, address B it says interface 2 I mean interface 1, address E it says interface 2, address G it says interface 3 so essentially it says that if a frame comes for reaching to E right which is this much the frame has to be sent on to this particular interface.

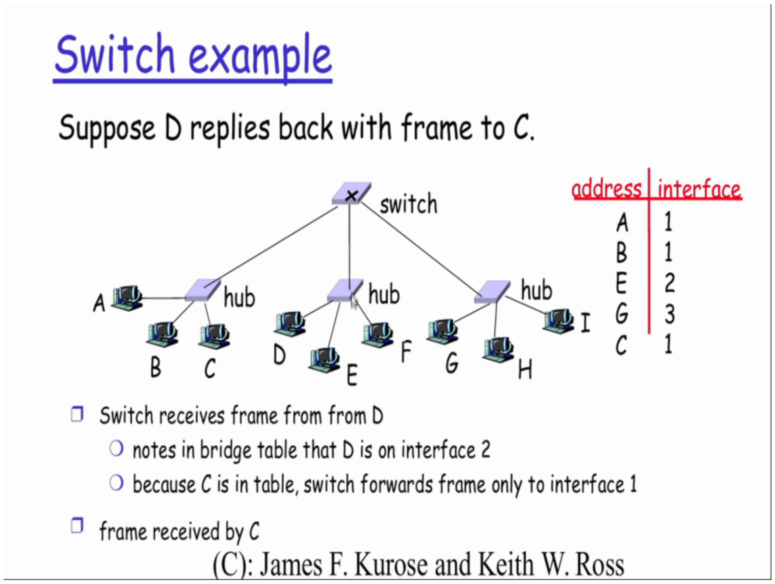
The frame comes for going to G that is on this particular segment the frame has to be dispatched onto this particular interface right, so that's basically what this switch table is actually telling, now if the switch is receiving a frame from C right, now C is not having an interface listing here but the C has actually sent a frame across to be sent to some particular mission through the switch.

Now the moment the frame is actually received by the switch it will look at the source MAC address of C and then it will find that that MAC address is not available in my switch table will go add an entry here saying that as a next entry in my switching table, so saying that address C is also reachable via interface 1 because that particular frame from C would have actually come on interface number 1 right, now if the C has its basically sending a the frame to D, right?

The interface D the address D is again not in this particular switch table so what it will do is it will basically forward that frame onto both 2 and 3 right. It doesn't forward it onto one for a simple reason like as we were discussing in the previous slide since it has actually come on 1 essentially means that d is not on one so that is why it has actually reached this particular interface right.

So it will basically sent it both to 2 and 3 and then it will the frame will be getting received by d because this the the system d is actually available on interface number 2 of the switch right. So even though it is actually getting sent on 2 and 3 since the system d is actually available on 2 it will basically be received through the switch interface 2 on which this particular frame has also been sent.

(Refer Slide Time: 15:17)



Switch example

Suppose D replies back with frame to C.

address	interface
A	1
B	1
E	2
G	3
C	1

- Switch receives frame from from D
  - notes in bridge table that D is on interface 2
  - because C is in table, switch forwards frame only to interface 1
- frame received by C

(C): James F. Kurose and Keith W. Ross

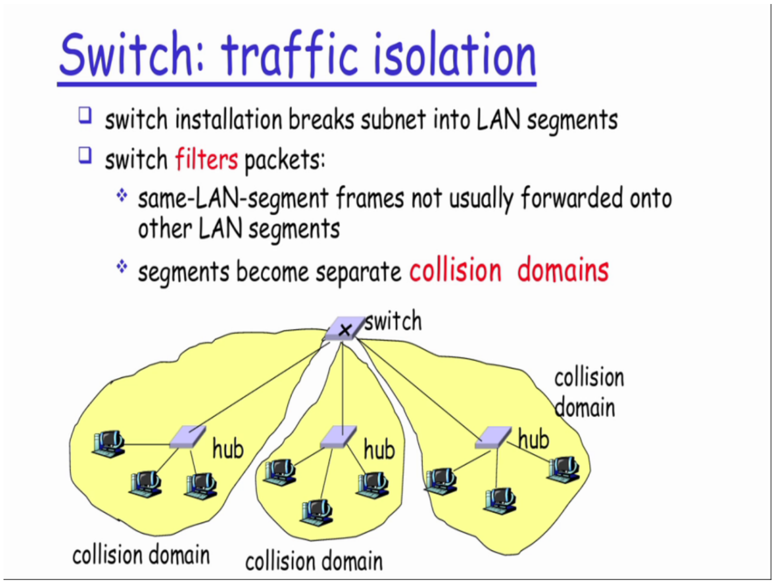
Now for this d will be replying back to C right because there is a frame that is come from c to d and then there in all probability there will be a response back from d to c. Now switch receives the frame from d and there is that the in this particular scenario it will basically know that d is on interface 2 because the a a frame with the MAC address of d has actually reached the switch on interface number 2.

So it will go add one more entry in the switch table basically saying that d is right now available on 2 and then by that time it would have already go an entry for c is on 1 from the previous frame request that has actually come in right.

So this time instead of sending the frame on both 1 and 3 the response frame from d instead of sending it both on 1 and 3 because of the fact that the destination address is the C's MAC address and the switch table is saying that c's MAC address is available on interface 1 it will only sent this response frame from d through c right to the interface 1 because the switch table already says that c is actually available on interface number 1 right so because of this it will unnecessarily not send it on interface number 3 also because c is not reachable via interface number 3, right?

so this is basically a example of how the switch device typically learns automatically by the arrival of frames and within a very short span of time the the the switch device will basically be doing a self learning and sort of build up the entire switch table in this particular format. So as I told you for simplicity purposes we've not listed the time to live value the validity value for each of those entries also but ideally in every switch table you will also have the time to live value is also added in in that, right?

(Refer Slide Time: 17:14)



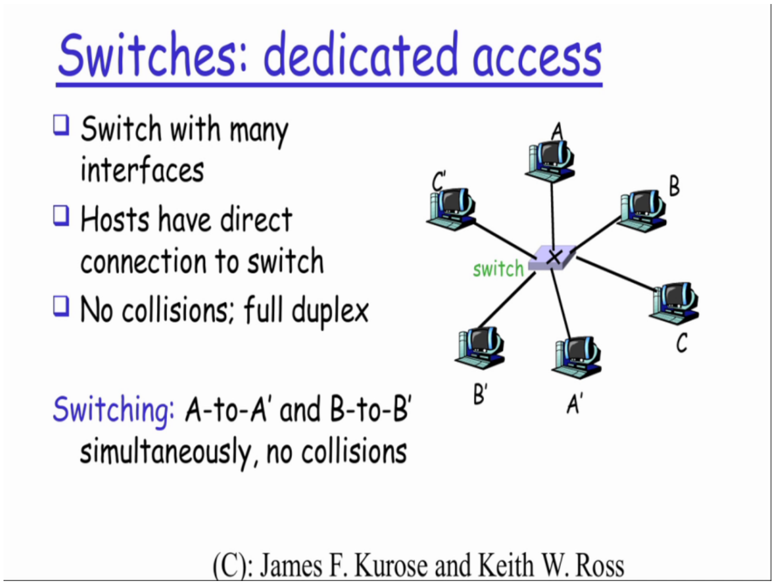
Switch: traffic isolation

- switch installation breaks subnet into LAN segments
- switch **filters** packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate **collision domains**

So as we were discussing with a switch I could possibly separate it into different segments if I basically using a hub device I could have individual collision domains thereby restricting the traffic unnecessarily going from this collision domain to this collision domain when I have a requirement of only communicating with another device in the same collision domains right.

So thereby if you see my overall bandwidth utilization will be much higher because unnecessarily the that has to be strictly going only on this domain collision domain is not transmitted and then wasting the bandwidth on the another collision domain completely unrelated to that so this basically helps me to sort of isolate the traffic If I appropriately arrive at the correct network topology right.

(Refer Slide Time: 18:00)



Switches: dedicated access

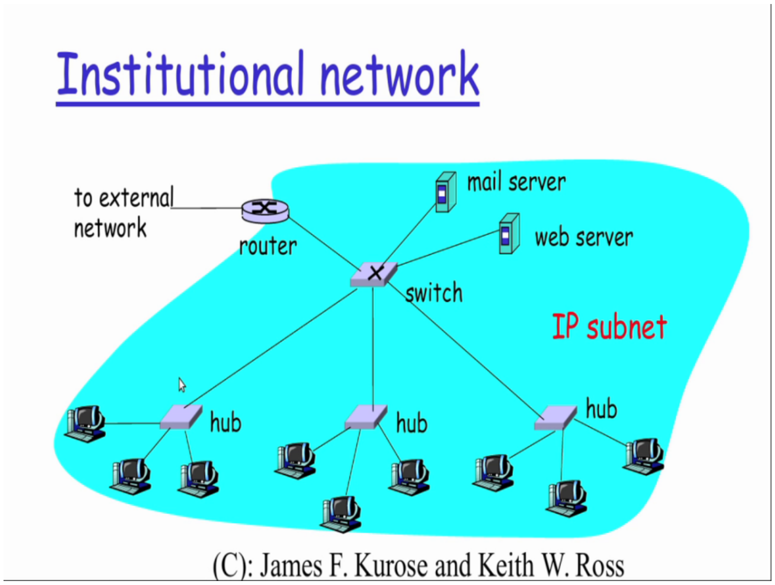
- ❑ Switch with many interfaces
- ❑ Hosts have direct connection to switch
- ❑ No collisions; full duplex

Switching: A-to-A' and B-to-B' simultaneously, no collisions

(C): James F. Kurose and Keith W. Ross

So switches typically has multiple interfaces and there is a possibility that the interfaces could also be directly connected to the host systems thereby I will have a full duplex connection between all the ports of the switch at any point in time without having any collisions also, right?

(Refer Slide Time: 18:22)



Institutional network

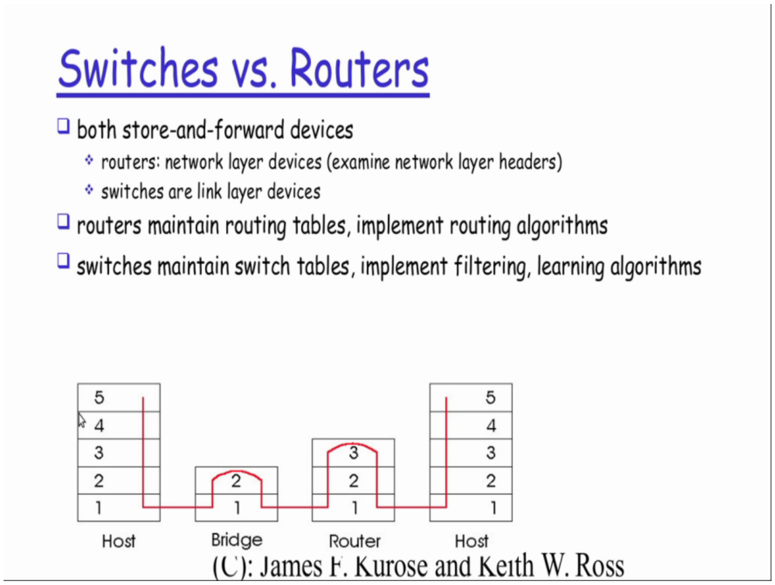
(C): James F. Kurose and Keith W. Ross

So typical institutional network in any kind of even a small organization would be something like this so I might have switch device which is my central device that switch device might have some ports of it some interfaces of it connected to hubs right and some of the ports of this devices could also be connected to main server or web servers.

The server that needs to be accessed by my end systems on my entire network and one port of the switch will be typically connected to a router device through which the entire organization will actually be going and accessing the external network.

So we will have to note here that the switch is basically a layer to device that is revise at my data link layer and a router is basically a layer 3 device which basically tries to take the packets from one network onto another network right so whereas a switch device will be able to sort of send the traffic across to the any other device on the same network, a layer 3 device like a router device will be able to send it across to an external network.

(Refer Slide Time: 19:26)



Switches vs. Routers

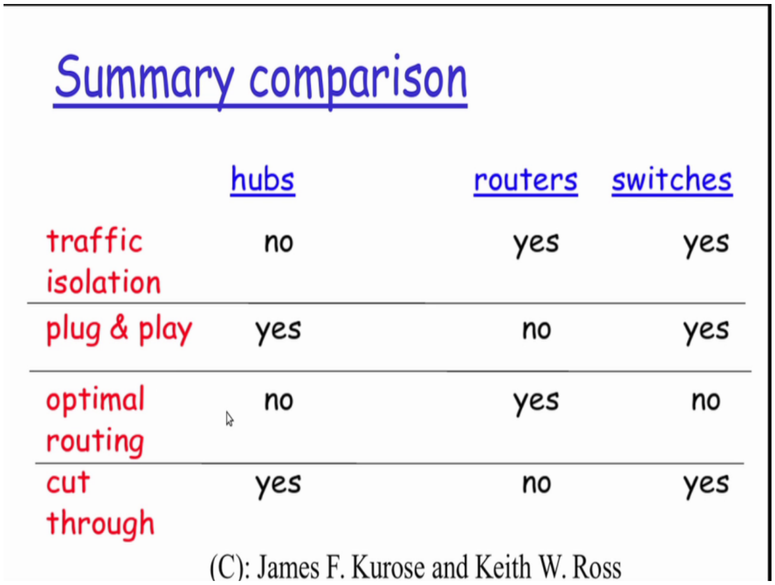
- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - switches are link layer devices
- routers maintain routing tables, implement routing algorithms
- switches maintain switch tables, implement filtering, learning algorithms

(C): James F. Kurose and Keith W. Ross

So it is just a very brief comparison between the switches and routers so both are basically store and forward devices but the only difference is routers they operate at layer 3 and bridges or switches is operate basically layer 2, whereas of the source and the destination host systems you see you'll have all the 5 layers that we've actually talked about in our previous module right,

So switches basically maintain my switch table and routers maintain a routing table and the routers implement the routing algorithms whereas in switches basically implement my filtering algorithms which do a sort of a self learning automatically right.

(Refer Slide Time: 20:01)



Summary comparison

	hubs	routers	switches
traffic isolation	no	yes	yes
plug & play	yes	no	yes
optimal routing	no	yes	no
cut through	yes	no	yes

(C): James F. Kurose and Keith W. Ross

So a very brief comparison between the different kinds of devices or traffic isolation hub generally do not provide this feature whereas routers and switches basically do, plug and play hubs and switches are generally plug and play so I just plugin the device into the network they go through a sort of auto learning mechanism by which whatever are required will be learnt by them

Whereas routers they will need some minimal configuration to be done by me so in that sense they are not plug and play enabled from a routing perspective hubs and switches both devices are not capable of doing it because router is only device that operate at layer 3 and from a cut through switching routing perspective hubs and switches are basically do that, whereas the router devices are not typically capable of doing that.

Thank you.