PDH, Plesyncronous Digital Heirarchy, Sanjay Verma

New Doc 2020-01-18 23.45.41

PDH ⇒ Plesynchronous is a Greek word meaning Almost Synchronous. But not fully Synchronous, In Plesynchronous System every equipment is generating its own clock of Synchronization.

PDH is a technology for transporting Voice OR Data between multiple devices. which are working with clock sources with accepted tolerance Level for Synchronization. PDH was built for Digital transmission of Signals.

* Pulse Code Modulation (PCM) is the technique used in P...

Networks ...

1:07 / 4:47

* Pulse Code Modulation (PCM) is the technique used in PDH Network. which is the based on TDM.

* PDH Data was thru twisted pair, co-axil Cable and Microwave.

p —— q

Disadvantage of PDH ⇒

- No World Standard format
- No Standrized Network Managment System
- PDH Allows only Point to Point Configuration
- PDH does not Support Hub

PDH, Plesyncronous Digital Heirarchy, Sanjay Verma

New Doc 2020-01-18 23.45.41

Disadvantage of PDH ⇒

- No World Standard format
- No Standarized Network Managment System
- PDH Allows only Point to Point Configuration
- PDH does not Support Hub.
- Multiplexing and DeMultiplexing is very Complex
- Copper Interface define

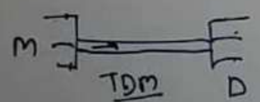
PDH = Plesynchronous Digital Hera—

3:48 / 4:47

SONET - Introduction

SONET - Synchronous Optical Network
↳ widely used in telephone network

→ SONET is primarily used in North America
↳ Europe & Japan used modified version
Synchronous Digital Hierarchy (SDH)



Synchronous, Asynchronous, plesiochronous

→ A set of synchronous signal, the digital transition in signal occur at same rate

Principle of SONET/SDH :-

All signal transition are fixed with refr to a very accurate atomic clock(s) called Primary Reference clock (PRC).

→ Basic signal of SONET is synchronous transport signal, called STS-1 · OC-2 → 51.84 Mbps

• SONET defines a technology for carrying m signals of different capacities through a synchronous, flexible, optical hierarchy.

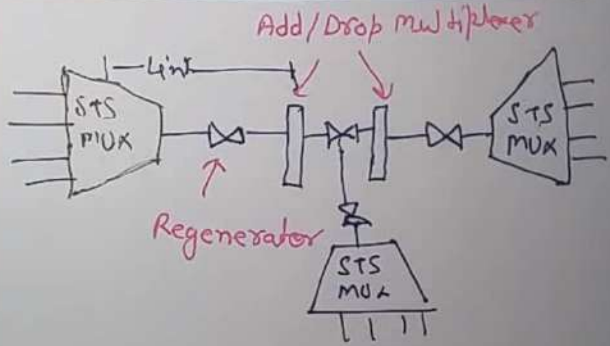
STS-1 → OC-1 → 51.84 Mbps
STS-3 → OC-3 → 155.52 "
STS-12 → OC-12 → 622.08 Mbps

SONET: Physical Configuration and Network Element

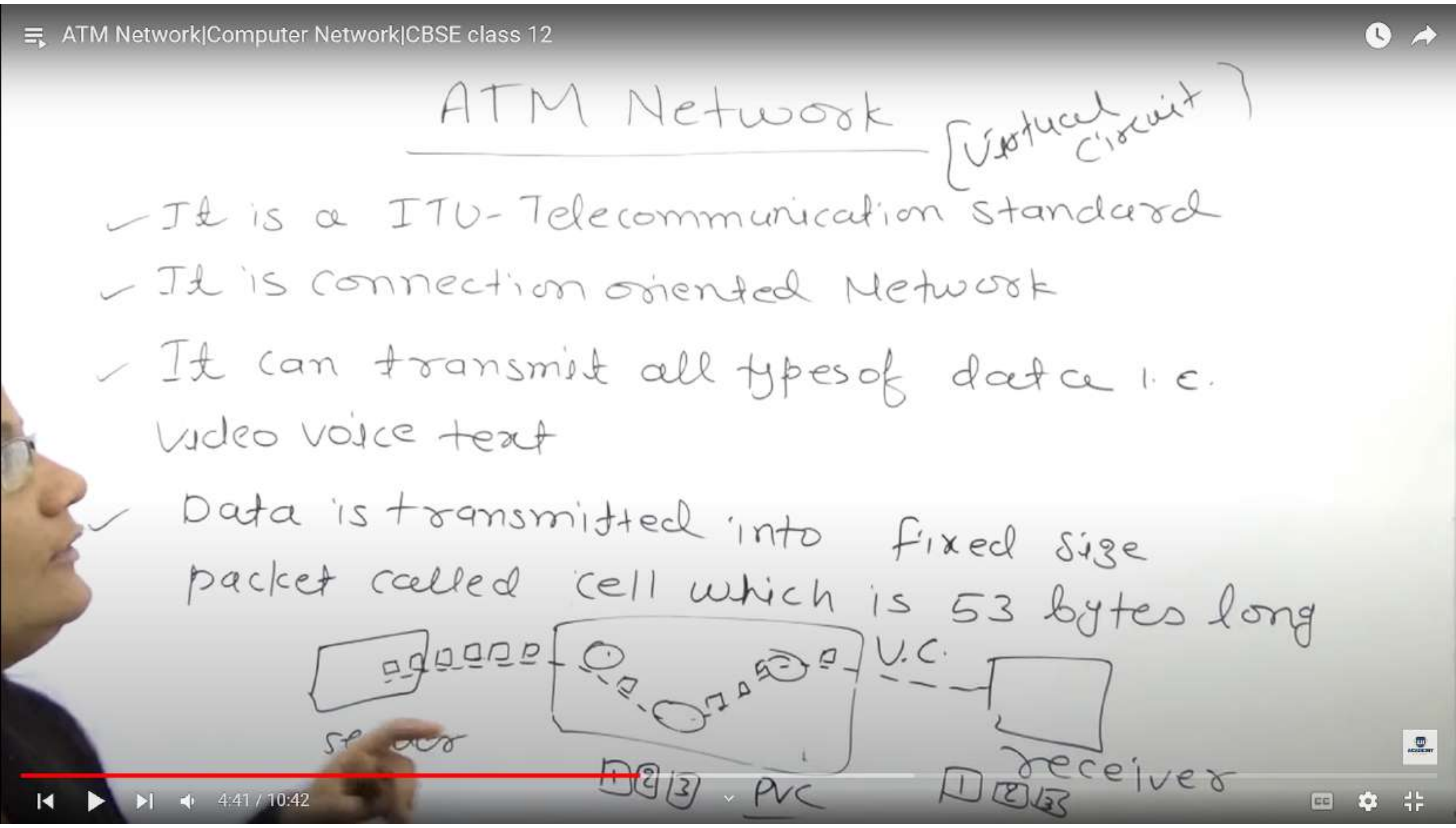
Three basic devices used in the SONET

- Synchronous Transport Signal (STS) multiplexer/ Demultiplexer:
- → Regenerator
- → Add/drop multiplexer

"Can add signals coming from different ~~path~~ sources into a given path or remove a signal"

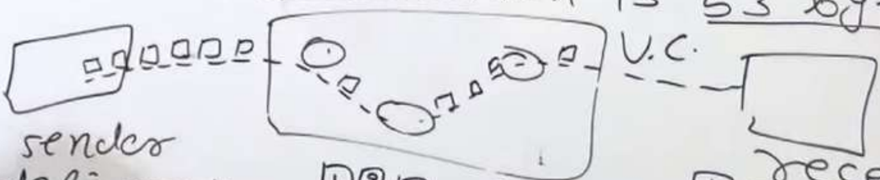


- → A section is optical link connecting two neighboring devices
- → A link is portion of network b/w two multiplexer
- → A path is end to end portion of network

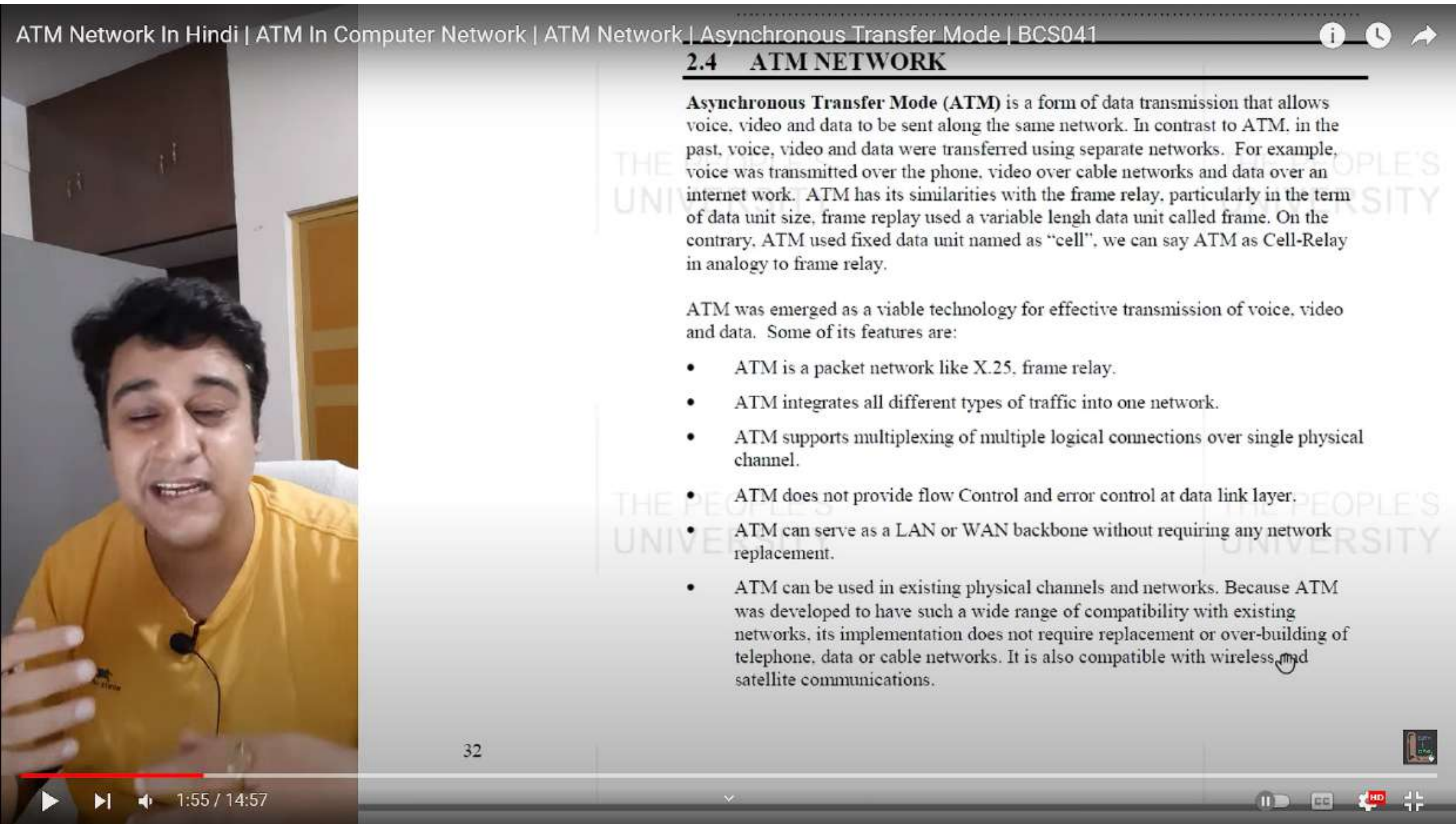

ATM Network|Computer Network|CBSE class 12
ATM Network
[Virtual Circuit]
It is a ITU-Telecommunication standard
It is connection oriented Network
It can transmit all types of data i.e. video voice text
Data is transmitted into fixed size packet called cell which is 53 bytes long
V.C
PVC
receiver
4:41 / 10:42

ATM Network
[Virtual Circuit]

- It is an ITU-Telecommunication standard
- It is connection oriented Network
- It can transmit all types of data i.e. video voice text
- Data is transmitted into fixed size packet called cell which is 53 bytes long



- It delivers the packets in order 1 2 3 PVC 1 2 3
- It operates at 155 Mbps & 622 Mbps

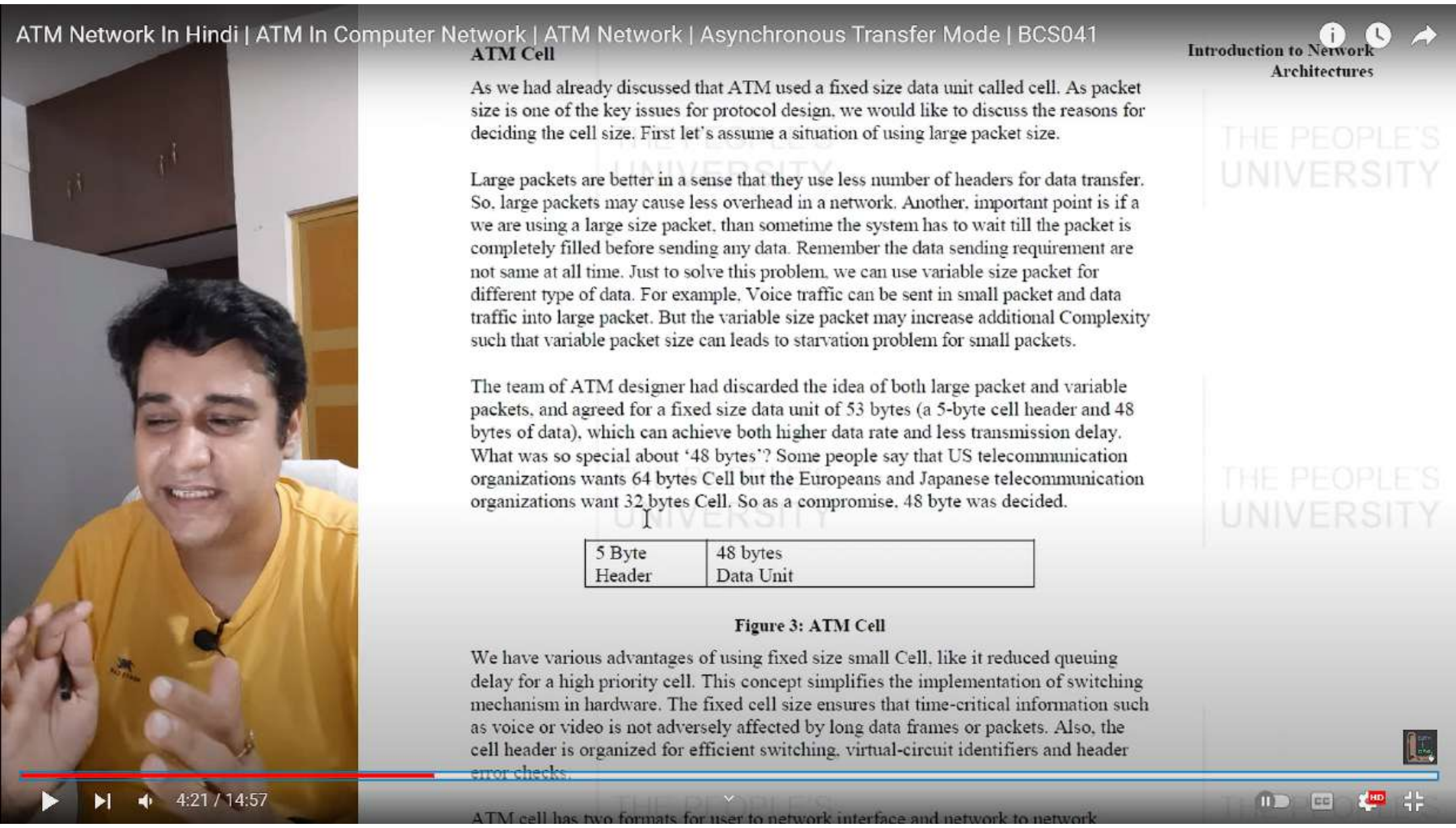


2.4 ATM NETWORK

Asynchronous Transfer Mode (ATM) is a form of data transmission that allows voice, video and data to be sent along the same network. In contrast to ATM, in the past, voice, video and data were transferred using separate networks. For example, voice was transmitted over the phone, video over cable networks and data over an internet work. ATM has its similarities with the frame relay, particularly in the term of data unit size, frame replay used a variable lengh data unit called frame. On the contrary, ATM used fixed data unit named as "cell", we can say ATM as Cell-Relay in analogy to frame relay.

ATM was emerged as a viable technology for effective transmission of voice, video and data. Some of its features are:

- ATM is a packet network like X.25, frame relay.
- ATM integrates all different types of traffic into one network.
- ATM supports multiplexing of multiple logical connections over single physical channel.
- ATM does not provide flow Control and error control at data link layer.
- ATM can serve as a LAN or WAN backbone without requiring any network replacement.
- ATM can be used in existing physical channels and networks. Because ATM was developed to have such a wide range of compatibility with existing networks, its implementation does not require replacement or over-building of telephone, data or cable networks. It is also compatible with wireless and satellite communications.



ATM Cell

As we had already discussed that ATM used a fixed size data unit called cell. As packet size is one of the key issues for protocol design, we would like to discuss the reasons for deciding the cell size. First let's assume a situation of using large packet size.

Large packets are better in a sense that they use less number of headers for data transfer. So, large packets may cause less overhead in a network. Another, important point is if a we are using a large size packet, than sometime the system has to wait till the packet is completely filled before sending any data. Remember the data sending requirement are not same at all time. Just to solve this problem, we can use variable size packet for different type of data. For example, Voice traffic can be sent in small packet and data traffic into large packet. But the variable size packet may increase additional Complexity such that variable packet size can leads to starvation problem for small packets.

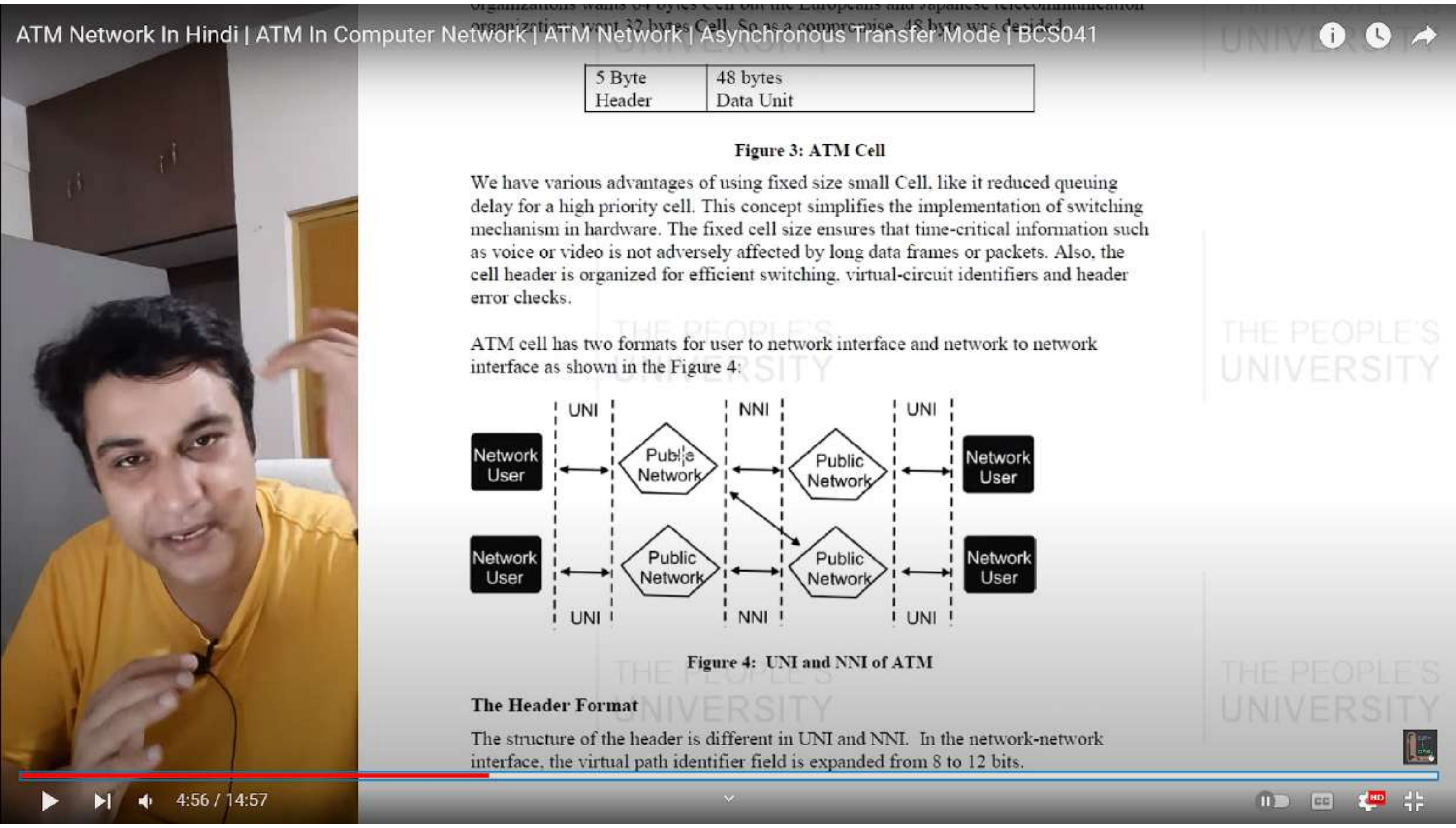
The team of ATM designer had discarded the idea of both large packet and variable packets, and agreed for a fixed size data unit of 53 bytes (a 5-byte cell header and 48 bytes of data), which can achieve both higher data rate and less transmission delay. What was so special about '48 bytes'? Some people say that US telecommunication organizations wants 64 bytes Cell but the Europeans and Japanese telecommunication organizations want 32 bytes Cell. So as a compromise, 48 byte was decided.

5 Byte Header	48 bytes Data Unit

Figure 3: ATM Cell

We have various advantages of using fixed size small Cell, like it reduced queuing delay for a high priority cell. This concept simplifies the implementation of switching mechanism in hardware. The fixed cell size ensures that time-critical information such as voice or video is not adversely affected by long data frames or packets. Also, the cell header is organized for efficient switching, virtual-circuit identifiers and header error checks.

ATM cell has two formats for user to network interface and network to network



organizations want 32 bytes Cell. So as a compromise, 48 byte was decided.

5 Byte Header	48 bytes Data Unit

Figure 3: ATM Cell

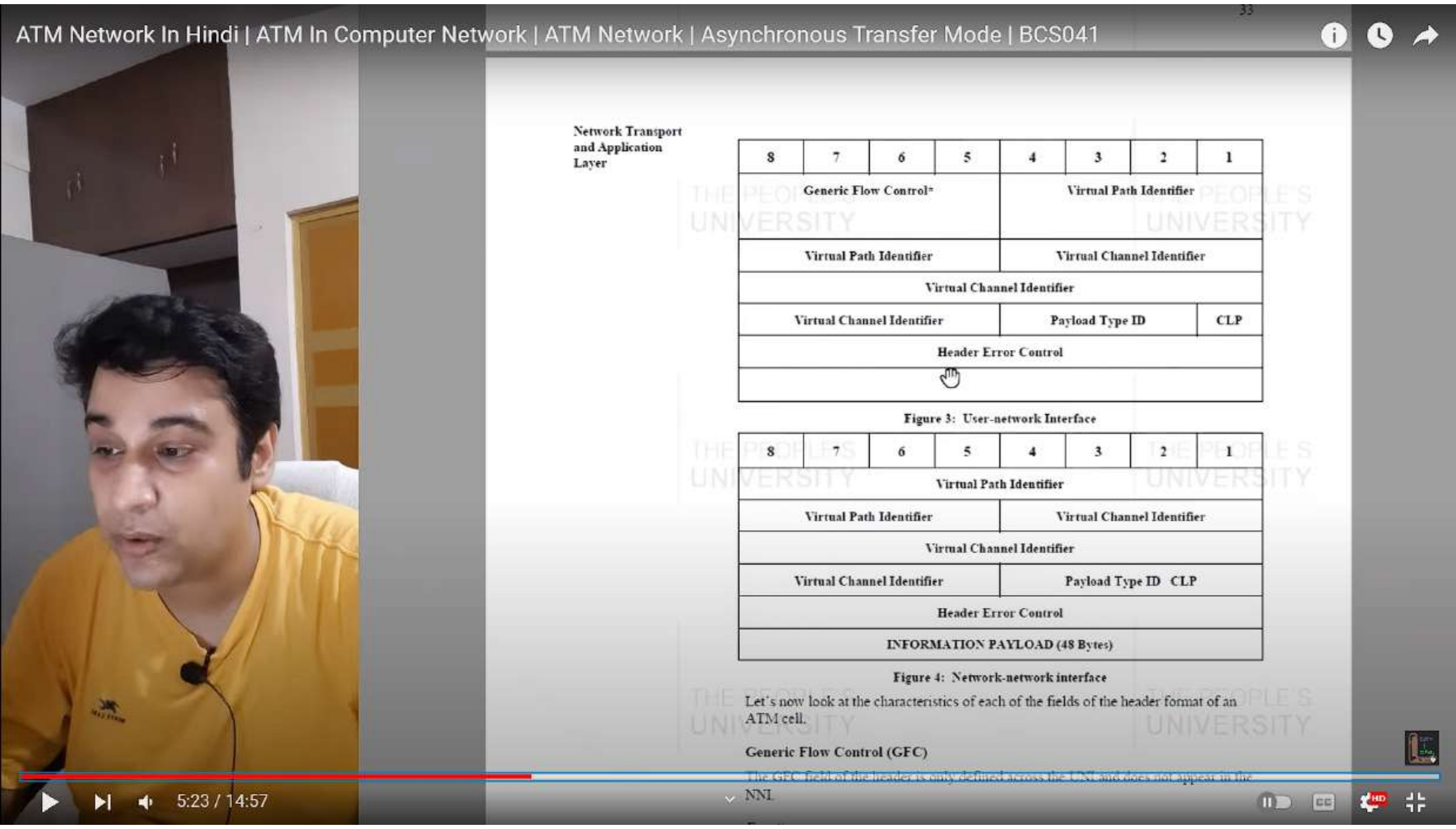
We have various advantages of using fixed size small Cell, like it reduced queuing delay for a high priority cell. This concept simplifies the implementation of switching mechanism in hardware. The fixed cell size ensures that time-critical information such as voice or video is not adversely affected by long data frames or packets. Also, the cell header is organized for efficient switching, virtual-circuit identifiers and header error checks.

ATM cell has two formats for user to network interface and network to network interface as shown in the Figure 4:

Figure 4: UNI and NNI of ATM

The Header Format

The structure of the header is different in UNI and NNI. In the network-network interface, the virtual path identifier field is expanded from 8 to 12 bits.



33

Network Transport and Application Layer

8	7	6	5	4	3	2	1
Generic Flow Control*				Virtual Path Identifier			
Virtual Path Identifier				Virtual Channel Identifier			
Virtual Channel Identifier							
Virtual Channel Identifier				Payload Type ID			CLP
Header Error Control							

Figure 3: User-network Interface

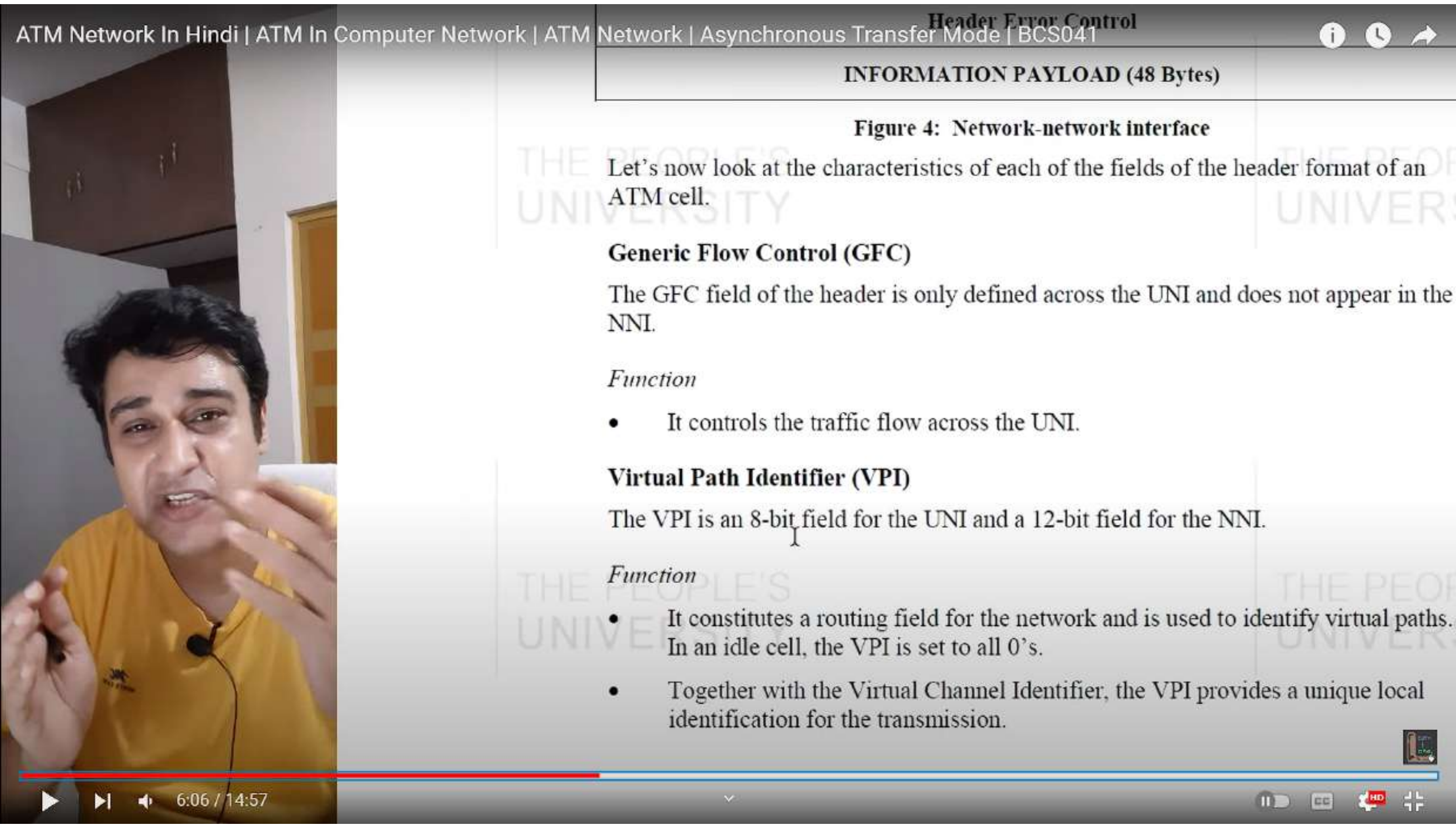
8	7	6	5	4	3	2	1
Virtual Path Identifier							
Virtual Path Identifier				Virtual Channel Identifier			
Virtual Channel Identifier							
Virtual Channel Identifier				Payload Type ID CLP			
Header Error Control							
INFORMATION PAYLOAD (48 Bytes)							

Figure 4: Network-network interface

Let's now look at the characteristics of each of the fields of the header format of an ATM cell.

Generic Flow Control (GFC)

The GFC field of the header is only defined across the UNI and does not appear in the NNI.



Header Error Control

INFORMATION PAYLOAD (48 Bytes)

Figure 4: Network-network interface

Let's now look at the characteristics of each of the fields of the header format of an ATM cell.

Generic Flow Control (GFC)

The GFC field of the header is only defined across the UNI and does not appear in the NNI.

Function

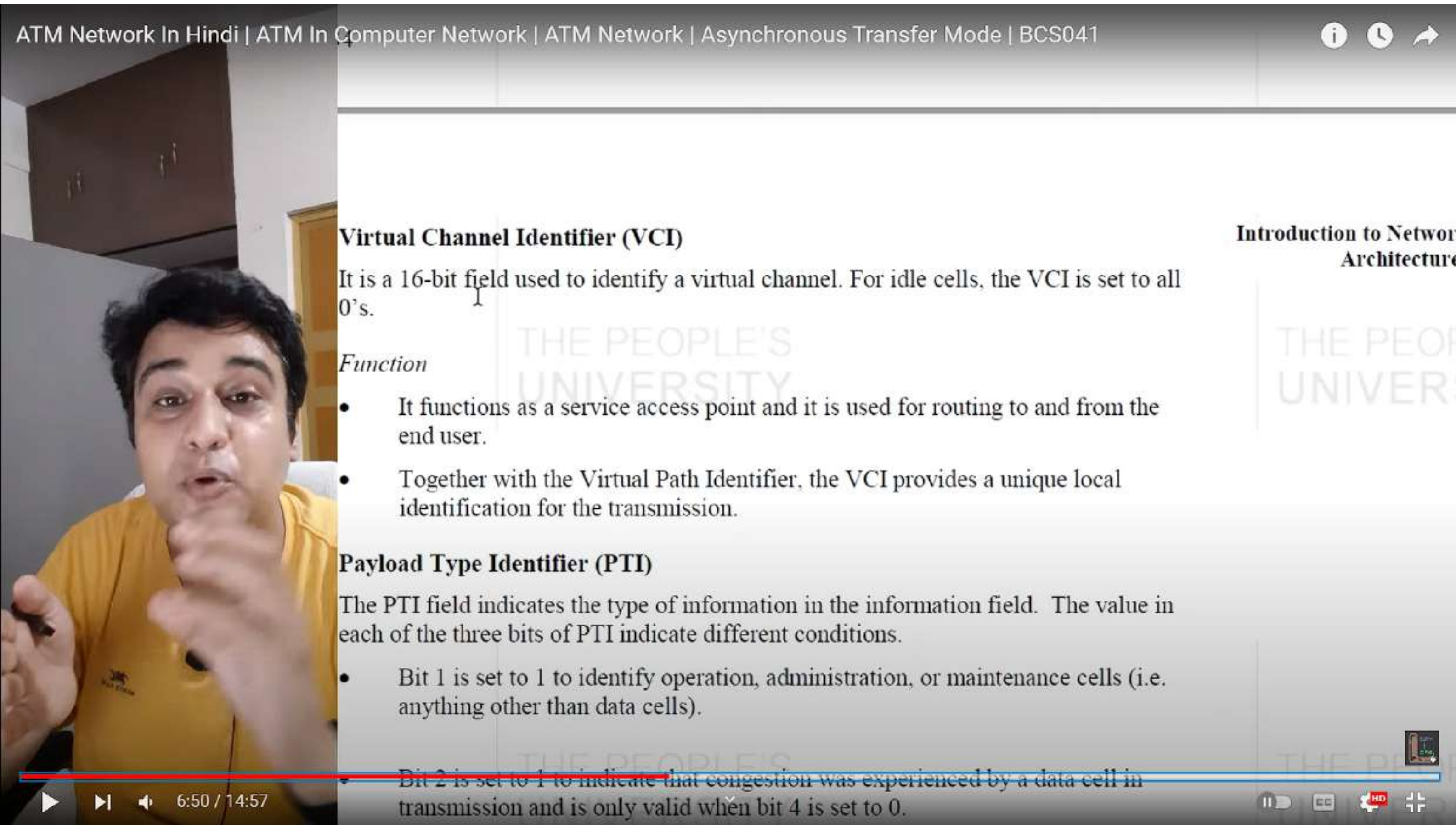
- It controls the traffic flow across the UNI.

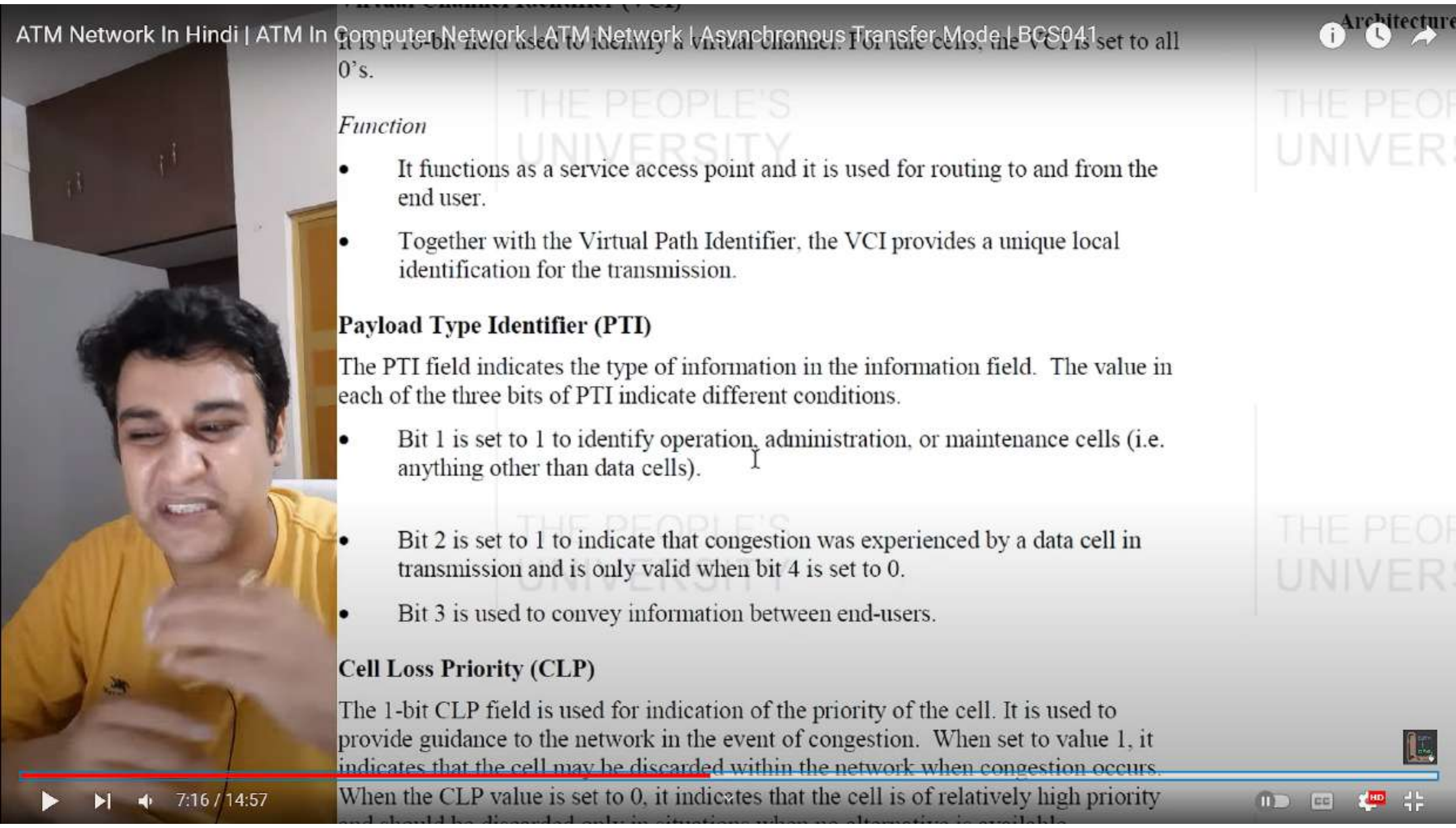
Virtual Path Identifier (VPI)

The VPI is an 8-bit field for the UNI and a 12-bit field for the NNI.

Function

- It constitutes a routing field for the network and is used to identify virtual paths. In an idle cell, the VPI is set to all 0's.
- Together with the Virtual Channel Identifier, the VPI provides a unique local identification for the transmission.


ATM Network In Hindi | ATM In Computer Network | ATM Network | Asynchronous Transfer Mode | BCS041
Virtual Channel Identifier (VCI)
It is a 16-bit field used to identify a virtual channel. For idle cells, the VCI is set to all 0's.
Function
It functions as a service access point and it is used for routing to and from the end user.
Together with the Virtual Path Identifier, the VCI provides a unique local identification for the transmission.
Payload Type Identifier (PTI)
The PTI field indicates the type of information in the information field. The value in each of the three bits of PTI indicate different conditions.
Bit 1 is set to 1 to identify operation, administration, or maintenance cells (i.e. anything other than data cells).
Bit 2 is set to 1 to indicate that congestion was experienced by a data cell in transmission and is only valid when bit 4 is set to 0.
Introduction to Networ
Architecture
THE PEOPLE'S
UNIVERSITY
6:50 / 14:57



It is a 16-bit field used to identify a virtual channel. For idle cells, the VCI is set to all 0's.

Function

- It functions as a service access point and it is used for routing to and from the end user.
- Together with the Virtual Path Identifier, the VCI provides a unique local identification for the transmission.

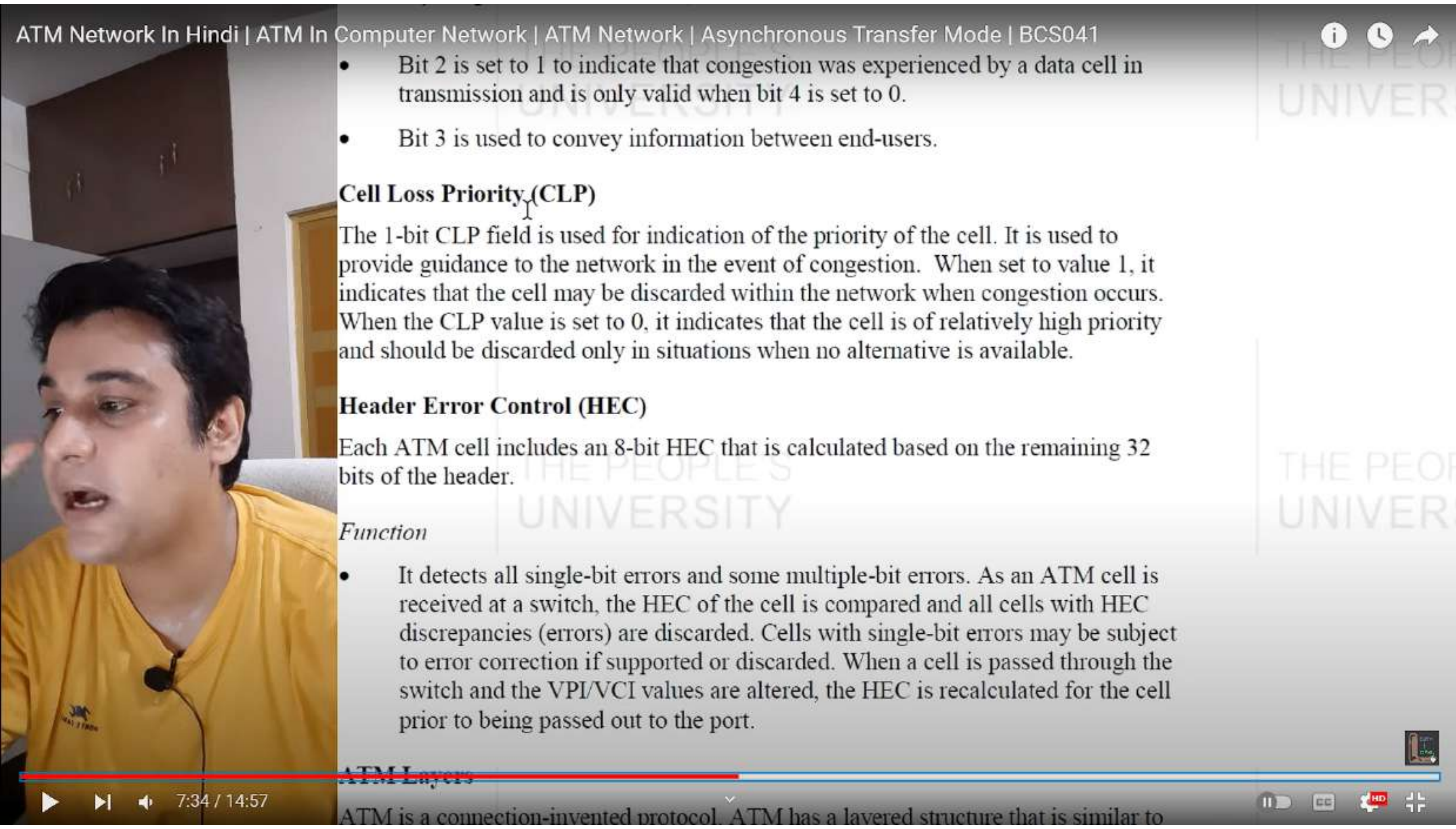
Payload Type Identifier (PTI)

The PTI field indicates the type of information in the information field. The value in each of the three bits of PTI indicate different conditions.

- Bit 1 is set to 1 to identify operation, administration, or maintenance cells (i.e. anything other than data cells).
- Bit 2 is set to 1 to indicate that congestion was experienced by a data cell in transmission and is only valid when bit 4 is set to 0.
- Bit 3 is used to convey information between end-users.

Cell Loss Priority (CLP)

The 1-bit CLP field is used for indication of the priority of the cell. It is used to provide guidance to the network in the event of congestion. When set to value 1, it indicates that the cell may be discarded within the network when congestion occurs. When the CLP value is set to 0, it indicates that the cell is of relatively high priority



- Bit 2 is set to 1 to indicate that congestion was experienced by a data cell in transmission and is only valid when bit 4 is set to 0.
- Bit 3 is used to convey information between end-users.

Cell Loss Priority (CLP)

The 1-bit CLP field is used for indication of the priority of the cell. It is used to provide guidance to the network in the event of congestion. When set to value 1, it indicates that the cell may be discarded within the network when congestion occurs. When the CLP value is set to 0, it indicates that the cell is of relatively high priority and should be discarded only in situations when no alternative is available.

Header Error Control (HEC)

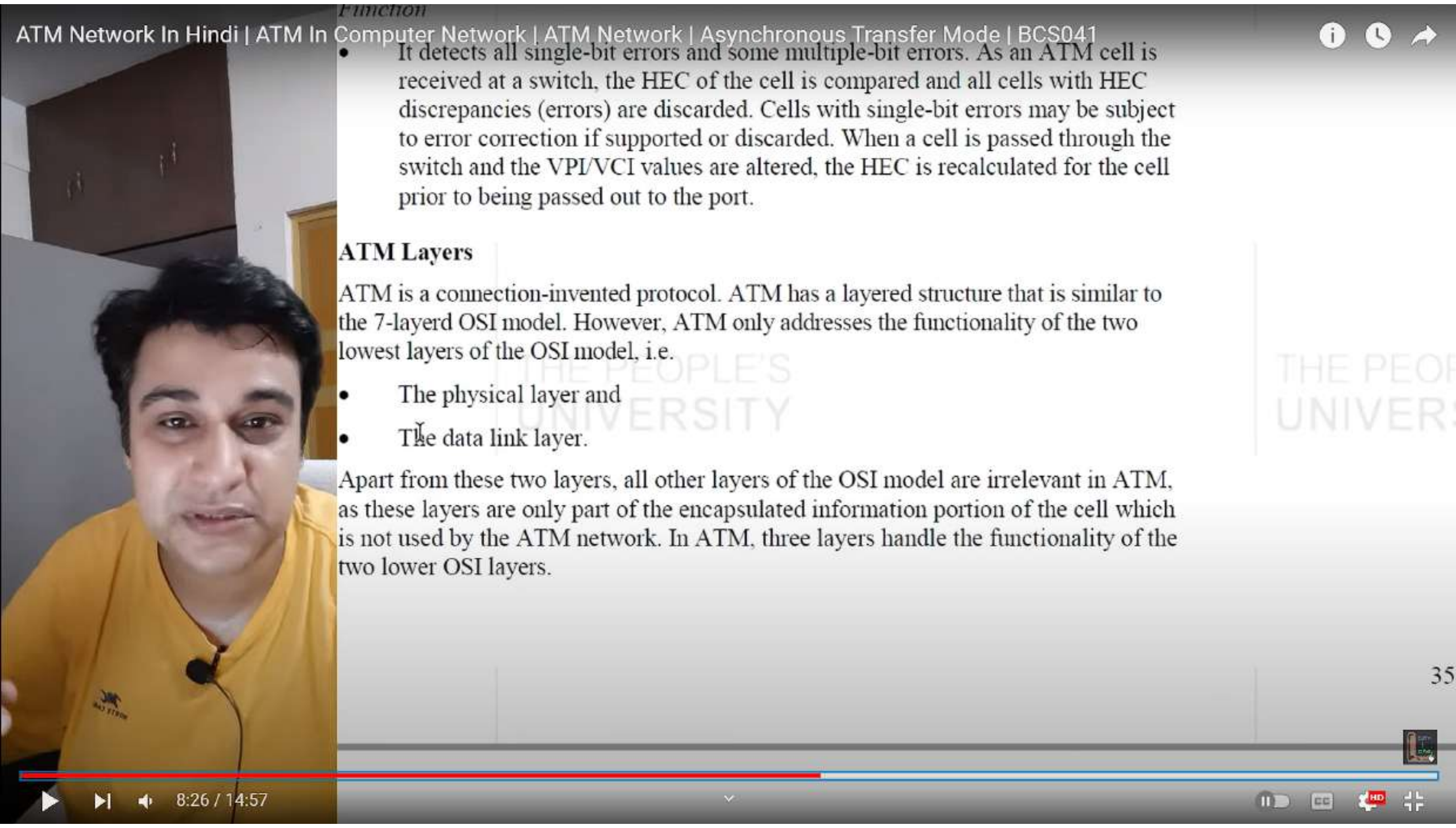
Each ATM cell includes an 8-bit HEC that is calculated based on the remaining 32 bits of the header.

Function

- It detects all single-bit errors and some multiple-bit errors. As an ATM cell is received at a switch, the HEC of the cell is compared and all cells with HEC discrepancies (errors) are discarded. Cells with single-bit errors may be subject to error correction if supported or discarded. When a cell is passed through the switch and the VPI/VCI values are altered, the HEC is recalculated for the cell prior to being passed out to the port.

ATM Layers

ATM is a connection-invented protocol. ATM has a layered structure that is similar to



Function

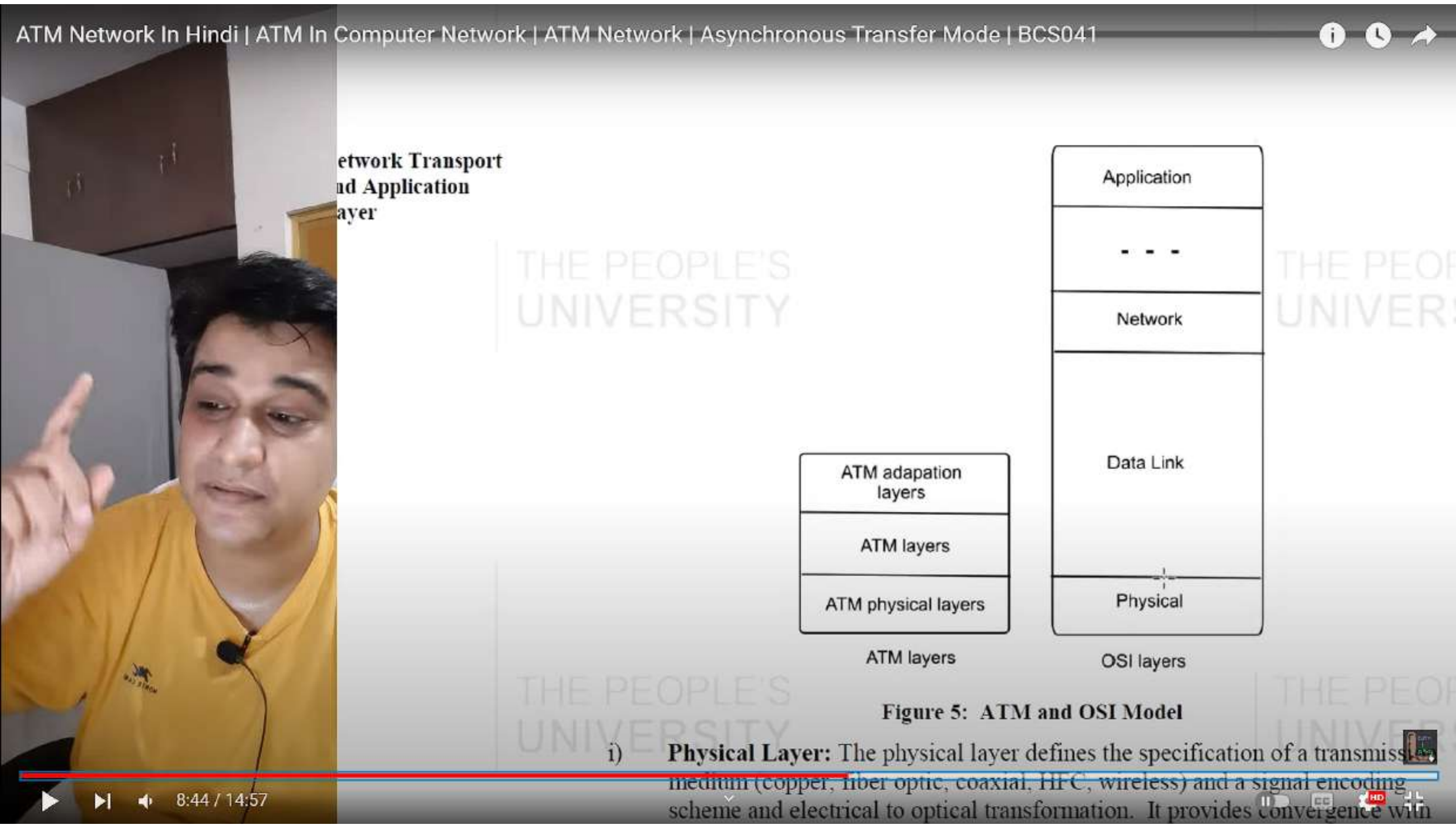
- It detects all single-bit errors and some multiple-bit errors. As an ATM cell is received at a switch, the HEC of the cell is compared and all cells with HEC discrepancies (errors) are discarded. Cells with single-bit errors may be subject to error correction if supported or discarded. When a cell is passed through the switch and the VPI/VCI values are altered, the HEC is recalculated for the cell prior to being passed out to the port.

ATM Layers

ATM is a connection-invented protocol. ATM has a layered structure that is similar to the 7-layerd OSI model. However, ATM only addresses the functionality of the two lowest layers of the OSI model, i.e.

- The physical layer and
- The data link layer.

Apart from these two layers, all other layers of the OSI model are irrelevant in ATM, as these layers are only part of the encapsulated information portion of the cell which is not used by the ATM network. In ATM, three layers handle the functionality of the two lower OSI layers.


ATM Network In Hindi | ATM In Computer Network | ATM Network | Asynchronous Transfer Mode | BCS041
etwork Transport
nd Application
ayer
THE PEOPLE'S
UNIVERSITY
Application
- - -
Network
Data Link
Physical
ATM adapation layers
ATM layers
ATM physical layers
ATM layers
OSI layers
Figure 5: ATM and OSI Model
i) Physical Layer: The physical layer defines the specification of a transmiss
medium (copper, fiber optic, coaxial, HFC, wireless) and a signal encoding
scheme and electrical to optical transformation. It provides convergence with
8:44 / 14:57

ATM Network In Hindi | ATM In Computer Network | ATM Network | Asynchronous Transfer Mode | BCS041

Figure 5: ATM and OSI Model

i) **Physical Layer:** The physical layer defines the specification of a transmission medium (copper, fiber optic, coaxial, HFC, wireless) and a signal encoding scheme and electrical to optical transformation. It provides convergence with physical transport protocols such as SONET as well as the mechanism for transforming the flow of cells into a flow of bits. The ATM form has left most of the specification for this level to the implementer.

ii) **The ATM Layer:** The ATM layer deals with cells and cell transport. It defines the layout of a cell and tells what the header fields mean. The size of a cell is 53 bytes (5 bytes of header and 48 bytes of payload). Because each cell is the same size and all are relatively small, delay and other problems with multiplexing different sized packets are avoided.

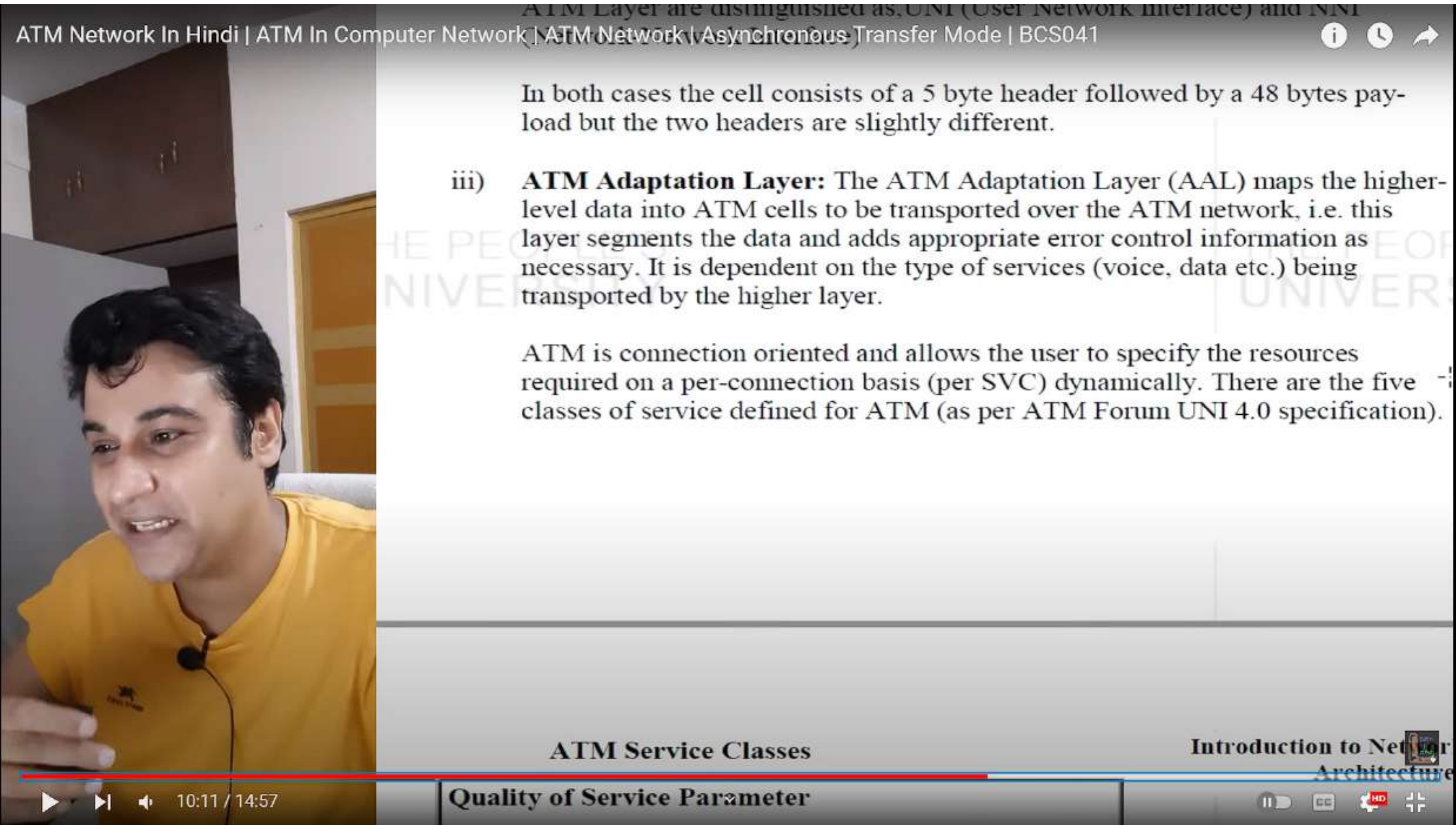
It also deals with establishment and release of virtual circuits. Congestion control is also located here. It resembles the network layer of the OSI model as it has got the characteristics of the network layer protocol of OSI model like Routing, Switching, End to end virtual circuit set up and Traffic management.

Switches in ATM provide both switching and multiplexing. A Cell format of ATM Layer are distinguished as,UNI (User Network Interface) and NNI (Network-Network Interface)

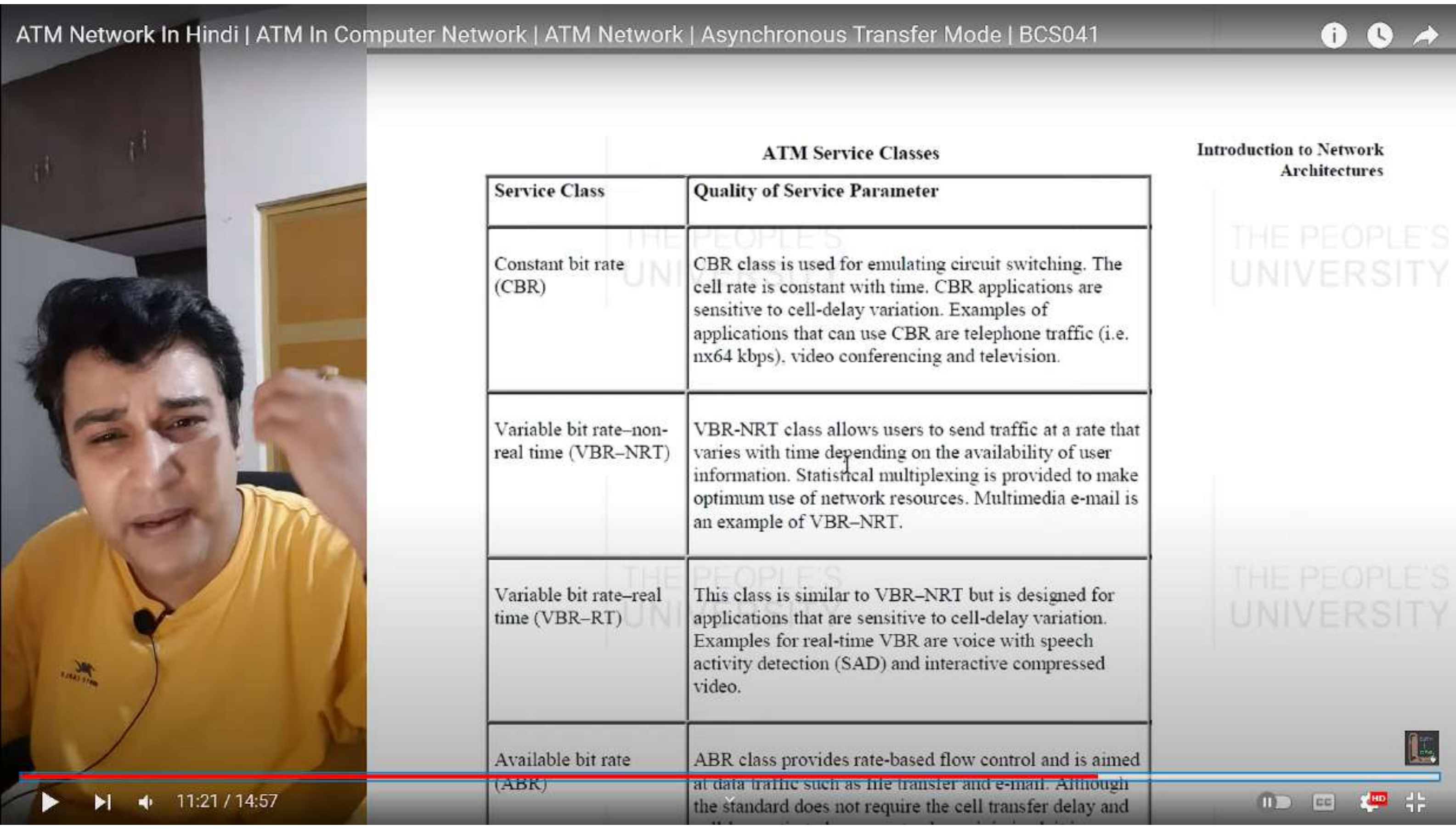
In both cases the cell consists of a 5 byte header followed by a 48 bytes pay-load but the two headers are slightly different.

9:28 / 14:57

iii) **ATM Adaptation Layer:** The ATM Adaptation Layer (AAL) maps the higher-

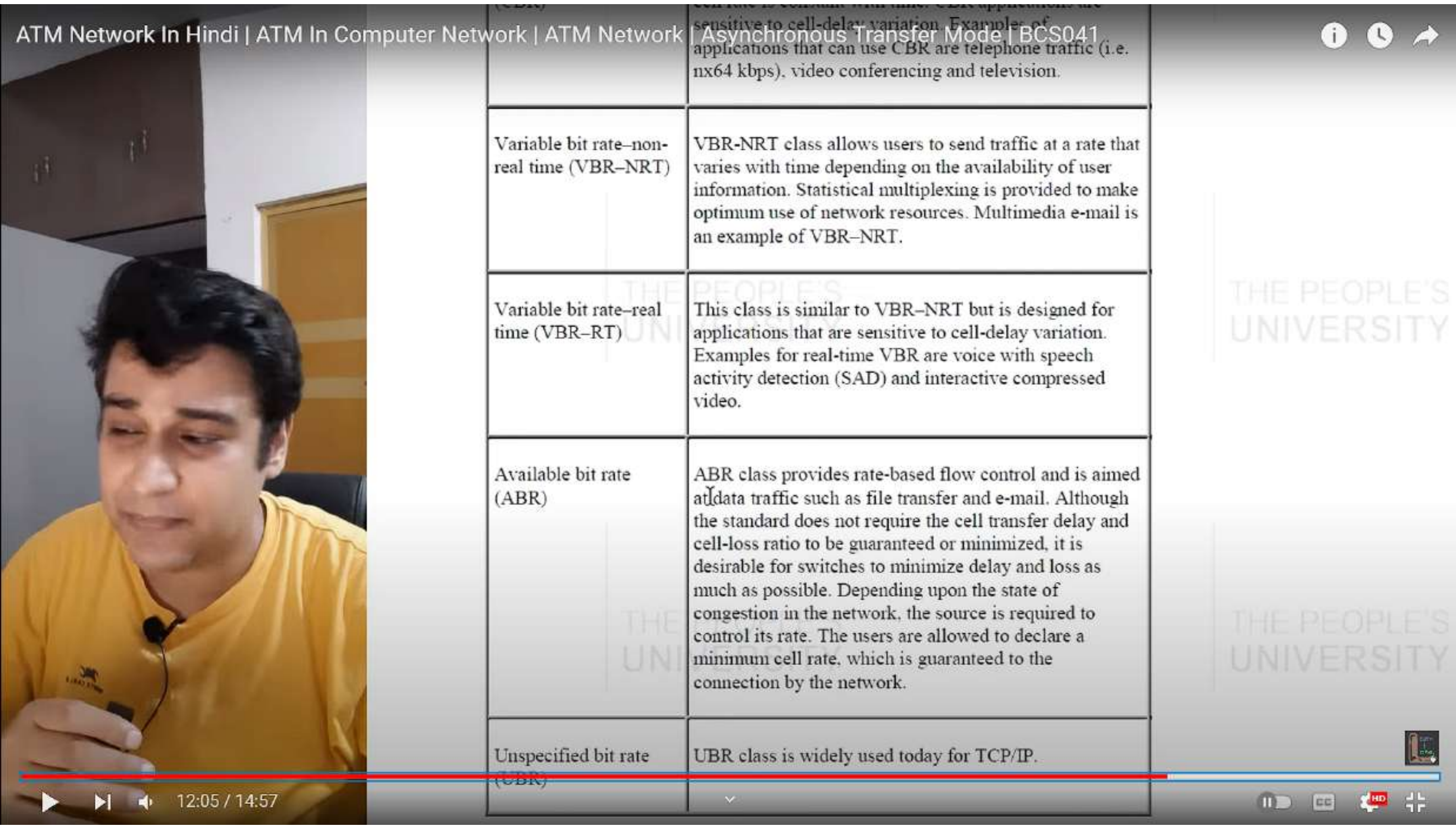


ATM Network In Hindi | ATM In Computer Network | ATM Network | Asynchronous Transfer Mode | BCS041
In both cases the cell consists of a 5 byte header followed by a 48 bytes pay-load but the two headers are slightly different.
iii) ATM Adaptation Layer: The ATM Adaptation Layer (AAL) maps the higher-level data into ATM cells to be transported over the ATM network, i.e. this layer segments the data and adds appropriate error control information as necessary. It is dependent on the type of services (voice, data etc.) being transported by the higher layer.
ATM is connection oriented and allows the user to specify the resources required on a per-connection basis (per SVC) dynamically. There are the five classes of service defined for ATM (as per ATM Forum UNI 4.0 specification).
ATM Service Classes
Quality of Service Parameter
10:11 / 14:57

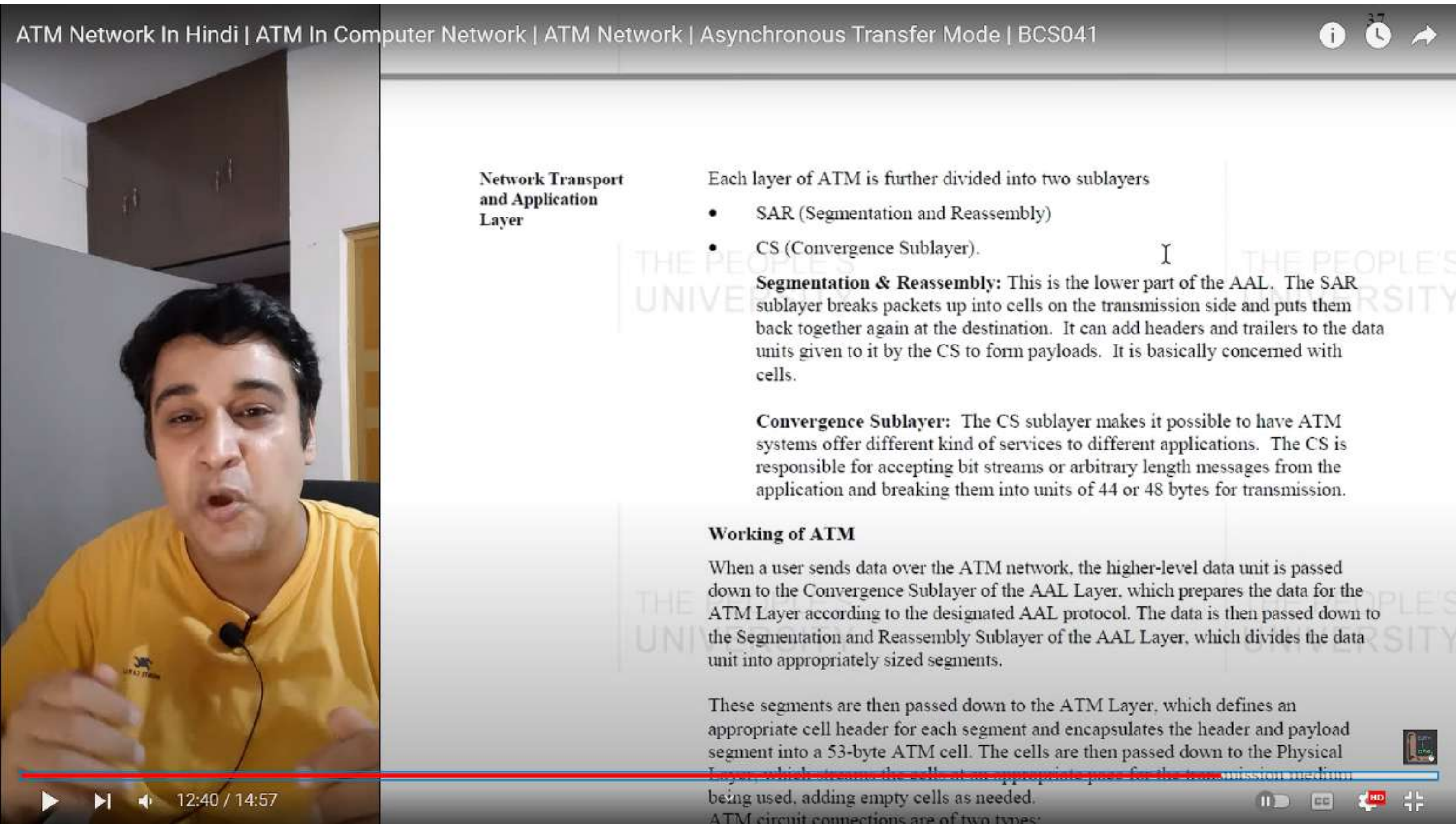


ATM Service Classes

Service Class	Quality of Service Parameter
Constant bit rate (CBR)	CBR class is used for emulating circuit switching. The cell rate is constant with time. CBR applications are sensitive to cell-delay variation. Examples of applications that can use CBR are telephone traffic (i.e. nx64 kbps), video conferencing and television.
Variable bit rate–non-real time (VBR–NRT)	VBR-NRT class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR–NRT.
Variable bit rate–real time (VBR–RT)	This class is similar to VBR–NRT but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.
Available bit rate (ABR)	ABR class provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail. Although the standard does not require the cell transfer delay and



(CBR)	sensitive to cell-delay variation. Examples of applications that can use CBR are telephone traffic (i.e. nx64 kbps), video conferencing and television.
Variable bit rate–non-real time (VBR–NRT)	VBR-NRT class allows users to send traffic at a rate that varies with time depending on the availability of user information. Statistical multiplexing is provided to make optimum use of network resources. Multimedia e-mail is an example of VBR–NRT.
Variable bit rate–real time (VBR–RT)	This class is similar to VBR–NRT but is designed for applications that are sensitive to cell-delay variation. Examples for real-time VBR are voice with speech activity detection (SAD) and interactive compressed video.
Available bit rate (ABR)	ABR class provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail. Although the standard does not require the cell transfer delay and cell-loss ratio to be guaranteed or minimized, it is desirable for switches to minimize delay and loss as much as possible. Depending upon the state of congestion in the network, the source is required to control its rate. The users are allowed to declare a minimum cell rate, which is guaranteed to the connection by the network.
Unspecified bit rate (UBR)	UBR class is widely used today for TCP/IP.



Network Transport and Application Layer

Each layer of ATM is further divided into two sublayers

- SAR (Segmentation and Reassembly)
- CS (Convergence Sublayer).

Segmentation & Reassembly: This is the lower part of the AAL. The SAR sublayer breaks packets up into cells on the transmission side and puts them back together again at the destination. It can add headers and trailers to the data units given to it by the CS to form payloads. It is basically concerned with cells.

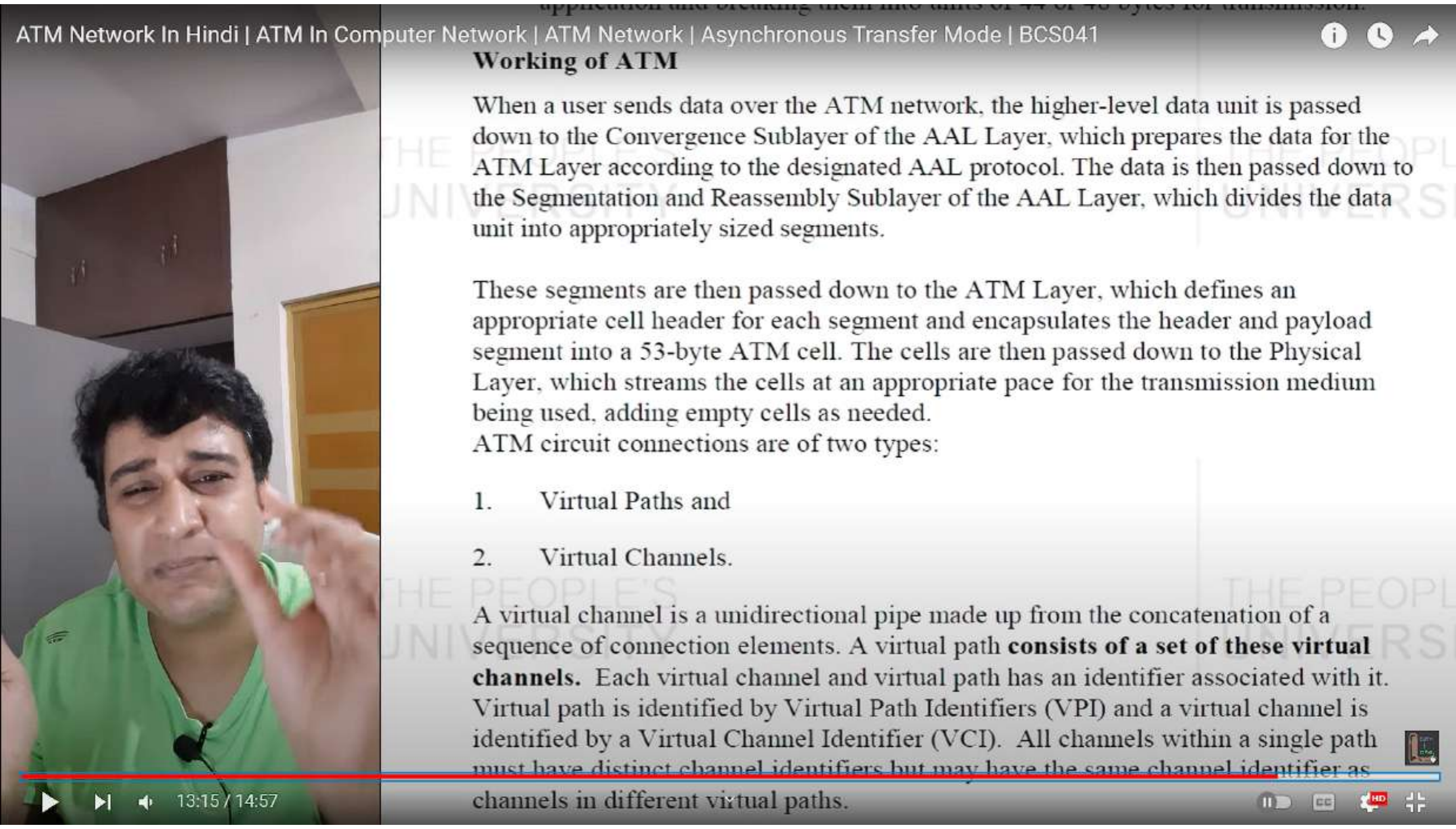
Convergence Sublayer: The CS sublayer makes it possible to have ATM systems offer different kind of services to different applications. The CS is responsible for accepting bit streams or arbitrary length messages from the application and breaking them into units of 44 or 48 bytes for transmission.

Working of ATM

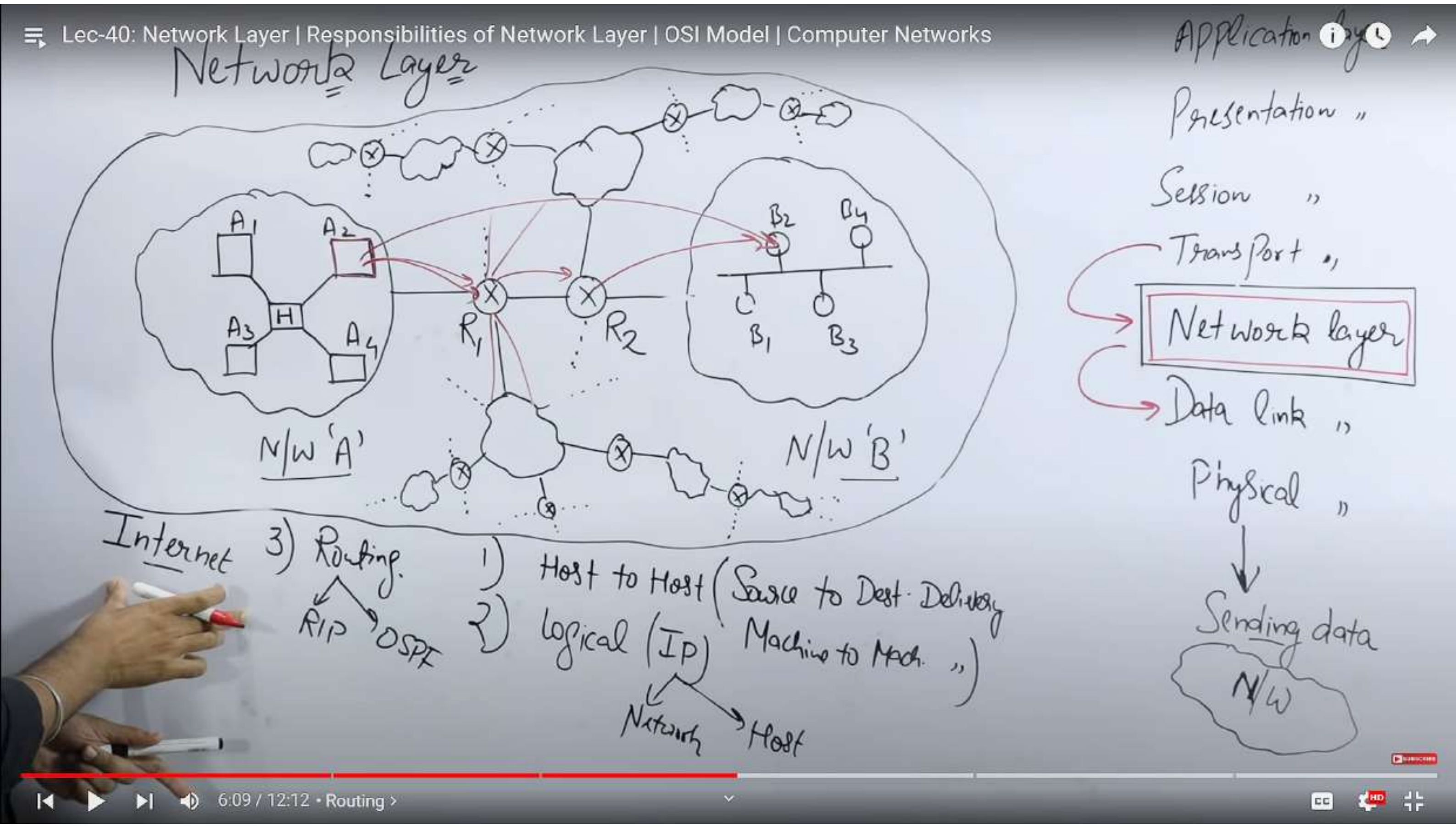
When a user sends data over the ATM network, the higher-level data unit is passed down to the Convergence Sublayer of the AAL Layer, which prepares the data for the ATM Layer according to the designated AAL protocol. The data is then passed down to the Segmentation and Reassembly Sublayer of the AAL Layer, which divides the data unit into appropriately sized segments.

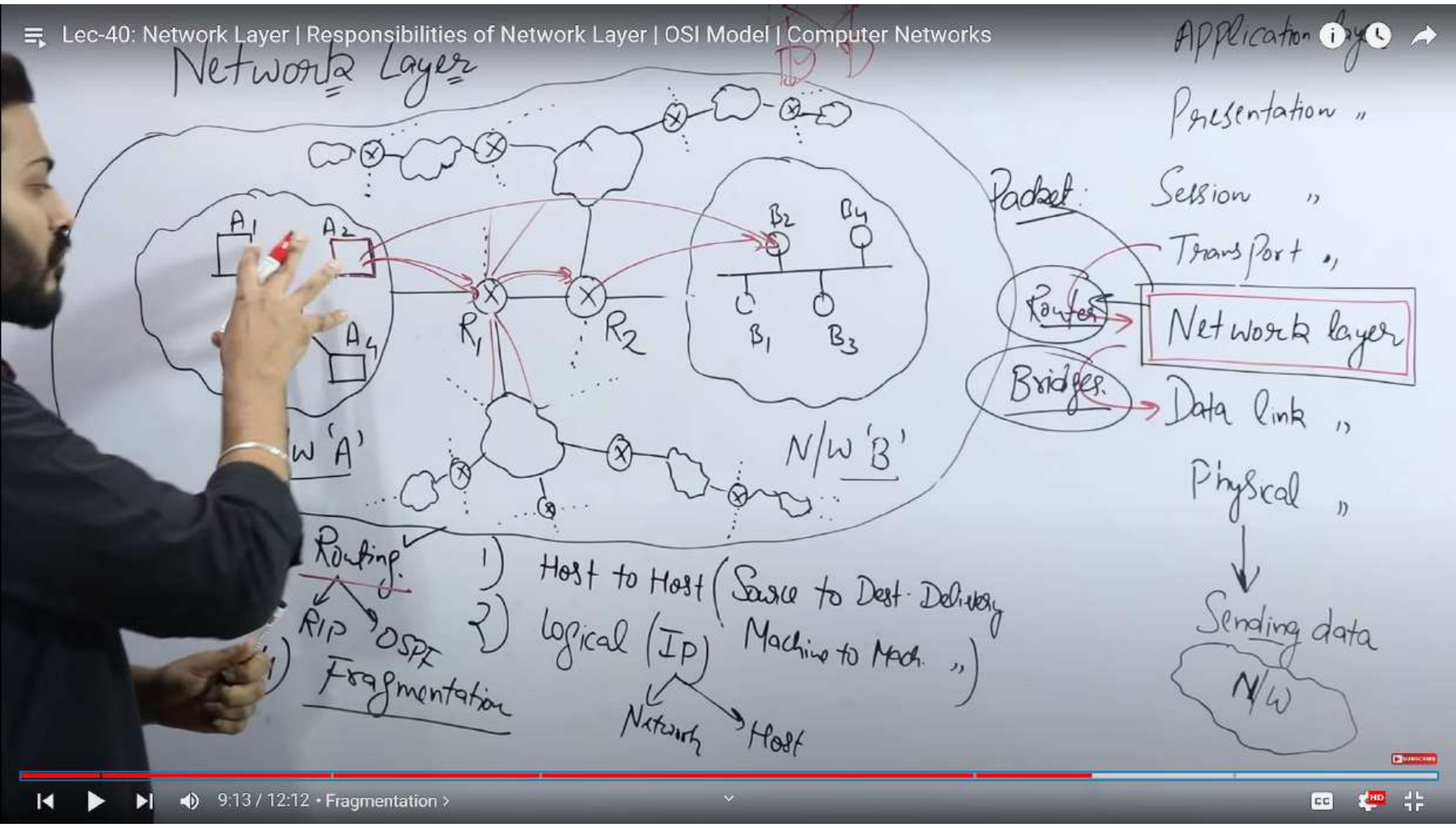
These segments are then passed down to the ATM Layer, which defines an appropriate cell header for each segment and encapsulates the header and payload segment into a 53-byte ATM cell. The cells are then passed down to the Physical Layer, which streams the cells at an appropriate pace for the transmission medium being used, adding empty cells as needed.

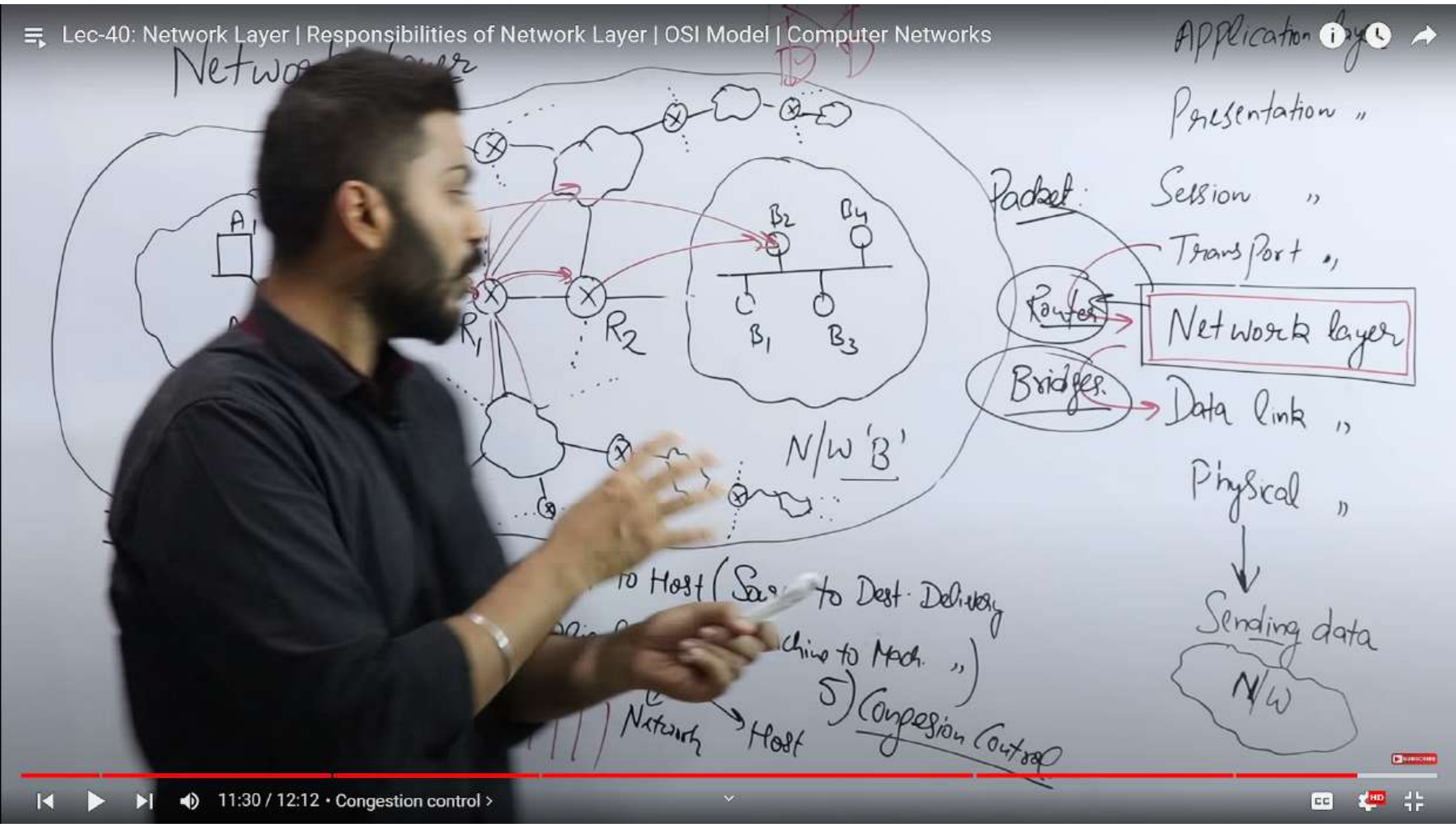
ATM circuit connections are of two types:



ATM Network In Hindi | ATM In Computer Network | ATM Network | Asynchronous Transfer Mode | BCS041
Working of ATM
When a user sends data over the ATM network, the higher-level data unit is passed down to the Convergence Sublayer of the AAL Layer, which prepares the data for the ATM Layer according to the designated AAL protocol. The data is then passed down to the Segmentation and Reassembly Sublayer of the AAL Layer, which divides the data unit into appropriately sized segments.
These segments are then passed down to the ATM Layer, which defines an appropriate cell header for each segment and encapsulates the header and payload segment into a 53-byte ATM cell. The cells are then passed down to the Physical Layer, which streams the cells at an appropriate pace for the transmission medium being used, adding empty cells as needed.
ATM circuit connections are of two types:
1. Virtual Paths and
2. Virtual Channels.
A virtual channel is a unidirectional pipe made up from the concatenation of a sequence of connection elements. A virtual path consists of a set of these virtual channels. Each virtual channel and virtual path has an identifier associated with it. Virtual path is identified by Virtual Path Identifiers (VPI) and a virtual channel is identified by a Virtual Channel Identifier (VCI). All channels within a single path must have distinct channel identifiers but may have the same channel identifier as channels in different virtual paths.
13:15 / 14:57

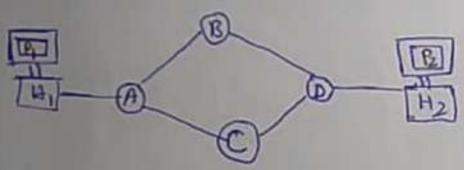

Lec-40: Network Layer | Responsibilities of Network Layer | OSI Model | Computer Networks
Network Layer
A1
A2
A3
A4
H
R1
R2
B1
B2
B3
B4
N/W 'A'
N/W 'B'
Internet
3) Routing
RIP
OSPF
1) Host to Host (Source to Dest. Delivery
Machine to Mach. ,,)
2) logical (IP)
Network
Host
Application
Presentation ,,
Session ,,
Transport ,,
Network layer
Data link ,,
Physical ,,
Sending data
N/W
6:09 / 12:12 • Routing


Lec-40: Network Layer | Responsibilities of Network Layer | OSI Model | Computer Networks
Network Layer
A1
A2
A4
R1
R2
B1
B2
B3
B4
N/W 'A'
N/W 'B'
Packet
Router
Bridges
Application layer
Presentation "
Session "
Transport "
Network layer
Data link "
Physical "
Sending data
N/W
Routing
RIP
OSPF
Fragmentation
1) Host to Host (Source to Dest. Delivery
Machine to Mach. ")
2) logical (IP)
Network
Host
9:13 / 12:12 • Fragmentation ›


Lec-40: Network Layer | Responsibilities of Network Layer | OSI Model | Computer Networks
Application
Presentation
Session
Transport
Network layer
Data link
Physical
Sending data
N/W
Packet
Router
Bridges
R1
R2
B1
B2
B3
B4
N/W 'B'
to Host (Sou... to Dest. Delivery
...chine to Mach.
5) Congestion Control
Network
Host
11:30 / 12:12 • Congestion control

NETWORK LAYER DESIGN ISSUES

issue



Designer of Network Layer must grapple with
- → Service provided to transport layer
- → Internal Design of network

→ Store and forward Packet switching

→ Services Provided to the Transport layer

Network layer provides services to Transport layer.

The services need to be carefully designed with following goals

- → Services should be independent of router technology
- → Transport layer should be shielded from the number, type and topology of router
- → Network addresses made available to transport layer should use uniform numbering plan

Implementation of Connectionless services
- Datagram and Datagram Network

Implementation of Connection oriented Services
- → Virtual circuit

3:33 / 9:23

Routing Algorithm

⇒ The main function of N/w layer.

- $\boxed{\text{Routing}}$
- Congestion Control
- Internetworking

Routing It is the process of forwarding a pkt in a n/w. So that it reaches its intended destination.

Routing Algorithm

⇒ The main function of N/w layer.

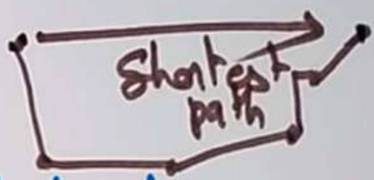
- $\boxed{\text{Routing}}$ ✓
- Congestion Control
- Internetworking

Routing It is the process of forwarding of a pkt in a n/w. So that it reaches its intended destination.

Main goal of routing algorithms :

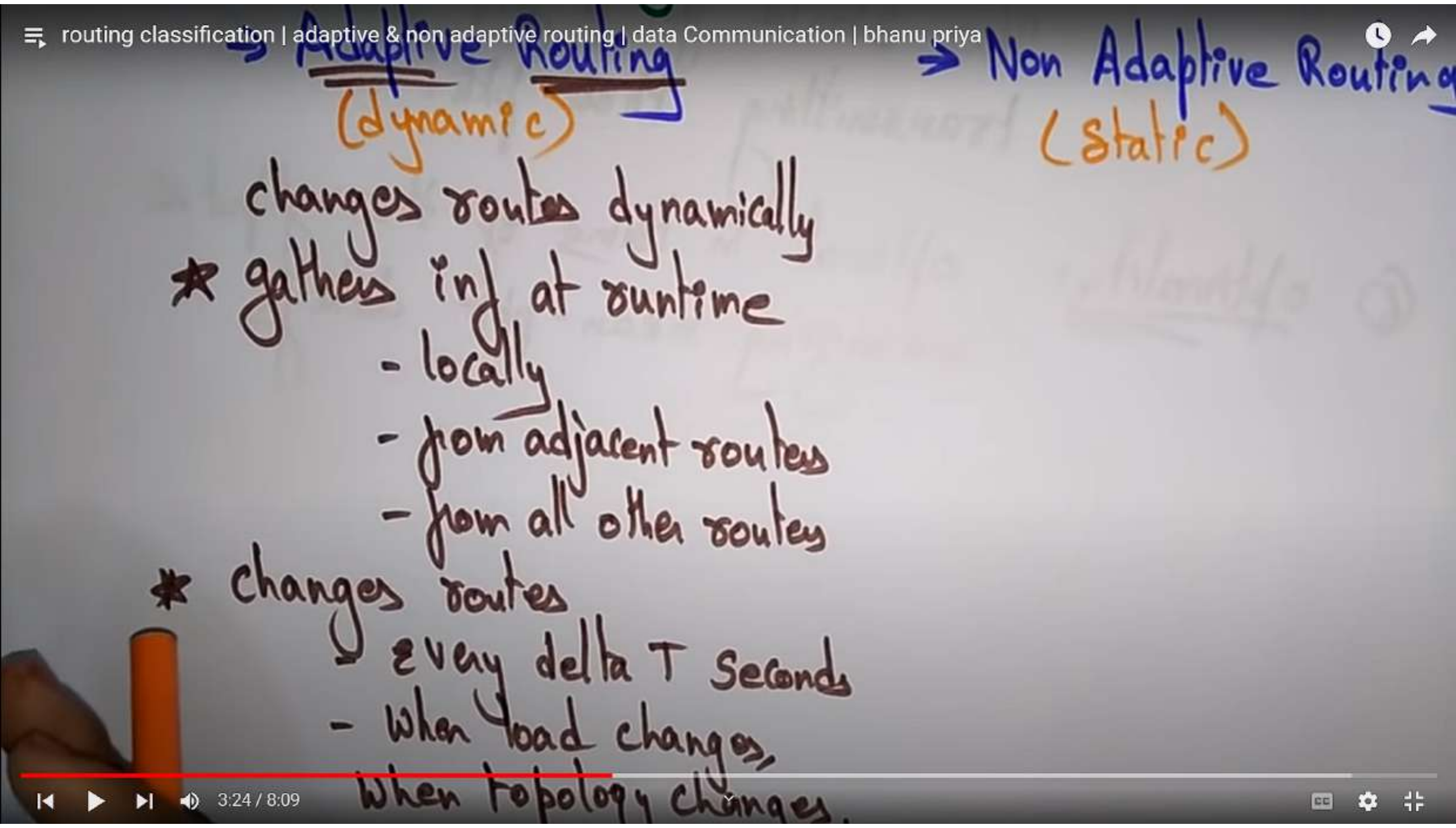
① Correctness :- routing should be done correctly

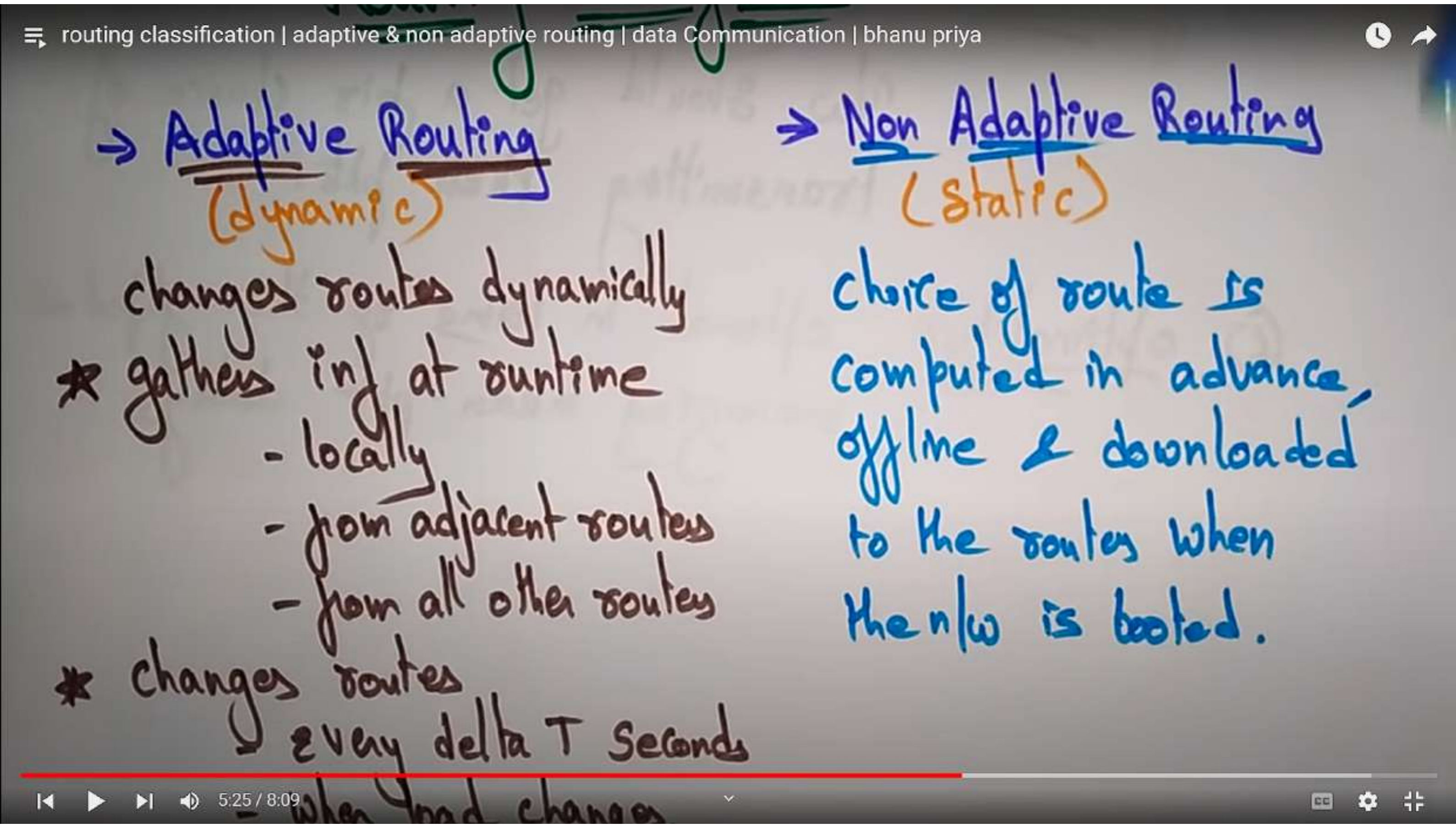
② Simplicity :- routing should be done in a simple manner.

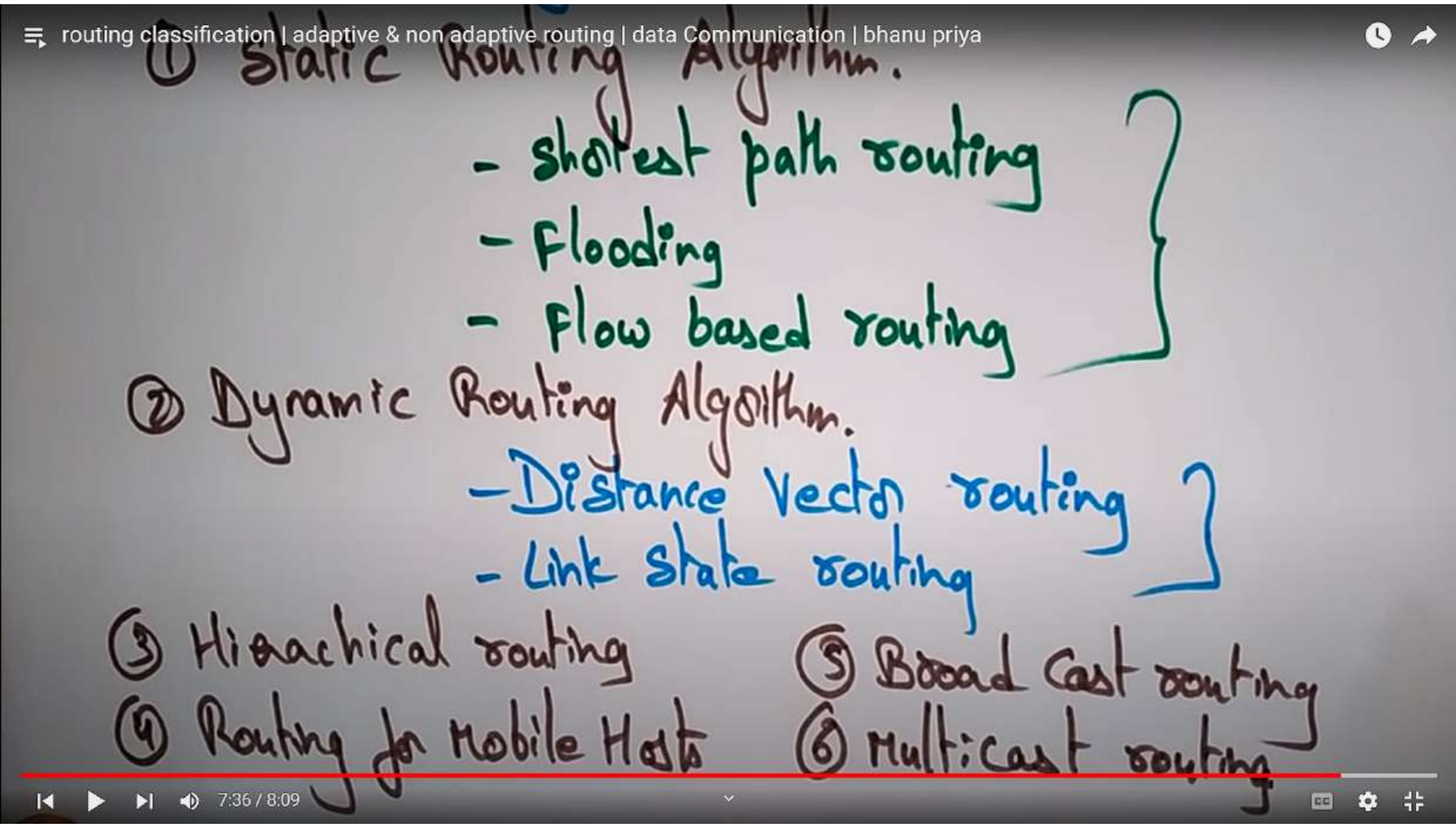


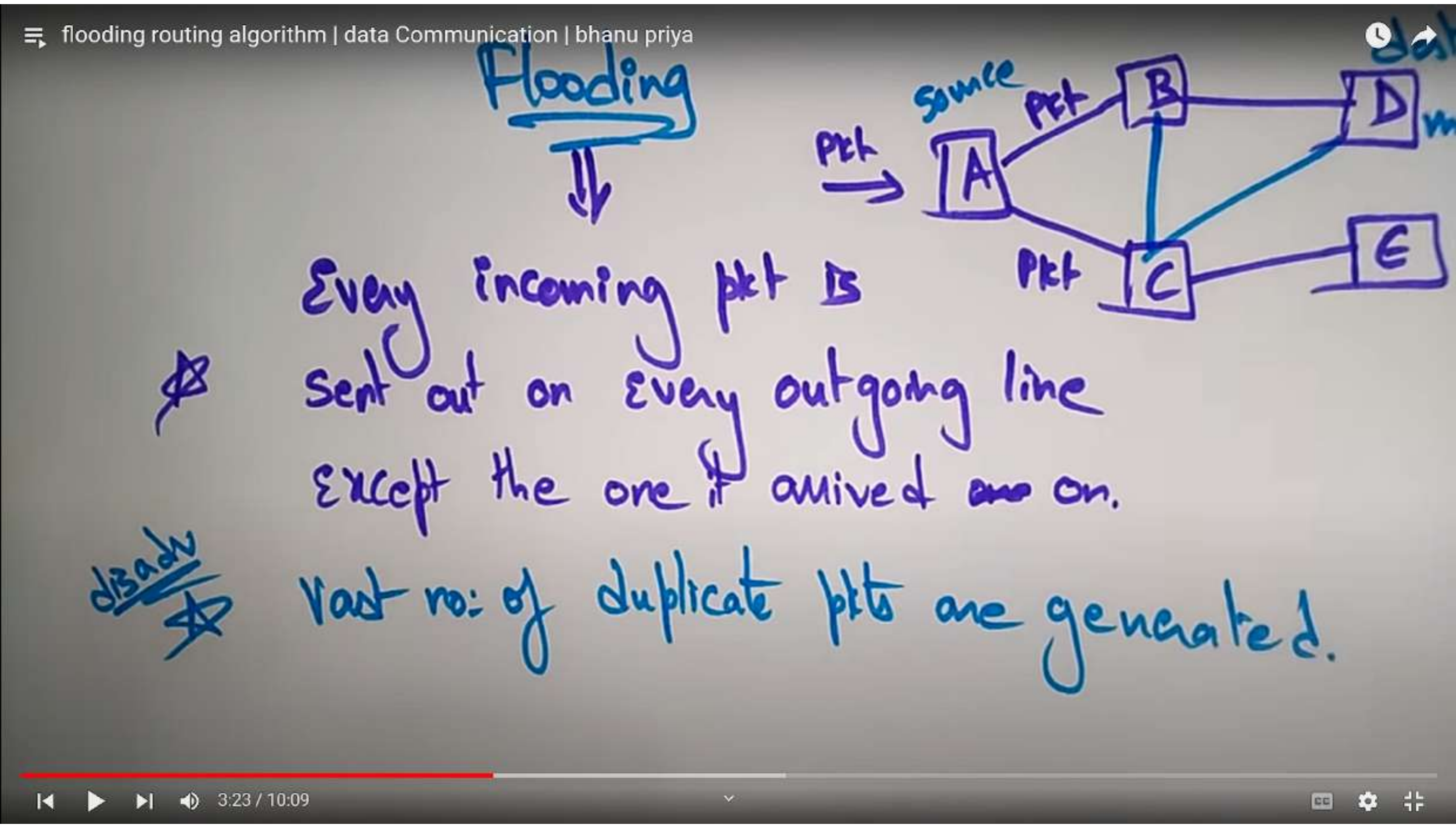
③ Robustness :- The ability to withstand the sys over a years.

④ stability :- routing alg should be stable under all circumstances

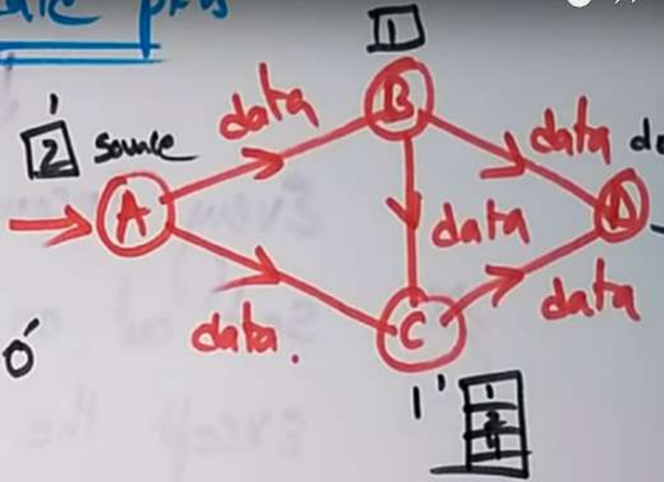

routing classification | adaptive & non adaptive routing | data Communication | bhanu priya
→ Adaptive Routing
(dynamic)
→ Non Adaptive Routing
(static)
changes routes dynamically
* gathers inf at runtime
- locally
- from adjacent routers
- from all other routers
* changes routes
every delta T seconds
- when load changes,
when topology changes.
3:24 / 8:09


routing classification | adaptive & non adaptive routing | data Communication | bhanu priya
→ Adaptive Routing
(dynamic)
changes routes dynamically
* gathers inf at runtime
- locally
- from adjacent routers
- from all other routers
* changes routes
every delta T seconds
→ Non Adaptive Routing
(static)
choice of route is computed in advance, offline & downloaded to the routers when the n/w is booted.
5:25 / 8:09


routing classification | adaptive & non adaptive routing | data Communication | bhanu priya
① Static Routing Algorithm.
- shortest path routing
- Flooding
- Flow based routing
② Dynamic Routing Algorithm.
- Distance Vector routing
- Link state routing
③ Hierachical routing
④ Routing for mobile Hosts
⑤ Broad Cast routing
⑥ Multicast routing
7:36 / 8:09


flooding routing algorithm | data Communication | bhanu priya
Flooding
Every incoming pkt is
sent out on every outgoing line
except the one it arrived on.
disadv
vast no: of duplicate pkts are generated.
source
pkt
A
B
C
D
E
3:23 / 10:09

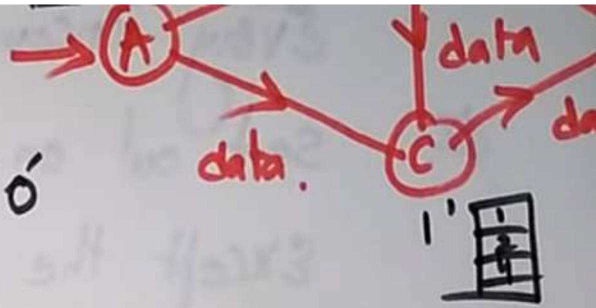
How to stop & Eliminate duplicate pkts



① using a hop counter
- decrement in Each router
- discard pkt if counter is '0'

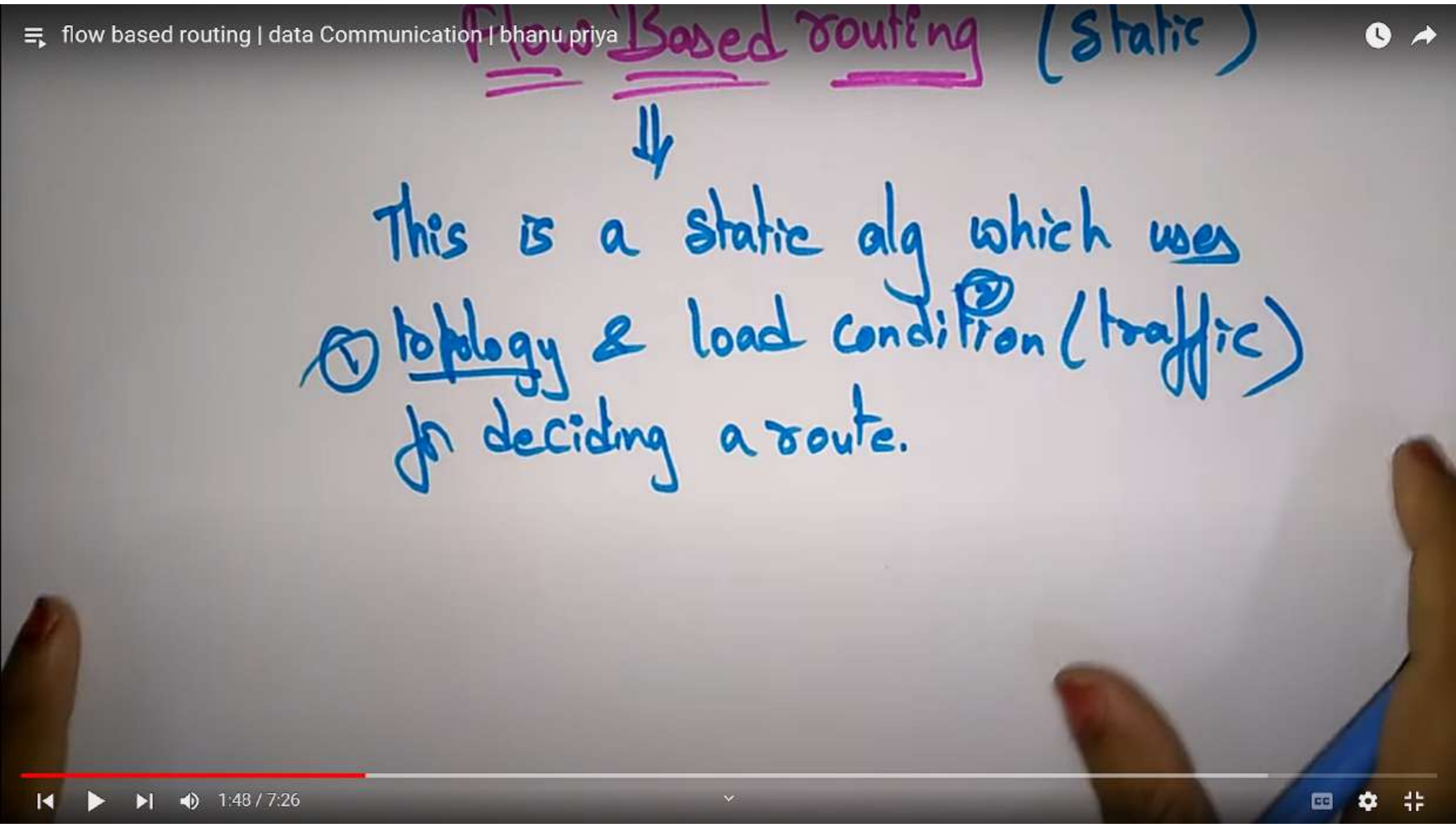
② sequence no: in pkt
- avoid sending the same pkt second time
- keep in Each router per source a lists of pkts already seen

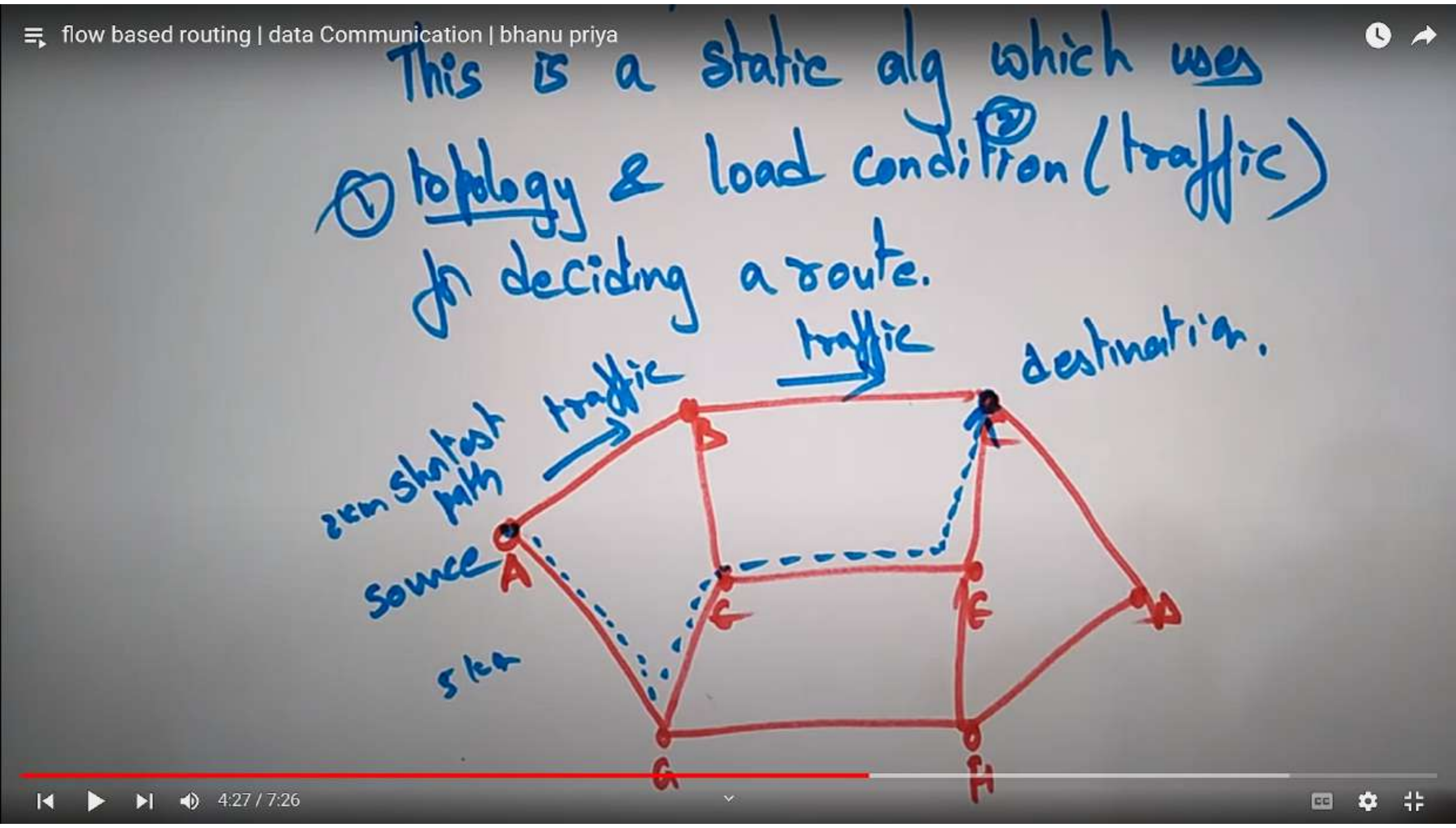
- decrement in Each router
- discard pkt if counter is '0'

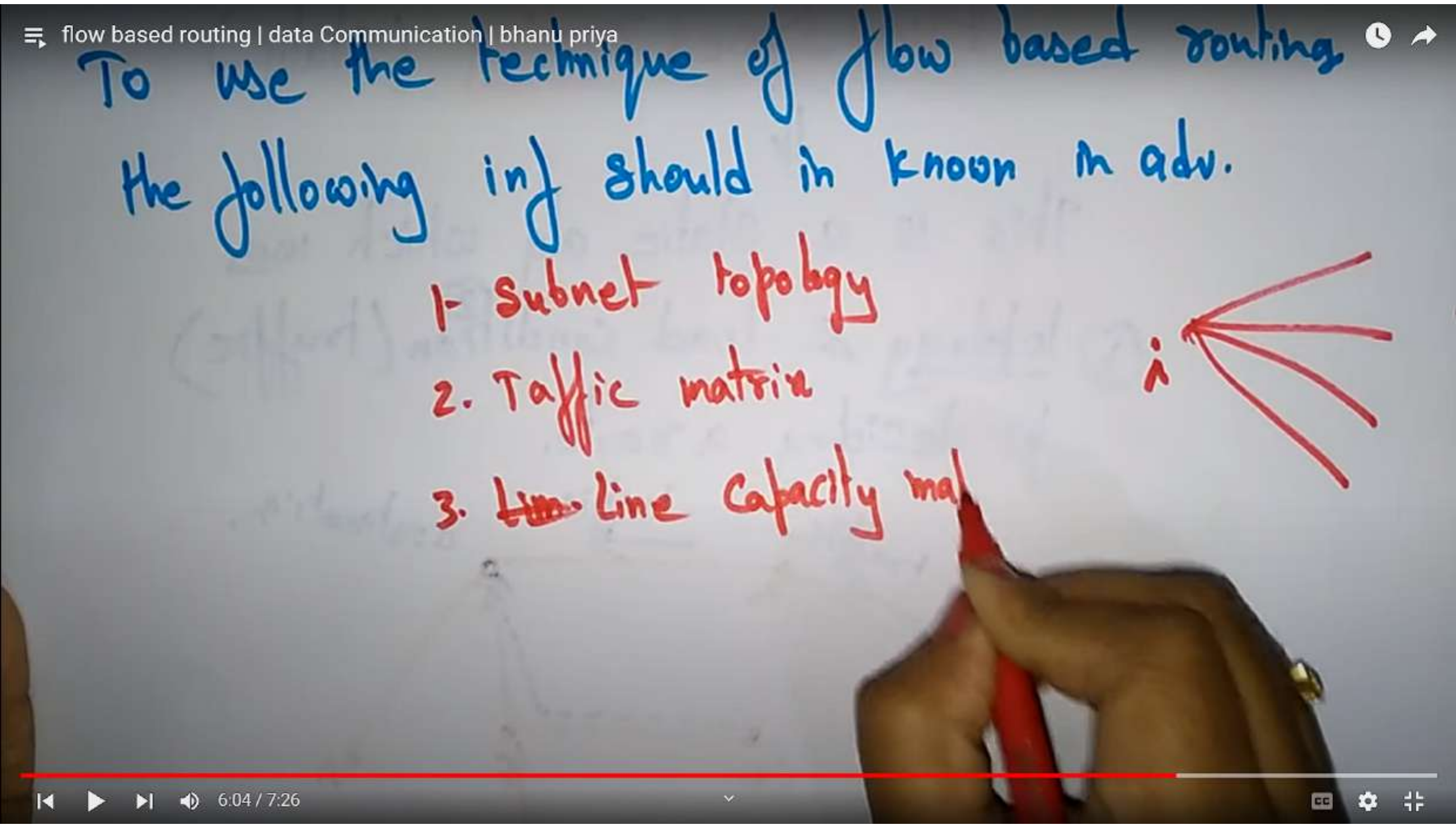


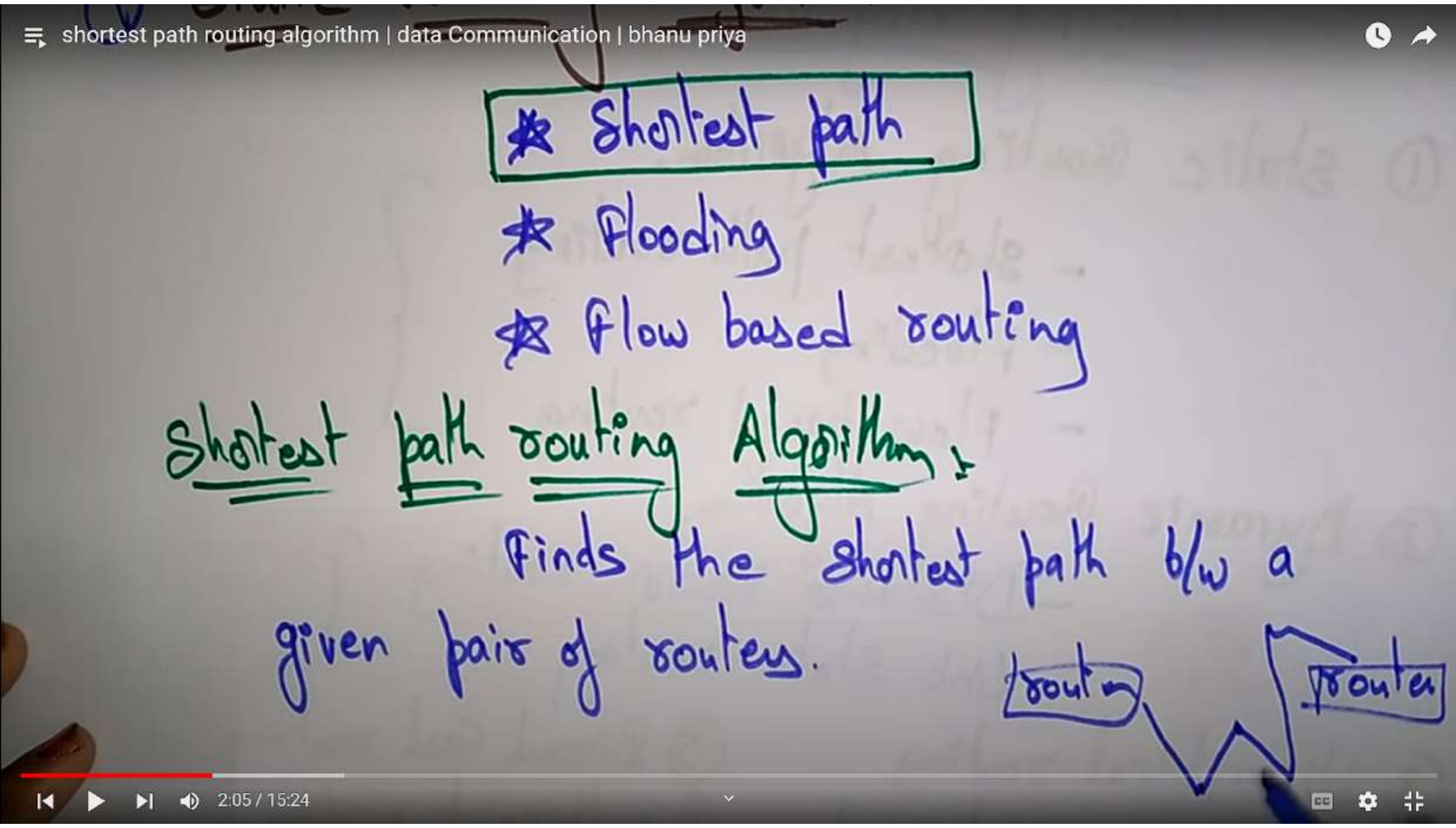
② sequence no: in pkt
- avoid sending the same pkt second time
- keep in Each router per source a lists of pkts already seen

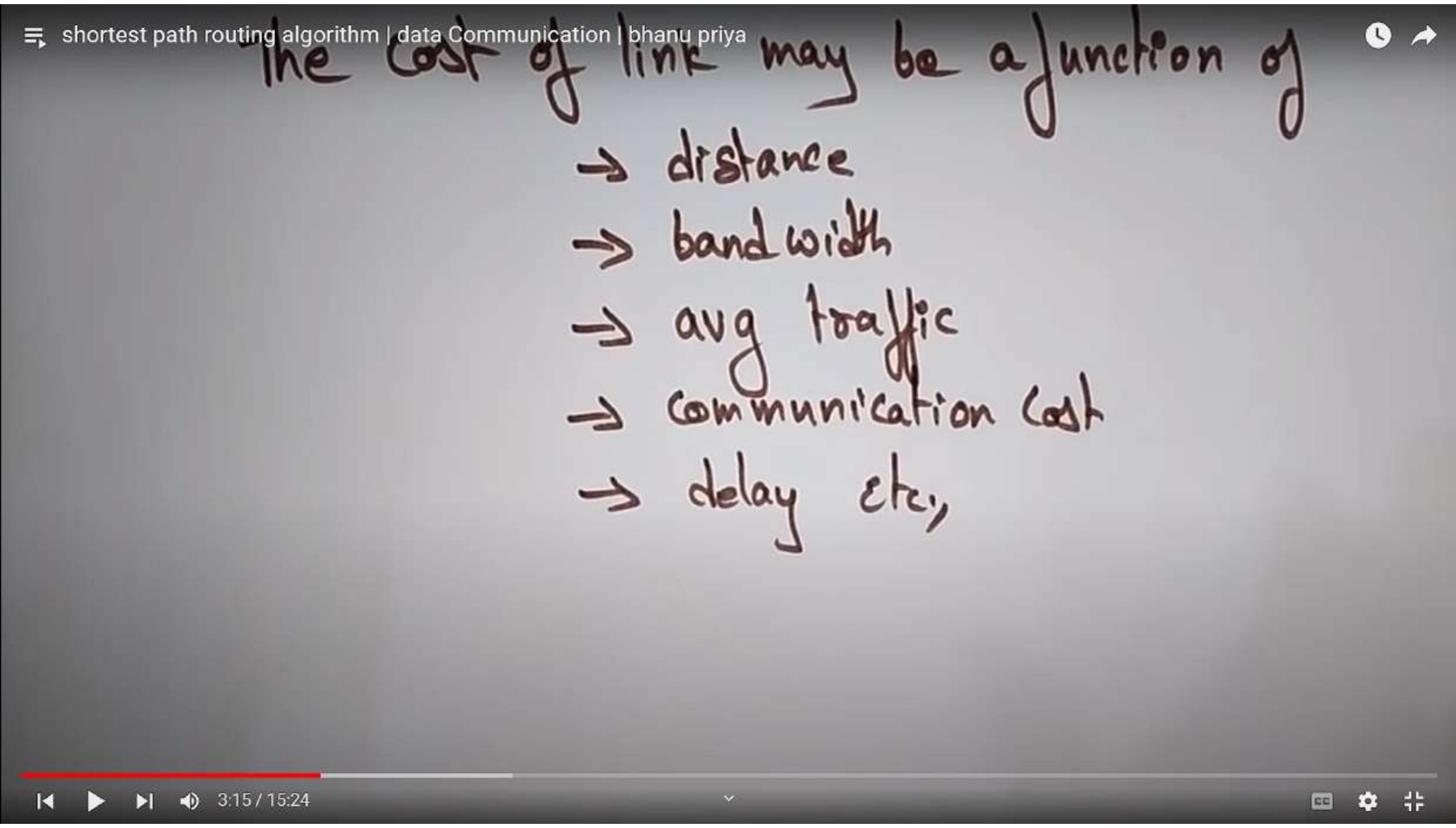
③ Selective flooding:
- use only those lines that are going approximately in right direction.

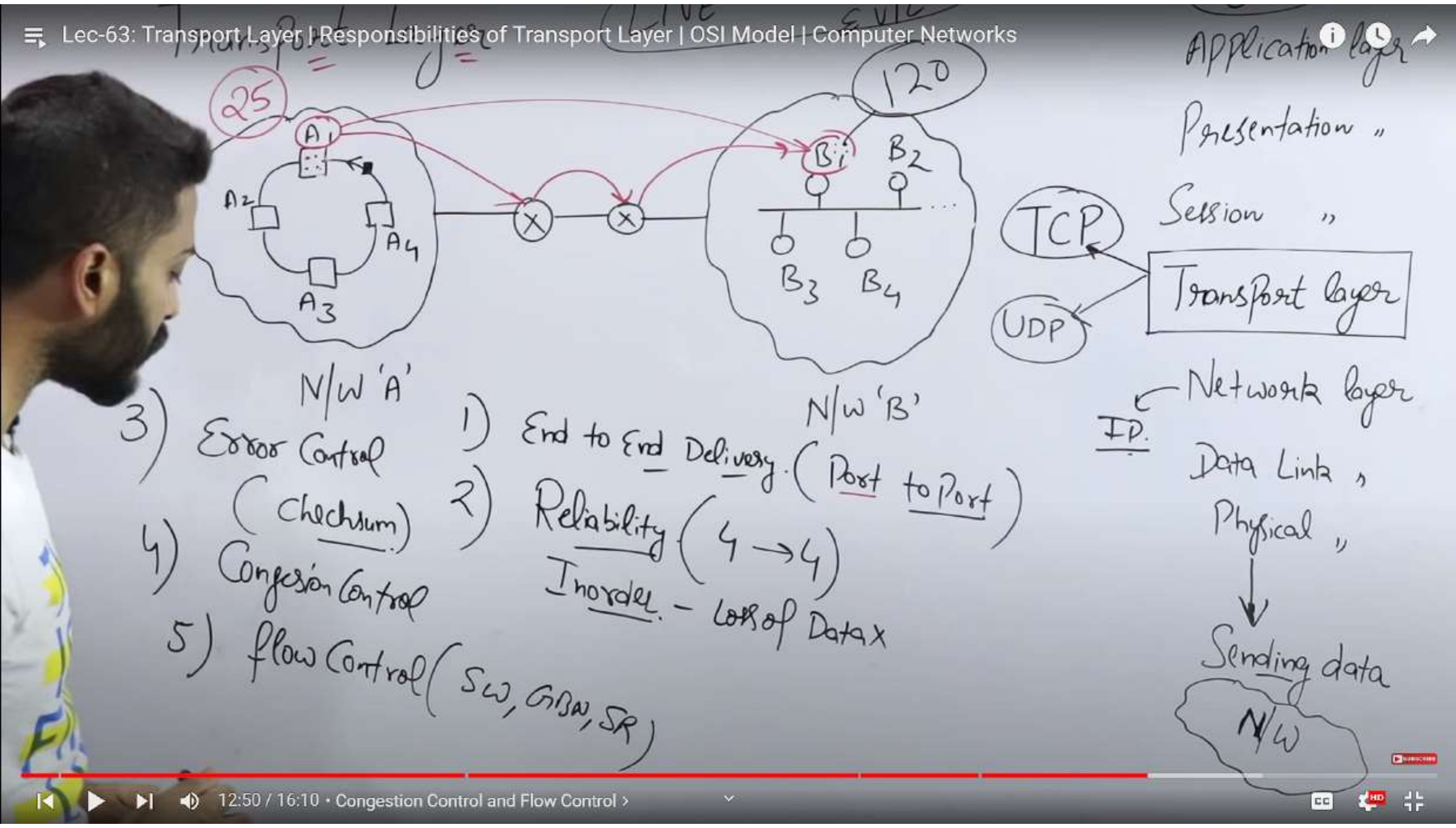

flow based routing | data Communication | bhanu priya
Flow Based routing (static)
This is a static alg which uses
① topology & ② load condition (traffic)
for deciding a route.
1:48 / 7:26


flow based routing | data Communication | bhanu priya
This is a static alg which uses
① topology & ② load condition (traffic)
for deciding a route.
traffic
traffic
destination.
2km shortest path
source
5 km
A
B
C
D
E
F
G
H
4:27 / 7:26

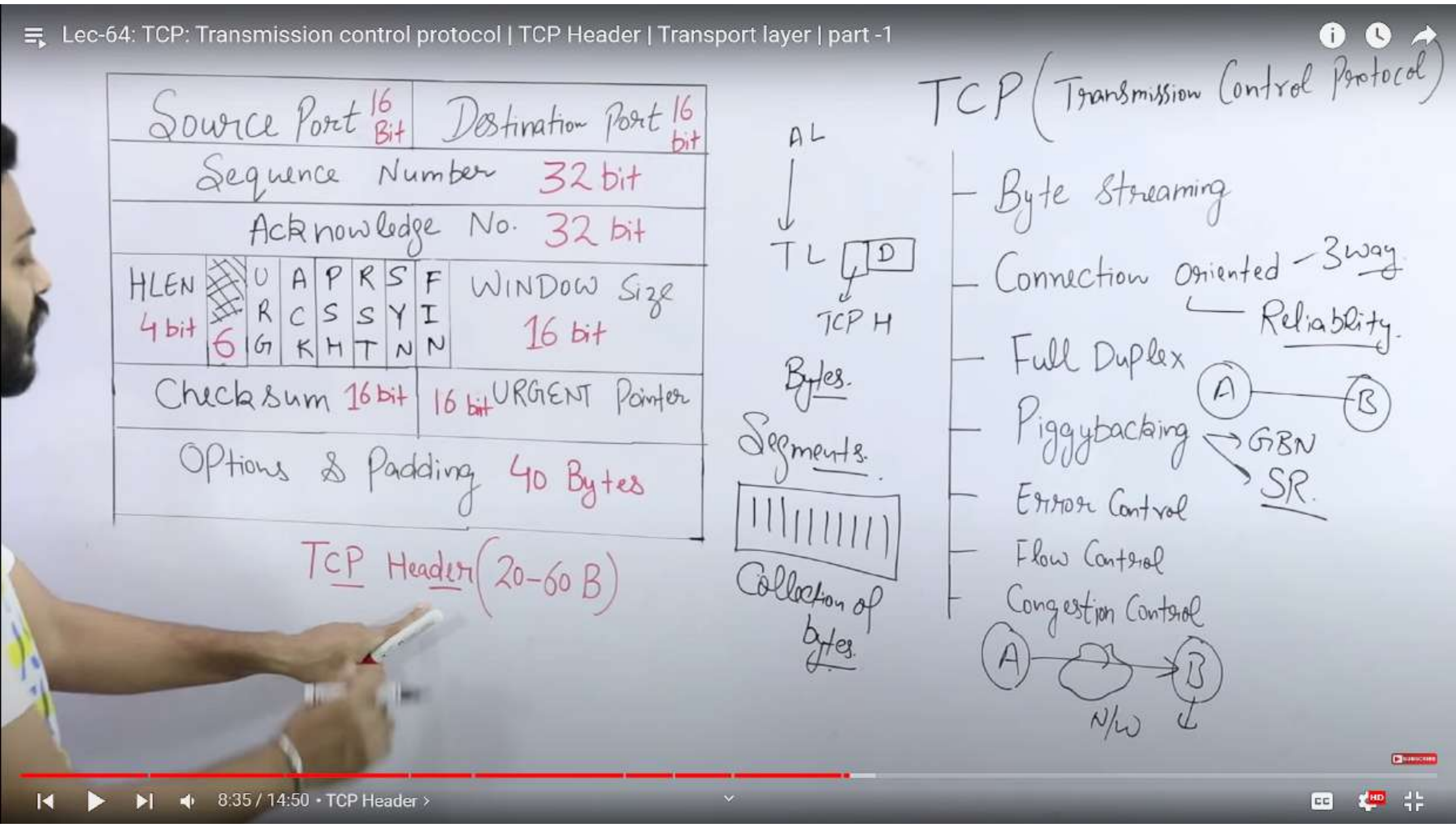

flow based routing | data Communication | bhanu priya
To use the technique of flow based routing
the following inf should in known in adv.
1. Subnet topology
2. Taffic matrix
3. Lin Line Capacity ma
i
6:04 / 7:26

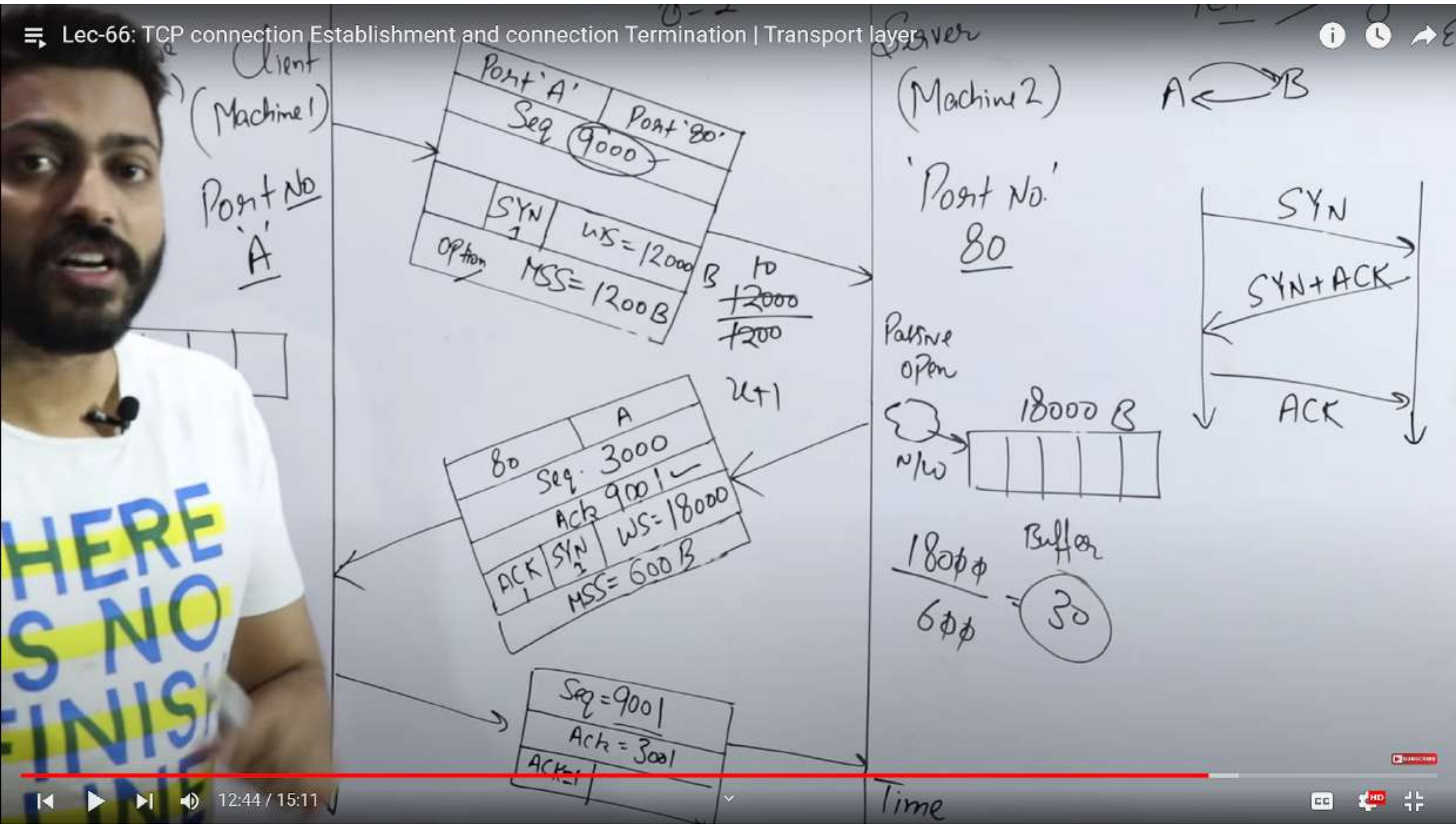

shortest path routing algorithm | data Communication | bhanu priya
* Shortest path
* Flooding
* Flow based routing
Shortest path routing Algorithm :
Finds the shortest path b/w a given pair of routers.
router
router
2:05 / 15:24

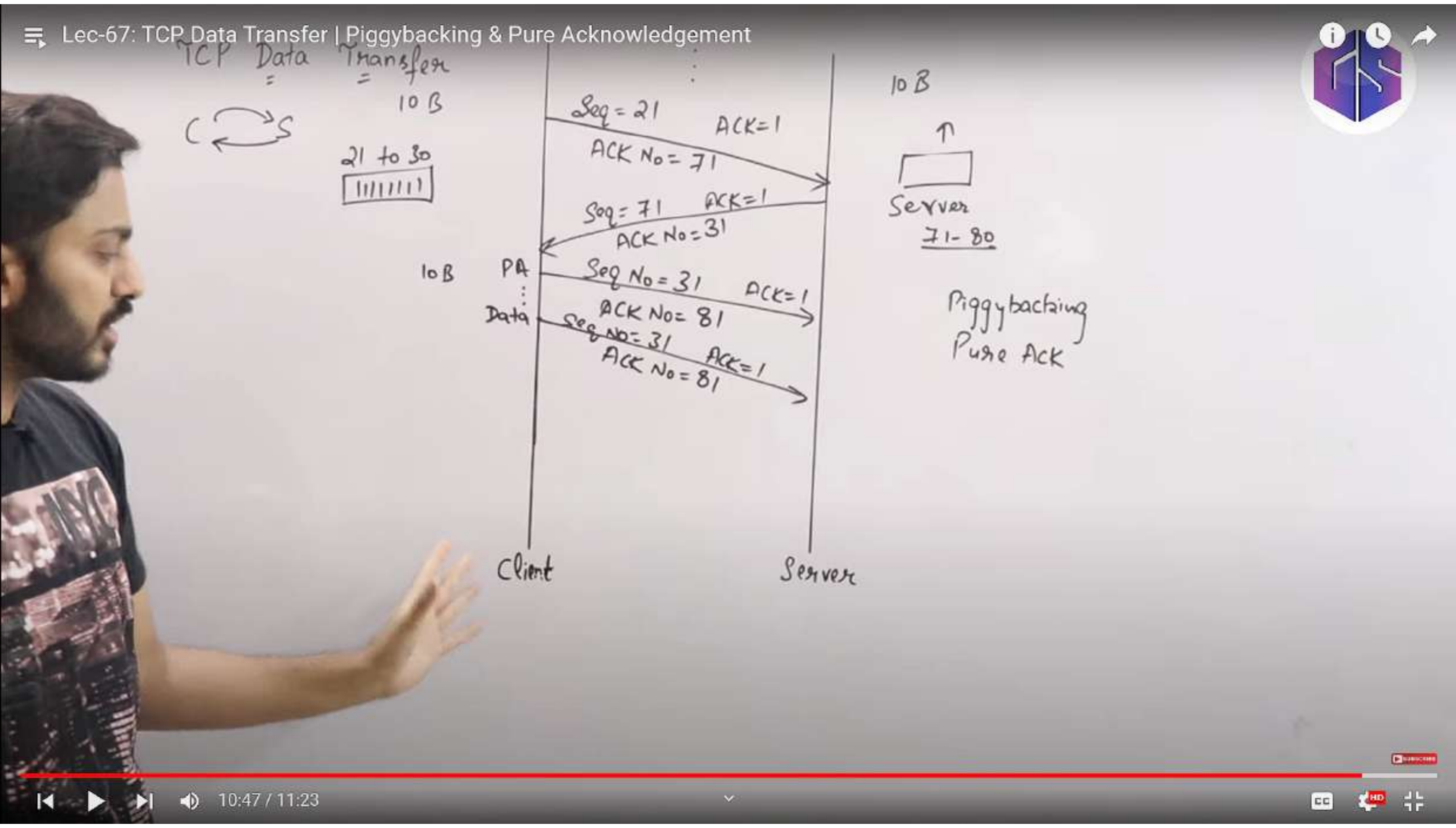

shortest path routing algorithm | data Communication | bhanu priya
The cost of link may be a function of
→ distance
→ bandwidth
→ avg traffic
→ communication cost
→ delay etc,
3:15 / 15:24

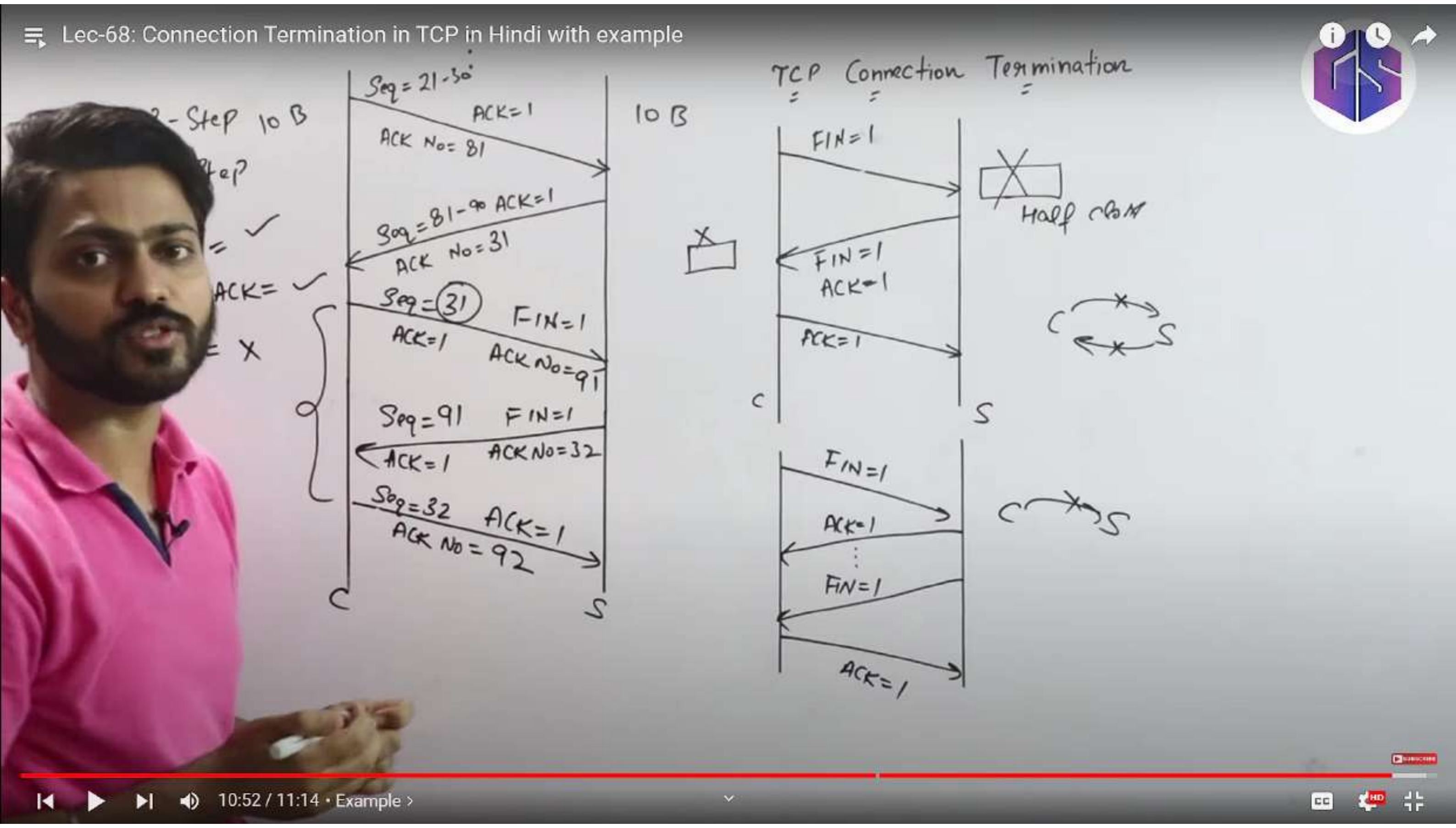


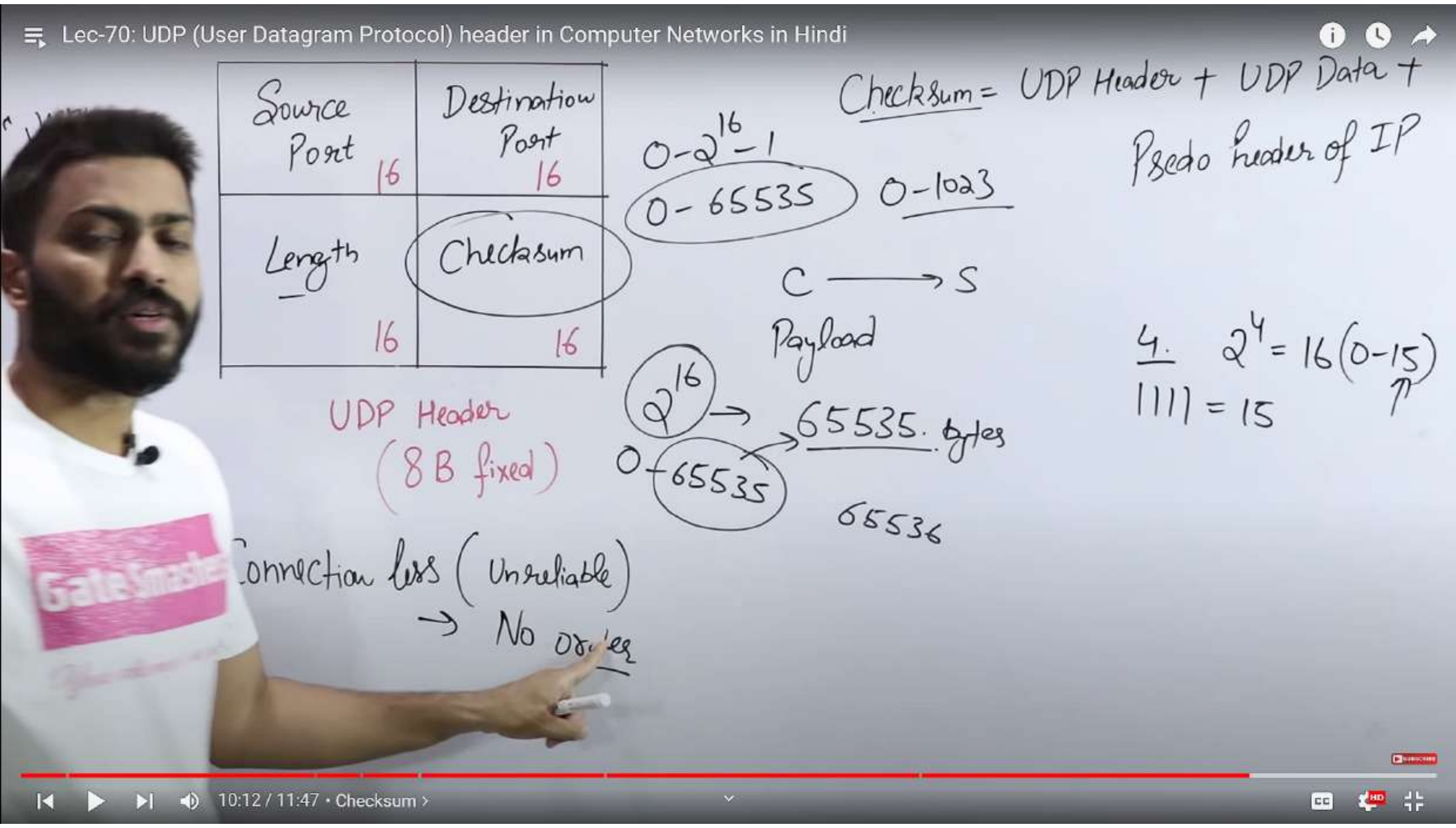
Lec-63: Transport Layer | Responsibilities of Transport Layer | OSI Model | Computer Networks
25
120
A1
A2
A3
A4
B1
B2
B3
B4
N/W 'A'
N/W 'B'
1) End to End Delivery. (Port to Port)
2) Reliability (4 → 4)
Inorder - Loss of Data X
3) Error Control
(Checksum)
4) Congesion Control
5) flow Control (SW, GBN, SR)
Application layer
Presentation "
Session "
Transport layer
TCP
UDP
Network layer
IP.
Data Link "
Physical "
Sending data
N/W
12:50 / 16:10 • Congestion Control and Flow Control ›

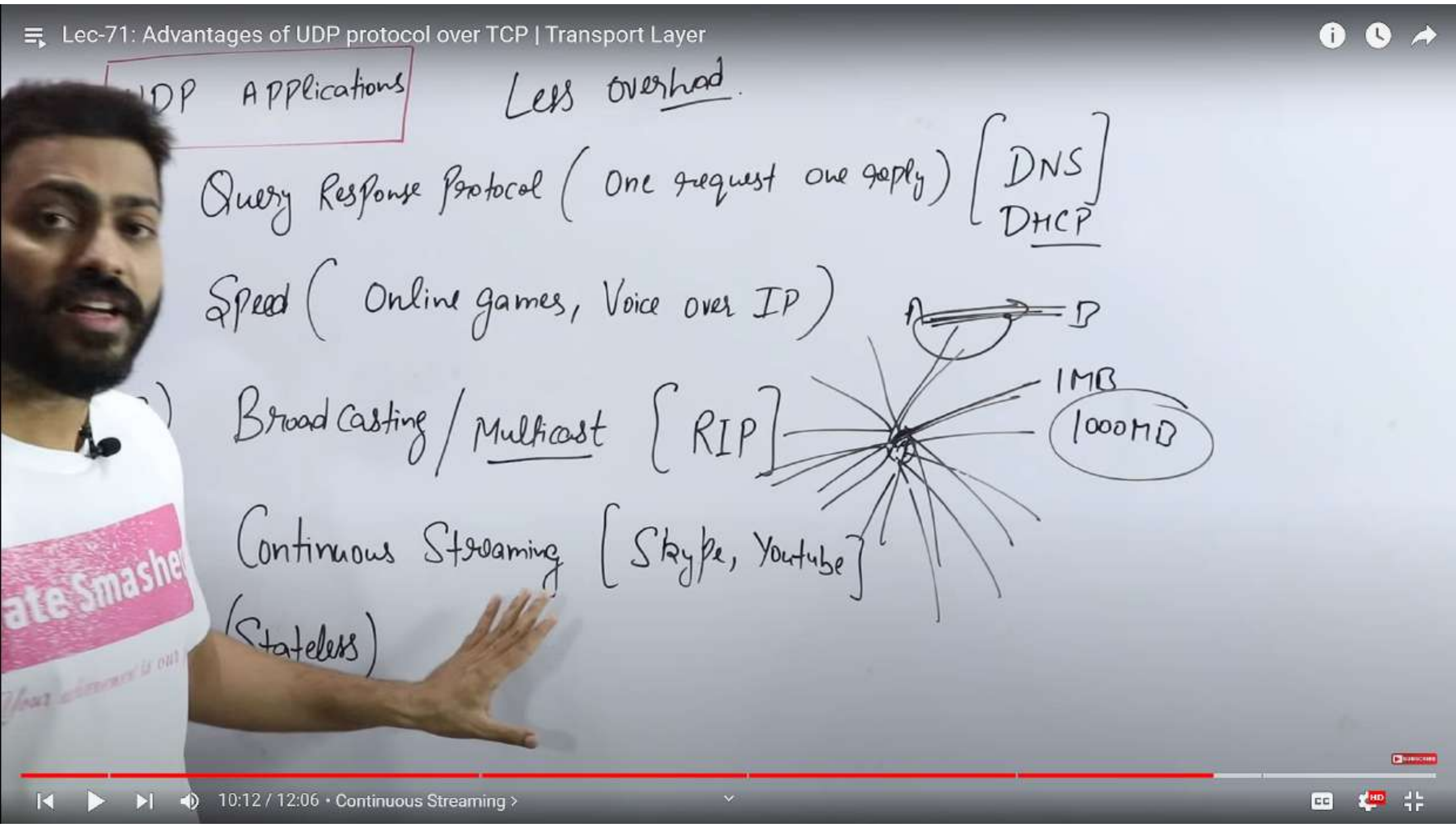

Lec-64: TCP: Transmission control protocol | TCP Header | Transport layer | part -1
Source Port 16 Bit
Destination Port 16 bit
Sequence Number 32 bit
Acknowledge No. 32 bit
HLEN 4 bit
6
URG ACK PSH RST SYN FIN
WINDOW Size 16 bit
Checksum 16 bit
16 bit URGENT Pointer
Options & Padding 40 Bytes
TCP Header (20-60 B)
AL
TL
D
TCP H
Bytes.
Segments.
Collection of bytes.
TCP (Transmission Control Protocol)
Byte streaming
Connection Oriented
3 way
Reliability.
Full Duplex
A
B
Piggybacking
GBN
SR.
Error Control
Flow Control
Congestion Control
N/W
8:35 / 14:50 • TCP Header ›


Lec-66: TCP connection Establishment and connection Termination | Transport layer
Client
(Machine 1)
Port No
'A'
Port 'A'
Port '80'
Seq 9000
SYN 1
WS = 12000 B
Option
MSS = 1200 B
10
12000
1200
x+1
80
A
Seq. 3000
Ack 9001
ACK 1
SYN 1
WS = 18000
MSS = 600 B
Seq = 9001
Ack = 3001
ACK = 1
Server
(Machine 2)
'Port No.'
80
Passive open
N/W
18000 B
Buffer
18000
600
= 30
A
B
SYN
SYN+ACK
ACK
Time
12:44 / 15:11

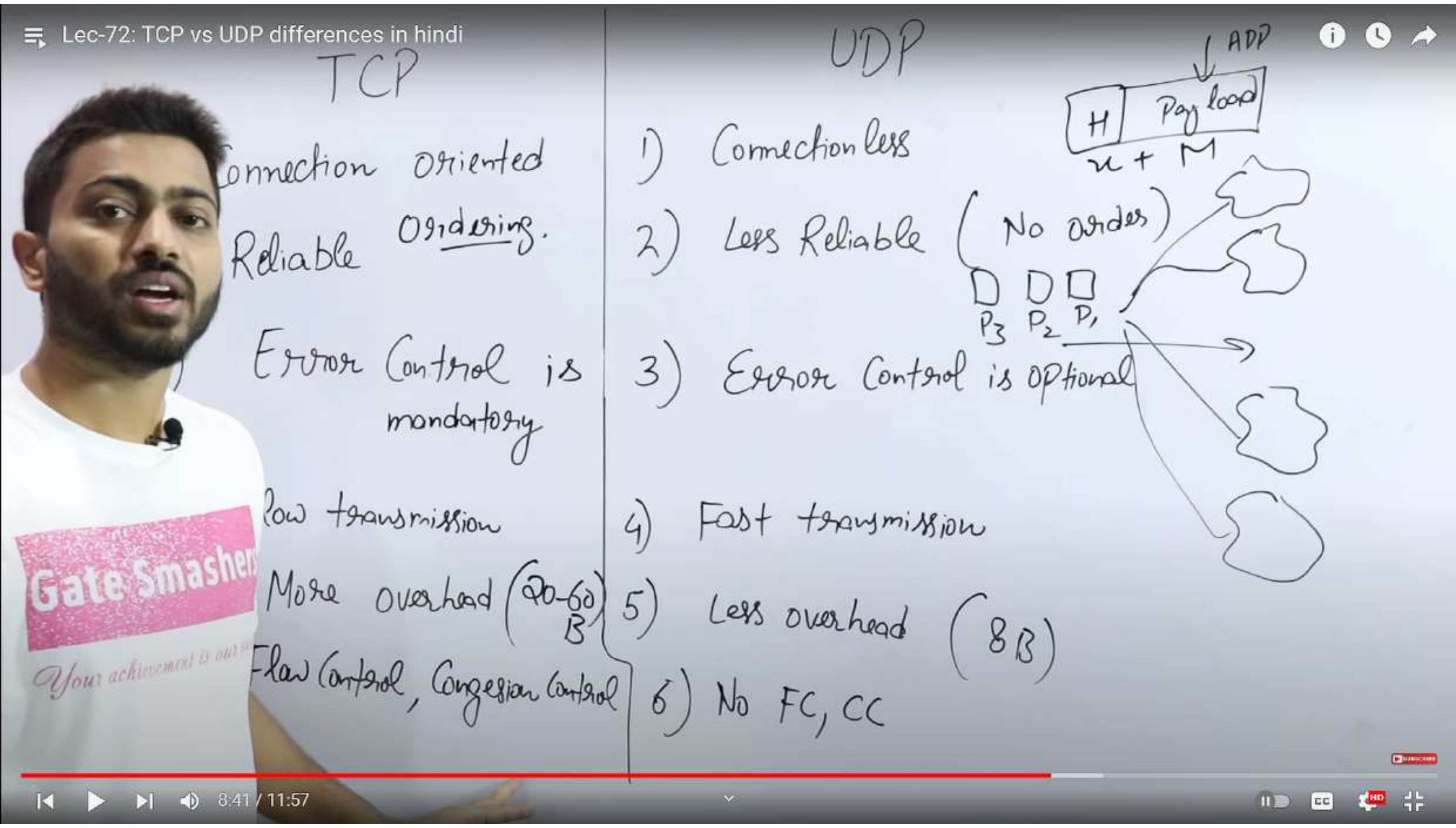

Lec-67: TCP Data Transfer | Piggybacking & Pure Acknowledgement
TCP Data Transfer
C S
10 B
21 to 30
Seq = 21
ACK = 1
ACK No = 71
Seq = 71
ACK = 1
ACK No = 31
10 B
PA
Seq No = 31
ACK = 1
ACK No = 81
Data
Seq No = 31
ACK = 1
ACK No = 81
Client
Server
10 B
Server
71 - 80
Piggybacking
Pure ACK
10:47 / 11:23

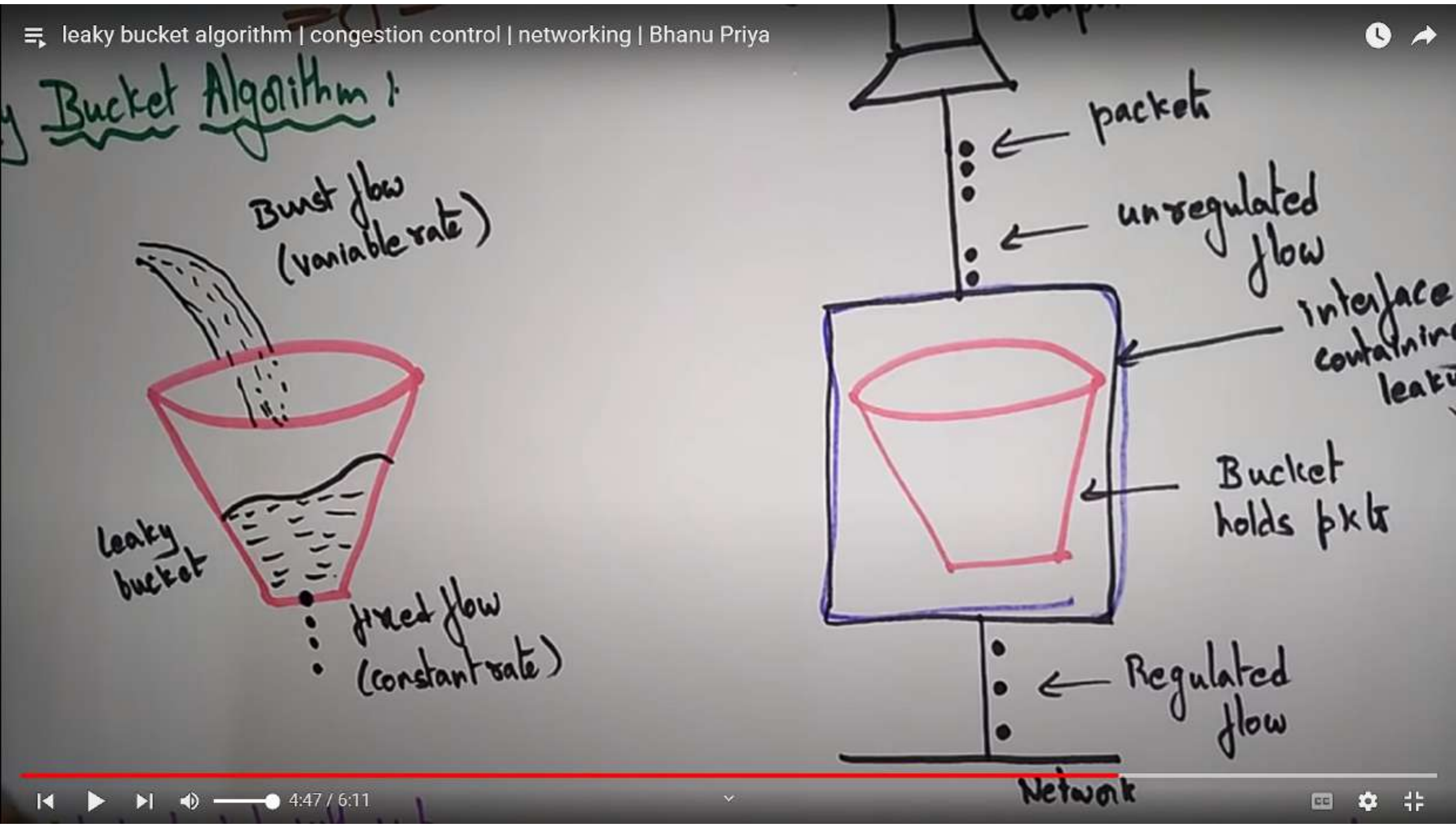

Lec-68: Connection Termination in TCP in Hindi with example
TCP Connection Termination
Seq = 21-30
ACK=1
ACK No= 81
10 B
Seq = 81-90 ACK=1
ACK No=31
Seq = 31
FIN=1
ACK=1
ACK No=91
Seq=91
FIN=1
ACK=1
ACK No=32
Seq=32
ACK=1
ACK No = 92
C
S
FIN=1
FIN=1
ACK=1
ACK=1
Half close
FIN=1
ACK=1
FIN=1
ACK=1
10:52 / 11:14 · Example

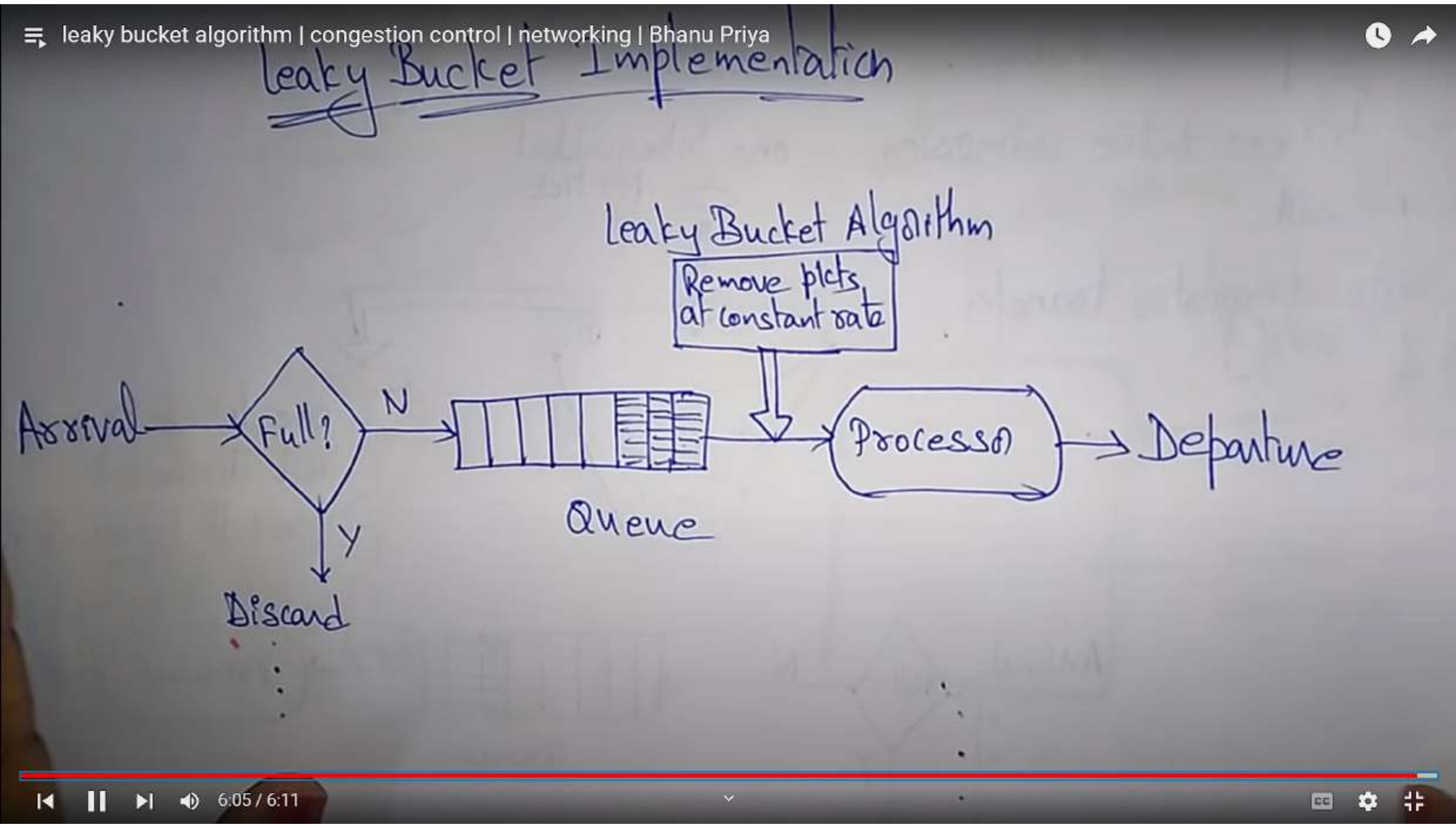

Lec-70: UDP (User Datagram Protocol) header in Computer Networks in Hindi
Source Port 16
Destination Port 16
Length 16
Checksum 16
UDP Header
(8 B fixed)
Connection less (Unreliable)
→ No order
0-2^16-1
0-65535
0-1023
C → S
Payload
2^16 → 65535. bytes
0-65535
65536
Checksum = UDP Header + UDP Data +
Psedo header of IP
4. 2^4 = 16 (0-15)
1111 = 15
10:12 / 11:47 • Checksum



Lec-71: Advantages of UDP protocol over TCP | Transport Layer
DP Applications
Less overhead.
Query Response Protocol (One request one reply) [DNS DHCP]
Speed (Online games, Voice over IP)
A
B
Broad Casting / Multicast [RIP]
1MB
1000MB
Continuous Streaming [Skype, Youtube]
(Stateless)
ate Smashe
10:12 / 12:06 • Continuous Streaming >


Lec-72: TCP vs UDP differences in hindi
TCP
onnection oriented
Reliable Ordering.
Error Control is mandatory
low transmission
More overhead (20-60 B)
Flow Control, Congesion Control
UDP
1) Connection less
2) Less Reliable (No order)
3) Error Control is optional
4) Fast transmission
5) Less overhead (8 B)
6) No FC, CC
ADP
H
Pay load
P3 P2 P1
Gate Smashers
8:41 / 11:57


leaky bucket algorithm | congestion control | networking | Bhanu Priya
Bucket Algorithm :
Burst flow
(variable rate)
leaky
bucket
fixed flow
(constant rate)
packets
unregulated
flow
Bucket
holds pkts
Regulated
flow
Network
4:47 / 6:11


leaky bucket algorithm | congestion control | networking | Bhanu Priya
Leaky Bucket Implementation
Leaky Bucket Algorithm
Remove pkts at constant rate
Arrival
Full?
N
Y
Discard
Queue
Processor
Departure
6:05 / 6:11

Quality of Service:- In QOS, we try to create an appropriate environment for the traffic.

Flow characteristics:-

↳ Reliability → Lack of Reliability means Losing or acknowledgment.

↳ Delay → Source to destination delay.

S 0 —— 4_D [4]

↳ Jitter → Variation in Delay.

$$P \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix} \qquad D \left.\begin{matrix} 4 \\ 5 \\ 6 \\ 7 \end{matrix}\right] 4 \qquad \left|\begin{matrix} 4 : 4 \\ 6 : 5 \\ 10 : 8 \\ 15 : 12 \end{matrix}\right] \text{jitter.}$$

↳ Bandwidth

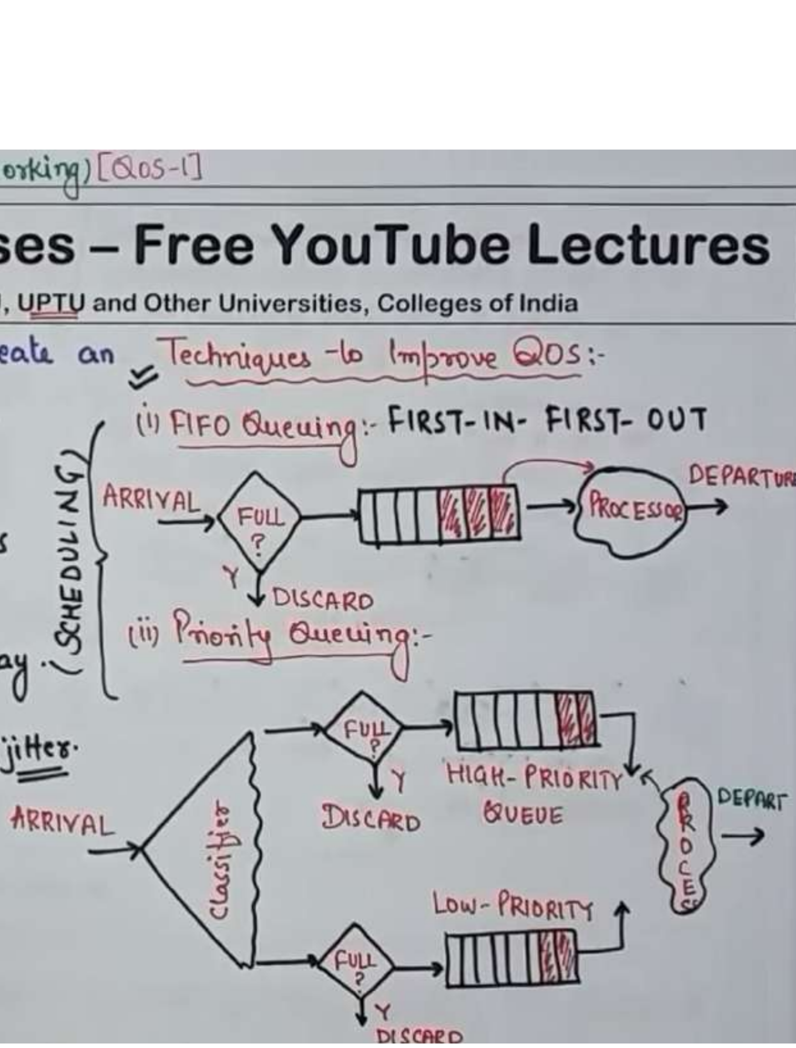
↳ Different Appl^n Requires diff. Bandwidth.

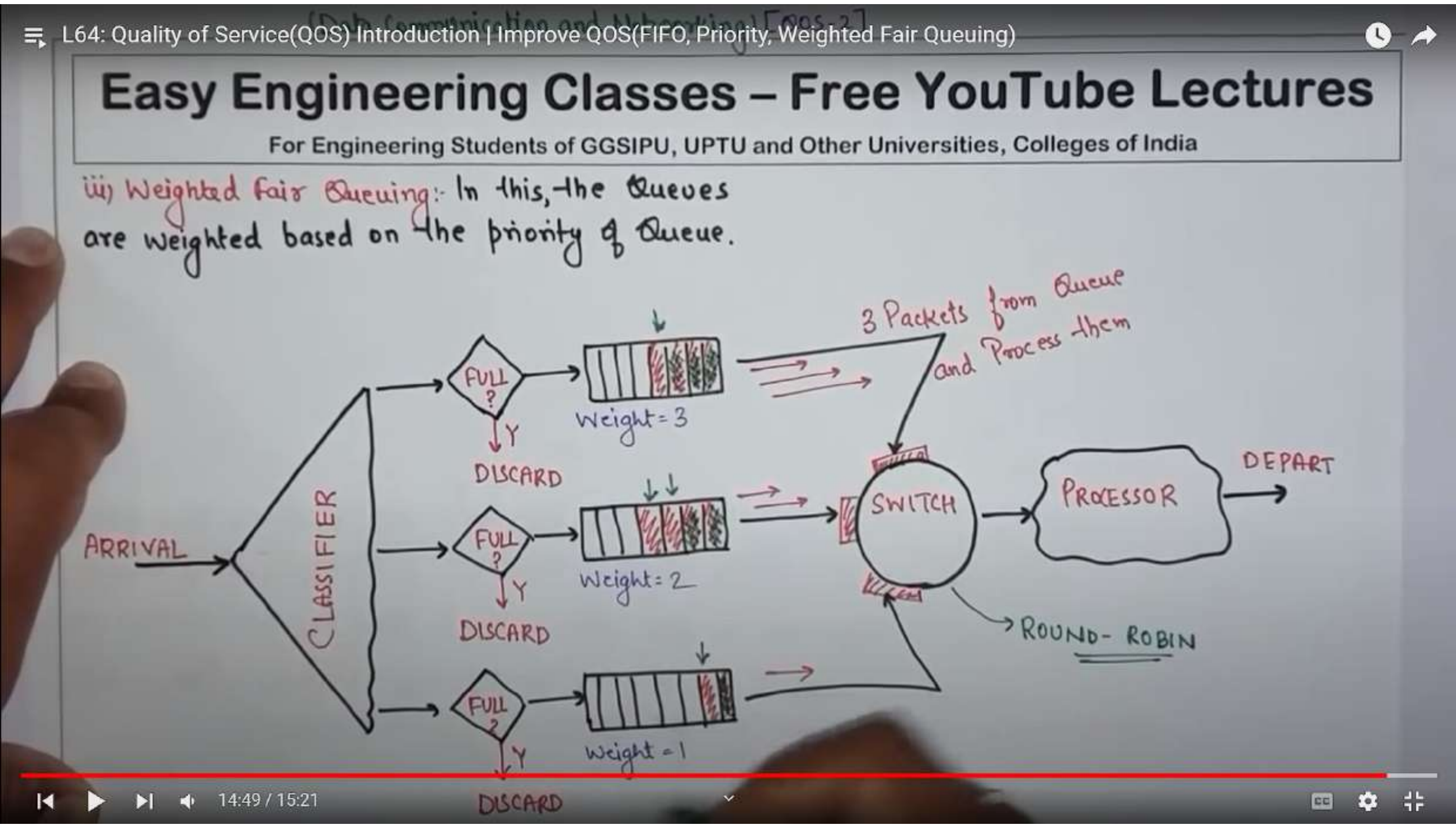
Techniques to Improve QOS:-

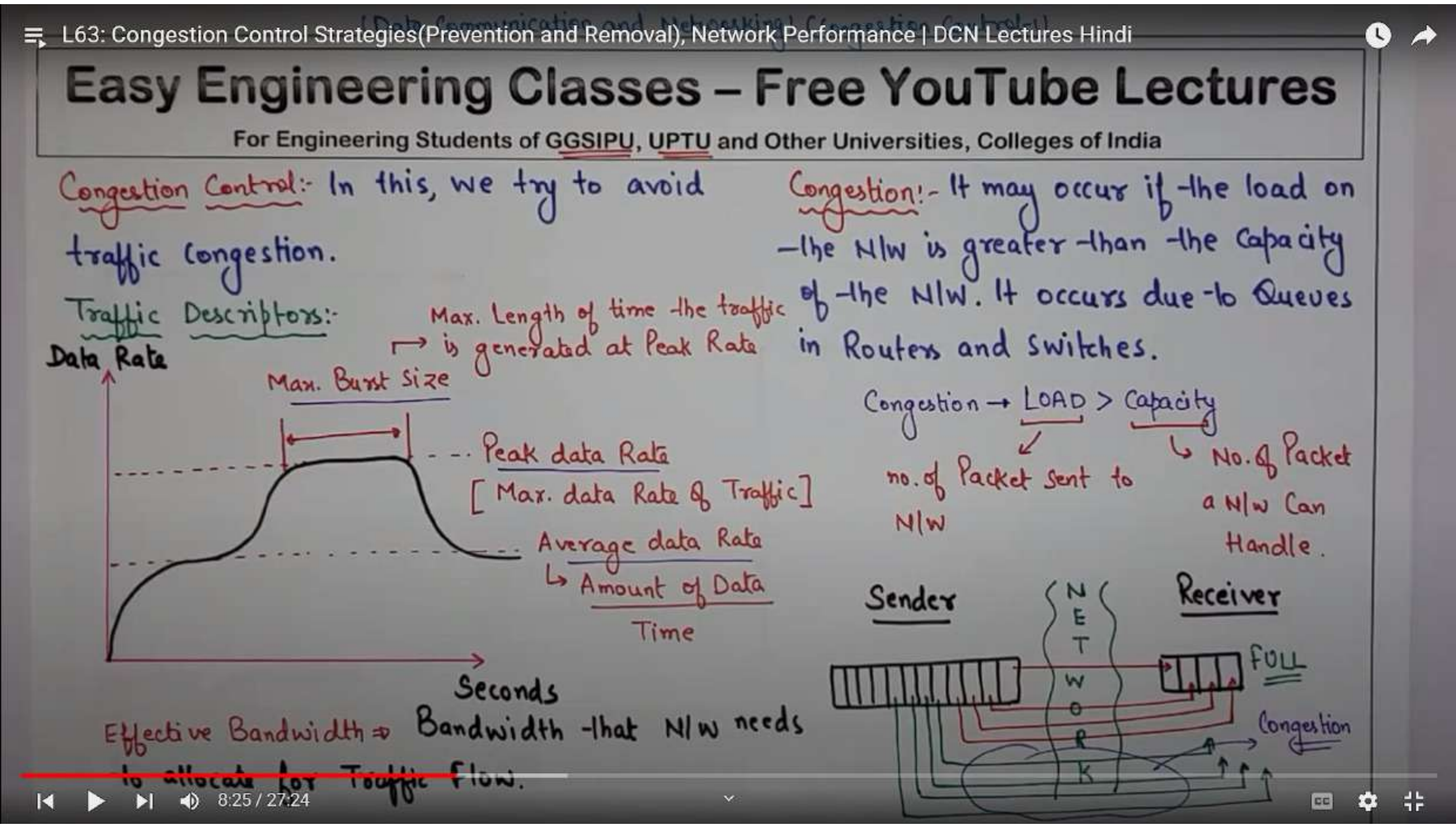
(SCHEDULING)

(i) FIFO Queuing:- FIRST-IN-FIRST-OUT

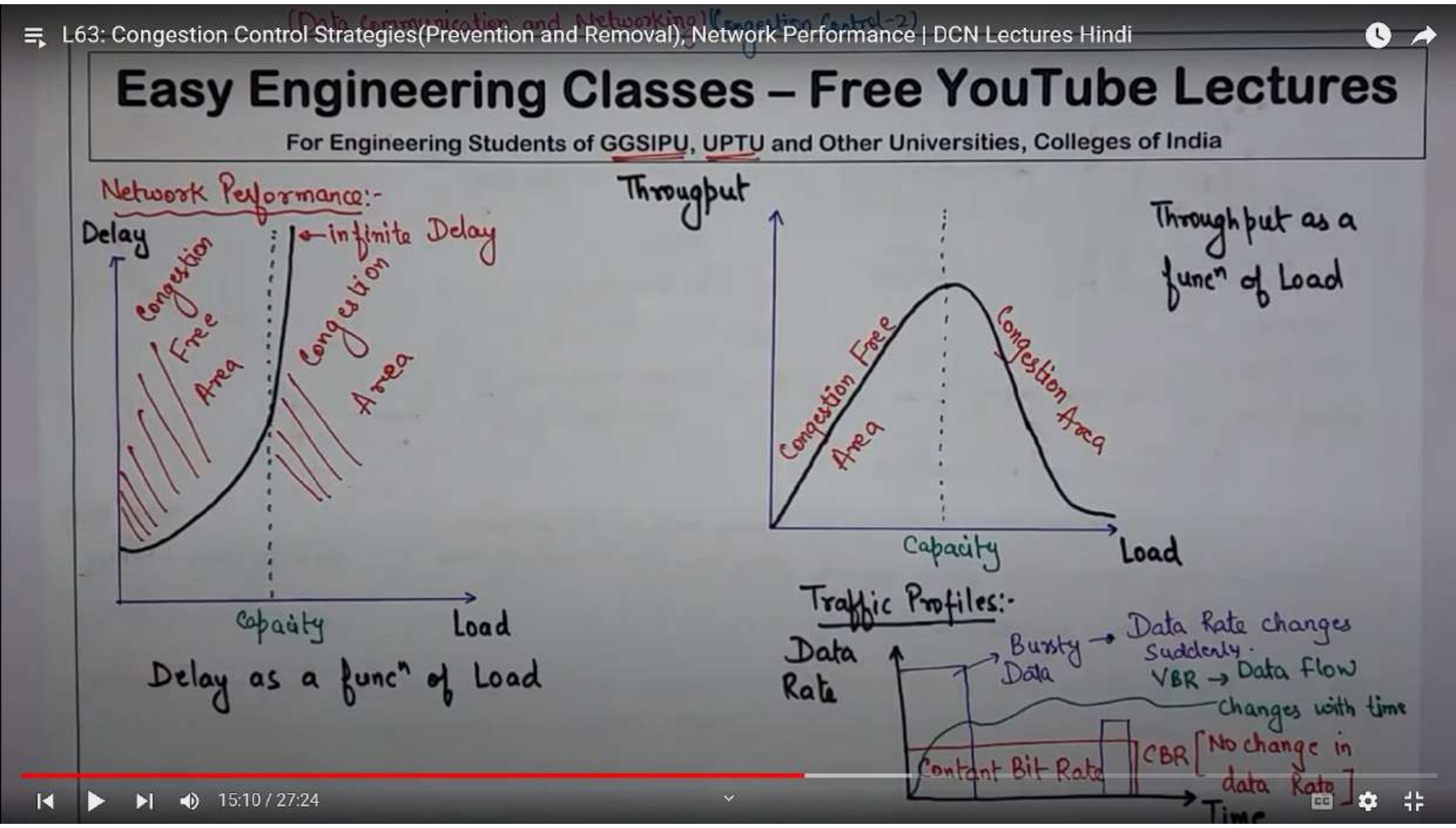
(ii) Priority Queuing:-

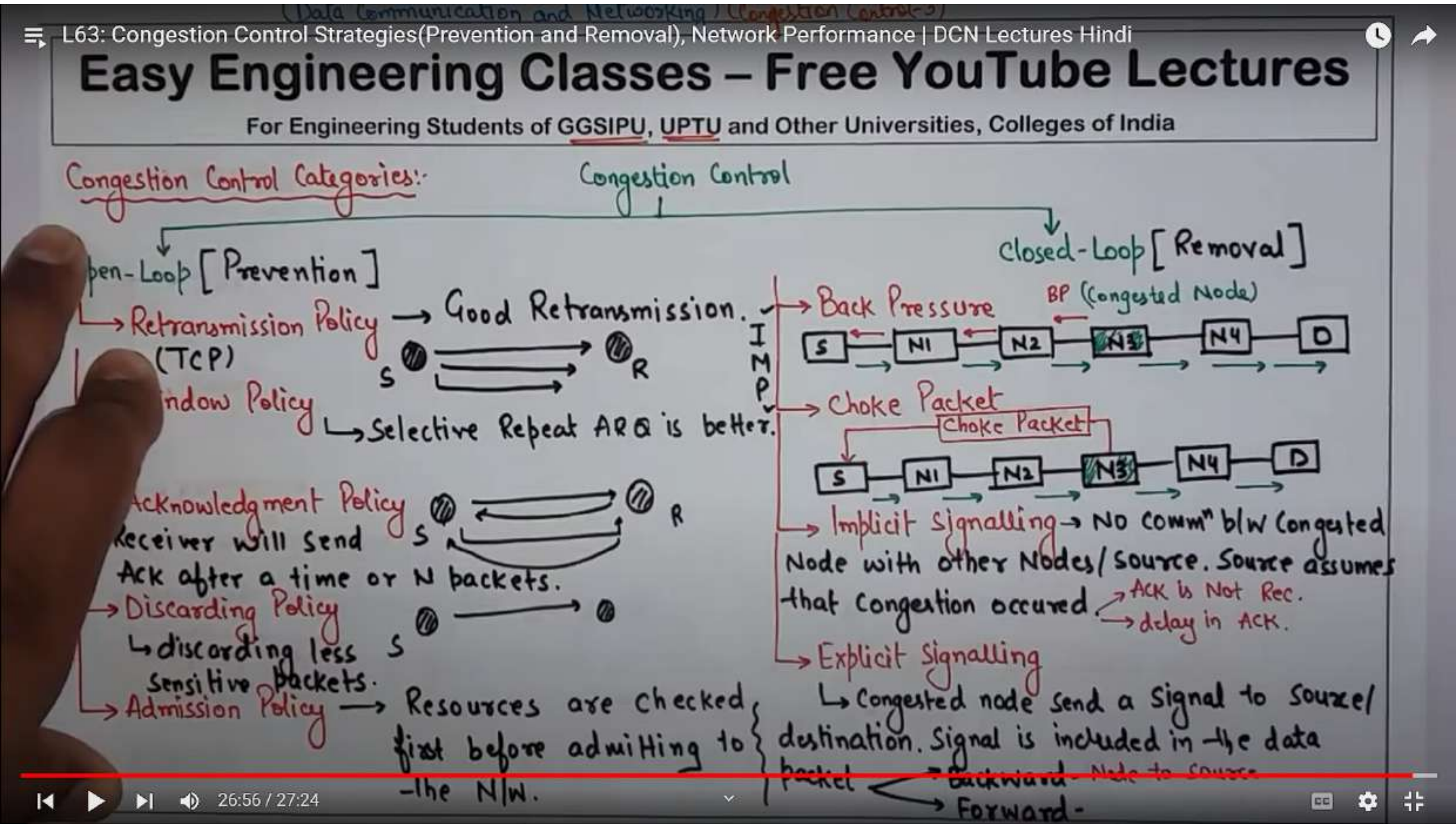



L64: Quality of Service(QOS) Introduction | Improve QOS(FIFO, Priority, Weighted Fair Queuing)
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
iii) Weighted fair Queuing:- In this, the Queues are weighted based on the priority of Queue.
3 Packets from Queue and Process them
ARRIVAL
CLASSIFIER
FULL ?
Y
DISCARD
Weight = 3
Weight = 2
Weight = 1
SWITCH
PROCESSOR
DEPART
ROUND- ROBIN
14:49 / 15:21



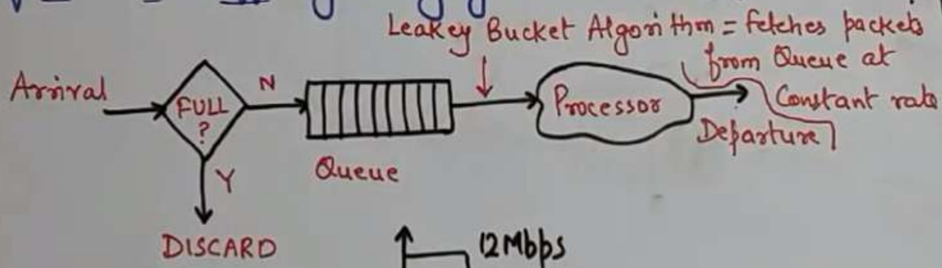
L63: Congestion Control Strategies(Prevention and Removal), Network Performance | DCN Lectures Hindi
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
Congestion Control:- In this, we try to avoid traffic congestion.
Traffic Descriptors:-
Data Rate
Max. Burst Size
Max. Length of time the traffic is generated at Peak Rate
Peak data Rate
[Max. data Rate of Traffic]
Average data Rate
Amount of Data
Time
Seconds
Effective Bandwidth ⇒ Bandwidth that N/W needs to allocate for Traffic Flow.
Congestion:- It may occur if the load on the N/W is greater than the capacity of the N/W. It occurs due to Queues in Routers and switches.
Congestion → LOAD > Capacity
no. of Packet sent to N/W
No. of Packet a N/W Can Handle.
Sender
NETWORK
Receiver
FULL
Congestion
8:25 / 27:24

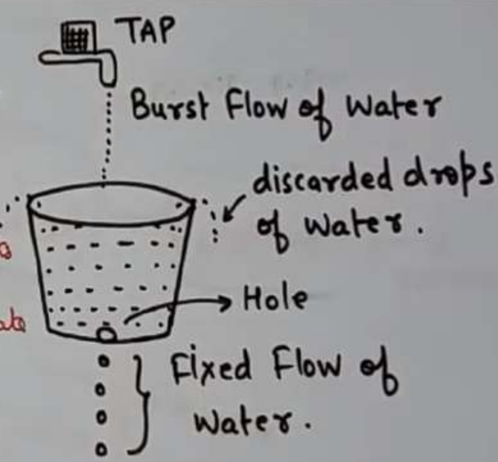

L63: Congestion Control Strategies(Prevention and Removal), Network Performance | DCN Lectures Hindi
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
Network Performance:-
Delay
infinite Delay
Congestion Free Area
Congestion Area
Capacity
Load
Delay as a funcn of Load
Througput
Congestion Free Area
Congestion Area
Capacity
Load
Throughput as a funcn of Load
Traffic Profiles:-
Data Rate
Bursty Data → Data Rate changes suddenly.
VBR → Data Flow changes with time
Constant Bit Rate
CBR [No change in data Rate]
Time
15:10 / 27:24

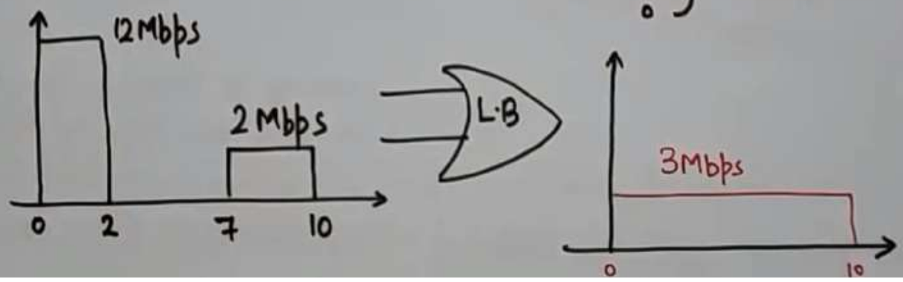

L63: Congestion Control Strategies(Prevention and Removal), Network Performance | DCN Lectures Hindi
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
Congestion Control Categories:-
Congestion Control
pen-Loop [Prevention]
Closed-Loop [Removal]
Retransmission Policy → Good Retransmission.
(TCP)
S
R
ndow Policy
↳Selective Repeat ARQ is better.
IMP
Back Pressure
BP (Congested Node)
S
N1
N2
N3
N4
D
Choke Packet
Choke Packet
cknowledgment Policy
eceiver will send
Ack after a time or N packets.
Discarding Policy
↳discarding less
sensitive packets.
Admission Policy → Resources are checked
first before admitting to
the N/W.
Implicit Signalling → No commⁿ b/w Congested
Node with other Nodes/Source. Source assumes
that congestion occured
ACK is Not Rec.
delay in ACK.
Explicit Signalling
↳Congested node send a signal to source/
destination. Signal is included in the data
packet
Backward - Node to Source
Forward -
26:56 / 27:24

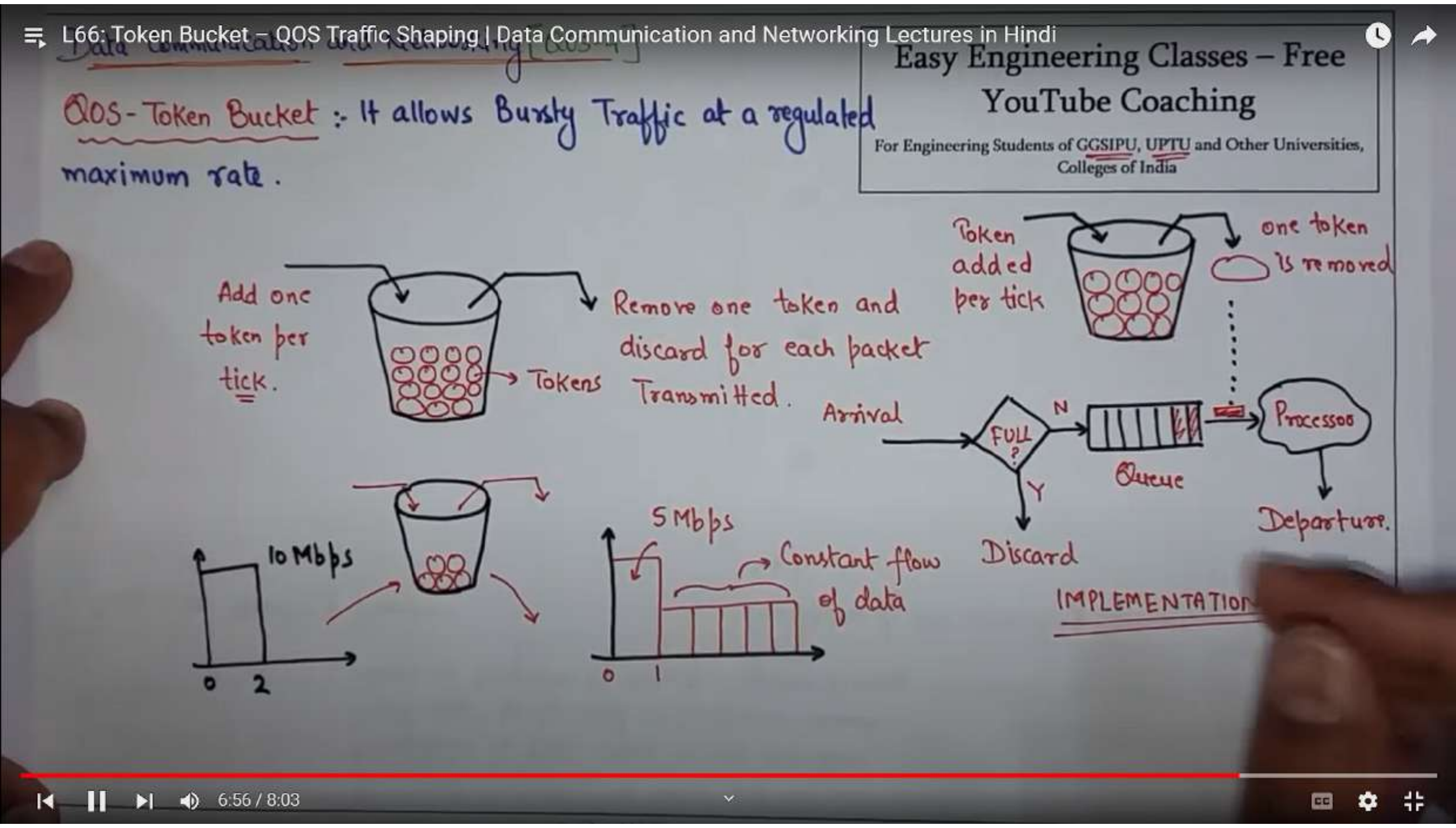
QOS-Traffic Shaping :- It is the mechanism to Control the amount and the rate of the traffic Sent to the N/W.

(i) Leakey Bucket :- This algorithm shapes Bursty traffic into fixed-rate traffic by averaging the data rate.







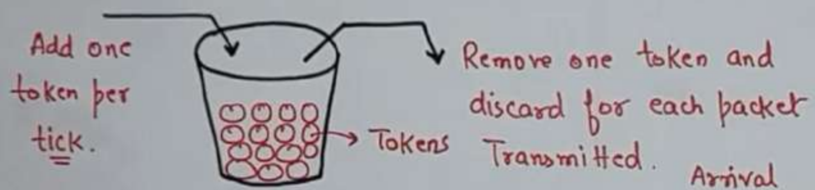

L66: Token Bucket – QOS Traffic Shaping | Data Communication and Networking Lectures in Hindi
Easy Engineering Classes – Free YouTube Coaching
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
QOS - Token Bucket :- It allows Bursty Traffic at a regulated maximum rate.
Add one token per tick.
Tokens
Remove one token and discard for each packet Transmitted.
10 Mbps
0
2
5 Mbps
Constant flow of data
0
1
Token added per tick
one token is removed
Arrival
FULL ?
N
Y
Queue
Processor
Departure.
Discard
IMPLEMENTATION
6:56 / 8:03

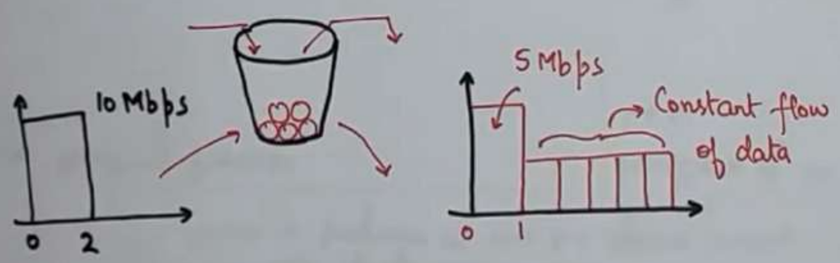
Data Communication and Networking [QOS-4]

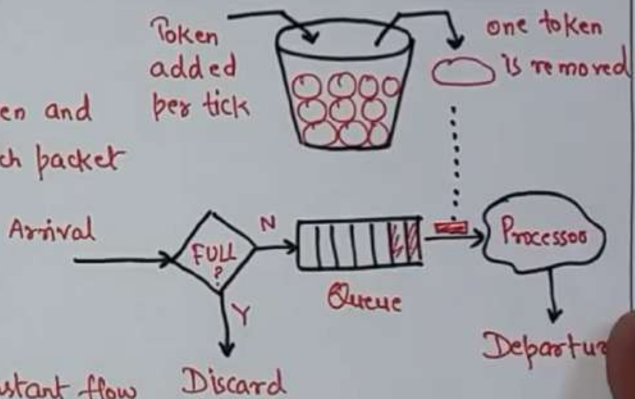
Easy Engineering Classes – Free YouTube Coaching

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

QOS-Token Bucket :- It allows Bursty Traffic at a regulated maximum rate.







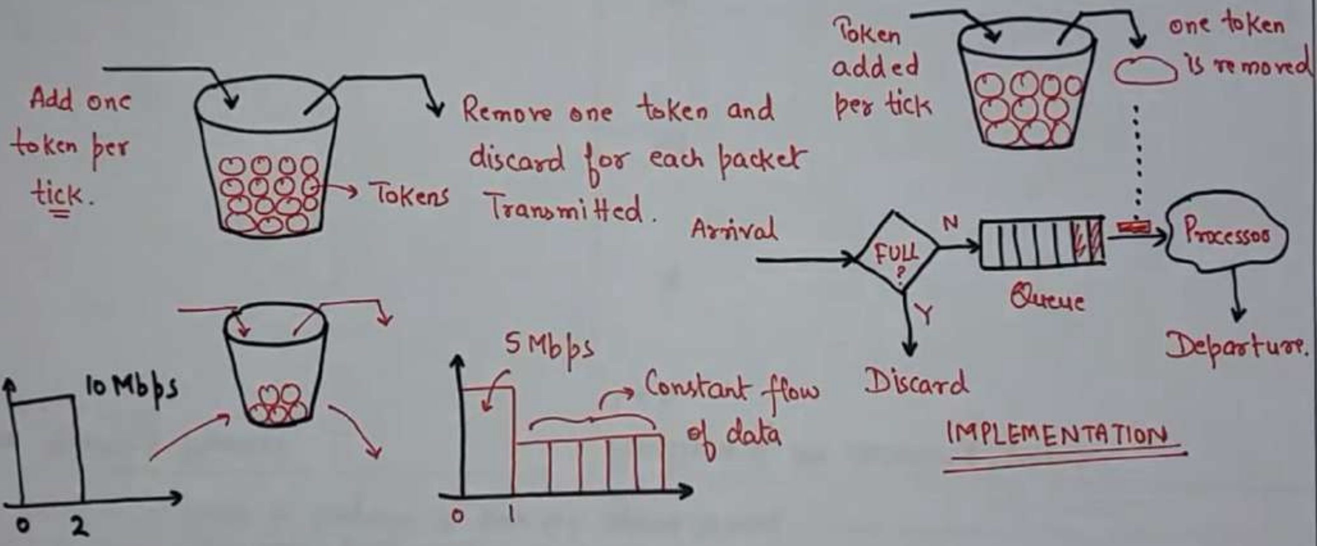
IMPLEMENTATION

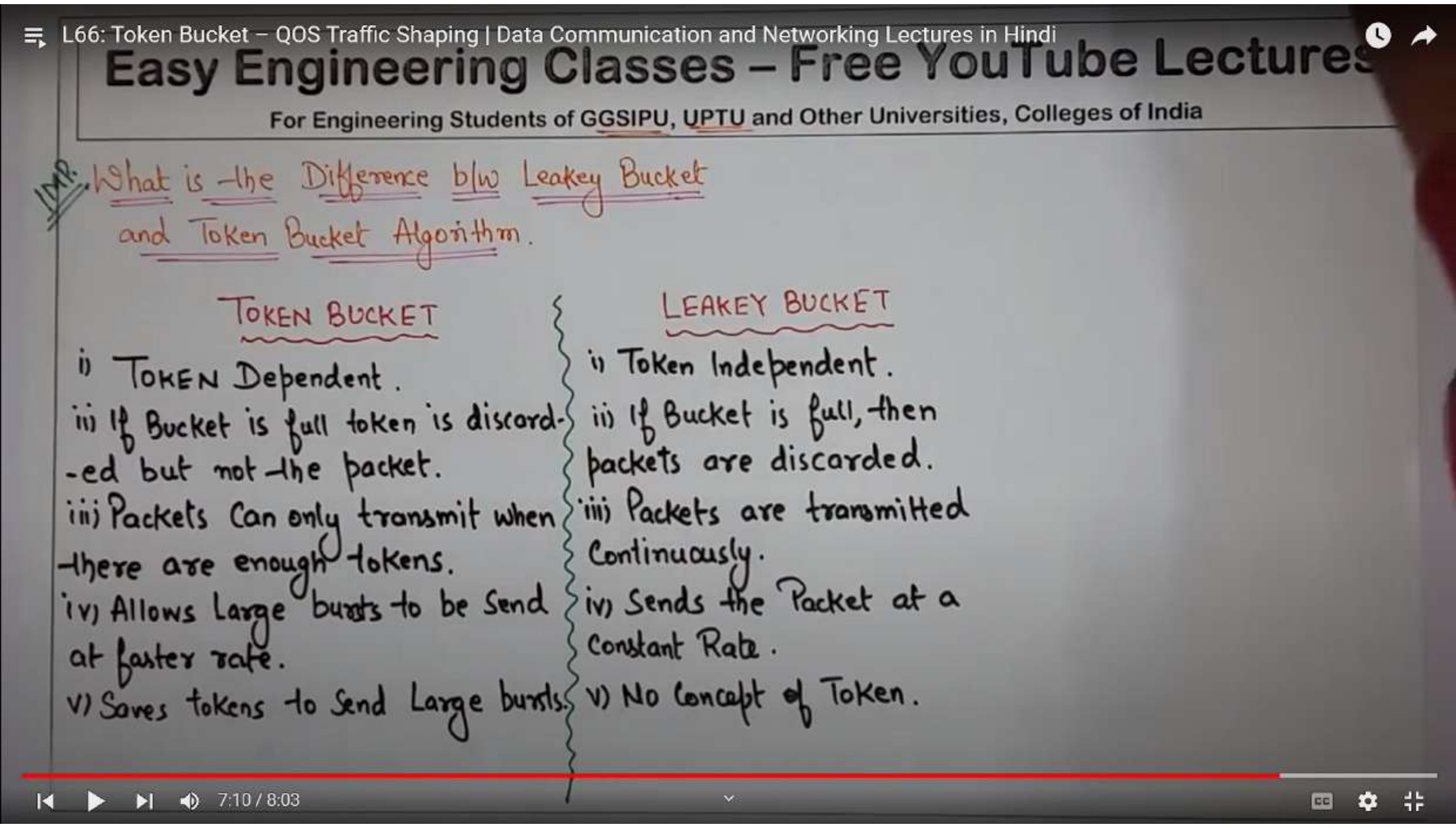
Data Communication and Networking [QOS-4]

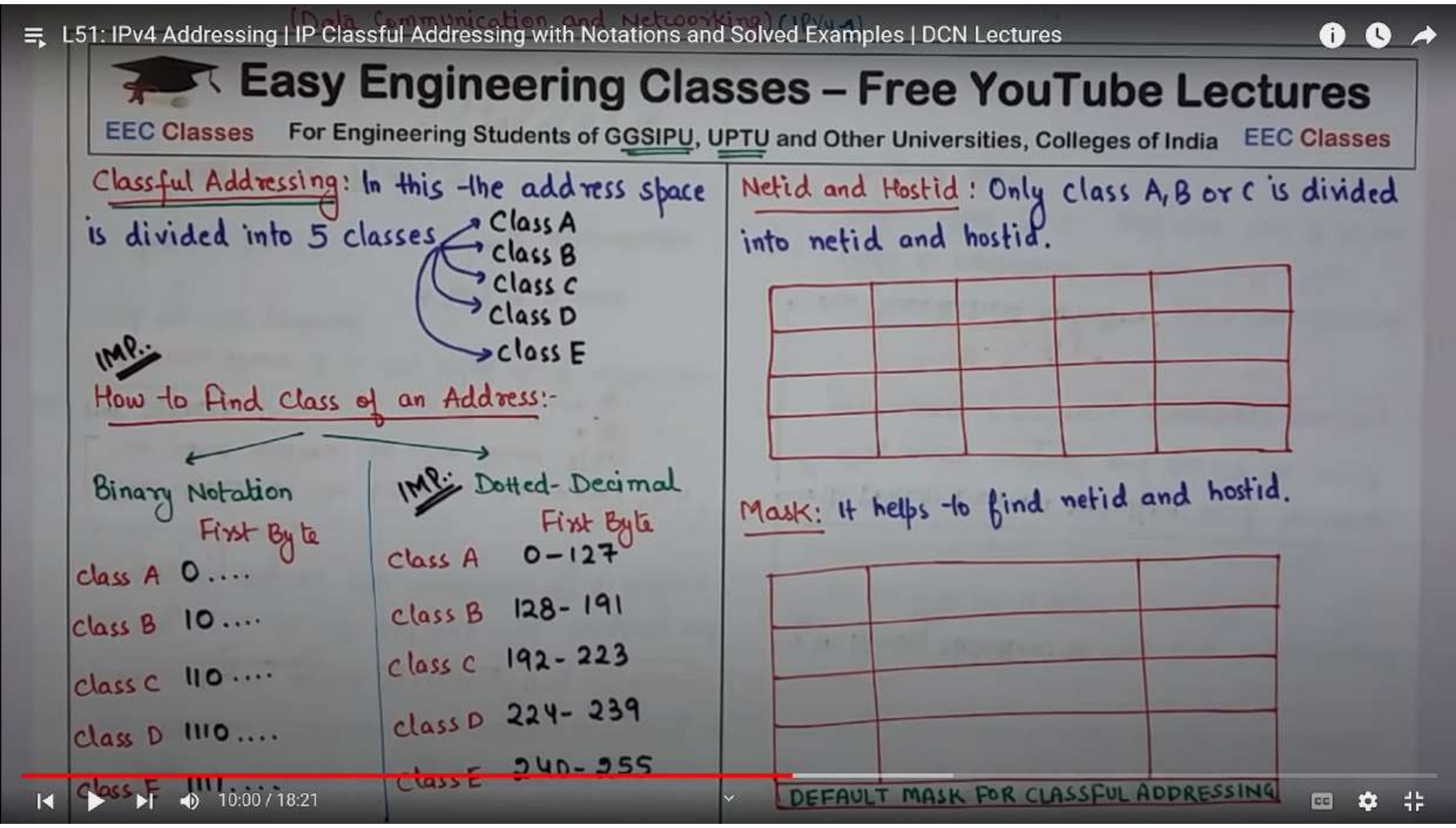
Easy Engineering Classes – Free YouTube Coaching

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

QOS - Token Bucket :- It allows Bursty Traffic at a regulated maximum rate.




L66: Token Bucket – QOS Traffic Shaping | Data Communication and Networking Lectures in Hindi
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
IMP. What is the Difference b/w Leakey Bucket and Token Bucket Algorithm.
TOKEN BUCKET
i) TOKEN Dependent.
ii) If Bucket is full token is discard-ed but not the packet.
iii) Packets Can only transmit when there are enough tokens.
iv) Allows Large bursts to be Send at faster rate.
v) Saves tokens to Send Large bursts.
LEAKEY BUCKET
i) Token Independent.
ii) If Bucket is full, then packets are discarded.
iii) Packets are transmitted Continuously.
iv) Sends the Packet at a Constant Rate.
v) No Concept of Token.
7:10 / 8:03


L51: IPv4 Addressing | IP Classful Addressing with Notations and Solved Examples | DCN Lectures
Easy Engineering Classes – Free YouTube Lectures
EEC Classes
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
EEC Classes
Classful Addressing: In this the address space is divided into 5 classes
Class A
class B
class C
class D
class E
IMP.
How to find class of an Address:-
Binary Notation
First Byte
class A 0....
class B 10....
class C 110....
class D 1110....
class E 1111....
IMP.
Dotted-Decimal
First Byte
class A 0-127
class B 128-191
class C 192-223
class D 224-239
class E 240-255
Netid and Hostid: Only class A, B or C is divided into netid and hostid.
Mask: It helps to find netid and hostid.
DEFAULT MASK FOR CLASSFUL ADDRESSING
10:00 / 18:21

(Decimal Dotted)

Ques1.) Find the class of each Address:-

Byte 1

a.) 227.12.14.87 ⇒ Class D

b.) 193.14.56.22 ⇒ class C

c.) 14.23.120.8 ⇒ Class A

d.) 252.5.15.111 ⇒ Class E

Easy Engineering Classes

EEC Classes For Engineering Students of GGSIPU, UPTU and

Classful Addressing: In this the address space is divided into 5 classes
- Class A
- Class B
- Class C
- Class D
- Class E

IMP.:

How to find class of an Address:-

Binary Notation

	First Byte
class A	0....
Class B	10....
class C	110....
class D	1110....
class E	1111....

IMP.: Dotted-Decimal

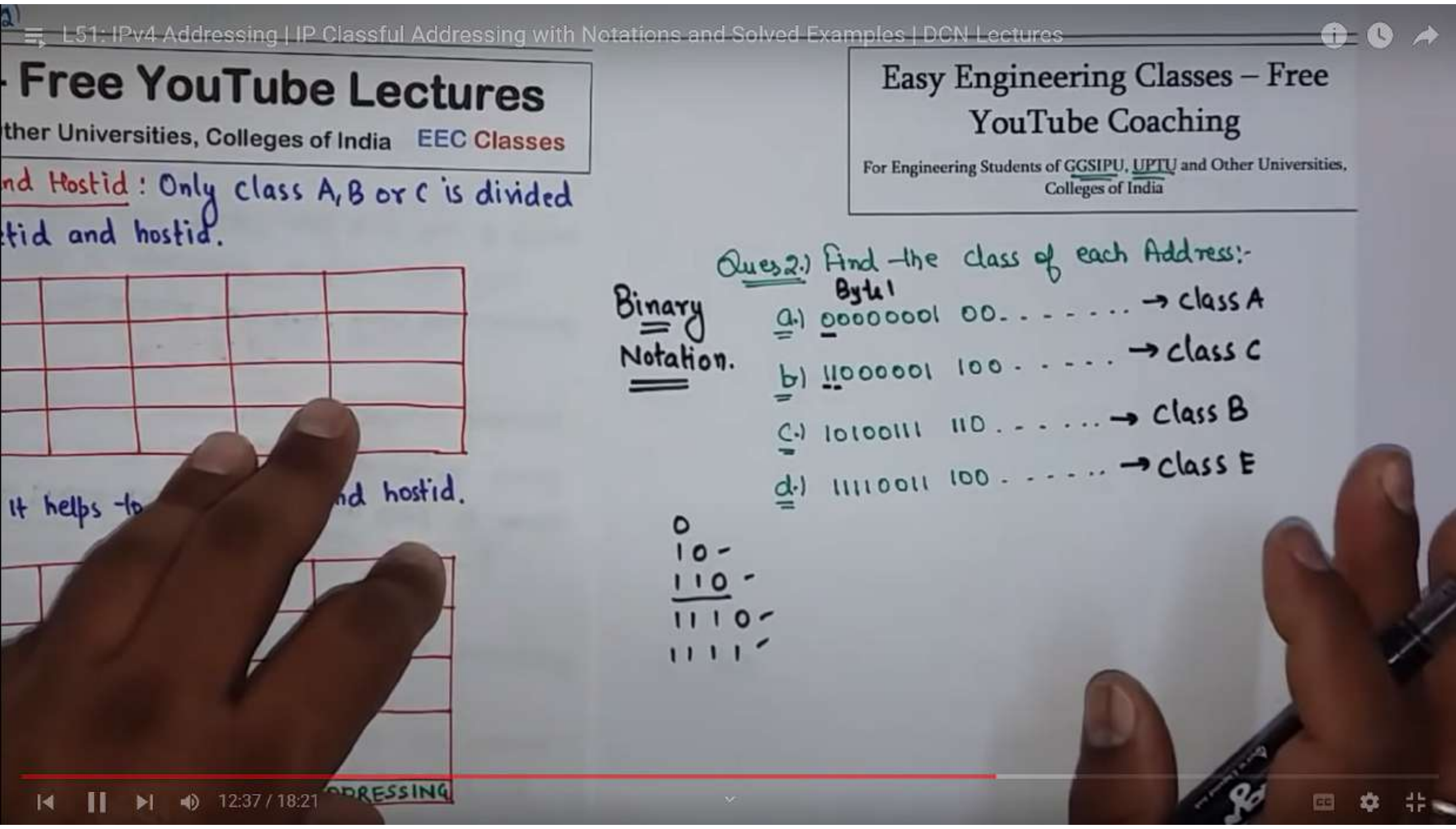
	First Byte
Class A	0-127
Class B	128-191
Class C	192-223
class D	224-239
Class E	240-255

Netid

into n

Mask

DE


L51: IPv4 Addressing | IP Classful Addressing with Notations and Solved Examples | DCN Lectures
Free YouTube Lectures
ther Universities, Colleges of India EEC Classes
Easy Engineering Classes – Free YouTube Coaching
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
nd Hostid : Only class A, B or C is divided
tid and hostid.
It helps to
nd hostid.
Binary Notation.
Ques 2.) Find the class of each Address:-
Byte 1
a.) 00000001 00. . . . . . . → class A
b) 11000001 100 . . . . . → class C
c.) 10100111 110 . . . . . → class B
d.) 11110011 100 . . . . . → class E
0
10-
110-
1110-
1111-
12:37 / 18:21

(Data Communication and Networking) (IPV4-2)

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Classful Addressing: In this the address space is divided into 5 classes
- Class A
- Class B
- Class C
- Class D
- Class E

IMP.:

How to find class of an Address:-

Binary Notation

	First Byte
class A	0....
Class B	10....
class C	110....
class D	1110....
class E	1111....

IMP.: Dotted-Decimal

	First Byte
Class A	0–127
class B	128–191
class C	192–223
class D	224–239
Class E	240–255

Netid and Hostid: Only class A, B or C is divided into netid and hostid.

class	Byte 1	Byte 2	Byte 3	Byte 4
class A	NetId	HostId	HostId	HostId
Class B	NetId	NetId	HostId	HostId
Class C	NetId	NetId	NetId	HostId

n bits = 1

(32-n) = 0

A = n = 8

B = n = 16

C = n = 24

Mask: It helps to find netid and hostid.

Class	Binary (Mask)	Decimal
class A	1111111 00......	255.0.0.0
Class B	1111111 1111111 00....	255.255.0.0
Class C	1111111 1111111 1111111 0..	255.255.

DEFAULT MASK FOR CLASSFUL ADDRESS

L52: IPv4 Classless Addressing | Mask, Solved Questions on Extracting Block Information | Networking

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

Restrictions:-

- (i) Addresses in a Block must be Contiguous.
- (ii) No. of Addresses in a Block must be a power of 2 [1, 2, 4, 8, 16, ----]
- (iii) The first address must be evenly divisible by the no. of addresses.

Block $16 = 2^4 =$

First → 205.16.37.32

→ 205.16.37.33

→ 205.16.37.34

⋮

Last → 205.16.37.47

Mask in classless Addressing Can take any Value from 0 to 32. $(n) = 1, (32-n) = 0$.

→ Slash/CIDR Notation.

x.y.z.t/n → defines the mask.

IMP Points:

- (i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.
- (ii) Last address can be found by setting the rightmost (32-n) bits to 1s.
- (iii) No. of Addresses: 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28 (n). Find first, last and total no. of addresses.

6:56 / 14:56

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

Restrictions:-

↳ (i) Addresses in a Block must be Contiguous.

(ii) No. of Addresses in a Block must be a power of 2 [1, 2, 4, 8, 16, ----]

(iii) The first address must be evenly divisible by the no. of addresses.

Block $16 = 2^4 =$

First → 205.16.37.32

↳ 205.16.37.33

↳ 205.16.37.34

⋮

La... .37.47

Mask in classless Addressing Can take any Value from 0 to 32. (n) = 1, (32-n) = 0.

↳ Slash/CIDR Notation.

x.y.z.t/n ↳ defines the mask.

IMP Points:

(i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.

(ii) Last address can be found by setting the rightmost (32-n) bits to 1s.

(iii) No. of Addresses: 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28 (n). Find first, last and total no. of addresses.

11001101 00010000 00100101 00100111

F.A:- ↓ ↓ ↓ 00100000

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

Restrictions:-

(i) Addresses in a Block must be Contiguous.

(ii) No. of Addresses in a Block must be a power of 2 [1, 2, 4, 8, 16, ----]

(iii) The first address must be evenly divisible by the no. of addresses.

$16 = 2^4 =$

Block

First → 205.16.37.32

→ 205.16.37.33

→ 205.16.37.34

Last ... 37.47

Mask in classless Addressing Can take any Value from 0 to 32. (n) = 1, (32-n) = 0.

→ Slash/CIDR Notation.

x.y.z.t/n → defines the mask.

IMP Points:

(i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.

(ii) Last address can be found by setting the rightmost (32-n) bits to 1s.

(iii) No. of Addresses: 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28 (n). Find first, last and total no. of addresses.

11001101 00010000 00100101 00100111

F.A:- 00100000

205.16.37.32

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

Restrictions:-

(i) Addresses in a Block must be Contiguous.

(ii) No. of Addresses in a Block must be a power of 2 [1, 2, 4, 8, 16, ----]

(iii) The first address must be evenly divisible by the no. of addresses.

Block $16 = 2^4 =$

First 205.16.37.32

205.16.37.33

205.16.37.34

⋮

Last 2 … 7.47

Mask in classless Addressing Can take any Value from 0 to 32. (n) = 1, (32-n) = 0.

Slash/CIDR Notation.

x.y.z.t/n defines the mask.

IMP Points:

(i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.

(ii) Last address can be found by setting the rightmost (32-n) bits to 1s.

(iii) No. of Addresses: 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28 (n).

Find first, last and total no. of addresses.

11001101 00010000 00100101 00100111 → 00101111

F.A:- 00100000

205.16.37.32 L.A = 205.16.37.47

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

Classless Addressing:- In this, Variable length blocks are used that belongs to no class.

...ictions:-

→ (i) Addresses in a Block must be Contiguous.

(ii) N... ...dresses in a Block must be ... of 2 [1, 2, 4, 8, 16, ...]

... first address must be evenly ...sible by the no. of addresses.

$16 = 2^4$

205.16.37.32
↳ 205.16.37.33
↳ 205.16.37.34

Last → 205.16.37.47

Mask in classless Addressing Can take any Value from 0 to 32. (n) = 1, (32-n) = 0.

↳ Slash/CIDR Notation.

x.y.z.t/n ↳ defines the mask.

IMP Points:

(i) First Address in block can be found by setting the rightmost (32-n) bits to 0s.

(ii) Last address can be found by setting the rightmost (32-n) bits to 1s.

(iii) No. of Addresses: 2^{32-n}

Example:- One of the Addresses is 205.16.37.39/28 (n).
Find first, last and total no. of addresses.

11001101 00010000 00100101 00100111 → 00101111

00100000

F.A:- 205.16.37.32   L.A = 205.16.37.47

N.A. = 2^4 = 16

L52: IPv4 Classless Addressing | Mask, Solved Questions on Extracting Block Information | Networking

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Students Studying Programming with C++ in Class XI and XII (CBSE, NCERT) and B.Tech Courses

One More Way of Extracting Block Info^n :-

↳ (i) No. of Addresses, $N = 2^{32-n}$

(ii) First Address = (Address) AND (MASK)

(iii) Last Address = (Address) OR (COMPLEMENT OF MASK)

Example:- For a Address 205.16.37.39/ $\underset{n}{28}$, Find

i) First Address

ii) Last Address

iii) No. of Addresses. $= 2^{32-28}$

$= 2^4$

$= 16$

Address:- 11001101 00010000 00100101 00100111

Mask:- 11111111 11111111 11111111 11110000

First Add. 11001101 00010000 00100101 00100000

AND

1+1=1

Mask Comp. 00000000 00000000 00000000 00001111

11001101 000100000 00100101 00101111

14:31 / 14:56

(Data Communication and Networking) (IPv4-7)

Easy Engineering Classes – Free YouTube Lectures

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

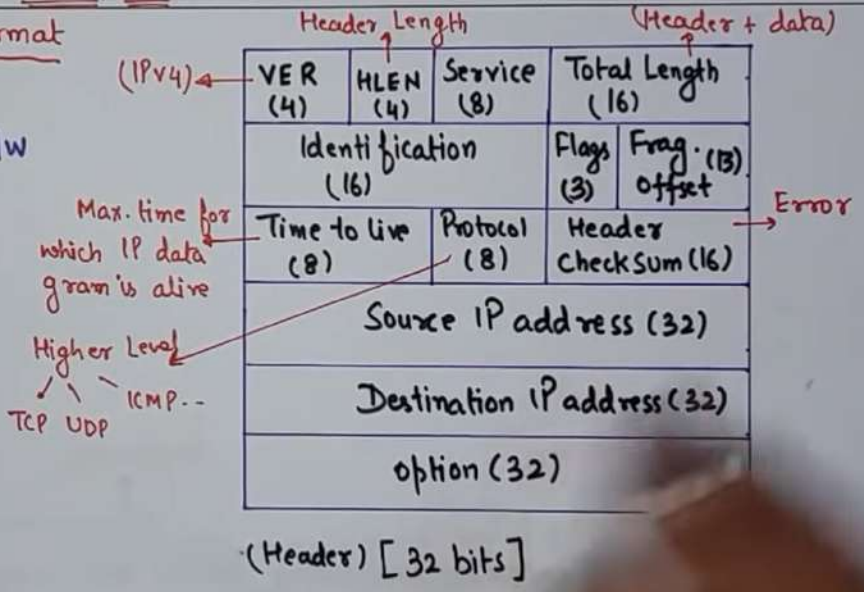
IPv4 Protocol: IP Packet/Datagram Format

IMP Points:-

i) Used by TCP/IP protocols at N/W Layer.

ii) ...reliable and Connectionless

Header	Data



L57: IPv6 Introduction | IPv6 Addresses Notations, Zero Compression, Packet Format, Changes in IPv6

2^{128}

IPv6 Addresses:- It is of 128 bits or 16 bytes.

↳ Length is 4 times the length address of IPv4.

Notations:-

(i) Dotted-Decimal:- It is used for IPv4 compatibility. 221.14.65.11.105.45.170.34.12.234.18.0.14.0.115.255] (16)

IMP (ii) Colon Hexadecimal:- It is used to make the address more readable. In this notation, the 128 bits are divided into 8 sections, each of 2 bytes in length. [Two bytes in Hexadecimal req. 4 Hexadecimal digits].

FDEC: BA98: 7654: 3210: ADBF: BBFF: 2922: FFFF

Abbreviation:- It is a technique to reduce the length of IPv6 address. It is done by omitting / removing the leading zeros of a section.

[NOTE:- Only the leading zeros can be dropped]

[Zero-Compression]

FDEC: 0074: 0000: 0000: 0000: BOFF: 0000: FFF0

omitting these zeros

FDEC: 74: 0: 0: 0: BOFF: 0: FFF0 } Abbreviated Address

↓

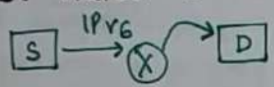
FDEC: 74 : : BOFF : 0: FFF0

↳ GAP.

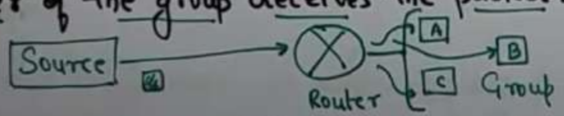
9:19 / 24:43

Types of Address Space in IPv6:-

(i) Unicast Addresses:- It defines single interface or Computer. The packet sent to a unicast address will be routed to the intended PC or recipient.

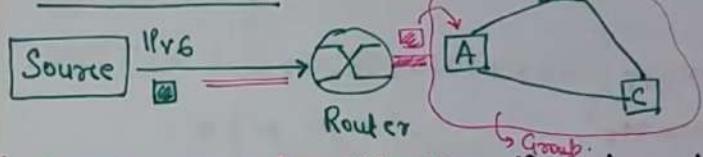


(ii) Multicast Addresses:- These are used to define a group of computers/hosts. In this, each member of the group receives the packet.

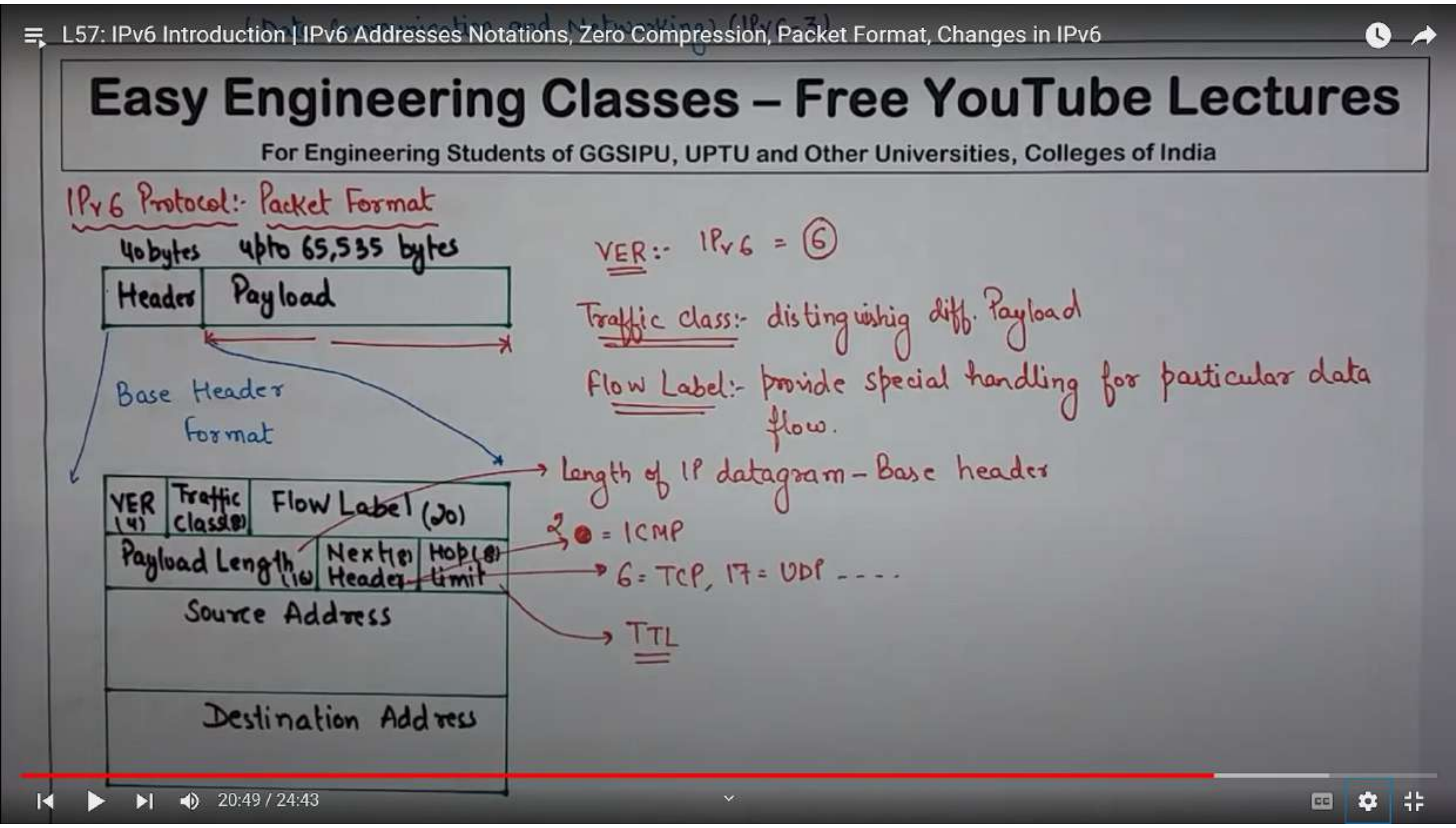


(iii) Anycast Addresses:- Defines group of nodes or computers that all share a single address. A packet with anycast address is delivered to

most reachable one.



(iv) Broadcasting and Multicasting:- IPv6 doesnot define broadcasting and considered it as a special case of multicasting.


L57: IPv6 Introduction | IPv6 Addresses Notations, Zero Compression, Packet Format, Changes in IPv6
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
IPv6 Protocol:- Packet Format
40 bytes
upto 65,535 bytes
Header
Payload
Base Header Format
VER (4)
Traffic class (8)
Flow Label (20)
Payload Length (16)
Next Header (8)
Hop Limit (8)
Source Address
Destination Address
VER:- IPv6 = 6
Traffic class:- distinguishing diff. Payload
Flow Label:- provide special handling for particular data flow.
Length of IP datagram – Base header
= ICMP
6 = TCP, 17 = UDP ....
TTL
20:49 / 24:43

L57: IPv6 Introduction | IPv6 Addresses Notations, Zero Compression, Packet Format, Changes in IPv6

Easy Engineering Classes – Free YouTube Lectures

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

hanges in IPv6:-

i) Larger address space $\Rightarrow 2^{128} - 2^{32} \Rightarrow 2^{96}$ time more address than IPv4.

ii) Better Header format $\Rightarrow$ options are separated from Base Header.

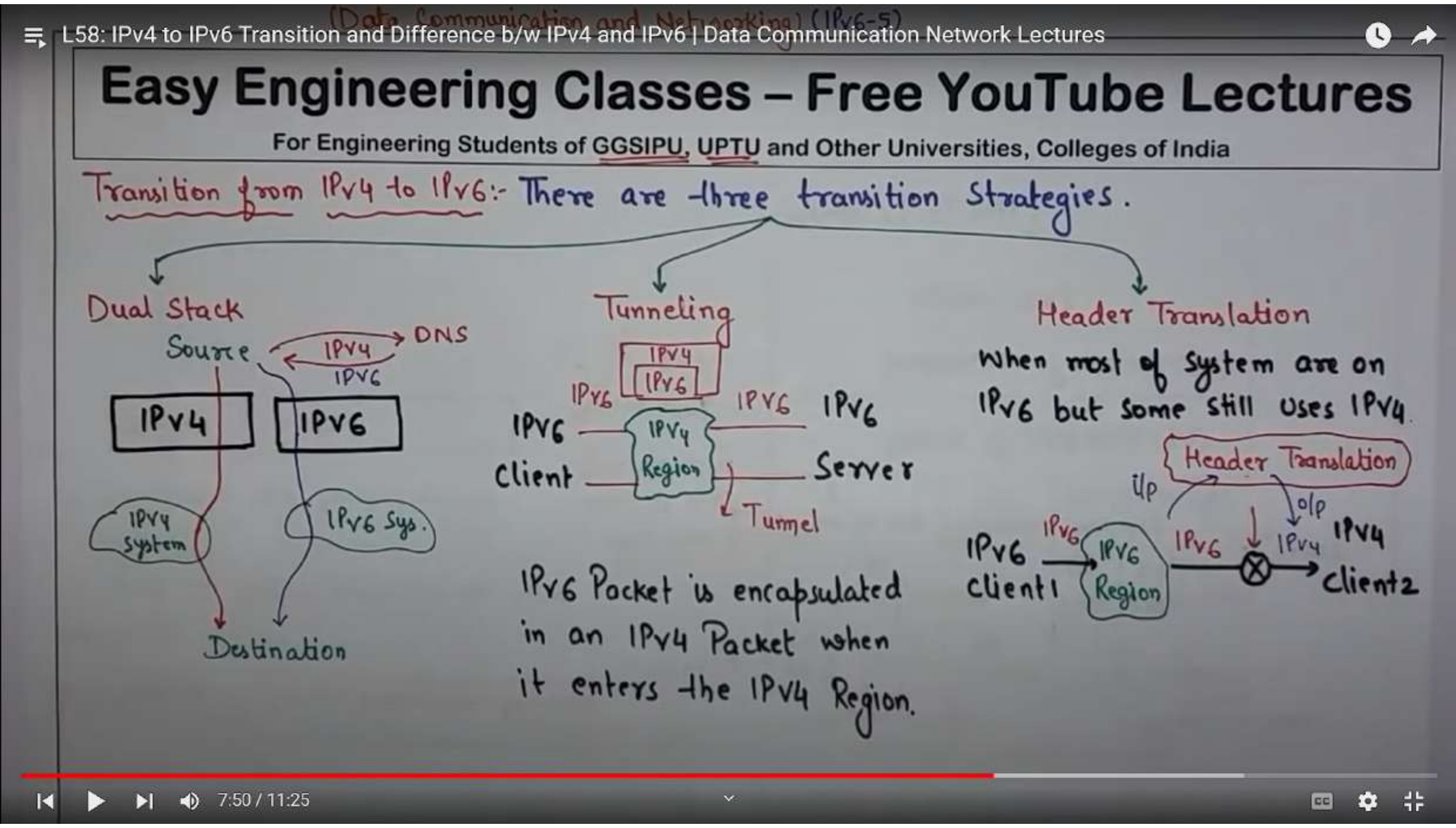
iii) New options $\Rightarrow$ Additional functionalities.

iv) Allowance for Extension $\Rightarrow$ Extension of Protocol

v) Support for Resource Allocation $\Rightarrow$ Traffic class, Flow Label $\rightarrow$ Special Handling of the packet

vi) Support for More Security $\Rightarrow$ Encryption.

24:00 / 24:43


L58: IPv4 to IPv6 Transition and Difference b/w IPv4 and IPv6 | Data Communication Network Lectures
Easy Engineering Classes – Free YouTube Lectures
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
Transition from IPv4 to IPv6:- There are three transition Strategies.
Dual Stack
Source
IPv4
IPv6
DNS
IPv4
IPV6
IPv4 system
IPv6 Sys.
Destination
Tunneling
IPv4
IPv6
IPv6
IPv6
IPv6
IPv6
Client
IPv4 Region
Server
Tunnel
IPv6 Packet is encapsulated in an IPv4 Packet when it enters the IPv4 Region.
Header Translation
When most of system are on IPv6 but some still uses IPv4.
Header Translation
i/p
o/p
IPv6
client1
IPv6
IPv6 Region
IPv6
IPv4
IPv4
Client2
7:50 / 11:25

DIFFERENCE BETWEEN IPv4 AND IPv6

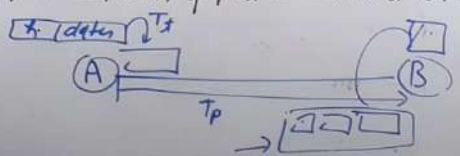
IPv4	IPv6
1.) Length of Address: 32 Bit	i) Length of Address: 128 Bit
2.) Represent in Decimal notation	ii) Represented in Hexadecimal notation
3.) IPsec support: optional	3.) IPsec Support: Inbuilt
4.) Packet Flow Indication: NONE	4.) Packet Flow: YES → FLOW Label field
5.) checksum field: YES	5.) checksum field: NONE
6) option field: YES	6) options field: NONE, IPv6 Extension Header
7.) Address (IP) to MAC = (ARP)	7.) Replaced By: Neighbour Discovery Protocol (NDP)
8) Broadcast Message: YES	8) Broadcast Message: Special type of Multicast Addr.
9.) Total No. of Addresses: 2^{32}	9.) Total No. of Addresses: 2^{128}

Delays in CN

The delay of network specifies how long it takes a bit of data to travel across the network from one node to another.

there are four different type of delay:

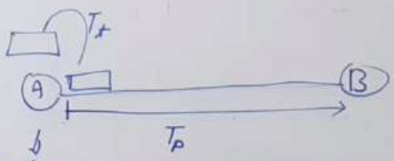
3 Queueing Delay: Time the packet spend in routing queueing. The queueing delay depends upon number of packet arrived earlier in the queue.



4 Processing Delay: A packet consist of head and data field. The head contain address of source and destination. The time require to examine header is called processing delay.

2. Propagation Delay: Time for a bit reach to destination. Time taken by first bit travel from source to destination

$$\boxed{\text{Propagation delay } T_p = \frac{\text{Distance}(d)}{\text{Transmission speed}(v)}}$$



light $= 3\times10^8$ m/sec

Speed of fiber line $= 3\times10^8 \times \frac{70}{100}$

$= 2.1\times10^8$ m/sec

$d = 2.1$ km

$v = 2.1\times10^8$ m/sec

$T_p = \frac{2.1\times10^3}{2.1\times10^8} = 10^{-5}$ sec

millisec $= 10^{-5}\times10^{3} = 10^{-2}$ millisec

microsec $= 10^{-5}\times10^{6} = 10^{1}$ microsec