MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

LECTURE HANDOUTS

L-1

CSE

III/VI

Course Name with Code   :High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : I- High Speed Networks   Date of Lecture:

| |
|---|
| **Topic of Lecture:** Frame relay Networks-Asynchronous Transfer Mode |
| **Introduction :**
 Designed to eliminate much of the overhead in X.25
 _ Call control signaling on separate logical connection from user data
 _ Multiplexing/switching of logical connections at layer 2 (not layer 3)
 _ No hop-by-hop flow control and error control
 _ Throughput an order of magnitude higher than X.25 |
| **Prerequisite knowledge for Complete understanding and learning of Topic:**
 • Open system
 • Closed system
 • Protocol
 • Host name
 • IP Address |
| **Detailed content of the Lecture:**

 Frame Relay Architecture

 X.25 has 3 layers: physical, link, network

 • Frame Relay has 2 layers: physical and data link (or LAPF)

 • LAPF core: minimal data link control

 • Preservation of order for frames

 • Small probability of frame loss

 • LAPF control: additional data link or network layer end-to-end functions

 LAPF Core

 1. Frame delimiting, alignment and transparency

 2. Frame multiplexing/demultiplexing

 3. Inspection of frame for length constraints

 4. Detection of transmission errors

 5. Congestion control

 User Data Transfer

 • No control field, which is normally used for: |

- Identify frame type (data or control)
- Sequence numbers
- Implication: Connection setup/teardown carried on separate channel
- Cannot do flow and error control

(a) X.25   (b) Frame relay   (c) Frame switching
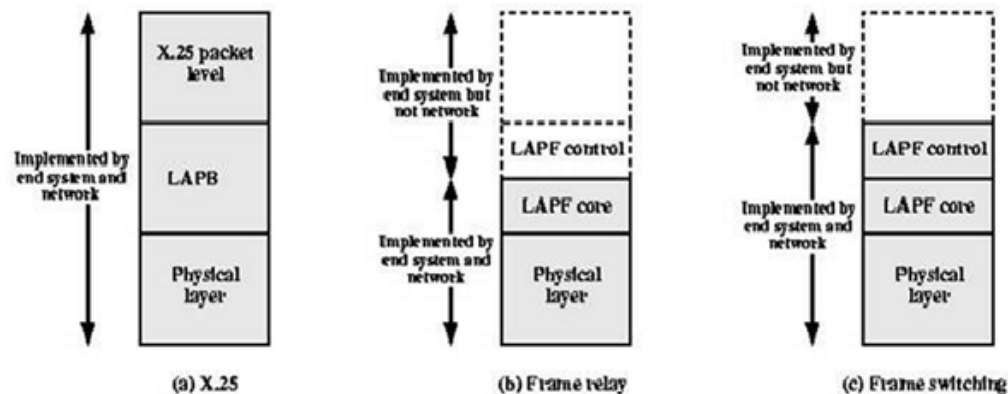
Frame Relay Call Control

- Frame Relay Call Control
- Data transfer involves:
- Establish logical connection and DLCI
- Exchange data frames
- Release logical connection

4 message types needed

- SETUP
- CONNECT
- RELEASE
- RELEASE COMPLETE

Asynchronous Transfer Mode (ATM):

- It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video or voice which is conveyed in small fixed size packets called cells.
- Cells are transmitted asynchronously and the network is connection oriented.
- ATM is a technology which has some event in the development of broadband ISDN in 1970s and 1980s, which can be considered an evolution of packet switching.
- *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.
- Subsequently all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic.
- Thus it can carry multiple types of traffic with **end-to-end** quality of service.
- ATM is independent of transmission medium, they maybe sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems.
- ATM networks use "Packet" or "cell" Switching with virtual circuits. It's design helps in

the implementation of high performance multimedia networking.

ATM Cell Format –

As information is transmitted in ATM in the form of fixed size units called **cells**. As known already each cell is 53 bytes long which consists of 5 bytes header and 48 bytes payload.

Asynchronous Transfer Mode can be of two format types which are as follows:

1. **UNI Header:** which is used within private networks of ATM for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (46-49)

Course Faculty

Verified by HOD

LECTURE HANDOUTS	L-2

CSE	III/VI

Course Name with Code :High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : I- High Speed Networks   **Date of Lecture:**

Topic of Lecture: ATM Protocol Architecture, ATM logical Connection

Introduction :
- A streamlined packet transfer interface
- Similarities to packet switching
- Transfers data in discrete chunks
- Supports multiple logical connections over a single physical interface

Prerequisite knowledge for Complete understanding and learning of Topic:
- Protocol
- Host name
- IP Address

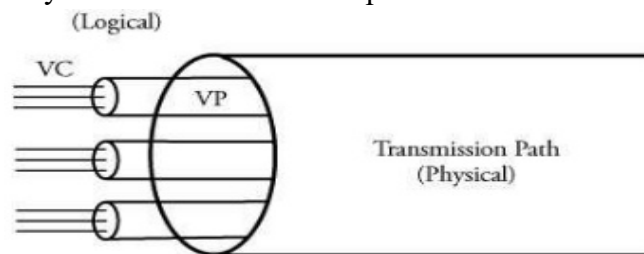**Detailed content of the Lecture:**

ATM Protocol Architecture
- The asynchronous transfer mode (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service.
- The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections.
- ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.
- The first thing to notice is that, as well as layers, the model has planes.
- The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes.
- The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane).
- The protocols in the ATM layer provide communication between ATM switches while the protocols in the ATM adaptation layer (AAL) operate end-to-end between users.
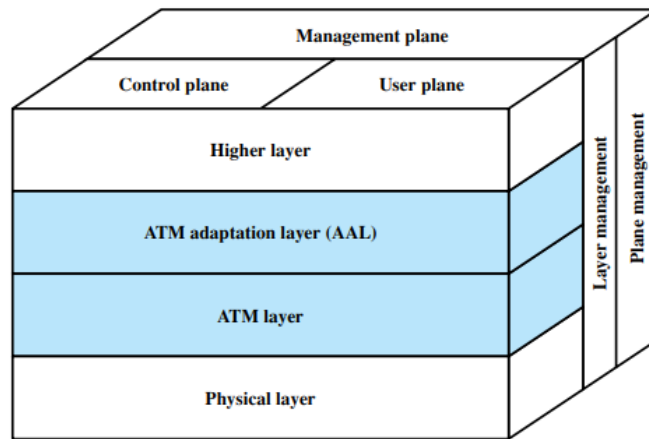
ATM logical Connection

- Each ATM cell consists of 53 bytes: the header is five bytes long and the remaining 48 bytes (the cell payload) carry information from higher layers. The only difference between the two types of ATM cell is that the cells at the user-network interface carry a data field for the flow control of data from users. This means that only eight bits are available for virtual path identifiers, rather than 12 bits at the network-node interface.

- The virtual connections set up in ATM networks are identified by the combination of the *virtual path identifier* and *virtual channel identifier*. These two fields provide a hierarchy in the numbering of virtual connections, whereby a virtual path contains a number of virtual channels. An advantage of this hierarchy is that in some cases the switching of ATM cells may be based on the virtual path identifier alone.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=P6Q5QZAZ8yc
https://www.youtube.com/watch?v=RzcFTVf-mCE&t=17s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No (46-49)

Course Faculty

Verified by HOD

Estd. 2000

IQAC

L-3

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code   :High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : I- High Speed Networks   Date of Lecture:

| |
|---|
| **Topic of Lecture:** ATM Cell |
| **Introduction :**
• ATM networks are connection oriented networks for cell relay that supports voice, video and data communications.
• It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium. The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload. |
| **Prerequisite knowledge for Complete understanding and learning of Topic:**
• Open system
• Closed system
• Protocol
• Host name
• IP Address |
| **Detailed content of the Lecture:**
ATM Cells
• Cell in ATM is a 53-byte packet of data, the standard packet size used by Asynchronous Transfer Mode (ATM) communication technologies.
• Cells are to ATM technologies what frames are to Ethernet networking.
• In other words, they form the smallest element of data for transmission over the network.

ATM cell

48-byte data payload   5-byte header
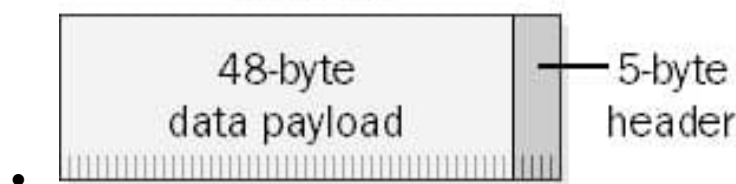
• ATM cells are standardized at a fixed-length size of 53 bytes to enable faster switching than is possible on networks using variable-packet sizes (such as Ethernet).
• It is much easier to design a device to quickly switch a fixed-length packet than to design a device to switch a variable-length packet.
• Using fixed-length cells also makes it possible to control and allocate ATM bandwidth more effectively, making support for different quality of service (QoS) levels for ATM possible. |

ATM Cell Format

GFC (4 Bits)		VPI (4 Bits)	
VPI (4 Bits)		VCI (4 Bits)	
VCI (8 Bits)			
VCI (4 Bits)		PT (3 Bits)	CLP Bit
HEC (8 Bits)			
Payload (48 Bytes)			
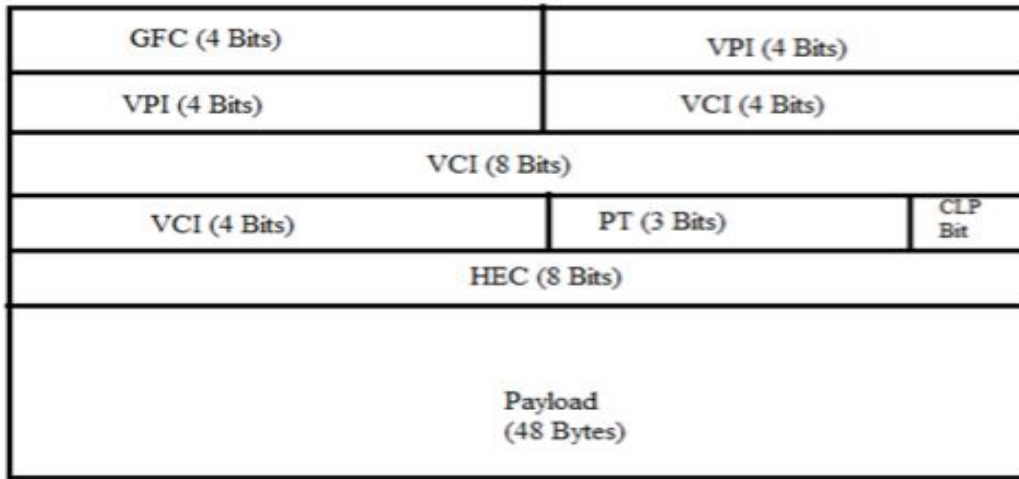
Header Format
- Generic flow control
- Only at user to network interface
- Controls flow only at this point
- Virtual path identifier
- Virtual channel identifier
- Payload type
- e.g. user info or network management
- Cell loss priority
- Header error control

Generic Flow Control (GFC)
- Control traffic flow at user to network interface (UNI) to alleviate short term overload
- Two sets of procedures
- Uncontrolled transmission
- Controlled transmission
- Every connection either subject to flow control or not
- Subject to flow control
- May be one group (A) default
- May be two groups (A and B)
- Flow control is from subscriber to network
- Controlled by network side

Single Group of Connections (1)
- Terminal equipment (TE) initializes two variables
- TRANSMIT flag to 1
- GO_CNTR (credit counter) to 0
- If TRANSMIT=1 cells on uncontrolled connection may be sent any time
- If TRANSMIT=0 no cells may be sent (on controlled or uncontrolled connections)
- If HALT received, TRANSMIT set to 0 and remains until NO_HALT

Single Group of Connections (2)
- If TRANSMIT=1 and no cell to transmit on any uncontrolled connection:
- If GO_CNTR>0, TE may send cell on controlled connection
- Cell marked as being on controlled connection
- GO_CNTR decremented
- If GO_CNTR=0, TE may not send on controlled connection
- TE sets GO_CNTR to GO_VALUE upon receiving SET signal
- Null signal has no effect

Header Error Control
- 8 bit error control field
- Calculated on remaining 32 bits of header
- Allows some error correction

HEC Operation at Receiver

Figure showing Correction Mode and Detection Mode states with transitions:
- Multibit error detected (cell discarded)
- No error detected (no action)
- No error detected (no action)
- Single-bit error detected (correction)
- Error detected (cell discarded)
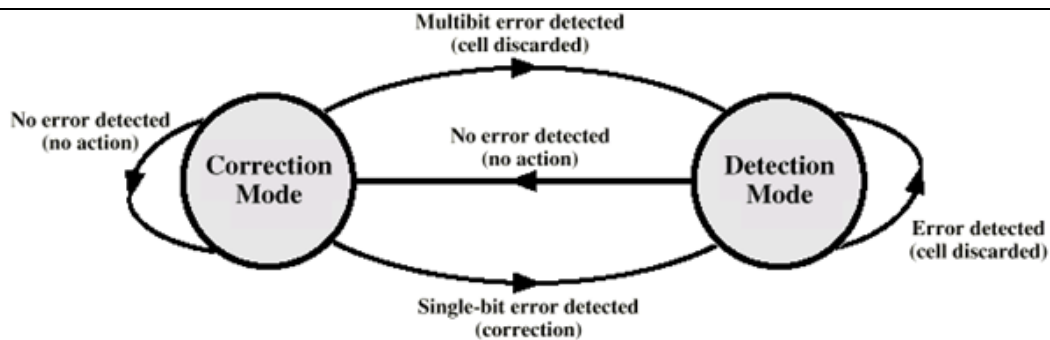
Real Time Services
- Amount of delay
- Variation of delay (jitter)

CBR
- Fixed data rate continuously available
- Tight upper bound on delay
- Uncompressed audio and video
- Video conferencing
- Interactive audio
- A/V distribution and retrieval

rt-VBR
- Time sensitive application
- Tightly constrained delay and delay variation
- rt-VBR applications transmit at a rate that varies with time
- e.g. compressed video
- Produces varying sized image frames
- Original (uncompressed) frame rate constant
- So compressed data rate varies
- Can statistically multiplex connections

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No (63-70)

Course Faculty

Verified by HOD

IQAC

Estd. 2000

L-4

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code	:High Speed Networks-16CSE10
Course Faculty	: C.Nithya
Unit	: I- High Speed Networks Date of Lecture:

Topic of Lecture: ATM Service Categories : AAL

Introduction :
Asynchronous Transfer Mode (ATM) is a telecommunications standard defined by ANSI and ITU (formerly CCITT) for digital transmission of multiple types of traffic, including telephony (voice), data, and video signals in one network without the use of separate overlay networks.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Open system
- Closed system
- Protocol
- Host name
- IP Address

Detailed content of the Lecture:
- In Asynchronous Transfer Mode (ATM) networks, the ATM Adaptation Layer (AAL) provides facilities for non-ATM based networks to connect to ATM network and use its services.
- AAL is basically a software layer that accepts user data, which may be digitized voice, video or computer data, and makes them suitable for transmission over an ATM network. The transmissions can be of fixed or variable data rate.
- AAL accepts higher layer packets and segments them into fixed sized ATM cells before transmission via ATM. It also reassembles the received segments to the higher layer packets.

Function of AAL
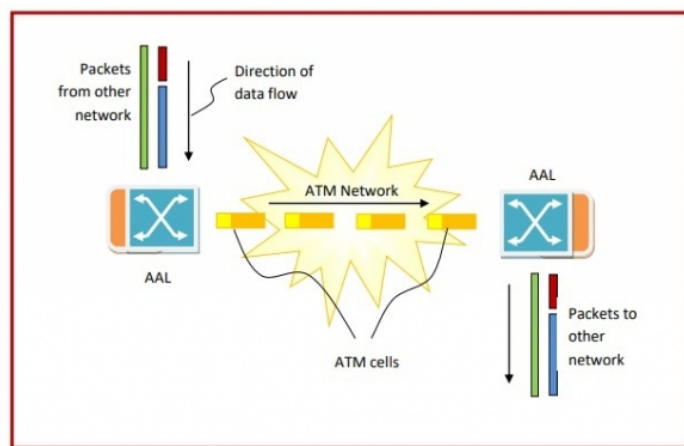
This layer has two sub layers −

- Convergence sub layer

- Segmentation and Reassembly sub layer.

Some networks that need AAL services are Gigabit Ethernet, IP, Frame Relay, SONET/SDH and UMTS/Wireless.

AAL Protocols

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) has defined five AAL protocols to provide the range of services.

- **AAL Type 0** − This is the simplest service that provides direct interface to ATM services without any restrictions. These cells are called raw cells that contain 48-byte payload field without any special fields. It lacks guaranteed delivery and interoperability.

- **AAL Type 1** − This service provides interface for synchronous, connection oriented traffic. It supports constant rate bit stream between the two ends of an ATM link. An AAL 1 cell contains a 4-bit sequence number, a 4-bit sequence number protection and a 47-byte payload field.

- **AAL Type 2** − This service also provides interface for synchronous, connection oriented traffic. However, this is for variable rate bit stream between the two ends of an ATM link. It is used in wireless applications.

- **AAL Type 3/4** − This includes a range of services for variable rate data or bit stream. It is suitable for both connection – oriented, asynchronous traffic as well as connectionless traffic. These ATM cells contain a 4-byte header.

- **AAL Type 5** − AAL 5 provides the similar services as AAL 3/4, but with simplified header information. It was originally named Simple and Efficient Adaptation Layer (SEAL). It is used in a number of areas like Internet Protocol (IP) over ATM, Ethernet over ATM and Switched Multimegabit Data Service (SMDS).

High Speed LAN's:
Fast Ethernet
- Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN). It was launched as the IEEE 802.3u standard in 1995, and stayed the fastest network till the introduction of Gigabit Ethernet.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002. -Pg.No (90-97)

Course Faculty

Verified by HOD

Estd. 2000

IQAC

| **LECTURE HANDOUTS** | **L-5** |

| **CSE** | **III/VI** |

Course Name with Code   :High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : I- High Speed Networks   Date of Lecture:

Topic of Lecture: High Speed LAN's: Fast Ethernet
Introduction : Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN). It was launched as the IEEE 802.3u standard in 1995, and stayed the fastest network till the introduction of Gigabit Ethernet.
Prerequisite knowledge for Complete understanding and learning of Topic: • Protocol • Host name • IP Address
Detailed content of the Lecture: **High Speed LAN's:** **Fast Ethernet** Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. The goals of Fast Ethernet are: 1. Upgrade the data rate to 100 Mbps. 2. Make it compatible with Standard Ethernet. 3. Keep the same 48-bit address. 4. Keep the same frame format. 5. Keep the same minimum and maximum frame lengths. **Physical Layer** The physical layer in Fast Ethernet is more complicated than the one in Standard Ethernet. **Topology:** Fast Ethernet is designed to connect two or more stations togethe r. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center **Implementation:** Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire. The two-wire implementation can be either category 5 UTP (lOOBase-TX) or fiber-optic cable (lOOBase- FX). The four-wire implementation is designed only for category 3 UTP (l00Base-T4).

Fast Ethernet topology

lOOBase-TX uses two pairs of twisted-pair cable (either category 5 UTP or STP). For this implementation, the MLT-3 scheme was selected since it has good bandwidth. But MLT-3 is not a selfsynchronous line coding scheme, so 4B/5B block coding is used to provide bit synchronization. This creates a data rate of 125 Mbps, which is fed into MLT-3 for encoding.

lOOBase-FX uses two pairs of fiber-optic cables. It uses NRZ-I encoding scheme for this implementation.

But NRZ-I has a bit synchronization problem, so 4B/5B block encoding is used. The block encoding increases the bit rate from 100 to 125 Mbps, which can easily be handled by fiber-optic cable.

lOOBase-T4, was designed to use category 3 or higher UTP. The implementation uses 4 pairs of UTP for transmitting 100 Mbps.

Video Content / Details of website for further learning (if any):   https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/   https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s
Important Books/Journals for further learning including the page nos.:   William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No (77-82)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

L-6

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code   :High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : I- High Speed Networks   Date of Lecture:

Topic of Lecture: Gigabit Ethernet
Introduction : Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks.
Prerequisite knowledge for Complete understanding and learning of Topic: • LAN • Ethernet • Cables
Detailed content of the Lecture: • **Gigabit Ethernet** has data rate of 1000 Mbps or Gbps. It is mainly designed to use optical fiber although the protocol does not eliminate the use of twisted pair cables. • Gigabit Ethernet is a term used to describe various Ethernet frame transmission techniques at Gigabit bit rate per second, as defined by the IEEE 802.3-2008 standard. • It came into use beginning in 1999, gradually supplanting Fast Ethernet in wired local networks, as a result of being considerably faster. • The cables and equipment are very similar to previous standards and have been very common and economical since 2010. **Features of Gigabit Ethernet** 1. Gigabit Ethernet provides a seamless migration path that fully protects your investment in your existing network infrastructure. Gigabit Ethernet will retain IEEE 802.3 and Ethernet frame formats and 802.3 managed object specifications, enabling organizations to retain existing cable, operating system, protocol, desktop applications while upgrading to gigabit performance Program and network management strategies and tools. 2. Relative to the original Fast Ethernet, FDDI, ATM and other backbone solutions, Gigabit Ethernet provides an optimal path. At least for the moment, it is a reliable and cost-effective way to improve connectivity between switches and switches and between switches and servers. 3. The IEEE 802.3 working group has set up 802.3z and 802.3ab Gigabit Ethernet working groups whose mission is to develop Gigabit Ethernet standards that meet different needs. The standard supports full duplex and half duplex 1000Mbps, the corresponding operation using IEEE 802.3 Ethernet frame format and CSMA / CD media access control methods.

Technical advantages

1. Compatibility

The main advantage of Gigabit Ethernet lies in its compatibility with existing Ethernet. Just like 100Mbit Ethernet, Gigabit Ethernet uses the same frame format and frame size as 10Mbit Ethernet, and the same CSMA / CD protocol. In the campus network backbone, and gradually occupy the main position.

2. Large bandwidth

Gigabit Ethernet compared to other technologies have the advantages of large bandwidth, and still have room for development, the relevant standards organizations are developing 10G Ethernet network technology specifications and standards. At the same time, priority control mechanisms and protocol standards based on the Ethernet frame layer and the IP layer, as well as various QoS support technologies, have gradually matured, providing a basis for implementing applications requiring better service quality. With advances in optical fiber manufacturing and transmission technologies, Gigabit Ethernet can transmit distances up to 100 kilometers, making it a technology choice to build metropolitan area networks and even wide area networks.

The other types of Ethernet

10 Gigabit Ethernet

The 10 Gigabit Ethernet specification, which is included in the IEEE 802.3ae supplement to the IEEE 802.3 standard, extends the IEEE 802.3 protocol and MAC specifications to support 10 Gb / s transfer rates. In addition, 10 Gigabit Ethernet can be tuned to lower transmission rates such as 9.584640 Gb / s (OC-192) through the WAN interface sublayer (WIS), allowing 10 Gigabit Ethernet devices are compatible with the Synchronous Optical Network (SONET) STS-192c transport format.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/difference-between-frame-relay-and-atm/
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002. -Pg.No (97-98)

Course Faculty

Verified by HOD

IQAC

L-7

LECTURE HANDOUTS

CSE	**III/VI**

Course Name with Code :High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : I- High Speed Networks   Date of Lecture:

| |
| --- |
| **Topic of Lecture:** Fibre Channel |
| **Introduction :**
Fibre Channel is a high-speed networking technology primarily used for transmitting data among data centers, computer servers, switches and storage at data rates of up to 128 Gbps. |
| **Prerequisite knowledge for Complete understanding and learning of Topic:**
• I/O Operations
• Buffers
• Error Detection
• Error Recovery |
| **Detailed content of the Lecture:**
I/O channel communication
Direct point-to-point or multipoint communications link and mainly designed for high speed over very short distance.
Network channel communication
• A Network is a collection of interconnected access points with a software protocol structure. It allows different types of data rates and provide flow and error control. Fiber channel is designed to combine the best features of both technologies .
• In fiber channel , the simplicity and speed of channel communication is combined with flexibility and
inter connectivity of network based communication .
Requirements of fibre channel
• Full duplex links with two fibers per link
• Performance from 100 Mbps TO 800 Mbps on a single line
• Support for distances up to 10 km
• High capacity utilization with distance insensitivity
• Broad availability
• Support multicost
Fibre channel elements
1. N- ports
Key elements of a fiber channel network are the end systems called nodes. Each node include one or more ports called **N-ports.**
2. F-ports
Network itself consists of one or more Switching elements. The collection of switching elements is |

referred to as a **fabric.** Each fabric switching elements include multiple ports called **F-ports.**

Fibre Channel Protocol Architecture
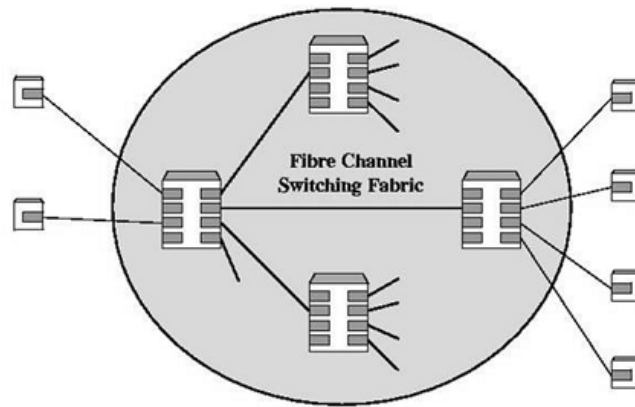
Fiber channel organized into five levels

1. **FC-0 Physical Media** -includes optical fiber for long distance, coaxial cable for high speed over short distance, shielded twisted pair for lower speeds over short distance.

2. **FC-1 Transmission Protocol** -it defines the signal encoding scheme.

3. **FC-2 Framing Protocol –**deals with topologies frame format, flow of error control

4. **FC-3 Common Services –**it includes multicasting

5. **FC-4 Mapping –**mapping of various channel and network protocols to fiber channel including **IEEE 802.11, ATM, IP, SCSI**

Transmission Media

- Video coaxial cable
- optical fiber
- shielded twisted pair

Topologies

Topology supported by fiber channel are

- Fabric or switcher topology
- point –to-point topology
- o arbitrated loop topology.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=Ac8824tFS8c
https://www.youtube.com/watch?v=Ish0DOaTdtA

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No(140-144)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS	**L-8**

CSE	**III/VI**

Course Name with Code   :High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : I- High Speed Networks   **Date of Lecture:**

Topic of Lecture: Wireless LAN's :WiFi and WiMax Networks applications, Requirements

Introduction :
- WiMax can be used to provide internet services such as mobile data and WiFi spots. Wifi is defined under IEEE 802.11x standards where x stands for various WiFi versions.
- WiMax is defined under IEEE 802.16y standards where y stands for various WiMax versions.
- WiFi is for LAN (Local Area Network) applications.

Prerequisite knowledge for Complete understanding and learning of Topic:
- LAN
- Ethernet
- Wireless Communication

Detailed content of the Lecture:
- WiMAX (Worldwide Interoperability for Microwave Access) is a family of wireless broadband communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options.
- The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors.
- The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.
- IEEE 802.16m or Wireless MAN-Advanced was a candidate for the 4G, in competition with the LTE Advanced standard.
- WiMAX was initially designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations.
- The latest version of WiMAX, WiMAX release 2.1, popularly branded as/known as WiMAX 2+, is a smooth, backwards-compatible transition from previous WiMAX generations. It is compatible and inter-operable with TD-LTE.

Uses of WiMAX

The scalable physical layer architecture that allows for data rate to scale easily with available channel bandwidth and range of WiMAX make it suitable for the following potential applications:
- Providing portable mobile broadband connectivity across cities and countries through various devices.
- Providing a wireless alternative to cable and digital subscriber line (DSL) for "last mile" broadband access.

- Providing data, telecommunications (VoIP) and IPTV services (triple play).
- Providing Internet connectivity as part of a business continuity plan.
- Smart grids and metering.

Requirements

A wireless LAN must meet the same sort of requirements typical of any LAN, including high capacity, ability to cover short distances, full connectivity among attached stations, and broadcast capability. In addition, a number of requirements are specific to the wireless LAN environment. The following are among the most important requirements for wireless LANs:

Throughput: The medium access-control (MAC) protocol should make as efficient use as possible of the wireless medium to maximize capacity.

Number of nodes: Wireless LANs may need to support hundreds of nodes across multiple cells.

Connection to backbone LAN: In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure wireless LANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users and ad hoc wireless networks.

Service area. A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.

Battery power consumption: Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. This suggests that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. Typical wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.

Transmission robustness and security: Unless properly designed, a wireless LAN may be interference-prone and easily eavesdropped. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.

Collocated network operation: As wireless LANs become more popular, it's quite likely that two or more wireless LANs will operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.

License-free operation: Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

Handoff/roaming: The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.

Dynamic configuration: The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion, and relocation of end systems without disruption to other users.

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/WiMAX
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No (173-181)

Course Faculty

Verified by HOD

IQAC

L-9

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code   : **High Speed Networks-16CSE10**

Course Faculty   : **C.Nithya**

Unit   : **I- High Speed Networks**   Date of Lecture:

Topic of Lecture: Architecture of 802.11

Introduction :
IEEE 802.11 supports three basic topologies for WLANs, the independent basic service set (IBSS), the basic service set, and the extended service set (ESS). The MAC layer supports implementations of IBSS, basic service set, and ESS configurations.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Station
- IEEE
- MAC Layer
- Access Point

Detailed content of the Lecture:
- IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs).
- WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802.11 Architecture
The components of an IEEE 802.11 architecture are as follows −
- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
- Each station has a wireless network interface controller.

Basic Service Set
A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−
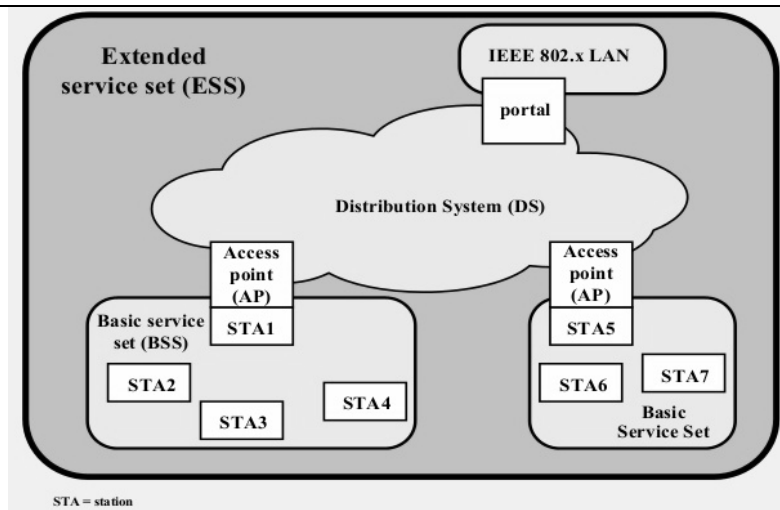- Infrastructure BSS − Here, the devices communicate with other devices through access points.
- Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.

Extended Service Set
- ESS is two or more BSS interconnected by DS appears as single logical LAN to LLC

Distribution System (DS)
- It connects access points in ESS.

Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.

IEEE 802.11 Frame Format

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=AWPgmEHVp1c
https://www.youtube.com/watch?v=O-FxxhONyPQ

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002-Pg.No(173-181)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

L-10

LECTURE HANDOUTS

CSE		III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   Date of Lecture:

Topic of Lecture: Queuing Analysis
Introduction : • Queuing system Data network where packets arrive, wait in various queues,– receive service at various points, and exit after some time • **Arrival rate:** Long-term number of arrivals per unit time • **Occupancy** :Number of packets in the system (averaged over a long time) • **Time in the system (delay)** :Time from packet entry to exit (averaged over many packets)
Prerequisite knowledge for Complete understanding and learning of Topic: • Queuing theory • Networking
Detailed content of the Lecture: • A single queue system is stable if packet arrival rate < system transmission capacity For a single queue, the ratiopacket arrival rate / system transmission capacity is called the utilization factor Describes the loading of a queue • In an unstable system packets accumulate in various queues and/or get dropped • For unstable systems with large buffers some packet delays become verylarge Flow/admission control may be used to limit the packet arrival rate • Prioritization of flows keeps delays bounded for the important traffic • Stable systems with time-stationary arrival traffic approach a steady-state **Little's Law** • For a given arrival rate, the time in the system is proportional to packet occupancy $N=\lambda T$ where N: average of packets in the system : packet arrival rate (packets per unit time)   T: average delay (time in the system) per packet Examples: On rainy days, streets and highways are more crowded • Fast food restaurants need a smaller dining room than regular restaurants with the same customer arrival rate Large buffering together with large arrival rate cause large delays **Delay is Caused by Packet Interference** • If arrivals are regular or sufficiently spaced apart, no queuing delay occurs • Burstiness Causes Interference • Packet Length Variation Causes Interference • High Utilization Exacerbates Interference • Variable packet sizes

Queueing models can be represented using Kendall's notation:

A/B/S/K/N/Disc

where:

- A is the interarrival time distribution
- B is the service time distribution
- S is the number of servers
- K is the system capacity
- N is the calling population
- Disc is the service discipline assumed

Some standard notation for distributions (A or B) are:

- M for a Markovian (exponential) distribution
- Eκ for an Erlang distribution with κ phases
- D for Deterministic (constant)
- G for General distribution
- PH for a Phase-type distribution

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=bpPZQJ2QJps
https://www.youtube.com/watch?v=ZXVL3WjZODs

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (82-85)

Course Faculty

Verified by HOD

IQAC

| LECTURE HANDOUTS | L-11 |

| CSE | III/VI |

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   Date of Lecture:

Topic of Lecture: Queuing Models

Introduction :
- Queuing Networks (QN) are models where customers (service requests) arrive at service stations (servers) to be served.
- When customers arrive at a busy service station, they are queued for a waiting time until the service station is free. Both the arrival and service times are described as stochastic processes.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Queuing theory
- Networking

Detailed content of the Lecture:

Queuing Models

- Construction and analysis Queuing models are generally constructed to represent the steady state of a queuing system, that is, the typical, long run or average state of the system.
- As a consequence, these are stochastic models that represent the probability that a queuing system will be found in a particular configuration or state.

A general procedure for constructing and analyzing such queuing models is:

1. Identify the parameters of the system, such as the arrival rate, service time, Queue capacity, and perhaps draw a diagram of the system.
2. Identify the system states. (A state will generally represent the integer number of customers, people, jobs, calls, messages, etc. in the system and may or may not be limited.)
3. Draw a state transition diagram that represents the possible system states and identify the rates to enter and leave each state. This diagram is a representation of a Markov chain.
4. Because the state transition diagram represents the steady state situation between state there is a balanced flow between states so the probabilities of being in adjacent states can be related mathematically in terms of the arrival and service rates and state probabilities.
5. Express all the state probabilities in terms of the empty state probability, using the inter-state transition relationships.
6. Determine the empty state probability by using the fact that all state probabilities always sum to 1. Whereas specific problems that have small finite state models are often able to be analyzed numerically, analysis of more general models, using calculus, yields useful formulae that can be applied to whole classes of problems.

Poisson arrivals and service

- M/M/1/∞/∞ represents a single server that has unlimited queue capacity and infinite calling population, both arrivals and service are Poisson (or random) processes, meaning the statistical distribution of both the inter-arrival times and the service times follow the exponential distribution.
- Because of the mathematical nature of the exponential distribution, a number of quite simple relationships are able to be derived for several performance measures based on knowing the arrival rate and service rate.

Characteristics

- The arrival pattern.
- The service mechanism.
- The queue discipline.
- The number of customers allowed in the system.
- The number of service channels.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=bpPZQJ2QJps
https://www.youtube.com/watch?v=ZXVL3WjZODs

Important Books/Journals for further learning including the page nos.:
John L Hennessey and David A Patterson, " Computer Architecture A Quantitative Approach",
Morgan Kaufmann/ Elsevier, Fifth Edition,2012,Page No: (85-112)

Course Faculty

Verified by HOD

IQAC

L-12

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : II- Congestion and Traffic Management   Date of Lecture:

Topic of Lecture: Single Server Queues

Introduction :
- The simplest queue is a line of customers, in which the customer at the head of the line receives service from a single server and then departs, and arriving customers join the tail of the line.
- At points where several wires meet, incoming packets are queued up, inspected, and sent out over the appropriate wire.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Queuing theory
- Networking

Detailed content of the Lecture:

Single-server queue
- A network of single-server nodes fed by customers of several classes is considered.
- Each customer is equipped with the random work to be done for completing service.
- The distribution of this work and the rate of its decreasing during the service depend on the node, the class of the customer, the queue contents and the residual workloads of the customers at the node.
- The service discipline is LCFS preemptive-resume.
- For both open and closed network, the stationary distribution is derived.
- In general, this distribution is not a product form.
- For the open network, sufficient conditions yielding the product form are given.
- For both open and closed network, sufficient invariance conditions are found.
- Single-server queues are, perhaps, the most commonly encountered queueing situation in real life. One encounters a queue with a single server in many situations, including business (e.g. sales clerk), industry (e.g. a production line), transport (e.g. a bus, a taxi rank, an intersection), telecommunications (e.g. Telephone line), computing (e.g. processor sharing).
- Even where there are multiple servers handling the situation it is possible to consider each server individually as part of the larger system, in many cases. (e.g A supermarket checkout has several single server queues that the customer can select from.)
- Consequently, being able to model and analyse a single server queue's behaviour is a particularly useful thing to do.
- Queues can also be used to model problems in insurance. Suppose an insurance broker starts

- with a certain amount of capital.
- Every day a certain amount of money is paid out in claims (the 'service' that day), and a certain amount of money is paid in in premiums (the 'arrivals' that day), and the capital at the end of the day is the starting capital plus arrivals minus service.
- We may wish to know how likely it is that there is insufficient capital to meet the claims on a given day. Another application is to packet-based data networks.
- Data is parceled up into packets and these are sent over wires.
- At points where several wires meet, incoming packets are queued up, inspected, and sent out over the appropriate wire.
- When the total number of packets in the queue (the 'amount of work' in the queue) reaches a certain threshold (the 'buffer size'), incoming packets are discarded.
- We may wish to know the frequency of packet discard, to know how large to make the buffer.
- There are many more applications, and many extensions—multiple servers, different service disciplines, networks of queues, etc. etc.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=6Ojr-Q319r8

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002 .Page No(110-120)

Course Faculty

Verified by HOD

IQAC

L-13

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   **Date of Lecture:**

Topic of Lecture: Effects of Congestion
Introduction :   • Congestion shrinks the delivery area that any one driver and vehicle can serve. This means that there is a need to have more vehicles on the road (to maintain and grow distribution and trucking markets), and routes need to be changed more often.
Prerequisite knowledge for Complete understanding and learning of Topic: • Queuing theory   • Networking   • Queuing Networks

Detailed content of the Lecture:
 Effects of Congestion
 Congestion-Control Mechanisms
 Backpressure
   – Request from destination to source to reduce rate
   – Useful only on a logical connection basis
   – Requires hop-by-hop flow control mechanism
 Policing
   – Measuring and restricting packets as they enter the network
 Choke packet
   – Specific message back to source
       E.g., ICMP Source Quench
 Implicit congestion signaling
   – Source detects congestion from transmission delays and lost packets and reduces flow
 Explicit congestion signaling
 • Frame Relay reduces network overhead by implementing simple congestion notification mechanisms rather than explicit, per-virtual-circuit flow control.
 • Frame Relay typically is implemented on reliable network media, so data integrity is not sacrificed because flow control can be left to higher-layer protocols.
     o Frame Relay implements two congestion-notification mechanisms:
     o Forward-explicit congestion notification (FECN)
 • Backward-explicit congestion notification (BECN) FECN and BECN each is controlled by a single bit contained in the Frame Relay frame header.

- The Frame Relay frame header also contains a Discard Eligibility (DE) bit, which is used to identify less important traffic that can be dropped during periods of congestion.
- If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1.
- When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination.
- The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored.

Frame Relay Discard Eligibility
- The Discard Eligibility (DE) bit is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header.
- DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not.
- This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

Frame Relay Error Checking
- Frame Relay uses a common error-checking mechanism known as the cyclic redundancy check (CRC). The CRC compares two calculated values to determine whether errors occurred during the transmission from source to destination.
- Frame Relay reduces network overhead by implementing error checking rather than error correction. Frame Relay typically is implemented on reliable network media, so data integrity is not sacrificed because error correction can be left to higher-layer protocols running on top of Frame Relay.

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-14

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   Date of Lecture:

Topic of Lecture: Congestion Control

Introduction :
- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
- In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal)

Prerequisite knowledge for Complete understanding and learning of Topic:
- Queuing theory
- Networking
- Protocols

Detailed content of the Lecture:

Congestion Control

Backpressure:
- If node becomes congested it can slow down or halt flow of packets from other nodes
- May mean that other nodes have to apply control on incoming packet rates
- Propagates back to source
- Can restrict to logical connections generating most traffic
- Used in connection oriented that allow hop by hop congestion control (e.g. X.25)
- Not used in ATM nor frame relay
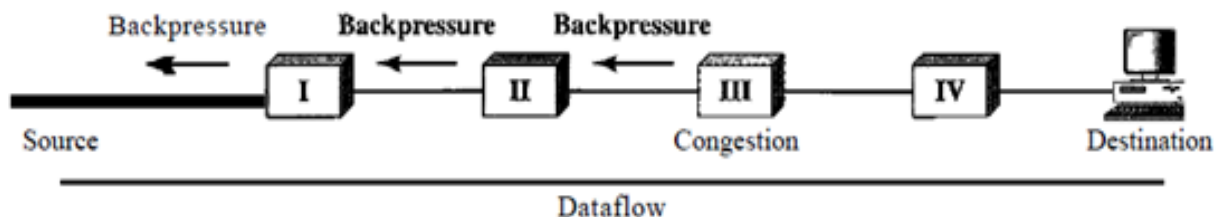
Choke Packet : A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure choke packet send the message to source directly.
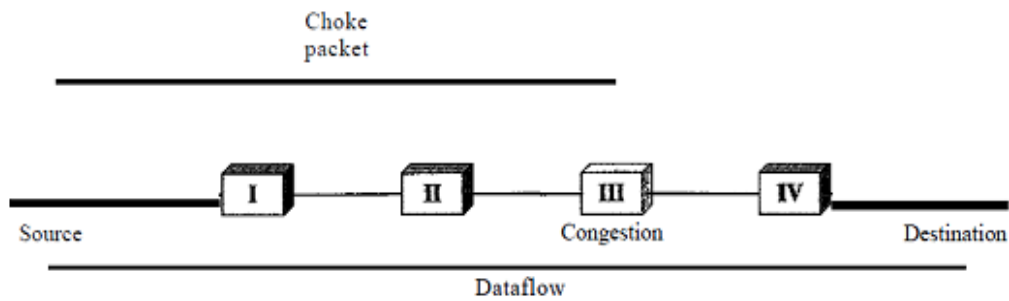
Control packet

— Generated at congested node

— Sent to source node

— e.g. ICMP source quench

- From router or destination
- Source cuts back until no more source quench message
- Sent for every discarded packet, or anticipated
- Rather crude mechanism

Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms.

Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method.

Explicit congestion signaling approaches can work in one of two directions:

• Backward and

• Forward.

We can divide explicit congestion signaling approaches into three general

categories:

• BINARY: A bit is set in a data packet as it is forwarded.

• CREDIT BASED: by the congested node.

These schemes are based on providing an explicit credit to a source

over a logical connection.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=6Ojr-Q319r8

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (146-147)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

LECTURE HANDOUTS

L-15

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : II- Congestion and Traffic Management   **Date of Lecture:**

Topic of Lecture: Traffic Management

Introduction :
- In an ATM network, a **traffic source descriptor** is used to describe an end user service to the network.
- In the ITU these user services have been classified based upon their Quality of Service (QoS) requirements.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Queuing theory
- Networking
- Protocols

Detailed content of the Lecture:

Traffic Management
- In an ATM network, a **traffic source descriptor** is used to describe an end user service to the network.
- In the ITU these user services have been classified based upon their Quality of Service (QoS)
requirements.

The following **parameters** have been identified as being important to service
provisioning:

   • End-to-end delay
   • Delay variation (jitter)
   • Cell loss ratio

Given those three parameters the following QoS classes of service have been defined by the **ITU**:

   • **Class 1** corresponding to Class A - CBR traffic
   • **Class 2** corresponding to Class B - VBR traffic with timing
   • **Class 3** corresponding to Class C - connection oriented data
   • **Class 4** corresponding to Class D - connectionless data

The **ATM Forum** has specified a different set of classes of service:

   • **Constant Bit Rate (CBR)** - continuous bit stream with timing
   • **Real-time Variable Bit Rate (rt-VBR)** - low transit delay with guaranteed delivery service (i.e. low
losses) and timing.
   • **Non-real-time Variable Bit Rate (nrt-VBR)** - guaranteed delivery service but with less

stringent delay
requirements.

• **Unspecified Bit Rate (UBR)** - for best effort delivery of data traffic, no
guarantees whatsoever.

• **Available Bit Rate (ABR)** - guaranteed delivery service for a minimum bandwidth
requirement. If more bandwidth is available the service can use it.

Admission and Congestion Control in ATM Networks

Traffic control incorporates two functions: Connection Admission Control (CAC) and Usage
Parameter Control (UPC).

- **CAC** is implemented during the call setup procedure to ensure that the admission of a call will
  not jeopardize the existing connections and also that enough network resources are available for
  this call. If the connection is admitted, a certain amount of bandwidth (BW) and buffer will be
  reserved according to the source traffic descriptor and the required quality of service (QoS). A
  service contract is also specified stating the traffic behavior the input bit stream should
  conform to in order to achieve the desired QoS.

- **UPC** is performed during a connection's lifetime to monitor and control the input traffic. Its
  main purpose is to **protect network resources** from malicious as well as unintentional
  misbehavior which can affect the QoS of other established connections by detecting violations
  of negotiated parameter values.

- If excessive traffic is detected, it can be either immediately discarded or tagged for selective
  discarding if congestion is encountered in the network.

Traffic Management in Congested Network – Some Considerations

Fairness

- Various flows should "suffer" equally
- Last-in-first-discarded may not be fair

Quality of Service (QoS)

- Flows treated differently, based on need
- Voice, video: delay sensitive, loss insensitive
- File transfer, mail: delay insensitive, loss sensitive
- Interactive computing: delay and loss sensitive

Reservations

Policing: excess traffic discarded or handled on best-effort basis

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=RP4OAbyVjV8&t=597s

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (146-147)

Course Faculty

Verified by HOD

IQAC

L-16

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   **Date of Lecture:**

Topic of Lecture: Congestion Control in Packet Switching Networks
Introduction :   - Congestion control in packet-switched data networks is necessary if the performance of the network in the presence of severe overload conditions is to be maintained.   - The routers in the Network Layer implement a congestion control scheme, part of which measures the sustainable traffic rate across the network for each traffic flow
Prerequisite knowledge for Complete understanding and learning of Topic: - Queuing theory   - Networking   - Protocols
Detailed content of the Lecture: **Congestion Control in Packet Switching Networks**   Number of control mechanisms for congestion control in packet-switching networks have been suggested and tried: - Send a control packet from a congested node to some or all source nodes.   - Rely on routing information. Routing algorithms provide link delay information to other nodes, which influences routing decisions.   - Make use of an end-to-end probe packet; such a packet could be time stamped to measure the delay between two particular endpoints.   - Allow packet-switching nodes to add congestion information to packets; as they go by there are two possible approaches: - A node could add such information to packets going in the direction opposite to the congestion. This information reaches to the source node, which can reduce the flow of packets into the network.   - A node could add such information to packets going in the same direction as the congestion.   **Frame relay congestion control techniques**   - It is difficult to design congestion control in frame relay network because limited tools available at frame handler.   - Frame relay protocol streamlined to get maximum throughput and efficiency   - Therefore the frame handler cannot control flow of frames from any subscriber   - Discard strategy   - Congestion avoidance (explicit signaling)

- Congestion recovery (implicit signaling)

Congestion avoidance (explicit signaling)

This procedure used at beginning stage of congestion to minimize its effects. It prevents the congestion.

There are two bits for explicit congestion notification

Forward Explicit Congestion Notification

      i. For traffic in same direction as received frame

      ii. The means that this frame has encountered congestion

Backward Explicit Congestion Notification

      i. For traffic in opposite direction of received frame

      ii. The bit means that the Frames transmitted may encounter congestion

Congestion recovery procedures

Congestion recovery procedures are used to prevent network collapse in the face of severe congestion. These procedures are typically initiated when the network has begun to drop frames due to congestion. These dropped packets serve as implicit signaling mechanism.

      1. The response to BECN signal is that the user simply reduces the rate at which frames are transmitted until the signal ceases.

      2. The response to FECN is that the user notifies its peer user of this connection to restrict its flow of frames.

Discard strategy

Discard strategy deals with the most fundamental response to congestion. When the congestion becomes severe enough, the network is forced to discard frames. This is also called as Traffic control management.

Video Content / Details of website for further learning (if any):
https://www.sciencedirect.com/science/article/abs/pii/0140366480900687

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (148-149)

Course Faculty

Verified by HOD

IQAC

L-17

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : II- Congestion and Traffic Management   **Date of Lecture:**

Topic of Lecture: Congestion Control in Packet Switching Networks

Introduction :
- Congestion control in packet-switched data networks is necessary if the performance of the network in the presence of severe overload conditions is to be maintained.
- The routers in the Network Layer implement a congestion control scheme, part of which measures the sustainable traffic rate across the network for each traffic flow

Prerequisite knowledge for Complete understanding and learning of Topic:
- Queuing theory
- Networking
- Protocols

Detailed content of the Lecture:

Congestion Control in Packet Switching Networks

Number of control mechanisms for congestion control in packet-switching networks have been suggested and tried:

1. Send a control packet from a congested node to some or all source nodes.
2. Rely on routing information. Routing algorithms provide link delay information to other nodes, which influences routing decisions.
3. Make use of an end-to-end probe packet; such a packet could be time stamped to measure the delay between two particular endpoints.
4. Allow packet-switching nodes to add congestion information to packets; as they go by there are two possible approaches:
5. A node could add such information to packets going in the direction opposite to the congestion. This information reaches to the source node, which can reduce the flow of packets into the network.
6. A node could add such information to packets going in the same direction as the congestion.

Frame relay congestion control techniques
- It is difficult to design congestion control in frame relay network because limited tools available at frame handler.
- Frame relay protocol streamlined to get maximum throughput and efficiency
- Therefore the frame handler cannot control flow of frames from any subscriber
- Discard strategy
- Congestion avoidance (explicit signaling)

- Congestion recovery (implicit signaling)

Congestion avoidance (explicit signaling)

This procedure used at beginning stage of congestion to minimize its effects. It prevents the congestion.

There are two bits for explicit congestion notification

Forward Explicit Congestion Notification

      i. For traffic in same direction as received frame

      ii. The means that this frame has encountered congestion

Backward Explicit Congestion Notification

      i. For traffic in opposite direction of received frame

      ii. The bit means that the Frames transmitted may encounter congestion

Congestion recovery procedures

Congestion recovery procedures are used to prevent network collapse in the face of severe congestion. These procedures are typically initiated when the network has begun to drop frames due to congestion. These dropped packets serve as implicit signaling mechanism.

      1. The response to BECN signal is that the user simply reduces the rate at which frames are transmitted until the signal ceases.

      2. The response to FECN is that the user notifies its peer user of this connection to restrict its flow of frames.

Discard strategy

Discard strategy deals with the most fundamental response to congestion. When the congestion becomes severe enough, the network is forced to discard frames. This is also called as Traffic control management.

Video Content / Details of website for further learning (if any):
https://www.sciencedirect.com/science/article/abs/pii/0140366480900687

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (148-149)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

LECTURE HANDOUTS	**L-18**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : II- Congestion and Traffic Management   Date of Lecture:

Topic of Lecture: Frame Relay Congestion Control
Introduction :   - Frame Relay uses congestion avoidance by means of two bit fields present in the Frame Relay frame to explicitly warn source and destination of presence of congestion   - BECN: Backward Explicit Congestion Notification (BECN) warns the sender of congestion present in the network.
Prerequisite knowledge for Complete understanding and learning of Topic: - Queuing theory   - Networking   - Protocols
Detailed content of the Lecture: **Frame Relay :-**   Frame Format is shown below:-   C/R: Command/response   BECN: Backward explicit congestion notification   EA: Extended address   DE: Discard eligibility   FECN: Forward explicit congestion notification   DLCI: Data link connection identifier   - This frame is very similar to the HDLC frame except for the missing control field here.   - The control field is not needed because flow and error control are not needed.   - The Flag, FCS and information fields are same as those of HDLC.   - The address field defines the DLCI along with some other bits required for congestion control and traffic control.
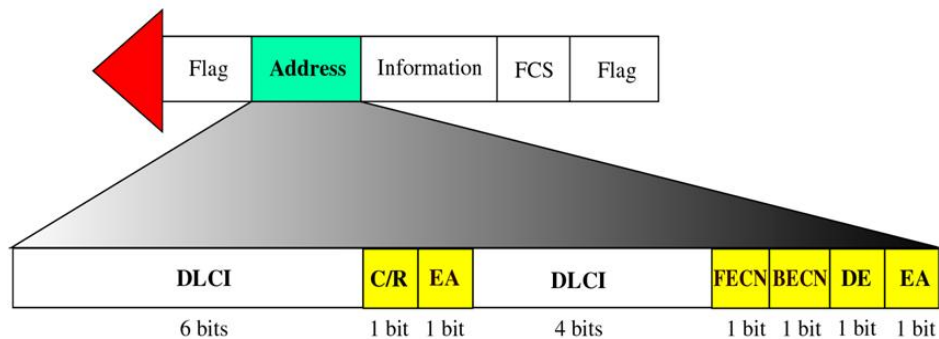
Their description is as follows:

1. DLCI field:

The first part of DLCI is of 6 bits and the second part is of 4 bits. They together form a 10 bit data link connection identifier.

2. Command / Response (C / R):

The C/R bit allows the upper layers to identify a frame as either a command or response. It is not used by the frame relay protocol.

3. Extended Address (EA):

- This bit indicates whether the current byte is the final byte of the address.

- If EA = 1 it indicates that the current byte is the final one but if EA = 0, then it tells that another address byte is going to follow.

4. Forward Explicit Congestion Notification (FECN):

- This bit can be set by any switch to indicate that traffic is congested in the direction of travel of the frame.

- The destination is informed about the congestion via this bit.

5. Backward Explicit Congestion Notification (BECN):

- This bit indicates the congestion in the direction opposite to the direction of frame travel.

- It informs the sender about the congestion.

6. Discard Eligibility (DE):

- The DE bit indicates the priority level of the frame. In the overload situations a frame may have to be discarded.

- If DE = 1 then that frame can be discarded in the event of congestion.

- DE bit can be set by the sender or by any switch in the network.

Video Content / Details of website for further learning (if any):
https://fossbytes.com/congestion-control-frame-relay/

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (148-149)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

L-19

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: TCP Flow control – TCP Congestion Control
Introduction : • TCP is the protocol that guarantees we can have a reliable communication channel over an unreliable network. • When we send data from a node to another, packets can be lost, they can arrive out of order, the network can be congested or the receiver node can be overloaded.
Prerequisite knowledge for Complete understanding and learning of Topic: • Transmission control protocol • Window size • Acknowledgement
Detailed content of the Lecture: Flow Control basically means that TCP will ensure that a sender is not overwhelming a receiver by sending packets faster than it can consume. It's pretty similar to what's normally called *Back pressure*. **TCP uses a form of sliding window** • Differs from mechanism used in LLC, HDLC, X.25, and others • Decouples acknowledgement of received data units from granting permission to send more • TCP's flow control is known as a credit allocation scheme • Each transmitted octet is considered to have a sequence number **TCP Header Fields for Flow Control** • Sequence number (SN) of first octet in data segment • Acknowledgement number (AN) • Window (W) • Acknowledgement contains AN = i, W = j: • Octets through SN = i - 1 acknowledged • Permission is granted to send W = j more octets   i.e., octets i through i + j – 1 **Credit Allocation is Flexible** Suppose last message B issued was AN = i, W = j • To increase credit to k (k > j) when no new data, B issues AN = i, W = k • To acknowledge segment containing m octets (m < j), B issues AN = i + m, W = j – m

TCP Credit Allocation Mechanism

Transport Entity A   Transport Entity B

A may send 1400 octets — B is prepared to receive 1400 octets, beginning with 1001

A shrinks its transmit window with each transmission

B acknowledges 3 segments (600 octets), but is only prepared to receive 200 additional octets beyond the original budget (i.e., B will accept octets 1601 through 2600)

A adjusts its window with each credit

A exhausts its credit

B acknowledges 5 segments (1000 octets) and restores the original amount of credit

A receives new credit

$SN = 1001$
$SN = 1201$
$SN = 1401$
$AN = 1601, W = 1000$
$SN = 1601$
$SN = 1801$
$SN = 2001$
$SN = 2201$
$SN = 2401$
$AN = 2601, W = 1400$

Flow Control Perspectives

Data octets so far acknowledged
Data octets already transmitted
Octets not yet acknowledged
Window of octets that may be transmitted

Initial Sequence Number (ISN)
Last octet acknowledged (AN – 1)
Last octet transmitted
Window shrinks from trailing edge as segments are sent
Window expands from leading edge as credits are received

(a) Send sequence space

Data octets so far acknowledged
Data octets already received
Octets not yet acknowledged
Window of octets that may be accepted

Initial Sequence Number (ISN)
Last octet acknowledged (AN – 1)
Last octet received
Window shrinks from trailing edge as segments are received
Window expands from leading edge as credits are sent

(b) Receive sequence space

Credit Policy

- Receiver needs a policy for how much credit to give sender
- Conservative approach: grant credit up to limit of available buffer space
- May limit throughput in long-delay situations
- Optimistic approach: grant credit based on expectation of freeing space before data arrives

Effect of Window Size

W = TCP window size (octets)

R = Data rate (bps) at TCP source

D = Propagation delay (seconds)

- After TCP source begins transmitting, it takes D seconds for first octet to arrive, and D seconds for acknowledgement to return
- TCP source could transmit at most 2RD bits, or RD/4 octets

The sliding window

- TCP uses a sliding window protocol to control the number of bytes in flight it can have. In other words, the number of bytes that were sent but not yet acked.
- Both Flow Control and Congestion Control are the traffic controlling methods in different situations.
- The main difference between flow control and congestion control is that, In flow control, Traffics are controlled which are flow from sender to a receiver. On the other hand, In congestion control, Traffics are controlled entering to the network.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=CQFtBaEzDnU
https://www.brianstorti.com/tcp-flow-control/
 https://www.youtube.com/watch?v=4l2_BCr-bhw
https://www.geeksforgeeks.org/difference-between-flow-control-and-congestion-control/

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (189-190)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS	L-20

CSE	III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: Retransmission – Timer Management- Exponential RTO- backoff – KARN's Algorithm
Introduction : To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received. If the timer expires timeout occurs and the segment is retransmitted.
Prerequisite knowledge for Complete understanding and learning of Topic: • Acknowledgement • TCP • Retransmission • Segment
Detailed content of the Lecture: **Retransmission Strategy** • TCP relies exclusively on positive acknowledgements and retransmission on acknowledgement timeout • There is no explicit negative acknowledgement • Retransmission required when: • Segment arrives damaged, as indicated by checksum error, causing receiver to discard segment • Segment fails to arrive **Timers** • A timer is associated with each segment as it is sent • If timer expires before segment acknowledged, sender must retransmit **Key Design Issue:** • value of retransmission timer • Too small: many unnecessary retransmissions, wasting network bandwidth • Too large: delay in handling lost segment **Two Strategies** • Timer should be longer than round-trip delay (send segment, receive ack) • Delay is variable **Strategies:** • Fixed timer

- Adaptive

Problems with Adaptive Scheme
- Peer TCP entity may accumulate acknowledgements and not acknowledge immediately
- For retransmitted segments, can't tell whether acknowledgement is response to original transmission or retransmission
- Network conditions may change suddenly

Implementation Policy Options
- Send
- Deliver
- Accept
- In-order
- In-window
- Retransmit
- First-only
- Batch
- individual
- Acknowledge
- immediate
- cumulative

TCP Flow and Congestion Control
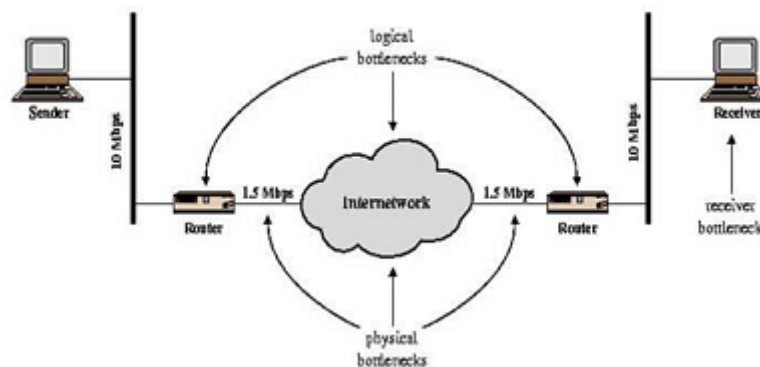
Retransmission Timer Management

Three Techniques to calculate retransmission timer (RTO):
- RTT Variance Estimation
- Exponential RTO Backoff
- Karn's Algorithm

RTT Variance Estimation (Jacobson's Algorithm)

3 sources of high variance in RTT
- If data rate relative low, then transmission delay will be relatively large, with larger variance due to variance in packet size
- Load may change abruptly due to other sources
- Peer may not acknowledge segments immediately

Two Other Factors

Jacobson's algorithm can significantly improve TCP performance

Exponential RTO Backoff
- Increase RTO each time the same segment retransmitted – backoff process

Multiply RTO by constant:

RTO = q × RTO

q = 2 is called binary exponential backoff

Which Round-trip Samples?

- If an ack is received for retransmitted segment, there are 2 possibilities:
- Ack is for first transmission
- Ack is for second transmission
- TCP source cannot distinguish 2 cases
- No valid way to calculate RTT:

–From first transmission to ack, or

–From second transmission to ack?

Karn's Algorithm

   The first part of Karn's Algorithm states that when there is retransmission ambiguity, RTT measurements are ignored instead of being incorporated into SRTT to avoid skewing SRTT incorrectly. For each retransmission, TCP applies a "backoff factor" to each RTO, so subsequent retransmission timers are double the previous

- Do not use measured RTT to update SRTT and SDEV
- Calculate backoff RTO when a retransmission occurs
- Use backoff RTO for segments until an ack arrives for a segment that has not been retransmitted
- Then use Jacobson's algorithm to calculate RTO

Video Content / Details of website for further learning (if any):

https://en.wikipedia.org/wiki/Karn%27s_algorithm
https://www.extrahop.com/company/blog/2016/retransmission-timeouts-rtos-application-performance-degradation/
https://www.youtube.com/watch?v=Og4Br2Jog5Y
https://www.geeksforgeeks.org/tcp-timers/

Important Books/Journals for further learning including the page nos.:

William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (190-193)

Course Faculty

Verified by HOD

IQAC

L-21

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : **C.Nithya**

Unit : **III- TCP and ATM Congestion Control** Date of Lecture:

Topic of Lecture: Window management- Performance of TCP over ATM
Introduction :   Sliding windows, a technique also known as **windowing**, is used by the Internet's Transmission Control Protocol (**TCP**) as a method of controlling the flow of packets between two computers or network hosts. **TCP** requires that all transmitted data be acknowledged by the receiving host.
Prerequisite knowledge for Complete understanding and learning of Topic: • Window size   • Asynchronous Transfer Mode   • Fast recovery   • Congestion
Detailed content of the Lecture: **Window Management**   • Slow start   • Dynamic window sizing on congestion   • Fast retransmit   • Fast recovery   • Limited transmit   **Slow Start**   awnd = MIN[credit, cwnd]   where   awnd = allowed window in segments   cwnd = congestion window in segments   credit = amount of unused credit granted in most recent ack   cwnd = 1 for a new connection and increased by 1 for each ack received, up to a maximum   **Dynamic Window Sizing on Congestion**   • A lost segment indicates congestion   • Prudent to reset cwsd = 1 and begin slow start process   • May not be conservative enough: ― easy to drive a network into saturation but hard for the net to recover‖ (Jacobson)   • Instead, use slow start with linear growth in cwnd   **Fast Retransmit**   • RTO is generally noticeably longer than actual RTT   • If a segment is lost, TCP may be slow to retransmit   • TCP rule: if a segment is received out of order, an ack must be issued immediately for the last in-

order segment
- Fast Retransmit rule: if 4 acks received for same segment, highly likely it was lost, so retransmit immediately, rather than waiting for timeout

Effect of Slow Start
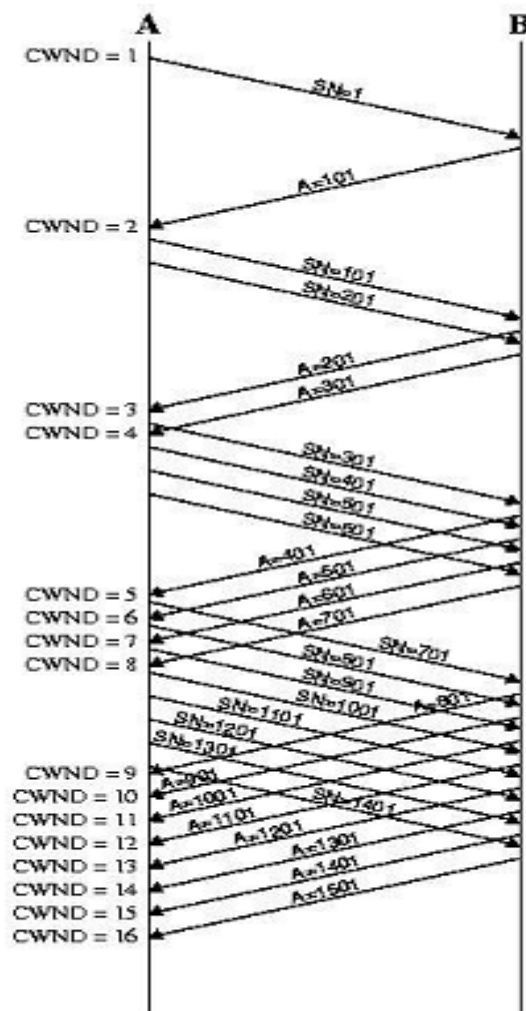
Fast Recovery
- When TCP retransmits a segment using Fast Retransmit, a segment was assumed lost
- Congestion avoidance measures are appropriate at this point
- E.g., slow-start/congestion avoidance procedure
- This may be unnecessarily conservative since multiple acks indicate segments are getting through
- Fast Recovery: retransmit lost segment, cut cwnd in half, proceed with linear increase of cwnd
- This avoids initial exponential slow-start

Limited Transmit
- If congestion window at sender is small, fast retransmit may not get triggered, e.g., cwnd = 3
- Under what circumstances does sender have small congestion window?
- If the problem is common, why not reduce number of duplicate acks needed to trigger retransmit?

Limited Transmit Algorithm

Sender can transmit new segment when 3 conditions are met:
- Two consecutive duplicate acks are received
- Destination advertised window allows transmission of segment
- Amount of outstanding data after sending is less than or equal to cwnd + 2

Performance of TCP over ATM
- How best to manage TCP's segment size, window management and congestion control at the same time as ATM's quality of service and traffic control policies

- TCP may operate end-to-end over one ATM network, or there may be multiple ATM LANs or WANs with non-ATM networks

TCP/IP over AAL5/ATM
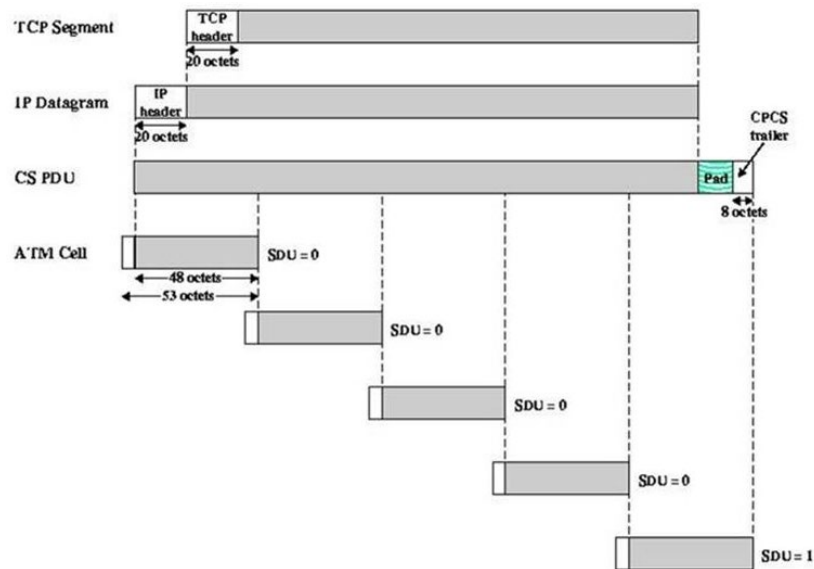
Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=hkXPXJA8-UA
https://en.wikipedia.org/wiki/Sliding_window_protocol
https://searchnetworking.techtarget.com/definition/fast-retransmit-and-recovery

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002.Page No: (193-197)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

LECTURE HANDOUTS	L-22

CSE	III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: Traffic and Congestion control in ATM – Requirements – Attributes

Introduction :
Control needed to prevent switch buffer overflow
- High speed and small cell size gives different problems from other networks
- Limited number of overhead bits
- ITU-T specified restricted initial set – I.371
- ATM forum Traffic Management Specification

Prerequisite knowledge for Complete understanding and learning of Topic:
- Congestion
- Buffer
- QOS
- Traffic Control

Detailed content of the Lecture:
Congestion problem
- Framework adopted by ITU-T and ATM forum
  – Control schemes for delay sensitive traffic
- Voice & video
  – Not suited to bursty traffic
  – Traffic control
  – Congestion control
- Bursty traffic
  – Available Bit Rate (ABR)
  – Guaranteed Frame Rate (GFR)

Requirements for ATM Traffic and Congestion Control
Most packet switched and frame relay networks carry non-real-time bursty data
        – No need to replicate timing at exit node
        – Simple statistical multiplexing
        – User Network Interface capacity slightly greater than average of channels

Problems with ATM Congestion Control
Most traffic not amenable to flow control
        – Voice & video cannot stop generating
Feedback slow
        – Small cell transmission time v propagation delay

Wide range of applications
- From few kbps to hundreds of Mbps
- Different traffic patterns
- Different network services

Key Performance Issues-Latency/Speed Effects
- E.g. data rate 150Mbps - Transfer time depends on number of intermediate switches, switching time and propagation delay. Assuming no switching delay and speed of light propagation, round trip delay of 48 x 10-3 sec across USA

Cell Delay Variation
- For digitized voice delay across network must be small
- Rate of delivery must be constant
- Variations will occur
- Dealt with by Time Reassembly of CBR cells (see next slide)
- Results in cells delivered at CBR with occasional gaps due to dropped cells
- Subscriber requests minimum cell delay variation from network provider

Network Contribution to Cell Delay Variation
In packet switched network
- Queuing effects at each intermediate switch
- Processing time for header and routing
Less for ATM networks
- Minimal processing overhead at switches
Fixed cell size, header format
No flow control or error control processing
- ATM switches have extremely high throughput
- Congestion can cause cell delay variation
Build up of queuing effects at switches
Total load accepted by network must be controlled

ATM Traffic-Related Attributes
Six service categories (see chapter 5)
- Constant bit rate (CBR)
- Real time variable bit rate (rt-VBR)
- Non-real-time variable bit rate (nrt-VBR)
- Unspecified bit rate (UBR)
- Available bit rate (ABR)
- Guaranteed frame rate (GFR)
Characterized by ATM attributes in four categories
- Traffic descriptors
- QoS parameters
- Congestion

Video Content / Details of website for further learning (if any):

https://www.cse.wustl.edu/~jain/cis788-95/ftp/atm_cong/index.html

https://www.slideshare.net/danielayalew1/traffic-and-congestion-control-in-atm-networks-chapter-13

https://pdfs.semanticscholar.org/fac5/2c0cf673577606e40ed5d1d5a45deb4e52be.pdf

Important Books/Journals for further learning including the page nos.:

William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (279-280)

Course Faculty

Verified by HOD

L-23

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: Traffic Management Frame work, Traffic Control
Introduction :   A traffic management framework, which couples the usage parameter control (UPC) and connection admission control (CAC) functions in an ATM network, is described.Untagged cells are protected in the backbone network nodes, whereas tagged cells are selectively discarded upon the onset of congestion.
Prerequisite knowledge for Complete understanding and learning of Topic: • Traffic Management   • Congestion Control   • TCP and UDP
Detailed content of the Lecture: Congestion problem   Framework adopted by ITU-T and ATM forum   – Control schemes for delay sensitive traffic   Voice & video   – Not suited to bursty traffic   – Traffic control   – Congestion control   Bursty traffic   – Available Bit Rate (ABR)   – Guaranteed Frame Rate (GFR)   **Requirements for ATM Traffic and Congestion Control**   Most packet switched and frame relay networks carry non-real-time burst data   – No need to replicate timing at exit node   – Simple statistical multiplexing   – User Network Interface capacity slightly greater than average of channels   Congestion control tools from these technologies do not work in ATM   **Problems with ATM Congestion Control**   Most traffic not amenable to flow control

– Voice & video can not stop generating

Feedback slow

– Small cell transmission time v propagation delay

Wide range of applications

– From few kbps to hundreds of Mbps

– Different traffic patterns

– Different network services

High speed switching and transmission

– Volatile congestion and traffic control

Key Performance Issues-Latency/Speed Effects

E.g. data rate 150Mbps

Takes $(53 \times 8 \text{ bits})/(150 \times 10^6)$ =2.8 x 10-6 seconds to insert a cell

Transfer time depends on number of intermediate switches, switching time and propagation delay. Assuming no switching delay and speed of light propagation, round trip delay of 48 x 10-3 sec across USA

A dropped cell notified by return message will arrive after source has transmitted N further cells

N=(48 x 10-3 seconds)/(2.8 x 10-6 seconds per cell)

=1.7 x 104 cells = 7.2 x 106 bits

i.e. over 7 Mbits

Cell Delay Variation

- For digitized voice delay across network must be small
- Rate of delivery must be constant
- Variations will occur
- Dealt with by Time Reassembly of CBR cells (see next slide)
- Results in cells delivered at CBR with occasional gaps due to dropped cells
- Subscriber requests minimum cell delay variation from network provider
    - Increase data rate at UNI relative to load
    - Increase resources within network

Video Content / Details of website for further learning (if any):

https://www.youtube.com/watch?v=-J55l7XJv0c

https://www.youtube.com/watch?v=JtYrwgzua0g

https://www.youtube.com/watch?v=be7mvlCJ67w

Important Books/Journals for further learning including the page nos.:

William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: (280-293)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

L-24

LECTURE HANDOUTS

CSE	III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: ABR traffic Management – ABR rate control

Introduction :
- QoS for CBR, VBR based on traffic contract and UPC described previously
- No congestion feedback to source
- Open-loop control
- Not suited to non-real-time applications
    – File transfer, web access, RPC, distributed file systems
    – No well defined traffic characteristics except PCR
    – PCR not enough to allocate resources
- Use best efforts or closed-loop control

Prerequisite knowledge for Complete understanding and learning of Topic:
- Loop Control
- Quality of Service

Detailed content of the Lecture:
Best Efforts
- Share unused capacity between applications
- As congestion goes up:
    – Cells are lost
    – Sources back off and reduce rate
    – Fits well with TCP techniques
    – Inefficient

Closed-Loop Control
- Sources share capacity not used by CBR and VBR
- Provide feedback to sources to adjust load
- Avoid cell loss
- Share capacity fairly
- Used for ABR

Characteristics of ABR
ABR connections share available capacity
        – Access instantaneous capacity unused by CBR/VBR
        – Increases utilization without affecting CBR/VBR QoS
Share used by single ABR connection is dynamic
        – Varies between agreed MCR and PCR
Network gives feedback to ABR sources

– ABR flow limited to available capacity

　　　　　– Buffers absorb excess traffic prior to arrival of feedback

Low cell loss

　　　　　– Major distinction from UBR

Feedback Mechanisms

Cell transmission rate characterized by:

　　　　　– Allowable cell rate

Current rate

　　　　　– Minimum cell rate

Min for ACR

May be zero

　　　　　– Peak cell rate

Max for ACR

　　　　　– Initial cell rate

Start with ACR=ICR

Adjust ACR based on feedback

Feedback in resource management (RM) cells

　　　　　– Cell contains three fields for feedback

Congestion indicator bit (CI)

No increase bit (NI)

Explicit cell rate field (ER)

Source Reaction to Feedback

If CI=1

　　　　　– Reduce ACR by amount proportional to current ACR but not less than CR

Else if NI=0

　　　　　– Increase ACR by amount proportional to PCR but not more than PCR

If ACR>ER set ACR<-max[ER,MCR]

Cell Flow on ABR

Two types of cell

　　　　　– Data & resource management (RM)

Source receives regular RM cells

　　　　　– Feedback

Bulk of RM cells initiated by source

　　　　　– One forward RM cell (FRM) per (Nrm-1) data cells

Nrm preset – usually 32

　　　　　– Each FRM is returned by destination as backwards RM (BRM) cell

　　　　　– FRM typically CI=0, NI=0 or 1 ER desired transmission rate in range ICR<=ER<=PCR

　　　　　– Any field may be changed by switch or destination before return

ATM Switch Rate Control Feedback

- EFCI marking
- Explicit forward congestion indication
- Causes destination to set CI bit in ERM
- Relative rate marking
- Switch directly sets CI or NI bit of RM
- If set in FRM, remains set in BRM
- Faster response by setting bit in passing BRM
- Fastest by generating new BRM with bit set
- Explicit rate marking
- Switch reduces value of ER in FRM or BRM

ARB Feedback v TCP ACK

ABR feedback controls rate of transmission

　　　　　– Rate control

TCP feedback controls window size

　　　　　– Credit control

ARB feedback from switches or destination

TCP feedback from destination only

RM Cell Format
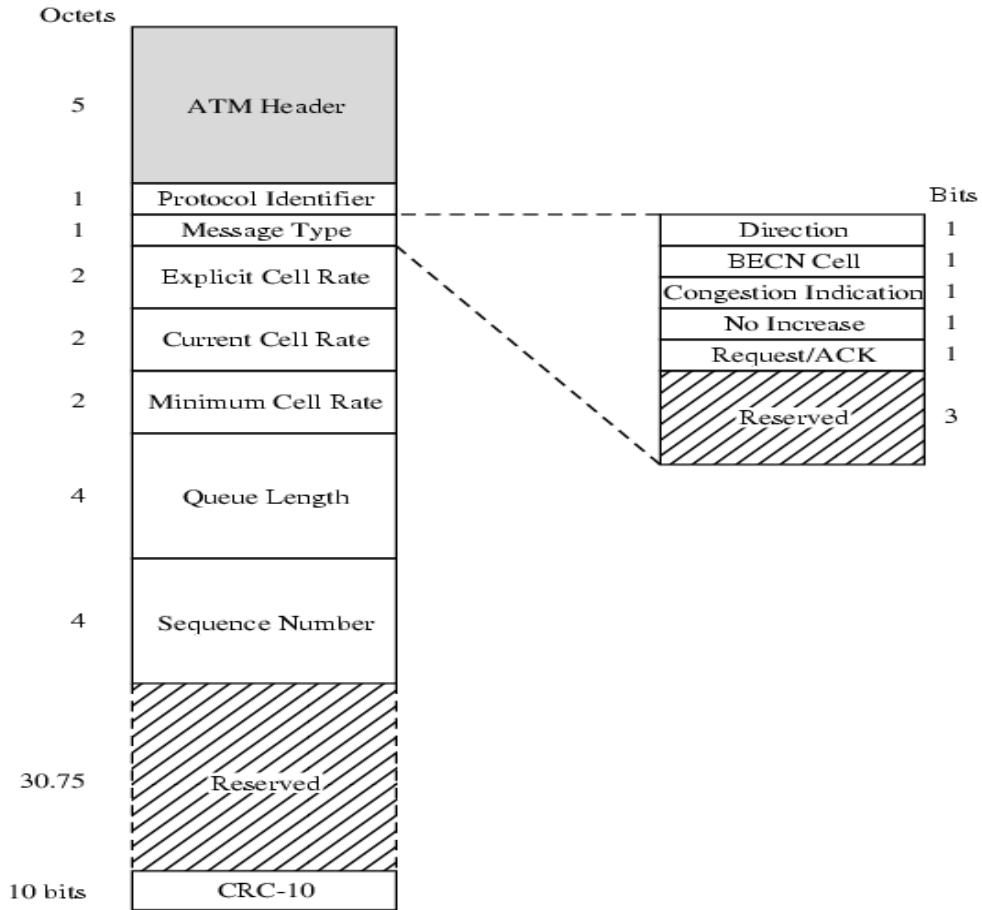
RM Cell Format Notes
- ATM header has PT=110 to indicate RM cell
- On virtual channel VPI and VCI same as data cells on connection
- On virtual path VPI same, VCI=6
- Protocol id identifies service using RM (ARB=1)
- Message type
  – Direction FRM=0, BRM=1
  – BECN cell. Source (BN=0) or switch/destination (BN=1)
  – CI (=1 for congestion)
  – NI (=1 for no increase)
  – Request/Acknowledge (not used in ATM forum spec)

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=oMpj4a6Qhm0

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: 293-297

Course Faculty

Verified by HOD

![Muthayammal Engineering College Logo]

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

![IQAC Logo]

L-25

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: RM Cell Formats
Introduction : • In asynchronous transfer mode (ATM), a flow control feedback mechanism that communicates to the originating end-user device to change the transfer characteristics of the connection during periods of congestion. • ABR is a best-effort category in which the network attempts to pass the maximum number of cells, but with no absolute guarantees. See also ABR, best effort, buffer, cell, congestion, and flow control.
Prerequisite knowledge for Complete understanding and learning of Topic: • Loop Control • Quality of Service

Detailed content of the Lecture:
RM Cell Format
• In asynchronous transfer mode (ATM), a flow control feedback mechanism that communicates to the originating end-user device to change the transfer characteristics of the connection during periods of congestion.
• The network buffers cells and advises the sender to throttle back on the rate of transmission. The available bit rate (ABR) class of service makes use of RMCells.
• ABR is a best-effort category in which the network attempts to pass the maximum number of cells, but with no absolute guarantees. See also ABR, best effort, buffer, cell, congestion, and flow control.
 	
RM Cell Format Notes
• ATM header has PT=110 to indicate RM cell
• On virtual channel VPI and VCI same as data cells on connection
• On virtual path VPI same, VCI=6
• Protocol id identifies service using RM (ARB=1)
• Message type
   – Direction FRM=0, BRM=1
   – BECN cell. Source (BN=0) or switch/destination (BN=1)
   – CI (=1 for congestion)
   – NI (=1 for no increase)

– Request/Acknowledge (not used in ATM forum spec)

Octets			Bits
5	ATM Header		
1	Protocol Identifier		
1	Message Type	Direction	1
2	Explicit Cell Rate	BECN Cell	1
		Congestion Indication	1
2	Current Cell Rate	No Increase	1
		Request/ACK	1
2	Minimum Cell Rate	Reserved	3
4	Queue Length		
4	Sequence Number		
30.75	Reserved		
10 bits	CRC-10		

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=oMpj4a6Qhm0

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: 293-297

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

LECTURE HANDOUTS	**L-26**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: ABR Capacity allocations
Introduction : ATM switch must perform: - Congestion control   - Monitor queue length   - Fair capacity allocation
Prerequisite knowledge for Complete understanding and learning of Topic: - Single Queues   - Multiple Queues   - Congestion Control
Detailed content of the Lecture: **Congestion Control Algorithms-Binary Feedback**   - Use only EFCI, CI and NI bits   - Switch monitors buffer utilization   - When congestion approaches, binary notification – Set EFCI on forward data cells or CI or NI on FRM or BRM   Three approaches to which to notify – Single FIFO queue – Multiple queues – Fair share notification **Single FIFO Queue**   - When buffer use exceeds threshold (e.g. 80%) – Switch starts issuing binary notifications – Continues until buffer use falls below threshold – Can have two thresholds   - One for start and one for stop   - Stops continuous on/off switching   - Biased against connections passing through more switches   **Multiple Queues**   - Separate queue for each VC or group of VCs

- Separate threshold on each queue
- Only connections with long queues get binary notifications
  - Fair
  - Badly behaved source does not affect other VCs
  - Delay and loss behaviour of individual VCs separated
- Can have different QoS on different VCs

Fair Share
- Selective feedback or intelligent marking
- Try to allocate capacity dynamically

E.g.
- fairshare =(target rate)/(number of connections)
- Mark any cells where CCR>fairshare

Explicit Rate Feedback Schemes
- Compute fair share of capacity for each VC
- Determine current load or congestion
- Compute explicit rate (ER) for each connection and send to source
- Three algorithms
  - Enhanced proportional rate control algorithm
  - Explicit rate indication for congestion avoidance
  - Congestion avoidance using proportional control

Load Factor

Adjustments based on load factor

LF=Input rate/target rate
  - Input rate measured over fixed averaging interval
  - Target rate slightly below link bandwidth (85 to 90%)
  - LF>1 congestion threatened

VCs will have to reduce rate

Explicit Rate Indication for Congestion Avoidance (ERICA)

Attempt to keep LF close to 1

fairshare = (target rate)/(number of connections)

VCshare = CCR/LF

   = (CCR/(Input Rate)) *(Target Rate)

Video Content / Details of website for further learning (if any):

https://gpontutorials.com/a-review-of-dynamic-bandwidth-allocation-algorithm-for-gpon-networks/

Important Books/Journals for further learning including the page nos.:

William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: 249-277

Course Faculty

Verified by HOD

IQAC

Estd. 2000

LECTURE HANDOUTS	**L-27**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : III- TCP and ATM Congestion Control   Date of Lecture:

Topic of Lecture: GFR traffic management
Introduction :   Traffic management deals with the process of monitoring and controlling the activities of network besides transforming the network into a managed resource by improving performance, efficiency, and security. It also helps to operate, administer, and maintain the network systems
Prerequisite knowledge for Complete understanding and learning of Topic: • Cell loss priority   • ATM network   • Traffic Control

Detailed content of the Lecture
 GFR traffic management
 Simple as UBR from end system view
 – End system does no policing or traffic shaping
 – May transmit at line rate of ATM adaptor
     • Modest requirements on ATM network
     • No guarantee of frame delivery
     • Higher layer (e.g. TCP) react to congestion causing dropped frames
     • User can reserve cell rate capacity for each VC
  Application can send at min rate without loss
     • Network must recognise frames as well as cells
     • If congested, network discards entire frame
     • All cells of a frame have same CLP setting
       – CLP=0 guaranteed delivery, CLP=1 best efforts
 GFR Conformance Definition
 UPC function
       – UPC monitors VC for traffic conformance
       – Tag or discard non-conforming cells
 Frame conforms if all cells in frame conform
 – Rate of cells within contract
 Generic cell rate algorithm PCR and CDVT specified for connection
       – All cells have same CLP
       – Within maximum frame size (MFS)

QoS Eligibility Test

Test for contract conformance
  – Discard or tag non-conforming cells
Looking at upper bound on traffic
  – Determine frames eligible for QoS guarantee
Under GFR contract for VC
Looking at lower bound for traffic
Frames are one of:
  – Nonconforming: cells tagged or discarded
  – Conforming ineligible: best efforts
  – Conforming eligible: guaranteed delivery

Simplified Frame Based GCRA
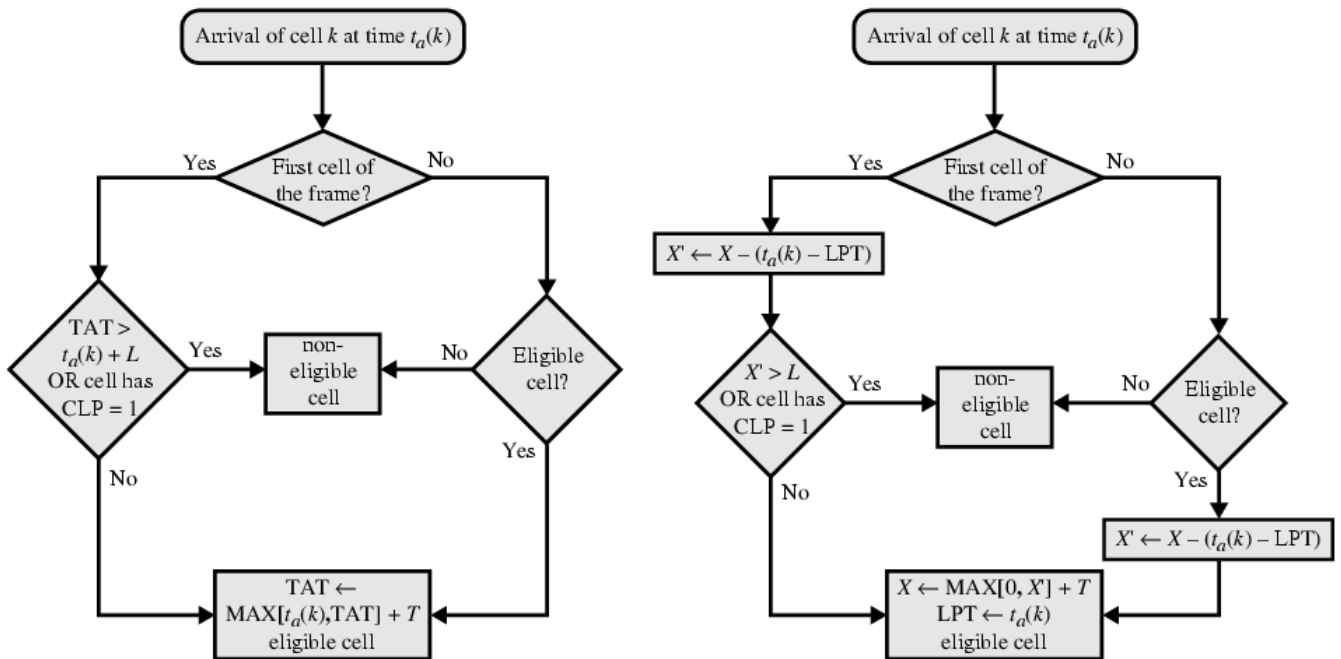
T = Increment
L = Limit
$t_a(k)$ = Time of arrival of a cell

X = Value of the leaky bucket counter
X' = Auxiliary variable
LPT = Last pass time

TAT = Theoretical arrival time

At the time of arrival $t_a(1)$ of the first cell
of the connection, TAT = $t_a(1)$

At the time of arrival $t_a(1)$ of the first cell
of the connection, $X = 0$ and LPT = $t_a(1)$

(a) Virtual scheduling algorithm　　　(b) Continuous-state leaky bucket algorithm

---

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=lHmmHB9QaY8
https://www.slideshare.net/sohitagarwal/lecture-13-42984614

Important Books/Journals for further learning including the page nos.:
William Stallings, "High speed networks and internet", Pearson Education 2002,Page No: 249-277

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

L-28

LECTURE HANDOUTS

CSE		III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: Integrated Services Architecture
Introduction :   Integrated services or IntServ is an architecture that specifies the elements to guarantee quality of service (QoS) on networks. IntServ can for example be used to allow video and sound to reach the receiver without interruption.
Prerequisite knowledge for Complete understanding and learning of Topic: • Transmission control protocol   • Window size   • Acknowledgement
Detailed content of the Lecture: **Integrated Services Architecture (Int-Serv)**   • Integrated services or IntServ is an architecture that specifies the elements to guarantee quality of service (QoS) on networks. Under IntServ, every router in the system implements IntServ, and every application that requires some kind of QoS guarantee has to make an individual reservation.   **An Overview of Int-Serv**   • IntServ was defined in IETF RFC 1633, which proposed the resource reservation protocol (RSVP) as a working protocol for signaling in the IntServ architecture.   • This protocol assumes that resources are reserved for every flow requiring QoS at every router hop in the path between receiver and transmitter using end-to-end signaling.   The IntServ model for IP QoS architecture defines three classes of service based on applications' delay requirements (from highest performance to lowest):   ·   **Guaranteed-service class** - with bandwidth, bounded delay, and no-loss guarantees;   ·   **Controlled-load service class** - approximating best-effort service in a lightly loaded network, which provides for a form of statistical delay service agreement (nominal delay) that will not be violated more often than in an unloaded network;   ·   **Best-effort service class** - similar to that which the Internet currently offers, which is further partitioned into three categories: ·   interactive burst (e.g., Web),   ·   interactive bulk (e.g., FTP) and   ·   asynchronous (e.g., e-mail)   The main point is that the guaranteed service and controlled load classes are based on quantitative service requirements, and both require signaling and admission control in network nodes. These services

can be provided either per-flow or per-flow-aggregate, depending on flow concentration at different points in the network. Although the IntServ architecture need not be tied to any particular signaling protocol, Resource Reservation Protocol (RSVP) described below, is often regarded as the signaling protocol in IntServ. Best-effort service, on the other hand, does not require signaling.
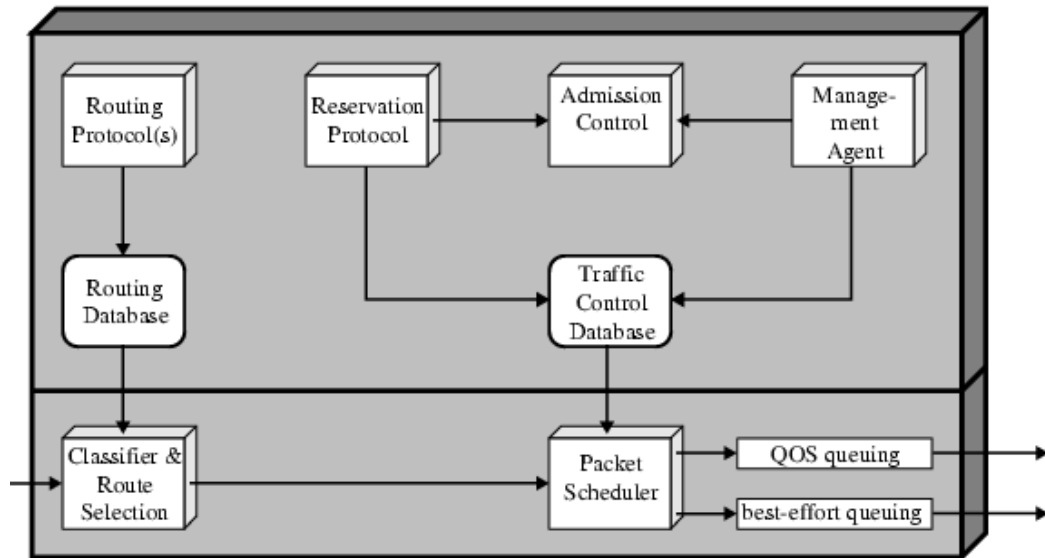
Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Integrated_services
https://www.sciencedirect.com/topics/computer-science/integrated-service
https://www.slideshare.net/ayyakathir/unit4-29753244

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (243-247)

Course Faculty

Verified by HOD

![Muthayammal Engineering College logo]

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

LECTURE HANDOUTS	**L-29**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : S.Pragadeeswaran

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: Approach, Components, Services

Introduction:

ISA Approach
- Provision of QoS over IP
- Sharing available capacity when congested
- Router mechanisms

–Routing Algorithms
- Select to minimize delay

–Packet discard
- Causes TCP sender to back off and reduce load
- Enhanced by ISA

Prerequisite knowledge for Complete understanding and learning of Topic:
- Routing
- Quality of Service
- Packet Scheduler

Detailed content of the Lecture:

ISA Approach
- Provision of QoS over IP
- Sharing available capacity when congested
- Router mechanisms

–Routing Algorithms
- Select to minimize delay

–Packet discard
- Causes TCP sender to back off and reduce load
- Enahnced by ISA

Flow

IP packet can be associated with a flow
   –Distinguishable stream of related IP packets
   –From single user activity
   –Requiring same QoS
   –E.g. one transport connection or one video stream
   –Unidirectional
   –Can be more than one recipient

Multicast
   –Membership of flow identified by source and destination IP address, port numbers, protocol type

–IPv6 header flow identifier can be used but is not necessarily equivalent to ISA flow

ISA Functions

Admission control

  –For QoS, reservation required for new flow

  –RSVP used

Routing algorithm

  –Base decision on QoS parameters

Queuing discipline

  –Take account of different flow requirements

Discard policy

ISA Implementation in Router

- Background Functions
- Forwarding functions

ISA Components – Background Functions

Reservation Protocol

  –RSVP

Admission control

Management agent

  –Can use agent to modify traffic control database and direct admission control

Routing protocol

ISA Components – Forwarding

Classifier and route selection

  –Incoming packets mapped to classes

Single flow or set of flows with same QoS

  –E.g. all video flows

Based on IP header fields

  –Determines next hop

Packet scheduler

  –Manages one or more queues for each output

  –Order queued packets sent

Based on class, traffic control database, current and past activity on outgoing port

  –Policing

Video Content / Details of website for further learning (if any):
https://www.slideshare.net/ayyakathir/unit4-29753244
https://www.slideshare.net/ThamerAlamery/intserv-diffserv
https://www.sciencedirect.com/topics/computer-science/integrated-service

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002.
(247-251)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

LECTURE HANDOUTS	**L-30**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   **:C.Nithya**

Unit   **: IV- Integrated and Differentiated Services**   **Date of Lecture:**

Topic of Lecture: Queuing Discipline

Introduction :

The queuing discipline allows high-priority packets to cut to the front of the line. The idea of the fair queuing (FQ) discipline is to maintain a separate queue for each flow currently being handled by the router. The router then services these queues in a round-robin manner.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Queue
- Priority
- Packet Scheduler

Detailed content of the Lecture:

- **Population of Customers** can be considered either limited (closed systems) or unlimited (open systems).
- Example of a limited population may be a number of processes to be run (served) by a computer or a certain number of machines to be repaired by a service man. It is necessary to take the term "customer" very generally. Customers may be people, machines of various nature, computer processes, telephone calls, etc.
- **Arrival** defines the way customers enter the system. Mostly the arrivals are random with random intervals between two adjacent arrivals. Typically the arrival is described by a random distribution of intervals also called Arrival Pattern.
- **Queue** represents a certain number of customers waiting for service (of course the queue may be empty). Typically the customer being served is considered not to be in the queue. Sometimes the customers form a queue literally (people waiting in a line for a bank teller). Sometimes the queue is an abstraction (planes waiting for a runway to land). There are two important properties of a queue: Maximum Size and Queuing Discipline.
- Maximum Queue Size (also called System capacity) is the maximum number of customers that may wait in the queue (plus the one(s) being served). Queue is always limited, but some theoretical models assume an unlimited queue length. If the queue length is limited, some customers are forced to renounce without being served.
- Queuing Discipline represents the way the queue is organized (rules of inserting and removing customers to/from the queue). There are these ways:
  1) FIFO (First In First Out) also called FCFS (First Come First Serve) - orderly queue.
  2) LIFO (Last In First Out) also called LCFS (Last Come First Serve) - stack.
  3) SIRO (Serve In Random Order).

4) Priority Queue that may be viewed as a number of queues for various priorities.

5) Many other more complex queuing methods that typically change the customer's position in the queue according to the time spent already in the queue, expected service duration, and/or priority. These methods are typical for computer multi-access systems.

- Most quantitative parameters (like average queue length, average time spent in the system) do not depend on the queuing discipline. That's why most models either do not take the queuing discipline into account at all or assume the normal FIFO queue. In fact the only parameter that depends on the queuing discipline is the variance (or standard deviation) of the waiting time. There is this important rule (that may be used for example to verify results of a simulation experiment):

- The two extreme values of the waiting time variance are for the FIFO queue (minimum) and the LIFO queue (maximum).

- Theoretical models (without priorities) assume only one queue. This is not considered as a limiting factor because practical systems with more queues (bank with several tellers with separate queues) may be viewed as a system with one queue, because the customers always select the shortest queue. Of course, it is assumed that the customers leave after being served. Systems with more queues (and more servers) where the customers may be served more times are called Queuing Networks.

- **Service** represents some activity that takes time and that the customers are waiting for. Again take it very generally. It may be a real service carried on persons or machines, but it may be a CPU time slice, connection created for a telephone call, being shot down for an enemy plane, etc. Typically a service takes random time.

- Theoretical models are based on random distribution of service duration also called Service Pattern. Another important parameter is the number of servers. Systems with one server only are called Single Channel Systems, systems with more servers are called Multi Channel Systems.

Video Content / Details of website for further learning (if any):
https://www.slideshare.net/ayyakathir/unit4-29753244
https://www.youtube.com/results?search_query=Queuing+Discipline+&pbjreload=10

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (270-274)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

L-31

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   :C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture :FQ – PS
Introduction : • **Fair queuing** is a family of scheduling algorithms used in some process and network schedulers. The algorithm is designed to achieve fairness when a limited resource is shared, for example to prevent flows with large packets or processes that generate small jobs from consuming more throughput or CPU time than other flows or processes. • **Processor sharing** is a service policy where the customers, clients or jobs are all served simultaneously, each receiving an equal fraction of the service capacity available. In such a system all jobs start service immediately.
Prerequisite knowledge for Complete understanding and learning of Topic: ➢ Queue ➢ Process Sharing ➢ Scheduling Algorithm

Detailed content of the Lecture:
Fair Queuing (FQ)
• Multiple queues for each port
   –One for each source or flow
   –Queues services round robin
   –Each busy queue (flow) gets exactly one packet per cycle
   –Load balancing among flows
   –No advantage to being greedy
Your queue gets longer, increasing your delay
   –Short packets penalized as each queue sends one packet per cycle
• A simple variation on basic FIFO queuing is priority queuing.
• The idea is to mark each packet with a priority; the mark could be carried, for example, in the IP header, as we'll discuss in a later section. The routers then implement multiple FIFO queues, one for each priority class.
• The router always transmits packets out of the highest-priority queue if that queue is nonempty before moving on to the next priority queue.
• Within each priority, packets are still managed in a FIFO manner.
• This idea is a small departure from the best-effort delivery model, but it does not go so far as to make guarantees to any particular priority class. It just allows high-priority packets to cut to the front of the line.

FIFO and FQ
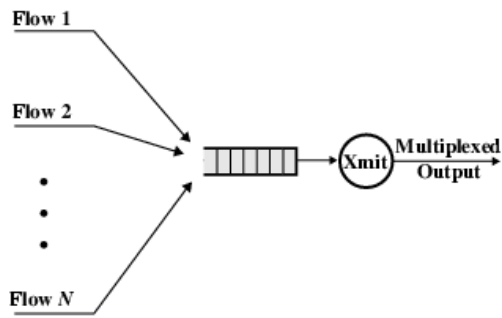
(a) FIFO Queuing
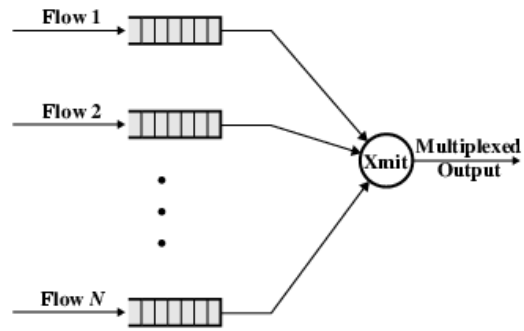
(b) Fair Queuing

Processor Sharing
- Multiple queues as in FQ
- Send one bit from each queue per round

Longer packets no longer get an advantage
- Can work out virtual (number of cycles) start and finish time for a given packet
- However, we wish to send packets, not bits

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Processor_sharing
https://en.wikipedia.org/wiki/Fair_queuing
https://www.youtube.com/watch?v=6MyBum2Njls

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002.
(261-269)

Course Faculty

Verified by HOD

L-32

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   :C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: BRFQ
Introduction :   In **BRFQ** (Bit Round Fair Queuing) a bit-by-bit round robin discipline is followed. In this we set up multiple queues and transmit one bit from each queue on each round. In this way, longer packets no longer receive an advantage and each busy source receives exactly the same amount of capacity.
Prerequisite knowledge for Complete understanding and learning of Topic: • Queuing   • FIFO   • Reservation
Detailed content of the Lecture: **Bit-Round Fair Queuing (BRFQ)**   • Compute virtual start and finish time as before   • When a packet finished, the next packet sent is the one with the earliest virtual finish time   • Good approximation to performance of PS   –Throughput and delay converge as time increases   **Generalized Processor Sharing (GPS)**   • **Generalized processor sharing** (**GPS**) is an ideal scheduling algorithm for process schedulers and network schedulers.   • It is related to the fair-queuing principle which groups packets into classes and shares the service capacity between them. **GPS** shares this capacity according to some fixed weights.   • BRFQ cannot provide different capacities to different flows   Enhancement called Weighted fair queue (WFQ)   • From PS, allocate weighting to each flow that determines how many bots are sent during each round   • If weighted 5, then 5 bits are sent per round   • Gives means of responding to different service requests   • Guarantees that delays do not exceed bounds   **Weighted Fair Queue**   **Weighted fair queueing** (WFQ) is a network scheduler scheduling algorithm. WFQ is both a packet-based implementation of the generalized processor sharing (GPS) policy, and a natural extension of **fair queuing** (FQ).   • Emulates bit by bit GPS

- Same strategy as BRFQ

Comparison of FIFO, FQ and BRFQ
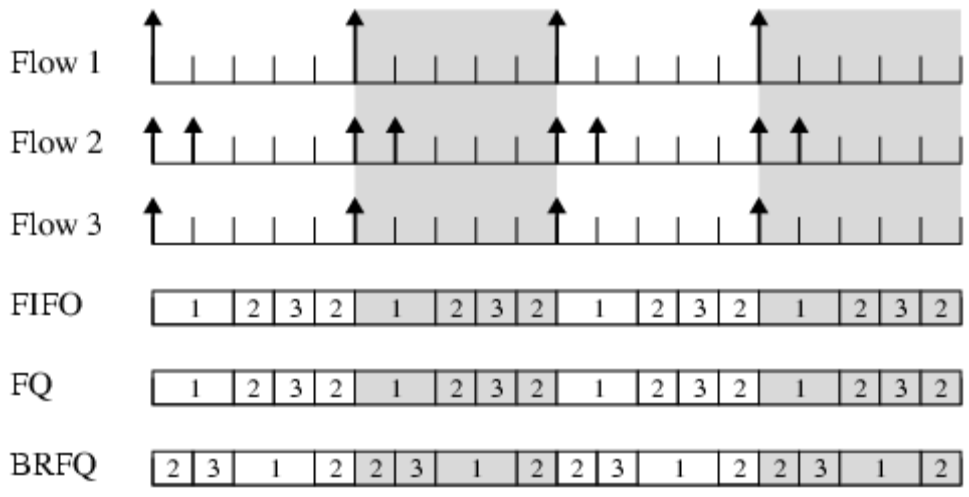
(a) Load equals capacity
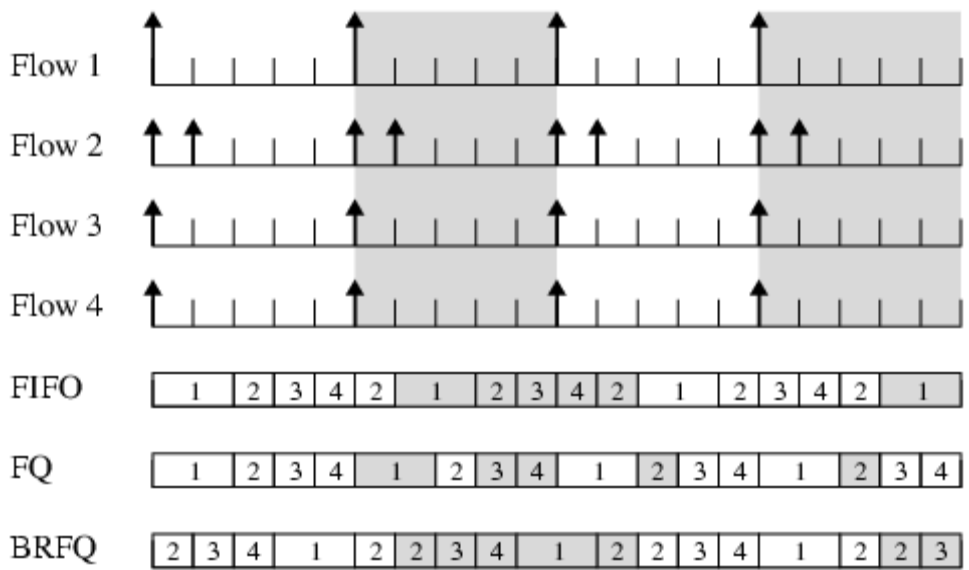
(b) Load exceeds capacity

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Generalized_processor_sharing
https://en.wikipedia.org/wiki/Weighted_fair_queueing

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (297-301)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

L-33

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   :C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: GPS
Introduction : • **Generalized processor sharing** (**GPS**) is an ideal scheduling algorithm for process schedulers and network schedulers. • It is related to the fair-queuing principle which groups packets into classes and shares the service capacity between them. **GPS** shares this capacity according to some fixed weights.
Prerequisite knowledge for Complete understanding and learning of Topic: • Queuing • FIFO • Reservation
Detailed content of the Lecture: **Generalized Processor Sharing (GPS)** • **Generalized processor sharing** (**GPS**) is an ideal scheduling algorithm for process schedulers and network schedulers. • It is related to the fair-queuing principle which groups packets into classes and shares the service capacity between them. **GPS** shares this capacity according to some fixed weights. • BRFQ cannot provide different capacities to different flows. • In process scheduling, GPS is "an idealized scheduling algorithm that achieves perfect fairness. All practical schedulers approximate GPS and use it as a reference to measure fairness."[• Generalized processor sharing assumes that traffic is fluid (infinitesimal packet sizes), and can be arbitrarily split. There are several service disciplines which track the performance of GPS quite closely such as weighted fair queuing (WFQ), also known as packet-by-packet generalized processor sharing (PGPS). • In a network such as the internet, different application types require different levels of performance. • For example, email is a genuinely store and forward kind of application, but videoconferencing isn't since it requires low latency. • When packets are queued up on one end of a congested link, the node usually has some freedom in deciding the order in which it should send the queued packets. • One example ordering is simply first-come, first-served, which works fine if the sizes of the queues are small, but can result in problems if there are latency sensitive packets being blocked by packets from bursty, higher bandwidth applications. Enhancement called Weighted fair queue (WFQ)

- From PS, allocate weighting to each flow that determines how many bots are sent during each round
- If weighted 5, then 5 bits are sent per round
- Gives means of responding to different service requests
- Guarantees that delays do not exceed bounds

Implementations, parametrization and fairness

- In GPS, and all protocols inspired by GPS, the choice of the weights is left to the network administrator.
- Generalized processor sharing assumes that the traffic is fluid, i.e., infinitely divisible so that whenever an application type has packets in the queue, it will receive exactly the fraction of the server given by the formula above.
- However, traffic is not fluid and consists of packets, possibly of variable sizes. Therefore, GPS is mostly a theoretical idea, and several scheduling algorithms have been developed to approximate this GPS ideal: PGPS, aka Weighted fair queuing, is the most known implementation of GPS, but it has some drawbacks, and several other implementations have been proposed, as Deficit round robin or WF2Q.
- GPS is considered as a fair ideal, and all its approximations "use it as a reference to measure fairness."Nevertheless, several Fairness measures exist.
- GPS is insensible to packet sizes, since it assumes a fluid model.

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Generalized_processor_sharing
https://en.wikipedia.org/wiki/Weighted_fair_queueing

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (297-301)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

Estd. 2000

L-34

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : IV- Integrated and Differentiated Services   **Date of Lecture:**

| |
|---|
| **Topic of Lecture:** WFQ |
| **Introduction :**
• Weighted fair queueing is a network scheduling algorithm.
• WFQ is both a packet-based implementation of the generalized processor sharing policy, and a natural extension of fair queuing. |
| **Prerequisite knowledge for Complete understanding and learning of Topic:**
• Queuing
• FIFO
• Reservation |
| **Detailed content of the Lecture:**
Weighted Fair Queue
Weighted fair queueing (WFQ) is a network scheduler scheduling algorithm. WFQ is both a packet-based implementation of the generalized processor sharing (GPS) policy, and a natural extension of **fair queuing** (FQ).
• Emulates bit by bit GPS
• Same strategy as BRFQ
Parametrization and fairness
• Like other GPS-like scheduling algorithms, the choice of the weights is left to the network administrator. There is no unique definition of what is "fair"
• By regulating the WFQ weights dynamically, WFQ can be utilized for controlling the quality of service, for example, to achieve guaranteed data rate.
• Proportionally fair behavior can be achieved by setting the weights to, where is the cost per data bit of data flow.
• For example in CDMA spread spectrum cellular networks, the cost may be the required energy (the interference level), and in dynamic channel allocation systems, the cost may be the number of nearby base station sites that cannot use the same frequency channel, in view to avoid co-channel interference.
• WFQ has little or no effect on the speed at which narrowband signals are transmitted, but tends to slow down the transmission of broadband signals, especially during times of peak network traffic. Broadband signals share the resources that remain after low-bandwidth signals have been transmitted.
• The resource sharing is done according to assigned weights. In flow-based WFQ, also called |

standard WFQ, packets are classified into flows according to one of four criteria: the source Internet Protocol address (IP address), the destination IP address, the source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, or the destination TCP or UDP port. Each flow receives an equal allocation of network bandwidth, hence the term fair.

- There are two other forms of WFQ, known as VIP-distributed WFQ for VIP2-40 or greater interface processors, and class-based WFQ in which the traffic is categorized into user-defined classes. Both of these forms of WFQ operate according to principles similar to that of standard (flow-based) WFQ.
- WFQ can prevent high-bandwidth traffic from overwhelming the resources of a network, a phenomenon which can cause partial or complete failure of low-bandwidth communications during periods of high traffic in poorly managed networks.

WFQ as a GPS approximation

- WFQ, under the name PGPS, has been designed as "an excellent approximation to GPS", and it has been proved that it approximates GPS "to within one packet transmission time, regardless of the arrival patterns.
- Since WFQ implementation is similar to fair queuing, it has the same $O(\log(n))$ complexity, where n is the number of flows. This complexity comes from the need to select the queue with the smallest virtual finish time each time a packet is sent.

After WFQ, several other implementations of GPS have been defined.

- Even if WFQ is at most "one packet" late w.r.t. the ideal GPS policy, it can be arbitrarily ahead. The Worst-case Fair Weighted Fair Queueing (WF2Q) fixes it by adding a virtual start of service to each packet, and selects a packet only if its virtual start of service is not less than the current time.
- The selection of the queue with minimal virtual finish time can be hard to implement at wire speed. Then, other approximations of GPS have been defined with less complexity, like deficit round robin.

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Generalized_processor_sharing
https://en.wikipedia.org/wiki/Weighted_fair_queueing

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (297-301)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

L-35

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   :C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: Random Early Detection
Introduction : • Random early detection (RED), also known as random early discard or random early drop is a queuing discipline for a network scheduler suited for congestion avoidance. • In the conventional tail drop algorithm, a router or other network component buffers as many packets as it can, and simply drops the ones it cannot buffer.
Prerequisite knowledge for Complete understanding and learning of Topic: • Queuing • FIFO • Buffering
Detailed content of the Lecture: **Random Early Detection(RED)** • Random Early Discard (RED) is a data queue control mechanism to improve data utilization during network congestion. Some radio vendors have made exaggerated claims about its capacity to improve "radio link utilization." • To help control network congestion (i.e., overloading) the Internet Transmission Control Protocol (TCP) uses a mechanism known as the TCP sliding window, which is designed to maximize bandwidth usage while avoiding traffic congestion. Under control of the sliding window, TCP connections have their window size (i.e., share of bandwidth) increased as acknowledgements (ACKs) are received. • With multiple connections in play this can reach a point where all bandwidth is consumed, resulting in network congestion and the dropping (i.e., tail dropping) of frames. At this point, the sliding window mechanism initiates a simultaneous reduction in window size for all TCP connections after which, with a return to stability, it ramps up their window size to create an oscillating traffic pattern. It results in inefficient use of the available traffic bandwidth. This oscillating behavior is termed "TCP global synchronization." **Counteracting the Problem** • In order to counteract this problem different queuing control mechanisms have been devised. A common one is Random Early Discard or Radom Early Detection (RED). In RED, when the queue exceeds a certain size the network component marks each arriving packet with a probability that depends on the queue size. • When the buffer is full, the probability reaches 1 and all incoming packets are dropped. The

chance that the network component notifies a particular sender to reduce its data transmission rate is proportional to the sender's share of the bandwidth of the link—an improvement over tail dropping.

- An issue that was realized early on about the RED algorithm is that it cannot differentiate between traffic types. A variation of the RED algorithm that addresses this problem is called Weighted Random Early Detection (WRED). In WRED, the probability of dropping packets is based on the size of the queue and the traffic flow type (IP precedence).

Improvement Using RED and WRED Algorithms are Modest

- Although some microwave vendors claim to obtain up to 25 percent improvement in "radio link utilization" with the RED and WRED algorithms, independent studies show that RED improvement for real data applications is more modest. Also, bear in mind that RED is only beneficial where the bulk of the traffic is TCP/IP.

- The first study from AT&T Labs and Stanford University using a simple analytical model showed that although RED may prevent the traffic rate from moving in lockstep, this algorithm was not enough to prevent the traffic rate from oscillating and wasting throughput for all traffic flows.

- The study suggests that if the buffer sizes are small, then randomized policies are unlikely to reduce aggregated periodic behavior.

- A second study from the University of North Carolina concludes that below saturation point (90 percent utilization) there is little difference in performance between RED and tail dropping.

- For loads from 90 percent to 100 percent, RED can be tuned to outperform tail dropping but only with careful RED parameter settings and degradation in latency response. Analyzing the results from these and other studies it becomes clear that the claim of 25 percent link improvement is not realistic.

RED Buffer
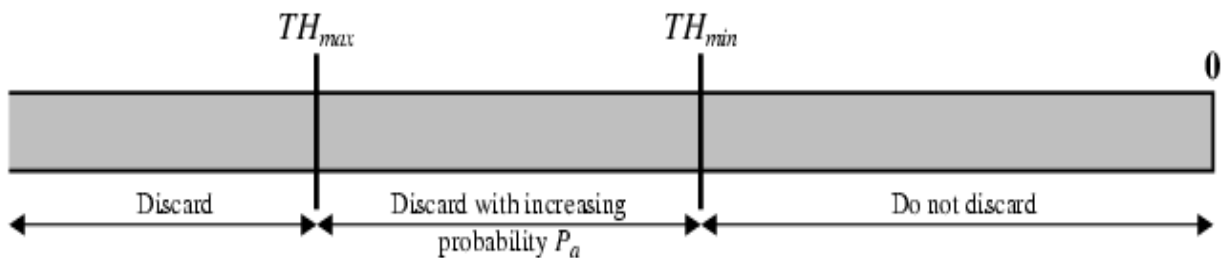
RED Algorithm Detail

The general RED algorithm:

```
procedure REDAlgorithm() is
avg ← average queue size
while packetsarrive
    if (minth <= avg AND avg < maxth)
        Compute pa with probability pb
        mark the arriving packet
    else if (maxth < avg)
        mark the arriving packet
    endif
end REDAlgorithm
```

RED algorithm contains two main sub algorithms (parts):

1. For computing the average queue size that determines the degree of burstiness that will be allowed in the routers queue.

2. For calculating the packet-*marking probability that determines how frequently the router *marks packets, given the current level of congestion. The goal is for the router to *mark packets at fairly even spaced intervals, in order to avoid biases and to avoid global synchronization, and to *mark packets sufficiently frequently to control the average queue size.

Video Content / Details of website for further learning (if any):
https://www.networkfashion.net/random-early-detection-red/

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (301-304)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS	**L-36**

CSE	**III/VI**

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   :C.Nithya

Unit   : IV- Integrated and Differentiated Services   Date of Lecture:

Topic of Lecture: Differentiated Services.
Introduction :   **Differentiated services** or DiffServ is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of **service** (QoS) on modern IP networks.
Prerequisite knowledge for Complete understanding and learning of Topic: • Mathematical Model   • Queuing   • Network analytics
Detailed content of the Lecture: **Differentiated Services**   • In the DiffServ model a packet's "class" can be marked directly in the packet, which contrasts with the IntServ model where a signaling protocol is required to tell the routers which flows of packets requires special QoS treatment.   • DiffServ achieves better QoS scalability, while IntServ provides a tighter QoS mechanism for real-time traffic. These approaches can be complimentary and are not mutually exclusive.   • The DiffServ architecture model (RFC 2475, December 1998) divides traffic into a small number of classes, and allocates resources on a per-class basis. Because DiffServ has only a few classes of traffic, a packet's "class" can be marked directly in the packet.   • In the DiffServ model, packets are classified and marked to receive a particular forwarding treatment (per-hop behavior or PHB) on nodes along their path. Sophisticated classification, marking, policing, and shaping operations need only be implemented at network boundaries or hosts, enabling greater scalability than other models of service differentiation.   • Modern data networks carry many different types of services, including voice, video, streaming music, web pages and email.   • Many of the proposed QoS mechanisms that allowed these services to co-exist were both complex and failed to scale to meet the demands of the public Internet.   • In December 1998, the IETF published RFC 2474 - Definition of the Differentiated services field (DS field) in the IPv4 and IPv6 headers, which replaced the IPv4 TOS field with the DS field.   • In the DS field, a range of eight values (Class Selectors) is used for backward compatibility with the IP precedence specification in the former TOS field.

- Today, DiffServ has largely supplanted TOS and other layer-3 QoS mechanisms, such as integrated services (IntServ), as the primary architecture routers use to provide QoS.
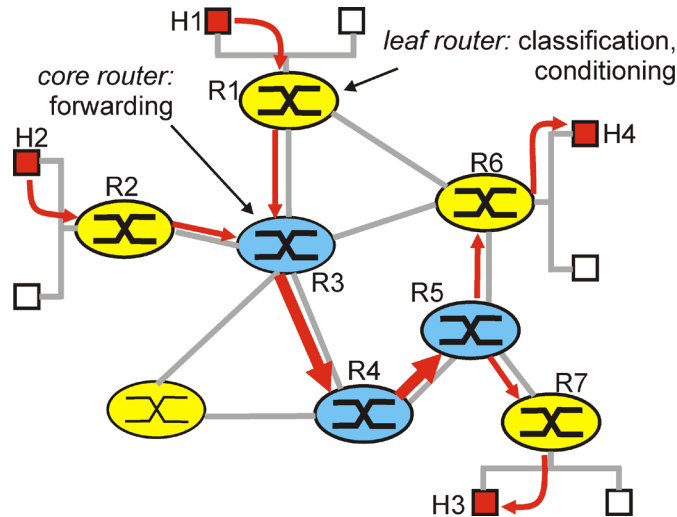
DS Traffic Conditioner
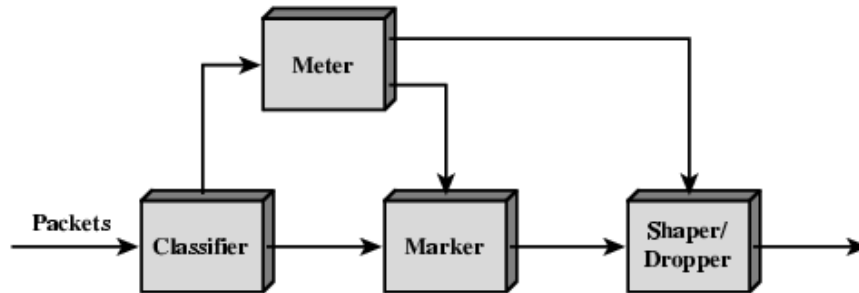
Per Hop Behaviour – Expedited forwarding

Premium service

- Low loss, delay, jitter; assured bandwidth end-to-end service through domains
- Looks like point to point or leased line
- Difficult to achieve
- Configure nodes so traffic aggregate has well defined minimum departure rate

EF PHB

–Condition aggregate so arrival rate at any node is always less that minimum departure rate

Boundary conditioners

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Differentiated_services

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (305-315)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-37

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   Date of Lecture:

Topic of Lecture: RSVP – Goals & Characteristics

Introduction :
- RSVP is a transport layer protocol that is used to reserve resources in a computer network to get different quality of services (QoS) while accessing Internet applications.
- It operates over Internet protocol (IP) and initiates resource reservations from the receiver's end.

Prerequisite knowledge for Complete understanding and learning of Topic:
- Quality of Service
- Internet Protocol
- Dynamic Routing

Detailed content of the Lecture:

Resource ReSerVation Protocol (RSVP) Design Goals
- ➢ Enable receivers to make reservations
- ➢ Different reservations among members of same multicast group allowed
- ➢ Deal gracefully with changes in group membership
- ➢ Dynamic reservations, separate for each member of group
- ➢ Aggregate for group should reflect resources needed
- ➢ Take into account common path to different members of group
- ➢ Receivers can select one of multiple sources (channel selection)
- ➢ Deal gracefully with changes in routes
- ➢ Re-establish reservations
- ➢ Control protocol overhead Independent of routing protocol

RSVP Characteristics
- ➢ Unicast and Multicast
- ➢ Simplex
– Unidirectional data flow
– Separate reservations in two directions
- ➢ Receiver initiated
– Receiver knows which subset of source transmissions it wants
- ➢ Maintain soft state in internet
– Responsibility of end users
 Providing different reservation styles

– Users specify how reservations for groups are aggregated

 Transparent operation through non-RSVP routers

Support IPv4 (ToS field) and IPv6 (Flow label field)

Increased Demands

 Need to incorporate bursty and stream traffic in TCP/IP architecture

 Increase capacity

– Faster links, switches, routers

– Intelligent routing policies

– End-to-end flow control

Multicasting

Quality of Service (QoS) capability

Transport protocol for streaming

Resource Reservation - Unicast

Prevention as well as reaction to congestion required

 Unicast

– End users agree on QoS for task and request from network

– May reserve resources

– Routers pre-allocate resources

– If QoS not available, may wait or try at reduced QoS

Resource Reservation – Multicast

- Generate vast traffic
- High volume application like video
- Lots of destinations
- Can reduce load
- Some members of group may not want current transmission
- Channels‖ of video
- Some members may only be able to handle part of transmission
- Basic and enhanced video components of video stream
- Routers can decide if they can meet demand
- Resource Reservation Problems on an Internet
- Must interact with dynamic routing
- Reservations must follow changes in route
- Soft state – a set of state information at a router that expires unless refreshed
- End users periodically renew resource requests

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Resource_Reservation_Protocol
https://www4.cs.fau.de/Projects/JRTP/pmt/node25.html
https://www.tutorialride.com/computer-network/resource-reservation-protocol-rsvp.htm

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (342-349)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-38

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   Date of Lecture:

Topic of Lecture: Data Flow, RSVP operation
Introduction :   **RSVP** operates over an IPv4 or IPv6 and provides receiver-initiated setup of resource reservations for multicast or unicast **data flows**. **RSVP operations** will generally result in resources being reserved in each node along a path.
Prerequisite knowledge for Complete understanding and learning of Topic: • RSVP   • Source Port   • Destination Port   • Session
Detailed content of the Lecture: **Data Flows - Session**   • Data flow identified by destination   • Resources allocated by router for duration of session   • Destination IP address   • Unicast or multicast   • IP protocol identifier   • TCP, UDP etc.   • Destination port   • May not be used in multicast   **Flow Descriptor**   Reservation Request   – **Flow spec**   Desired QoS   Used to set parameters in node's packet scheduler   Service class, Rspec (reserve), Tspec (traffic)   – **Filter spec**   Set of packets for this reservation   Source address, source prot   Treatment of Packets of One Session at One Router

RSVP Operation Diagram
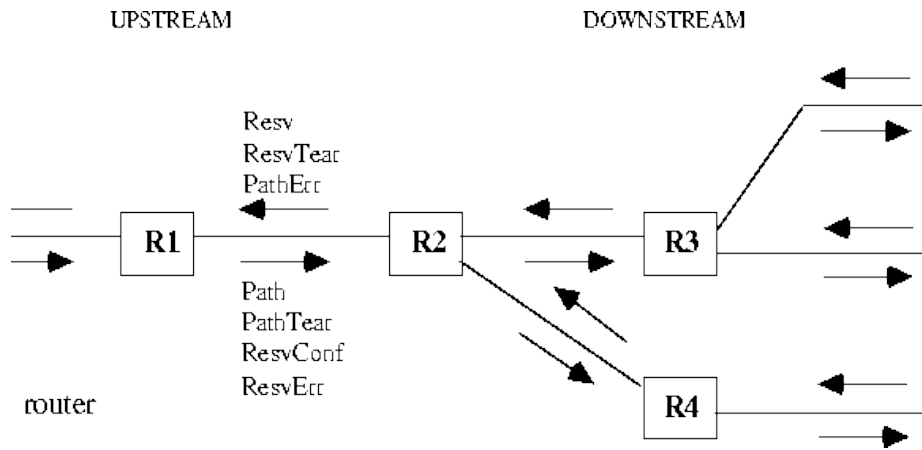
RSVP Operation
- G1, G2, G3 members of multicast group
- S1, S2 sources transmitting to that group
- Heavy black line is routing tree for S1, heavy grey line for S2
- Arrowed lines are packet transmission from S1 (black) and S2 (grey)
- All four routers need to know reservation s for each multicast address
- Resource requests must propagate back through routing tree

Filtering
- G3 has reservation filter spec including S1 and S2
- G1, G2 from S1 only
- R3 delivers from S2 to G3 but does not forward to R4
- G1, G2 send RSVP request with filter excluding S2
- G1, G2 only members of group reached through R4
- R4 doesn't need to forward packets from this session
- R4 merges filter spec requests and sends to R3
- R3 no longer forwards this session's packets to R4

Sender selection

– List of sources (explicit)

– All sources, no filter spec (wild card)

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/resource-reservation-protocol-in-real-time-systems/

Important Books/Journals for further learning including the page nos.:
Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002.
(342-349)

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to
Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

IQAC

L-39

LECTURE HANDOUTS

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   **Date of Lecture:**

Topic of Lecture: Protocol Mechanisms

Introduction :

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

Prerequisite knowledge for Complete understanding and learning of Topic:
- RSVP Data Flow
- Unicast
- Multicast

Detailed content of the Lecture:

RSVP Protocol Mechanisms

Two message types

– Resv

- Originate at multicast group receivers
- Propagate upstream
- Merged and packet when appropriate
- Create soft states
- Reach sender
- Allow host to set up traffic control for first hop

– Path

- Provide upstream routing information
- Issued by sending hosts
- Transmitted through distribution tree to all destinations

RSVP Host Model

- RSVP is a transport layer protocol that enables a network to provide differentiated levels of service to specific flows of data. Ostensibly, different application types have different performance requirements.

- RSVP acknowledges these differences and provides the mechanisms necessary to detect the levels of performance required by different applications and to modify network behaviors to accommodate those required levels.

- Over time, as time and latency-sensitive applications mature and proliferate, RSVP's capabilities will become increasingly important.
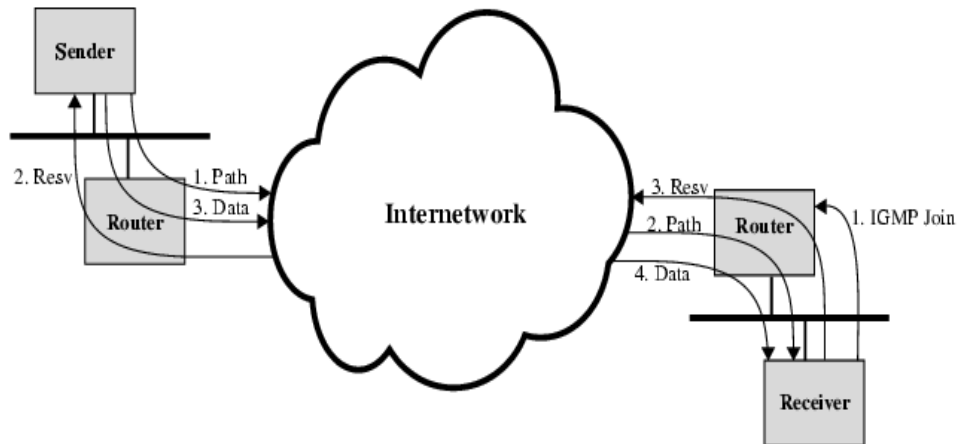
- Network protocols divide the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to
Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-40

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   Date of Lecture:

Topic of Lecture: Multiprotocol Label Switching
Introduction : • Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. • The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence the "multiprotocol" reference on its name
Prerequisite knowledge for Complete understanding and learning of Topic: • Routing • Paths • ATM • Traffic
Detailed content of the Lecture: **Multiprotocol Label Switching:** Routing algorithms provide support for performance goals • Distributed and dynamic • React to congestion • Load balance across network • Based on metrics • Develop information that can be used in handling different service needs • Enhancements provide direct support to IS, DS, RSVP • Nothing directly improves throughput or delay • MPLS tries to match ATM QoS support • Background • Efforts to marry IP and ATM • IP switching (Ipsilon) • Tag switching (Cisco) • Aggregate route based IP switching (IBM) • Cascade (IP navigator) • All use standard routing protocols to define paths between end points

- Assign packets to path as they enter network
- Use ATM switches to move packets along paths
- ATM switching (was) much faster than IP routers
- Use faster technology
- Developments
- IETF working group in 1997, proposed standard 2001
- Routers developed to be as fast as ATM switches

Remove the need to provide both technologies in same network

MPLS does provide new capabilities

– QoS support

– Traffic engineering

– Virtual private networks

– Multiprotocol support

  – Connection Oriented QoS Support
  – Guarantee fixed capacity for specific applications
  – Control latency/jitter
  – Ensure capacity for voice
  – Provide specific, guaranteed quantifiable SLAs
  – Configure varying degrees of QoS for multiple customers
  – MPLS imposes connection oriented framework on IP based internets
  – Traffic Engineering
  – Ability to dynamically define routes, plan resource commitments based on known
  – demands and optimize network utilization
  – Basic IP allows primitive traffic engineering
  – E.g. dynamic routing
  – MPLS makes network resource commitment easy
  – Able to balance load in face of demand
  – Able to commit to different levels of support to meet user traffic
  – requirements
  – Aware of traffic flows with QoS requirements and predicted demand
  – Intelligent re-routing when congested

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
https://www.youtube.com/watch?v=ZwK3c3UR4zk

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (361-365)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-41

CSE

III/VI

**Course Name with Code : High Speed Networks-16CSE10**

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   **Date of Lecture:**

Topic of Lecture: Operations
Introduction : • MPLS works by prefixing packets with an MPLS header, containing one or more labels. This is called a label stack.
Prerequisite knowledge for Complete understanding and learning of Topic: • Stack • Data Flow • Routers
Detailed content of the Lecture: **MPLS Operation** • Label switched routers capable of switching and routing packets based on label appended to packet • Labels define a flow of packets between end points or multicast destinations • Each distinct flow (forward equivalence class – FEC) has specific path through LSRs defined Connection oriented • Each FEC has QoS requirements • IP header not examined • Forward based on label value PLS works by prefixing packets with an MPLS header, containing one or more labels. This is called a label stack. Each entry in the label stack contains four fields: • A 20-bit label value. A label with the value of 1 represents the router alert label. • a 3-bit *Traffic Class* field for QoS (quality of service) priority and ECN (Explicit Congestion Notification). Prior to 2009 this field was called EXP. • a 1-bit *bottom of stack* flag. If this is set, it signifies that the current label is the last in the stack.

- an 8-bit TTL (time to live) field.

															MPLS Label																
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Label																			TC: Traffic Class (QoS and ECN)				S: Bottom-of-Stack				TTL: Time-to-Live				
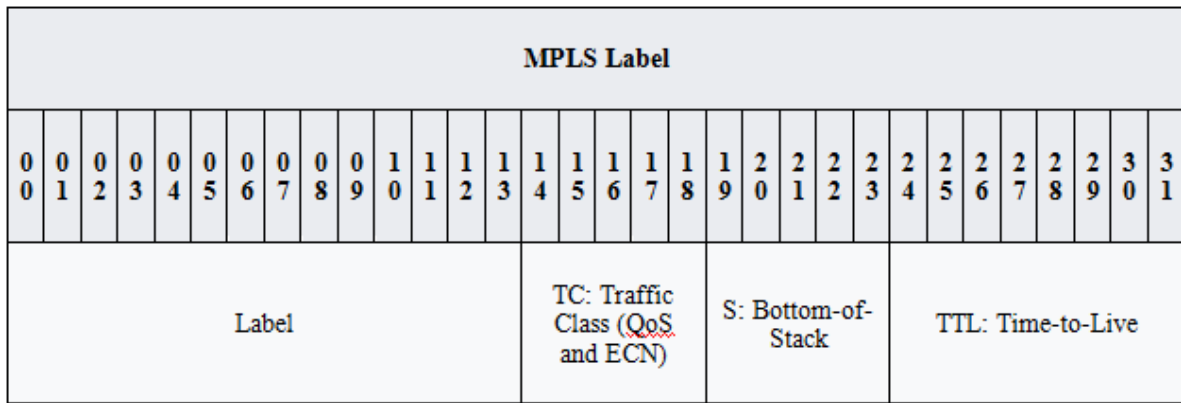
- These MPLS-labeled packets are switched after a label lookup/switch instead of a lookup into the IP table. As mentioned above, when MPLS was conceived, label lookup and label switching were faster than a routing table or RIB (Routing Information Base) lookup because they could take place directly within the switched fabric and avoid having to use the OS.
- The presence of such a label, however, has to be indicated to the router/switch. In the case of Ethernet frames this is done through the use of EtherType values 0x8847 and 0x8848, for unicast and multicast connections respectively.

Video Content / Details of website for further learning (if any):
https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94
https://www.youtube.com/watch?v=LYFUfywvjhs

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (352-353)

Course Faculty

Verified by HOD

Estd. 2000

IQAC

| **LECTURE HANDOUTS** | **L-42** |

| **CSE** | **III/VI** |

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   **Date of Lecture:**

Topic of Lecture: Label Stacking-Protocol details
Introduction :   • MPLS works by prefixing packets with an MPLS header, containing one or more labels. This is called a label stack.
Prerequisite knowledge for Complete understanding and learning of Topic: • Stack   • Data Flow   • Routers

Detailed content of the Lecture:
 Label Stacking
 	
 • Packet may carry number of labels
 LIFO (stack)
   – Processing based on top label
   – Any LSR may push or pop label
   Unlimited levels
   – Allows aggregation of LSPs into single LSP for part of route
   – C.f. ATM virtual channels inside virtual paths
   – E.g. aggregate all enterprise traffic into one LSP for access provider to handleReduces size of tables
 	
 Label Format Diagram
 	
 Exp = experimental
 S = bottom of stack bit
 	
 Time to Live Processing
   – Needed to support TTL since IP header not read
   – First label TTL set to IP header TTL on entry to MPLS domain
   – TTL of top entry on stack decremented at internal LSR

- If zero, packet dropped or passed to ordinary error processing (e.g. ICMP)
- If positive, value placed in TTL of top label on stack and packet forwarded
- At exit from domain, (single stack entry) TTL decremented
- If zero, as above
- If positive, placed in TTL field of Ip header and
- Label Stack
- Appear after data link layer header, before network layer header
- Top of stack is earliest (closest to network layer header)
- Network layer packet follows label stack entry with S=1
- Over connection oriented services
- Topmost label value in ATM header VPI/VCI field
- Facilitates ATM switching
- Top label inserted between cell header and IP header
- In DLCI field of Frame Relay
- Note: TTL problem

Position of MPLS Label Stack

(a) Data Link Frame

(b) IEEE 802 MAC Frame
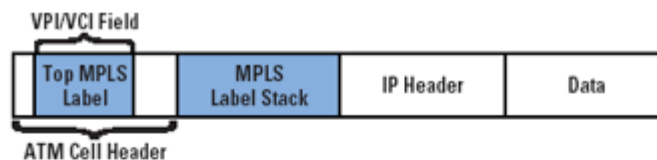
(c) ATM Cell
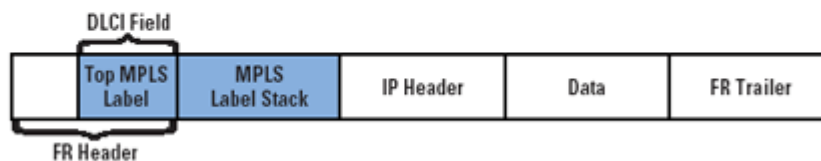
(d) Frame Relay Frame

FECs, LSPs, and Labels
- Traffic grouped into FECs
- Traffic in a FEC transits an MLPS domain along an LSP
- Packets identified by locally significant label
- At each LSR, labelled packets forwarded on basis of label.
- LSR replaces incoming label with outgoing label
- Each flow must be assigned to a FEC
- Routing protocol must determine topology and current conditions so LSP can be
- assigned to FEC
- Must be able to gather and use information to support QoS
- LSRs must be aware of LSP for given FEC, assign incoming label to LSP,communicate label to other LSRs

Explanation – Setup

Labelled switched path established prior to routing and delivery of packets

QoS parameters established along path

- – Resource commitment
- – Queuing and discard policy at LSR
- – Interior routing protocol e.g. OSPF used
- – Labels assigned
- – Source/destination IP address or network IP address
- – Port numbers
- – IP protocol id
- – Differentiated services codepoint
- – IPv6 flow label

Forwarding is simple lookup in predefined table

- – Map label to next hop

Can define PHB at an LSR for given FEC

Packets between same end points may belong to different FEC

Video Content / Details of website for further learning (if any):
https://www.dummies.com/programming/networking/juniper/label-stacking-in-mpls-networks/

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002. (352-353)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-43

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : **C.Nithya**

Unit : **V- Protocols for QoS Support** **Date of Lecture:**

Topic of Lecture: RTP – Protocol Architecture
Introduction : The **Real-time Transport Protocol** (**RTP**) is a network protocol for delivering audio and video over IP networks. RTP is used in communication and entertainment systems that involve streaming media,such as telephony, video teleconference applications including WebRTC, television services and web-based push-to-talk features.
Prerequisite knowledge for Complete understanding and learning of Topic: • TCP • UDP • Segments
Detailed content of the Lecture: **Real-time Transport Protocol** (**RTP**) TCP not suited to real time distributed application – Point to point so not suitable for multicast – Retransmitted segments arrive out of order – No way to associate timing with segments UDP does not include timing information nor any support for real time applications Solution is real-time transport protocol RTP **RTP Architecture** • Close coupling between protocol and application layer functionality • Framework for application to implement single protocol • Application level framing • Integrated layer processing • Application Level Framing • Recovery of lost data done by application rather than transport layer • Application may accept less than perfect delivery • Real time audio and video • Inform source about quality of delivery rather than retransmit • Source can switch to lower quality • Application may provide data for retransmission

- Sending application may recompute lost values rather than storing them
- Sending application can provide revised values
- Can send new data to ―fix‖ consequences of loss
- Lower layers deal with data in units provided by application
- Application data units (ADU)

Integrated Layer Processing
- Adjacent layers in protocol stack tightly coupled
- Allows out of order or parallel functions from different layers
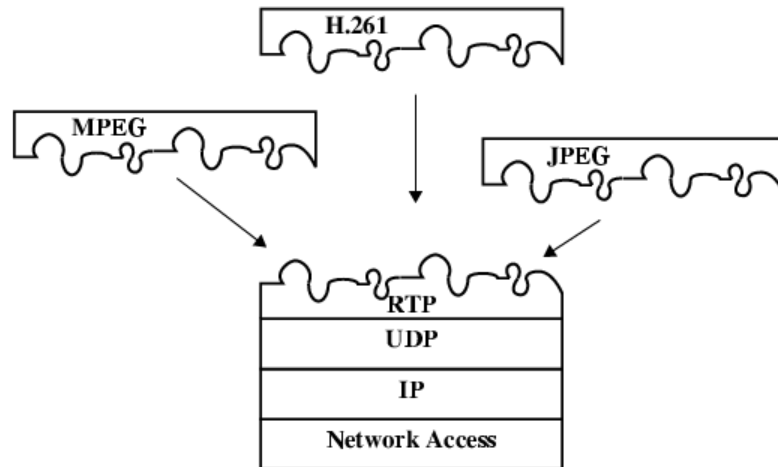
Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Real-time_Transport_Protocol
https://www.youtube.com/watch?v=CttYdLpGeGA
https://www.youtube.com/watch?v=bEYwHvLuy80

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002.
(353-355)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-44

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty : C.Nithya

Unit : V- Protocols for QoS Support   Date of Lecture:

Topic of Lecture: Data Transfer Protocol
Introduction :   • RTP – short for Real-time Transport Protocol defines a standard packet format for delivering audio and video over the Internet. It is defined in RFC 1889.   • It was developed by the Audio Video Transport Working group and was first published in 1996.
Prerequisite knowledge for Complete understanding and learning of Topic: • TCP   • UDP   • Network Layer
Detailed content of the Lecture: **Data Transfer Protocol**   • RTP applications can use the Transmission Control Protocol (TCP), but most use the User Datagram protocol (UDP) instead because UDP allows for faster delivery of data.   **RTP Data Transfer Protocol**   • Transport of real time data among number of participants in a session, defined by: • RTP Port number   • UDP destination port number if using UDP   • RTP Control Protocol (RTCP) port number   • Destination port address used by all participants for RTCP transfer   • IP addresses   • Multicast or set of unicast   • Multicast Support   • Each RTP data unit includes: • Source identifier   • Timestamp   • Payload format   • Relays   • Intermediate system acting as receiver and transmitter for given protocol layer   • Mixers   – Receives streams of RTP packets from one or more sources   – Combines streams

- Forwards new stream
- Translators

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=rMuhgZegNio
https://www.youtube.com/results?search_query=+RTCP.

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002 (365-368)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-45

CSE

III/VI

Course Name with Code : High Speed Networks-16CSE10

Course Faculty   : C.Nithya

Unit   : V- Protocols for QoS Support   **Date of Lecture:**

Topic of Lecture: RTCP
Introduction :   • The RTP Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP). Its basic functionality and packet structure is defined in RFC 3550. RTCP provides out-of-band statistics and control information for an RTP session.   • It partners with RTP in the delivery and packaging of multimedia data, but does not transport any media data itself.
Prerequisite knowledge for Complete understanding and learning of Topic: • TCP   • UDP   • Network Layer
Detailed content of the Lecture: **RTP Control Protocol (RTCP)**   • RTP is for user data   • RTCP is multicast provision of feedback to sources and session participants   • Uses same underlying transport protocol (usually UDP) and different port number   • RTCP packet issued periodically by each participant to other session members   **RTP Header**

RTCP Functions
- QoS and congestion control
- Identification
- Session size estimation and scaling
- Session control

RTCP Transmission

Number of separate RTCP packets bundled in single UDP datagram

– Sender report

– Receiver report

– Source description

– Goodbye

– Application specific

Packet Fields (All Packets)

Version (2 bit) currently version 2

Padding (1 bit) indicates padding bits at end of control information, with number of octets as last octet of padding

Count (5 bit) of reception report blocks in SR or RR, or source items in SDES or BYE

Packet type (8 bit)

Length (16 bit) in 32 bit words minus 1

In addition Sender and receiver reports have:

–Synchronization Source Identifier

Packet Fields (Sender Report) Sender Information Block
- NTP timestamp: absolute wall clock time when report sent
- RTP Timestamp: Relative time used to create timestamps in RTP packets
- Sender's packet count (for this session)
- Sender's octet count (for this session)

Packet Fields (Sender Report) Reception Report Block
- SSRC_n (32 bit) identifies source refered to by this report block
- Fraction lost (8 bits) since previous SR or RR
- Cumulative number of packets lost (24 bit) during this session
- Extended highest sequence number received (32 bit)
  –Least significant 16 bits is highest RTP data sequence number received from SSRC_n
  –Most significant 16 bits is number of times sequence number has wrapped to zero
- Interarrival jitter (32 bit)
- Last SR timestamp (32 bit)
- Delay since last SR (32 bit)

Receiver Report
- Same as sender report except:
  - Packet type field has different value
  - No sender information block

Source Description Packet
- Used by source to give more information
- 32 bit header followed by zero or more additional information chunks
  E.g.:

- 0 END End of SDES list
- 1 CNAME Canonical name
- 2 NAME Real user name of source
- 3 EMAIL Email address

Goodbye (BYE)

- Indicates one or more sources no linger active

    –Confirms departure rather than failure of network

Application Defined Packet

- Experimental use
- For functions & features that are application specific

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=rMuhgZegNio
https://www.youtube.com/results?search_query=+RTCP.

Important Books/Journals for further learning including the page nos.:
William Stallings, "High Speed Networks and Internet", Pearson Education, Second Edition, 2002 (365-368)

Course Faculty

Verified by HOD