UNIT I HIGH SPEED NETWORKS

Frame relay networks – Asynchronous transfer mode – ATM protocol architecture –ATM logical connection– ATM cell – ATM service categories – AAL – High speed LANs – Fast ethernet, gigabit ethernet – Fiber channel – Wireless LANs– Applications– Requirements – Architecture of 802.11

1.Define frame relay.
A form of packet switching based on the use of variable-length link-layer frames. There is no network layer, and many of the basic functions have been streamlined or eliminated to provide for greater throughput.

2. What is LAPB protocol?
The LAPB protocol provides a reliable data link control protocol across a link.
The packet level is used to define virtual circuits. Between the subscriber device and the packet switching node to which it is attached, an LAPB protocol is used to assure reliable transfer of frames.

3. What is LAPF protocol?
LAPF is a physical layer and a data link layer control protocol.
LAPF provides a minimal set of data link control functions, consisting of the following:
• Frame delimiting, alignment, and transparency
• Frame multiplexing/demultiplexing using the address field.
• Inspection of frame for length constraints
• Detection of transmission errors
• Congestion

4. Define ATM.
Asynchronous Transfer Mode (ATM) is a method for multiplexing and switching that supports a broad range of services. ATM is a connection-oriented packet switching technique that generalizes the notion of a virtual connection to one that Provides quality-of-service guarantees.
A form of packet transmission using fixed size packets, called cells. ATM is the data transfer interfaces for B-ISDN. Unlike X.25, ATM does not provide error control and flow control mechanisms.

5. What are the three planes in the protocol reference model?
• User plane
• Control plane
• Management plane

6. Define ATM adaptation layer (AAL)
The layer that maps information transfer protocols onto ATM

7. Name two WAN technologies.
a) Frame relay.
b) ATM

8. Write down the advantages of packet switching.
a) Flexibility
b) Resource sharing
c) Robustness
d) Responsiveness

9. Define Jitter
A phenomenon in real- time traffic caused by gaps between consecutive packets at the receiver.

10. How circuit switching networks began to be used increasingly for data Connections?
• In a typical terminal-to-host data connection, much of the time the line is idle. Thus, with data connections, a circuit-switching approach is inefficient.
• In a circuit-switching network, the connection provides for transmission at a constant data rate. Thus each of the two devices that are connected must transmit and receive at the same data rate as the other. This limits the utility of the network in interconnecting a variety of host computers and terminals.

11. Write down the advantages of packet switching network over circuit switching.
Line efficiency is greater, because a single node-to-node link can be dynamically shared by many packets over time.
• A packet-switching network can carry out data-rate conversion.
• Priorities can be used.

12. What are the advantages of virtual paths?
• Simplified network architecture
• Increased network performance and reliability
• Reduced processing and short connection setup time
• Enhanced network services

13. What are the main features of ATM?
• The service is connection-oriented, with data transfer over a virtual circuit.
• The data is transferred in 53 byte packets called cells.
• Cells from different VCs that occupy the same channel or link are statistically multiplexed.

• ATM switches may treat the cell streams in different VC connections unequally over the same channel in order to provide different qualities of services (QOS).

14. What are the traffic parameters of connection-oriented services?
• Peak Cell Rate (PCR)
• Sustained Cell Rate (SCR)
• Initial Cell Rate (ICR)
• Cell Delay Variation Tolerance (CDVT)
• Burst Tolerance (BT)
• Minimum Cell Rate (MCR)

15. What are the quality service (Quos) parameters of connection-oriented services?
1. Cell Loss Ratio (CLR)
2. Cell Delay Variation (CDV)
3. Peak-to-Peak Cell Delay Variation (Peak-to-Peak CDV)
4. Maximum Cell Transfer Delay (Max CTD)
5. Mean Cell Transfer Delay (Mean CTD)

16. What are the types of delays encountered by cells
1. Packetization delay (PD) at the source
2. Transmission and propagation delay (TD)
3. Queuing delay (QD) at each switch
4. Affixed processing delay (FD) at each switch
5. A jitter compression or depacketization delay (DD) at the destination

17. What do you mean by ATM addressing?
An ATM address indicates the location of an ATM interface in the network topology. This means that ATM address is not portable. The prefix of an address is associated with a group of interfaces with the same prefix.

18. Mention the types of ATM network interface.
Two most important interfaces are:
1. User-network interface (UNI)
2. Network-network interface or network-node interface (NNI).

19. What do you mean by user-network interface (UNI) and network-network interface or Network-node interface (NNI)?
UNI is the interface between an ATM end system and an ATM switch, NNI is the interface between two ATM switches.

20. What are the two sub layers of AAL?
1. Convergence Sub layer (CS)
2. Segmentation and Reassembly Sub layer (SAR).

21. What is the function of CS?
The Convergence Sub layer (CS) converts the information stream into four types of packets streams, called AAL Type1, Type2, Type3/4, and Type5.The packet formats match the requirements of the information stream.

22. What are the subdivisions of CS?
1. Upper, service-specific or SSCS sub layer
2. Lower, common part or CPCS sub layer.

23. What do you mean by Type1 traffic?
Type1 traffic is a traffic generated at constant bit rate, and it is required to be delivered at the same rate (with a fixed delay).

24. What is meant by traffic policing?
In management and control the network must monitor the data transfer to make sure that the source also conforms to the QoS specification and to drop its cells as appropriate, is said to be a traffic policing.

25. What are the functions of management and control?
1. Fault management
2. Traffic and congestion control
3. Network status monitoring and configuration
4. User/network signaling.

26. What are the layers of BISDN reference model?
User plane, Control plane, Layer management plane, Plane management plane.

27. What are the basic tasks required for internetworking over ATM?
Two basic tasks are:
1. Encapsulation of the protocol data unit
2. Routing of bridging of PDU.

28. What are the functions of user plane?
It compromise the functions required for the transmission of user information for instance, for an internet protocol over ATM, these layers could be HTTP/TCP/IP/AAL5.

29. What are the three strategies of IP over ATM?
The three strategies are
1. The classical IP model
2. The short cut models
3. The integrated models.

30. What are the basic signaling function between the network and user?
The basic signaling function between the network and user are as follows:
1. The user requests a switched virtual connection
2. The network indicates whether the request is accepted or not

3. The network indicates error conditions with a connection.

31. Define Virtual channel Link.
It a means of unidirectional transport of ATM cells between a point where a VCI value is assigned and the point where that value is translated or terminated

32. Define virtual channel Identifier.
It is a unique numerical tag that identifies a particular VC link for a given VPC.

33. What is Virtual channel connection?
VCC is a concatenation of VC links that extends between two points where ATM service users access the ATM layer. VCC's are provided for the purpose of user-user, user-network, or network-network information transfer. Cell sequences integrity is preserved for cells belonging to the same VCC.

34. Define Virtual path.
It is a generic term used to describe unidirectional transport of ATM cells belonging to virtual channels that are associated by a common unique identifier value.
35. Define VPC (Virtual Path Connection).
VPC is a concatenation of VP links that extends between the point where the VCI values are assigned and the point where those values are translated or removed ,i.e., extending the length of a bundle of VC links that share the same VPI. VPS's are provided for the purpose of user-user, user-network, or network-network information transfer.

36. What are the different categories of services provided by ATM?
• Real-time services
i. Constant Bit Rate(CBR)
ii. Real-Time Variable Bit Rate(rt-VBR)
• Non-Real Time Service
i. Non-Real-Time Variable Bit Rate(nrt-VBR)
ii. Unspecified Bit Rate(UBR)
iii. Guaranteed Frame Rate(GFR)

37. What are the two basic tasks required for internetworking over ATM?
The first is encapsulation of the protocol data units, and the second is Routing or bridging of these PDUs.

38. Define fast Ethernet
Fast Ethernet refers to a set of specifications developed by the IEEE 802.3 committee to provide a low-cost, Ethernet-compatible LAN operating at 100 Mbps.

39. Define gigabit Ethernet?

Gigabit Ethernet, which has a data rate of 1000 Mbps (Or) 1 Gbps. In which collision domain is reduced. Gigabit Ethernet is mainly designed to use optical fiber, although the protocol does not eliminate the use of twisted pair cables.
There are four implementations have been designed for gigabit Ethernet:
a) 1000Base-LX
b) 1000Base-SX
c) 1000Base-CX
d) 1000Base-T

40. List requirements for WLAN?
a). Throughput
b). Number of nodes
c). Connection to backbone LAN
d). Service area
e). Battery power consumption
f). Transmission robustness and security
g). Collocated network operation
h). License-free operation
i). Handoff/roaming
j). Dynamic configuration

41. List out the important services of IEEE 802.11?
a) Association
b) Reassociation
c) Disassociation
d) Authentication
e) Privacy

42. Mention the requirements for fiber channels?
a) Full duplex links with two fibers per link.
b) Performance from 100 Mbps TO 800 Mbps on a single line.
c) Small connectors
d) Support for distances up to 10 km.
e) High capacity utilization with distance insensitivity.
f) Broad availability.
g) Small systems
h) Interface and network protocols.

43. List out the fiber channel elements?
a a) Node: the key elements of a fiber channel network are the end systems.
b) Fabric: the collection of switching elements)

PART-B

1.Explain the features of Asynchronous transfer mode

Asynchronous Transfer Mode

It is a time slotted system but none of the time slots are reserved and there is no framing structure.

At connection set-up time, a contract is signed for bandwidth usage (i.e., no. of slots that may be used per unit of time by the connection).

User data is packetized and transmitted in the slots on a slot by slot basis.

As slots are not specifically assigned to user connections, access control schemes must be used to provide for a ‘‘fair’’ system. They are used to guarantee that users do not use more than their share (i.e., as agreed upon in the connection’s contract).

The slots are of a fixed size to simplify switch design and increase processing speed.
Deciding on the appropriate slot/packet size was quite controversial:
• For low volume real-time services such as voice, packets had to be small.
• For data, small packet sizes meant high overhead.
l Packet sizes that were considered (or put forward by the different interest groups): 32, 64, 128 bytes -> compromised solution: 48 bytes!

Features of an ATM network:

l High bit rate transmission trunks (155Mbps) and small cell size: -> very small transmission times: 53 bytes/155M = 2.8microsecs.
l Propagation delays have not changed (laws of physics): on the order of millisecs (e.g.: NY - SF: 20ms).

l This means that several thousand cells are in transit on long haul trunks: From NY - SF: 155Mx20ms/53bytes=7K
l Because of this phenomenon ATM uses neither error control nor flow control on user data streams!

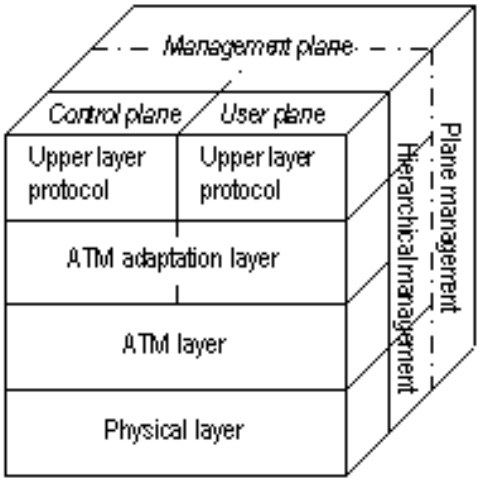
l Error control introduces too many delays and with the low error rates on fiber optic trunks it is not worth it.

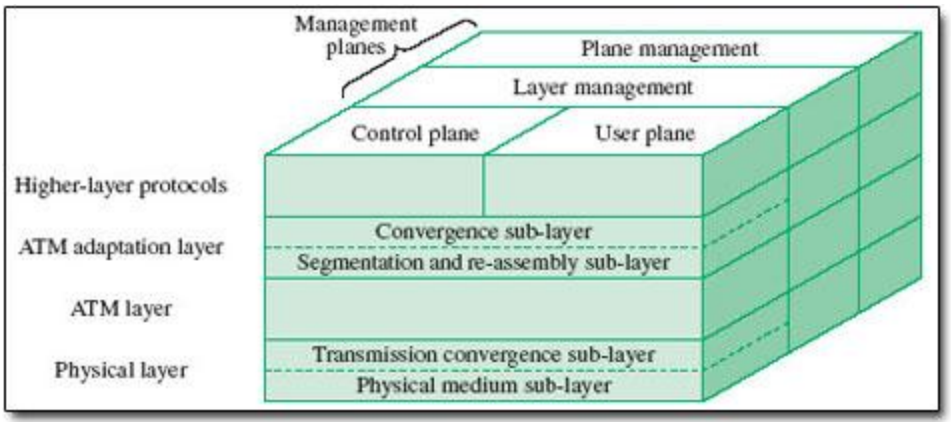
l Flow control is totally useless as too many packets are in transit between source and destination for a feedback mechanism to have any effect

2.**Draw and explain the ATM protocol architecture.**

ATM Layer:

- Common to all services and provides cell transfer capabilities.
- Provides logical connections upon the physical layer:
! Virtual Channels
! Virtual Paths
! ATM Adaptation Layer (AAL):
- Provides a range of alternative service types known as service classes.
- Converts the source information into streams of 48-octet segments.





The three planes in the protocol reference model are

- **User plane**
- **Control plane**
- **Management plane**

User plane

Provides for user information transfer

Control plane
Call and connection control

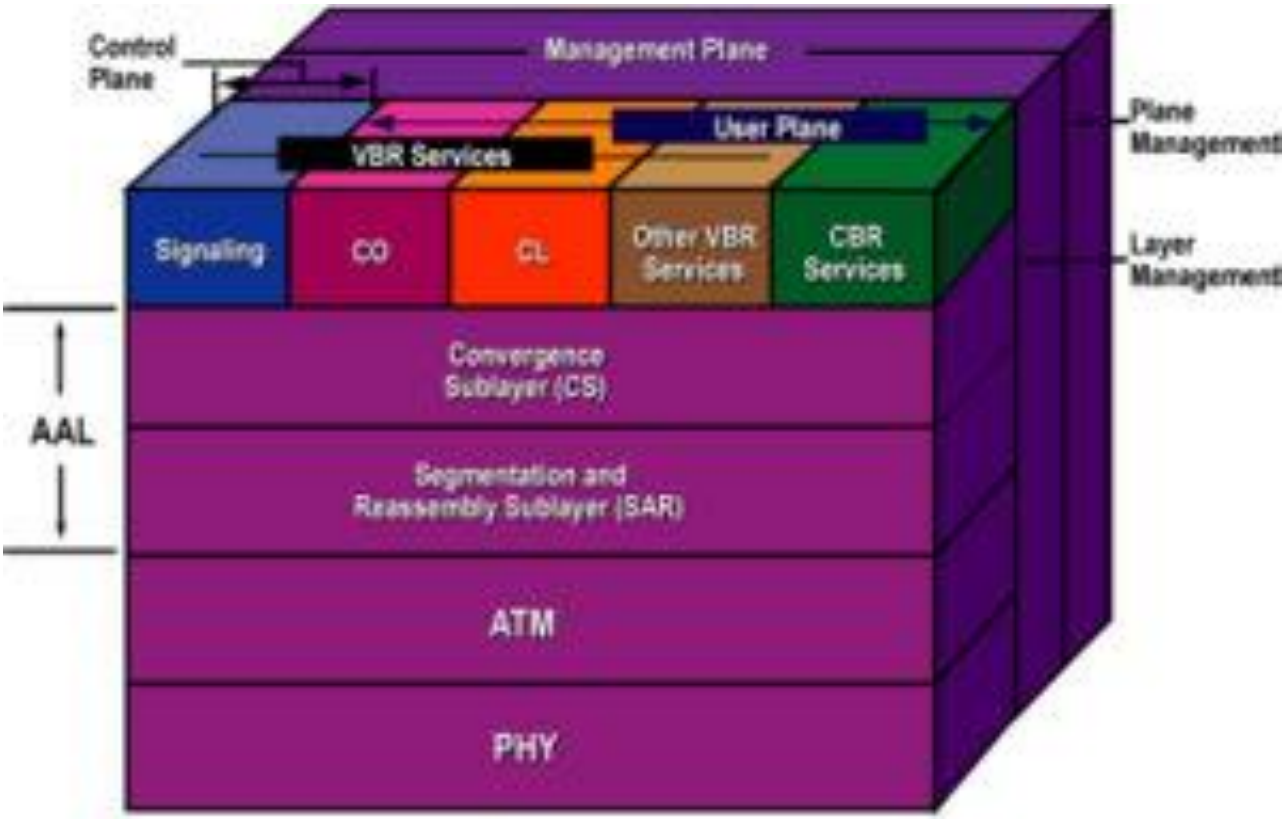
Management plane

Plane management
Whole system functions

Layer management
Resources and parameters in protocol entities

functions of management and control plane

1. Fault management
2. Traffic and congestion control
3. Network status monitoring and configuration
4. User/network signaling.



3.Write short note son ATM Logical Connections.

ATM Logical Connections

! Logical connections in ATM are referred to as Virtual Channel Connections (VCCs).
VCCs are used for:
- user-to-user exchange of variable rate, full duplex, fixed-size cells carrying user data.
- user-to-network exchange of control signaling information.
- network-to-network exchange of management and routing information.

! A Virtual Path Connection (VPC) is a bundle of VCCs that have the same endpoints.
! All the cells flowing over all VCCs in a single VPC are switched together.

To set up a VCC, there must first be a VPC to the required destination node with sufficient available capacity to support the VCC with the appropriate QOS.
The virtual path control mechanisms include:
- calculating routes
- allocating capacity
- storing connection state information

Virtual path concept was developed in response to a trend in high speed networking in which the control cost of the network is becoming an increasingly higher proportion of the overall cost.

– Controls the cost by grouping connections that share a common path
– Network management actions can then be applied to a small number of groups of connections instead of to a large number of individual connections.

The concepts of virtual path and virtual channel are defined in ITU-T Recommendations with reference to both the user network and the internal network operation.

Virtual Channel (VC)	A generic term used to describe unidirectional transport of ATM cells associated by a common unique identifier.value.
Virtual Channel Link	A means of unidirectional transport of ATM cells between a point where a VCI value is assigned and the point where that value is translated or terminated.
Virtual Channel Identifier (VCI)	Identifies a particular VC link for a given VPC.
Virtual Channel Connection (VCC)	A concatenation of VC links that extends between two points where the adaptation layer is accessed. VCCs are provided for the purpose of user-user, user-network, or network-network information transfer. Cell sequence integrity is preserved for cells belonging to the same VCC.
Virtual Path	A generic term used to describe unidirectional transport of ATM cells belonging to virtual channels that are associated by a common unique identifier value.
Virtual Path Link	A group of VC links, identified by a common value of VPI, between a point where a VPI value is assigned and the point where that value is translated or terminated.
Virtual Path Identifier (VPI)	Identifies a particular VP link.
Virtual Path Connection (VPC)	A concatenation of VP links that extends between the point where the VCI values are assigned and the point where those values are translated or removed, i.e., extending the length of a bundle of VC links that share the same VPI. VPCs are provided for the purpose of user-user, user-network, or network-network information transfer.

Virtual Channel Connection Uses

- **Between end users**

– to carry end-to-end user data

– A VPC between end users provides them with an overall capacity

- **Between an end user and a network entity**

– to carry user-network control signaling

– A user-to-network VPC can be used to aggregate traffic from an end user to a network exchange or network server

- **Between two network entities**

– used for network management and routing functions

– A network-to-network VPC can be used to define a common route for the exchange of network management information

4.**Draw the ATM Cells with its features.**

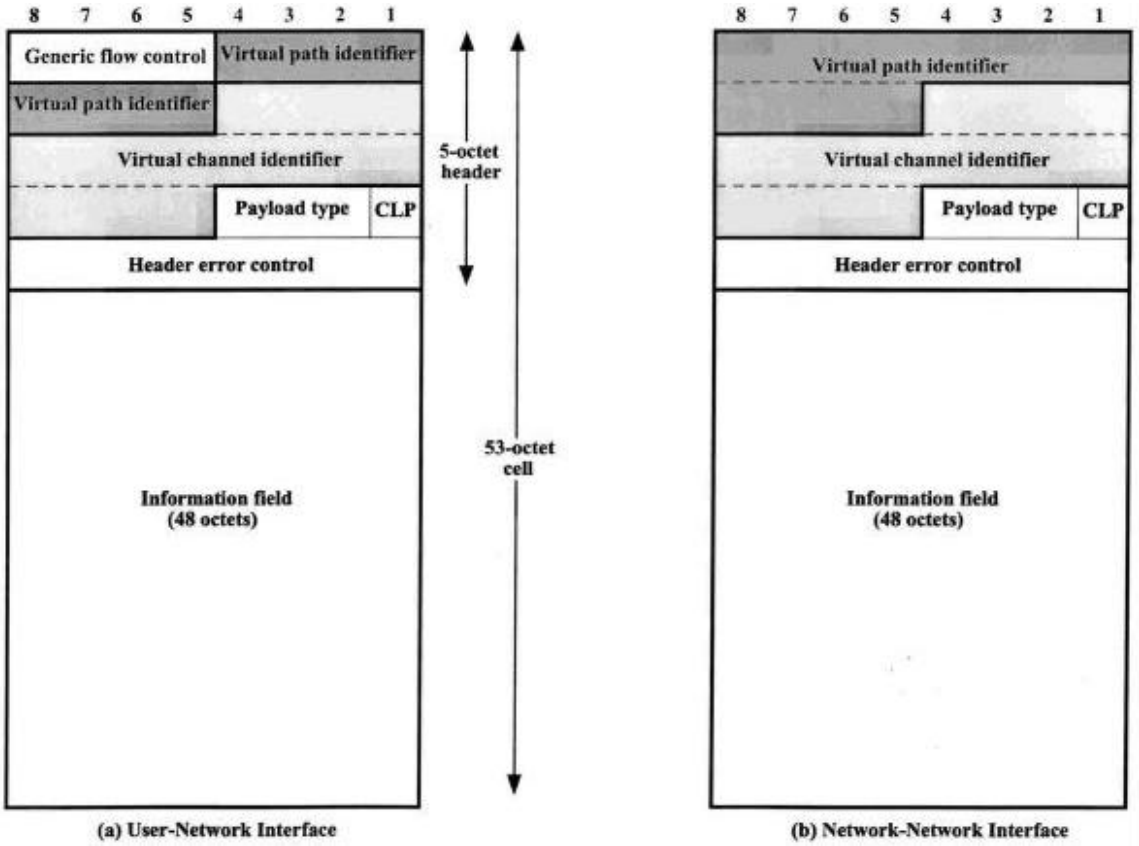
• ATM has fixed-size cells consists of a 5-byte and a 48-byte information field.

Advantages are:

– reducing queuing delay for high-priority cells

– cells can be switched more efficiently in high data rates of ATM

  – easier implementation of switching mechanism in hardware



The *generic flow control field* can be used for control of cell flow only atthe local user-network interface (details of applications for further study)– This field could be used to assist the customer in controlling the flow of traffic for different qualities of service.

– One usage would be a multiple-priority level indicator to control the flow of information in a service-dependent manner.

Virtual path identifier (VPI) constitutes a routing field for the network.
– 8 bits at the user-network interface and 12 bits in network-network interface
– for more virtual paths to be supported within the network

Virtual channel identifier (VCI) is used for routing to and from the end user; functions much as a service access point.

Payload-type (PT) field indicates the type of information in the information field.

PT coding	Interpretation
0 0 0	User data cell, AAU = 0, congestion not experienced
0 0 1	User data cell, AAU = 1, congestion not experienced
0 1 0	User data cell, AAU = 0, congestion experienced
0 1 1	User data cell, AAU = 1, congestion experienced
1 0 0	OAM F5 segment associated cell
1 0 1	OAM F5 end-to-end associated cell
1 1 0	Resource management cell
1 1 1	Reserved for future function

AAU = ATM user to ATM user indication

First bit of "0" shows user information
• Then the second bit indicates whether congestion has been experienced
• The third bit (AAU) is a one-bit field that can be used to convey information between end users
  – First bit of "1" indicates that the cell carries network management information
  –

• *Cell-loss priority (CLP)* is used to provide guidance to the network in the event of congestion.
– 0: indicates a cell of relatively higher priority (should be discarded only when no other alternative is available
– 1: indicates that this cell is subject to discard within the network
– A way for congestion control
– User can employ this field to insert extra information to the network
– In the case of congestion, a cell with marked CLP for discard will be in preference to cells fall within agreed traffic limits.

5.Explain the ATM Service Categories

ATM Service Categories

! Real-Time Service:

- Constant Bit Rate (CBR)
- Real-Time Variable Bit Rate (rt-VBR)

! Non-Real-Time Service:

- Non-Real-Time Variable Bit Rate (nrt-VBR)
- Available Bit Rate (ABR)
Application specifies a peak cell rate (PCR) that it will use and a minimum cell rate (MCR) that it requires.
- Unspecified Bit Rate (UBR)
This is a best-efforts service using capacity not allocated to any other service.

AAL Sublayers

! Convergence Sublayer (CS):

Performs a convergence function between the service offered at the layer interface and that provided by the underlying ATM layer.

! Segmentation and Reassembly (SAR) Sublayer:

Provides cell segmentation and reassembly functions

6.Describe the ATM Adaptation Layer and its protocols with diagrams.

ATM Adaptation Layer

• An adaptation layer in needed to support information transfer protocols not based on ATM such as

– **PCM**: it is necessary to assemble PCM bits into cells for transmission and to read them out on reception

– **LAPF**: to map LAPF frames of a frame relay network connected to an ATM network into ATM cells

AAL Services (ITU-T I.362)

• handling of transmission errors

• segmentation and reassembly, to enable larger blocks of data to be carried in the information field of ATM cells

• handling of lost and misinserted cells conditions

• flow control and timing control

	Class A	Class B	Class C	Class D
Timing relation between souce and destination	Required		Not required	
Bit rate	Constant	Variable		
Connection mode	Connection-oriented			Connectionless
AAL Protocol	Type 1	Type 2	Type 3/4,Type 5	Type 3/4

classification of services is based on

– whether timing relationship must be maintained between source and destination

– whether application requires a constant bit rate

– whether the transfer is connection-oriented or connectionless

AAL Protocols

• organizing the AAL into two logical sublayers

– **Convergence Sublayer (CS)**

• provides functions needed to support specific applications using AAL

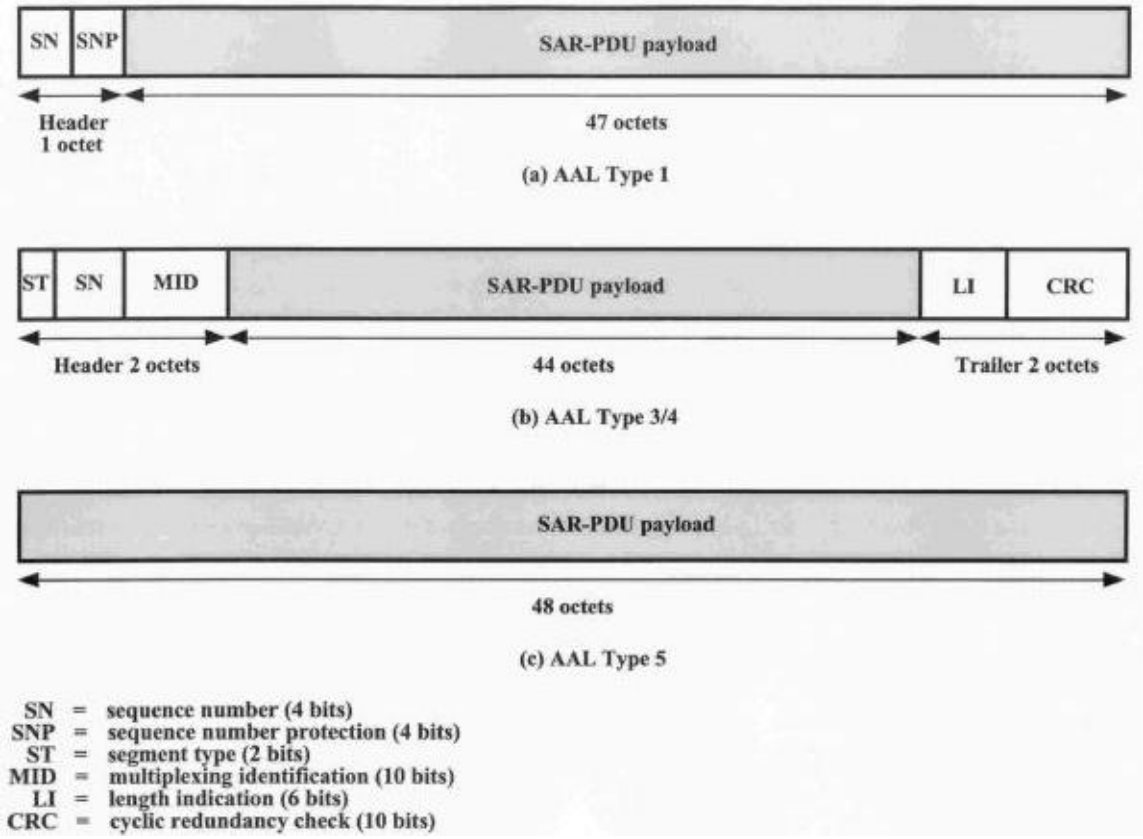
• each AAL user attaches to AAL at a service access point (SAP)

• SAP is simply the address of the application
• CS is service dependent

– **Segmentation and Reassembly Sublayer (SAR)**

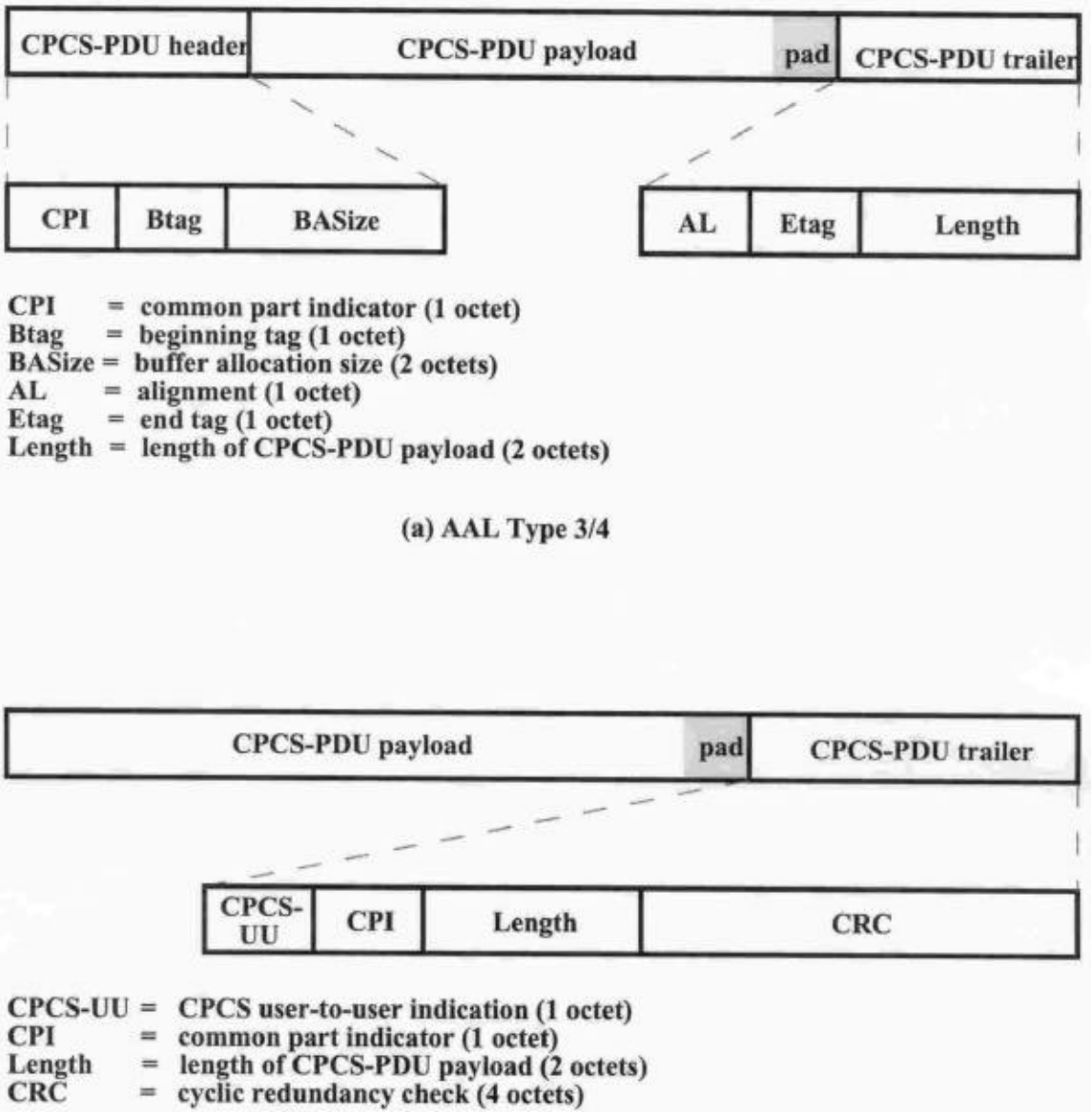
• responsible for packaging information received from CS into cells, and
• unpacking the information at the receiving end
• total SAR headers and trailersplus CS information is 48 bytes

• Originally ITU-T had one protocol type for each class
– recently types 3 and 4 merged into a Type 3/4, and a new type 5
– see below for PDU formats at SAR level except for Type 2 (to be defined)



AAL Type 5 is more popular especially in ATM LAN applications
– to reduce protocol-processing overhead
– to reduce transmission overhead
– to ensure adaptability to existing transport protocols

• A block of data from a higher layer is encapsulated into a protocol data unit (PDU) at the CS sublayer (referred to as the *common-part convergence sublayer*-CPCS)



AAL Type 3/4 and Type 5 CSPS PDU

Explain AAL with ATM AAL2 Cell Diagram

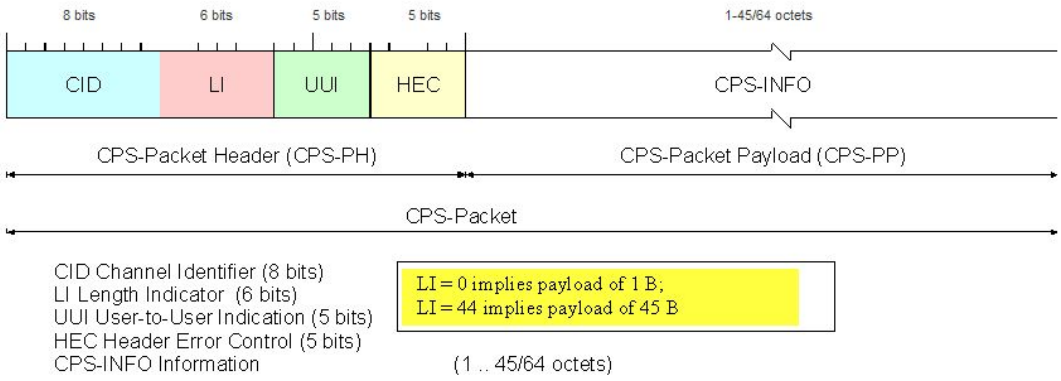
ATM Adaptation Layer (AAL)

• ATM **Adaptation Layer** (AAL): "adapts"upper layers (IP or native ATM applications)to ATM layer below

• AAL present **only in end systems**, not in switches

• AAL layer segment (header/trailer fields,data) fragmented across multiple ATM cells
– analogy: TCP segment in many IP packets

ATM AAL2 Cell Diagram



7.Draw and explain the Architecture of 802.11

IEEE 802 .11 Terminology

Station (STA) Architecture:

* Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system
*Most often end-stations available in terminals (work-stations, laptops etc.)
Implemented in Avaya Wireless IEEE 802.11PC-Card

Access-Point (AP) Architecture:

 Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations

Most often infra-structure products that connect to wired backbones

Stations select an Access-Point and "associate with it

Access-Points :

Support roaming

Provide time synchronization functions (beaconing)

Provide Power Management support

Traffic typically flows through Access-Point in IBSS direct Station-to-Station communication takes place

Basic Service Set (BSS):

 A set of stations controlled by a single "Coordination Function" (=the logical function that determines when a station can transmit or receive)

* Similar to a "cell" in pre IEEE terminology

* A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only)

* Diameter of the cell is app. twice the coverage-distance between two wireless stations

Independent Basic Service Set (IBSS):

 A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available

A BSS without an Access-Point

One of the stations in the IBSS can be configured to "initiate" the network and assume the Coordination Function

Diameter of the cell determined by coverage distance between two wireless stations

Extended Service Set (ESS):

 A set of one or more Basic Service Sets interconnected by a Distribution System (DS)

Traffic always flows via Access-Point

Diameter of the cell is double the coverage distance between two wireless stations

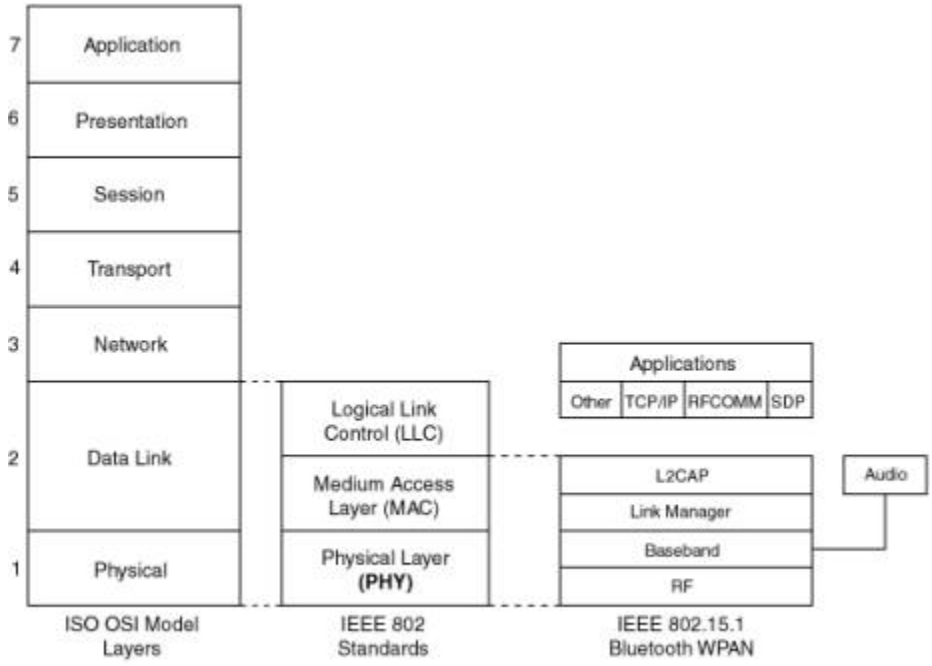
Distribution System (DS):

 A system to interconnect a set of Basic Service Sets Integrated; A single Access-Point in a standalone network

Wired; Using cable to interconnect the Access-Points

Wireless; Using wireless to interconnect the Access-Points

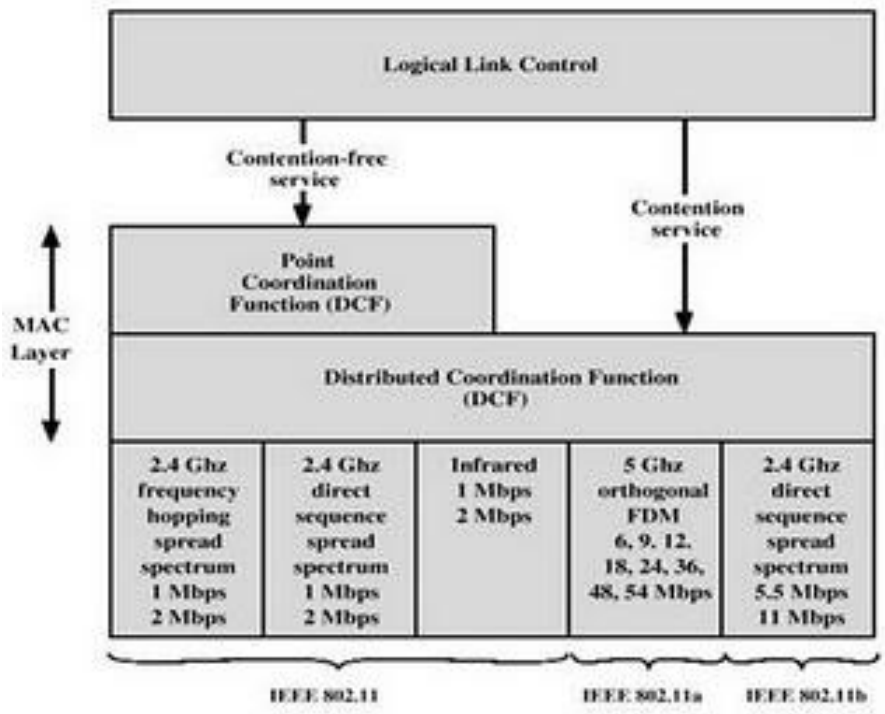
8.Draw and explain the architecture of IEEE 802.11



Important services of IEEE 802.11

a) Association
b) Reassociation
c) Disassociation
d) Authentication
e) Privacy

Architecture of 802.11



UNIT II CONGESTION AND TRAFFIC MANAGEMENT

Queuing analysis – Queuing models – Single server queues – Effects of congestion –Congestion control – Traffic management – Congestion control in packet switching networks – Frame relay congestion control.

PART-A(2 MARKS)

1. Define mean residence time?
The average time that an item spends in the system, waiting and being served is referred to as mean residence time.

2. What is Kendall's notation?
X/Y/N
X- Distribution of the inter arrival times
Y- Distribution of service times
N- Number of servers

3. Mention the techniques that can be used for congestion control.
• Backpressure
• Choke packet
• Implicit congestion signaling
• Explicit congestion signaling

4. Define backpressure technique for congestion control.
In this technique, if a node gets congested it will halt or slow down the flow of incoming packets. If this flow restriction persists then the previous node will slow down or halt the traffic on its incoming links. This flow restriction propagates backward to sources which are restricted in the flow of new packets into the network.

5.What is a choke packet?
A choke packet is a control packet generated at a congested node and transmitted back to a source node to restrict traffic flow. Either a router or a destination end system may send the message to a source end system, questing that it reduce the rate at which it is sending traffic to the internet destination.

6. **Write about implicit congestion signaling.**
When congestion occurs 2 things happen:
1) Packets are delayed
2) Packets are discarded
The Source detects congestion implicitly from transmission delays and discarded packets and reduces flow

7. Name two ways in which explicit congestion control techniques work.

• Backward
• Forward

8. Write about forward explicit congestion control technique.
It notifies the user that the congestion avoidance procedures should be initiated where applicable for traffic in the same direction as the received packet.
When a forward signal is received by an end system, it echoes the signal back along the logical connection to the source.

9. Write about backward explicit congestion control technique
Notifies the source that the congestion avoidance procedure should be initiated, where applicable for traffic in the opposite direction as the received packet. It indicates that the packets that the user transmits on this logical connection may encounter congested resources.

10. What are the three explicit congestion control approaches?
Binary
Credit-based
Rate based

11. **Write down the traffic management considerations for congestion control.**
Fairness
Quality of service
Reservations

12. What are the different frame relay congestion control techniques?
Discard strategy
Congestion avoidance
Congestion recovery

13. What 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

14. What is 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.

15. When congestion recovery procedures are done?
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.

16. Define CIR.

CIR – Committed Information Rate.

CIR is a rate in bits per second that the network agrees to support for a particular frame mode connection. Any data excess transmitted in excess of the CIR is vulnerable to discard in the event of congestion.

17. Define committed Burst size (B_c)

The maximum amount data that the network agrees to transfer, under normal conditions, over a measurement interval T.

18. Define Excess Burst size (Be)

The maximum amount of data in excess of **Bc** that the network will attempt to transfer, under normal conditions, over a measurement interval T. These data are uncommitted in the sense that the network does not commit to delivery under normal conditions.

19. What is the user's response to FECN or BECN?

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.

20.what are the application of traffic?

i.Voice and video
ii.file transfer and email
iii.interactive graphics and interactive computing applications.

PART-B

1.Explain any four congestion control mechanisms used in packet switching networks.

i) A 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

timestamped 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:
• 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.

2.Describe the effects congestion. Explain the various congestion control techniques.

i) Congestion at one point in the network can quickly propagate throughout a region or the entire network. While flow control is indeed a powerful tool, we need to use it in such a way as to manage the traffic on the entire network.
Congestion control techniques include:
• Back pressure
• Choke packet
• Implicit congestion signaling
• Explicit congestion signaling

Backpressure:
Backpressure can be exerted on the basis of links or logical connections. Backpressure can be selectively applied to logical connections, so that the flow from one node to the next in only restricted or halted on some connections. In this case, the restriction propagates back along the connection to the source. Backpressure is of limited utility. It can be used in a connection-oriented network that allows hop-by-hop flow control.

Choke packet:
A choke packet is a control packet generated at a congested node and transmitted back to a source node to restrict traffic flow.
e.g. ICMP (internet control message protocol) source quench packet.
The choke package is a relatively crude technique for controlling congestion.

Implicit congestion signaling:
When network congestion occurs, *two things* may happen:
(1) The transmission delay for an individual packet from source to destination increases, so that it is noticeably longer than the fixed propagation delay.
(2) *Packets are discarded.* If a source is able to detect increased delays and packets one discarded, then it has implicit evidence of network congestion.
Implicit signaling is an effective congestion control technique in connectionless, or datagram, configurations, such as IP-based internets.

Explicit congestion signaling:
It is desirable to use the available capacity in a network but still react to congestion in a controlled and fair manner.
For explicit congestion avoidance, the network alerts end systems to growing congestion within the network and the end systems take steps to reduce the offered load on the network.

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.

3.What are the Goals of Queuing Analysis?

Goals of Queuing Analysis

- Typically used in analysis of networking system; examples,
  - increase in disc access time
  - Increase in process load
  - Increase in rate of arrival of packets, processes

- Especially useful of analysis of performance when either the load on a system is expected to increase or a design change is contemplated.
- While it is a popular method in network analysis, it has gained popularity within a system esp. with the advent of multi-core processors.
-

Analysis methods

- After the fact analysis: let the system run some n number times, collect the "real" data and analyze – problems?
- Predict some simple trends /projections based on experience – problems?
- Develop analytical model based on queuing theory – problems?
- Rum simulation (not real systems) and collect data to analyze –problems?

4.Explain Traffic Management

Traffic Management

l In an ATM network, a **traffic source descriptor** is used to describe an end user service to the network.

l 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

l 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.

5.Explain the Frame relay congestion control.

Frame relay congestion control.

Frame Relay is a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.

Network providers commonly implement Frame Relay for voice (VoFR) and data as an encapsulation technique, used between local area networks (LANs) over a

wide area network (WAN). Each end-user gets a private line (or leased line) to a frame-relay node. The frame-relay network handles the transmission over a frequently-changing path transparent to all end-users.

Frame Relay has become one of the most extensively-used WAN protocols. Its cheapness (compared to leased lines) provided one reason for its popularity. The extreme simplicity of configuring user equipment in a Frame Relay network offers another reason for Frame Relay's popularity.

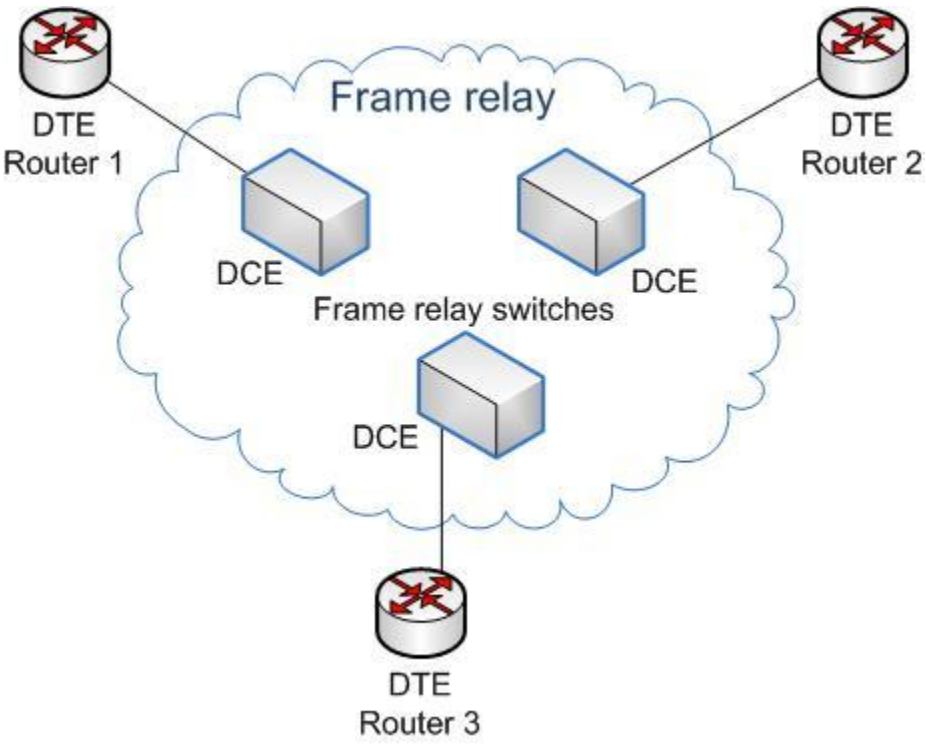
With the advent of Ethernet over fiber optics, MPLS, VPN and dedicated broadband services such as cable modem and DSL, the end may loom for the Frame Relay protocol and encapsulation. However many rural areas remain lacking DSL and cable modem services. In such cases the least expensive type of non-dial-up connection remains a 64-kbit/s frame-relay line. Thus a retail chain, for instance, may use Frame Relay for connecting rural stores into their corporate WAN.

The designers of Frame Relay aimed to a telecommunication service for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame Relay puts data in variable-size units called "frames" and leaves any necessary error-correction (such as re-transmission of data) up to the end-points. This speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line, while the service-provider figures out the route each frame travels to its destination and can charge based on usage.

An enterprise can select a level of service quality - prioritizing some frames and making others less important. Frame Relay can run on fractional T-1 or full T-carrier system carriers. Frame Relay complements and provides a mid-range service between basic rate ISDN, which offers bandwidth at 128 kbit/s, and Asynchronous Transfer Mode (ATM), which operates in somewhat similar fashion to frame Relay but at speeds from 155.520 Mbit/s to 622.080 Mbit/s.

Frame Relay has its technical base in the older X.25 packet-switching technology, designed for transmitting data on analog voice lines. Unlike X.25, whose designers expected analog signals, Frame Relay offers a fast packet technology, which means that the protocol does not attempt to correct errors. When a Frame Relay network detects an error in a frame, it simply drops that frame. The end points have the

responsibility for detecting and retransmitting dropped frames. (However, digital networks offer an incidence of error extraordinarily small relative to that of analog networks.)



Frame Relay often serves to connect local area networks (LANs) with major backbones as well as on public wide-area networks (WANs) and also in private network environments with leased lines over T-1 lines. It requires a dedicated connection during the transmission period. Frame Relay does not provide an ideal path for voice or video transmission, both of which require a steady flow of transmissions. However, under certain circumstances, voice and video transmission do use Frame Relay.

Frame Relay originated as an extension of Integrated Services Digital Network (ISDN). Its designers aimed to enable a packet-switched network to transport the

circuit-switched technology. The technology has become a stand-alone and cost-effective means of creating a WAN.

Frame Relay switches create virtual circuits to connect remote LANs to a WAN. The Frame Relay network exists between a LAN border device, usually a router, and the carrier switch. The technology used by the carrier to transport data between the switches is variable and may differ among carriers (i.e. to function, a practical Frame Relay implementation need not rely solely on its own transportation mechanism).

The sophistication of the technology requires a thorough understanding of the terms used to describe how Frame Relay works. Without a firm understanding of Frame Relay, it is difficult to troubleshoot its performance.

Frame-relay frame structure essentially mirrors almost exactly that defined for LAP-D. Traffic analysis can distinguish Frame Relay format from LAP-D by its lack of a control field.

Protocol data unit

Each Frame Relay Protocol data unit (PDU) consists of the following fields:

1. **Flag Field**. The flag is used to perform high-level data link synchronization which indicates the beginning and end of the frame with the unique pattern 01111110. To ensure that the 01111110 pattern does not appear somewhere inside the frame, bit stuffing and destuffing procedures are used.
2. **Address Field**. Each address field may occupy octet 2 to 3, octet 2 to 4, or octet 2 to 5, depending on the range of the address in use. A two-octet address field comprises the EA=ADDRESS FIELD EXTENSION BITS and the C/R=COMMAND/RESPONSE BIT.
    1. **DLCI**-Data Link Connection Identifier Bits. The DLCI serves to identify the virtual connection so that the receiving end knows which information connection a frame belongs to. Note that this DLCI has only local significance. A single physical channel can multiplex several different virtual connections.
    2. **FECN, BECN, DE** bits. These bits report congestion:
        - **FECN**=Forward Explicit Congestion Notification bit
        - **BECN**=Backward Explicit Congestion Notification bit
        - **DE**=Discard Eligibility bit
3. **Information Field**. A system parameter defines the maximum number of data bytes that a host can pack into a frame. Hosts may negotiate the actual

maximum frame length at call set-up time. The standard specifies the maximum information field size (supportable by any network) as at least 262 octets. Since end-to-end protocols typically operate on the basis of larger information units, Frame Relay recommends that the network support the maximum value of at least 1600 octets in order to avoid the need for segmentation and reassembling by end-users.

4. **Frame Check Sequence (FCS) Field**. Since one cannot completely ignore the bit error-rate of the medium, each switching node needs to implement error detection to avoid wasting bandwidth due to the transmission of *err*ed frames. The error detection mechanism used in Frame Relay uses the cyclic redundancy check (CRC) as its basis.

6.Explain the Congestion control techniques.

Congestion control

The Frame Relay network uses a simplified protocol at each switching node. It achieves simplicity by omitting link-by-link flow-control. As a result, the offered load has largely determined the performance of Frame Relay networks. When offered load is high, due to the bursts in some services, temporary overload at some Frame Relay nodes causes a collapse in network throughput. Therefore, frame-relay networks require some effective mechanisms to control the congestion.

Congestion control in frame-relay networks includes the following elements:

1. Admission Control. This provides the principal mechanism used in Frame Relay to ensure the guarantee of resource requirement once accepted. It also serves generally to achieve high network performance. The network decides whether to accept a new connection request, based on the relation of the requested traffic descriptor and the network's residual capacity. The traffic descriptor consists of a set of parameters communicated to the switching nodes at call set-up time or at service-subscription time, and which characterizes the connection's statistical properties. The traffic descriptor consists of three elements:
2. Committed Information Rate (CIR). The average rate (in bit/s) at which the network guarantees to transfer information units over a measurement interval T. This T interval is defined as: T = Bc/CIR.
3. Committed Burst Size (BC). The maximum number of information units transmittable during the interval T.

4. Excess Burst Size (BE). The maximum number of uncommitted information units (in bits) that the network will attempt to carry during the interval.

Once the network has established a connection, the edge node of the Frame Relay network must monitor the connection's traffic flow to ensure that the actual usage of network resources does not exceed this specification. Frame Relay defines some restrictions on the user's information rate. It allows the network to enforce the end user's information rate and discard information when the subscribed access rate is exceeded.

Explicit congestion notification is proposed as the congestion avoidance policy. It tries to keep the network operating at its desired equilibrium point so that a certain Quality of Service (QoS) for the network can be met. To do so, special congestion control bits have been incorporated into the address field of the Frame Relay: FECN and BECN. The basic idea is to avoid data accumulation inside the network.

FECN means Forward Explicit Congestion Notification. The FECN bit can be set to 1 to indicate that congestion was experienced in the direction of the frame transmission, so it informs the **destination** that congestion has occurred. BECN means Backwards Explicit Congestion Notification. The BECN bit can be set to 1 to indicate that congestion was experienced in the network in the direction opposite of the frame transmission, so it informs the *sender* that congestion has occurred.

7.Explain the Concepts of Quality of service

In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term **quality of service**

(*QoS*) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in

networks where the capacity is a limited resource, for example in cellular data communication.

A network or protocol that supports QoS may agree on a traffic contract with the application software and reserve capacity in the network nodes, for example during a session establishment phase. During the session it may monitor the achieved level of performance, for example the data rate and delay, and dynamically control scheduling priorities in the network nodes. It may release the reserved capacity during a tear down phase.

A best-effort network or service does not support quality of service. An alternative to complex QoS control mechanisms is to provide high quality communication over a best-effort network by over-provisioning the capacity so that it is sufficient for the expected peak traffic load. The resulting absence of network congestion eliminates the need for QoS mechanisms.

In the field of telephony, quality of service was defined in the ITU standard X.902 as "A set of quality requirements on the collective behavior of one or more objects". Quality of service comprises requirements on all the aspects of a connection, such as service response time, loss, signal-to-noise ratio, cross-talk, echo, interrupts, frequency response, loudness levels, and so on. A subset of telephony QoS is grade of service (GoS) requirements, which comprises aspects of a connection relating to capacity and coverage of a network, for example guaranteed maximum blocking probability and outage probability.

QoS is sometimes used as a quality measure, with many alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High QoS is often confused with a high level of performance or achieved service quality, for example high bit rate, low latency and low bit error probability.

- An alternative and disputable definition of QoS, used especially in application layer services such as telephony and streaming video, is requirements on a metric that reflects or predicts the subjectively experienced quality. In this context, QoS is the acceptable cumulative effect on subscriber satisfaction of all imperfections affecting the service. Other terms with similar meaning are the quality of experience (QoE) subjective business concept, the required "user perceived performance",[2] the required "degree of satisfaction of the user" or the targeted "number of happy customers". Examples of measures and measurement methods are Mean

Opinion Score (MOS), Perceptual Speech Quality Measure (PSQM) and Perceptual Evaluation of Video Quality (PEVQ). See also subjective video quality.

Conventional Internet routers and LAN switches operate on a best effort basis. This equipment is less expensive, less complex and faster and thus more popular than competing more complex technologies that provided QoS mechanisms. There were four "Type of service" bits and three "Precedence" bits provided in each IP packet header, but they were not generally respected. These bits were later re-defined as DiffServ Code Points (DSCP) and are sometimes honored in peered links on the modern Internet.

With the advent of IPTV and IP telephony, QoS mechanisms are increasingly available to the end user.

A number of attempts for layer 2 technologies that add QoS tags to the data have gained popularity during the years, but then lost attention. Examples are Frame relay and ATM. Recently, MPLS (a technique between layer 2 and 3) have gained some attention. However, today Ethernet may offer QoS through its 802.1p. Ethernet is, by far, the most popular layer 2 technology.

In Ethernet, Virtual LANs (VLAN) may be used to separate different QoS levels. For example in fibre-to-the-home switches typically offer several Ethernet ports connected to different VLAN:s. One VLAN may be used for Internet access (low priority), one for IPTV (higher priority) and one for IP telephony (highest priority). Different Internet providers may use the different VLANs.

Key qualities of traffic

When looking at packet-switched networks, quality of service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, Grade of Service, etc.

Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:

Low throughput

Due to varying load from other users sharing the same network resources, the bit rate (the maximum throughput) that can be provided to a certain data stream may be too low for real-time multimedia services if all data streams get the same scheduling priority.

Dropped packets
: The routers might fail to deliver (*drop*) some packets if their data is corrupted or they arrive when their buffers are already full. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

Errors
: Sometimes packets are corrupted due to bit errors caused by noise and interference, especially in wireless communications and long copper wires. The receiver has to detect this and, just as if the packet was dropped, may ask for this information to be retransmitted.

Latency
: It might take a long time for each packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. This is different from throughput, as the delay can build up over time, even if the throughput is almost normal. In some cases, excessive latency can render an application such as VoIP or online gaming unusable.

Jitter
: Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

Out-of-order delivery
: When a collection of related packets is routed through a network, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of sequence.

Applications

A defined quality of service may be desired or required for certain types of network traffic, for example:

- Streaming media specifically
  - Internet protocol television (IPTV)
  - Audio over Ethernet
  - Audio over IP
- IP telephony also known as Voice over IP (VoIP)
- Videoconferencing
- Telepresence
- Circuit Emulation Service
- Safety-critical applications such as remote surgery where availability issues can be hazardous
- Network operations support systems either for the network itself, or for customers' business critical needs
- Online games where real-time lag can be a factor
- Industrial control systems protocols such as Ethernet/IP which are used for real-time control of machinery

These types of service are called *inelastic*, meaning that they require a certain minimum level of bandwidth and a certain maximum latency to function. By contrast, *elastic* applications can take advantage of however much or little bandwidth is available. Bulk file transfer applications that rely on TCP are generally elastic.

Obtaining QoS

- In advance: When the expense of mechanisms to provide QoS is justified, network customers and providers typically enter into a contractual agreement termed a service level agreement (SLA) which specifies guarantees for the ability of a network/protocol to give guaranteed performance/throughput/latency bounds based on mutually agreed measures, usually by prioritizing traffic.
- Reserving resources: Resources are reserved at each step on the network for the call as it is set up. An example is RSVP, Resource Reservation Protocol.

Over-provisioning

An alternative to complex QoS control mechanisms is to provide high quality communication by generously over-provisioning a network so that capacity is based on peak traffic load estimates. This approach is simple and economical for networks with predictable and light traffic loads. The performance is reasonable for many applications. This might include demanding applications that can

compensate for variations in bandwidth and delay with large receive buffers, which is often possible for example in video streaming. Over-provisioning can be of limited use, however, in the face of transport protocols (such as TCP) that over time exponentially increase the amount of data placed on the network until all available bandwidth is consumed and packets are dropped. Such greedy protocols tend to increase latency and packet loss for all users.

Commercial VoIP services are often competitive with traditional telephone service in terms of call quality even though QoS mechanisms are usually not in use on the user's connection to his ISP and the VoIP provider's connection to a different ISP. Under high load conditions, however, VoIP may degrade to cell-phone quality or worse. The mathematics of packet traffic indicate that network requires just 60% more raw capacity under conservative assumptions.[4]

The amount of over-provisioning in interior links required to replace QoS depends on the number of users and their traffic demands. This is an important factor that limits usability of over-provisioning. Newer more bandwidth intensive applications and the addition of more users results in the loss of over-provisioned networks. This then requires a physical update of the relevant network links which is an expensive process. Thus over-provisioning cannot be blindly assumed on the Internet.

QoS mechanisms

Early work used the “IntServ” philosophy of reserving network resources. In this model, applications used the Resource reservation protocol (RSVP) to request and reserve resources through a network. While IntServ mechanisms do work, it was realized that in a broadband network typical of a larger service provider, Core routers would be required to accept, maintain, and tear down thousands or possibly tens of thousands of reservations. It was believed that this approach would not scale with the growth of the Internet, and in any event was antithetical to the notion of designing networks so that Core routers do little more than simply switch packets at the highest possible rates.

The second and currently accepted approach is “DiffServ” or differentiated services. In the DiffServ model, packets are marked according to the type of service they need. In response to these markings, routers and switches use various queuing strategies to tailor performance to requirements. — At the IP layer, differentiated services code point (DSCP) markings use the 6 bits in the IP packet

header. At the MAC layer, VLAN IEEE 802.1Q and IEEE 802.1p can be used to carry essentially the same information.

Routers supporting DiffServ use multiple queues for packets awaiting transmission from bandwidth constrained (e.g., wide area) interfaces. Router vendors provide different capabilities for configuring this behavior, to include the number of queues supported, the relative priorities of queues, and bandwidth reserved for each queue.

In practice, when a packet must be forwarded from an interface with queuing, packets requiring low jitter (e.g., VoIP or VTC) are given priority over packets in other queues. Typically, some bandwidth is allocated by default to network control packets (e.g., ICMP and routing protocols), while best effort traffic might simply be given whatever bandwidth is left over.

Additional bandwidth management mechanisms may be used to further engineer performance, to include:

- Traffic shaping (rate limiting):
  - Token bucket
  - Leaky bucket
  - TCP rate control—artificially adjusting TCP window size as well as controlling the rate of ACKs being returned to the sender[*citation needed*]
- Scheduling algorithms:
  - Weighted fair queuing (WFQ)
  - Class based weighted fair queuing
  - Weighted round robin (WRR)
  - Deficit weighted round robin (DWRR)
  - Hierarchical Fair Service Curve (HFSC)
- Congestion avoidance:
  - RED, WRED — Lessens the possibility of port queue buffer tail-drops and this lowers the likelihood of TCP global synchronization
  - Policing (marking/dropping the packet in excess of the committed traffic rate and burst size)
  - Explicit congestion notification
  - Buffer tuning

As mentioned, while DiffServ is used in many sophisticated enterprise networks, it has not been widely deployed in the Internet. Internet peering arrangements are already complex, and there appears to be no enthusiasm among providers for

supporting QoS across peering connections, or agreement about what policies should be supported in order to do so.

One compelling example of the need for QoS on the Internet relates to this issue of congestion collapse. The Internet relies on congestion avoidance protocols, as built into TCP, to reduce traffic load under conditions that would otherwise lead to Internet Meltdown. QoS applications such as VoIP and IPTV, because they require largely constant bitrates and low latency cannot use TCP, and cannot otherwise reduce their traffic rate to help prevent meltdown either. QoS contracts limit traffic that can be offered to the Internet and thereby enforce traffic shaping that can prevent it from becoming overloaded, hence they're an indispensable part of the Internet's ability to handle a mix of real-time and non-real-time traffic without meltdown

Protocols that provide quality of service

- The Type of Service (ToS) field in the IP(v4) header (now superseded by DiffServ)
- IP Differentiated services (DiffServ)
- IP Integrated services (IntServ)
- Resource reSerVation Protocol (RSVP)
- Multiprotocol Label Switching (MPLS) provides eight QoS classes
- RSVP-TE
- Frame relay
- X.25
- Some ADSL modems
- Asynchronous Transfer Mode (ATM)
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.11e
- HomePNA Home networking over coax and phone wires
- The ITU-T G.hn standard provides QoS by means of “Contention-Free Transmission Opportunities” (CFTXOPs) which are allocated to flows which require QoS and which have negotiated a “contract” with the network controller. G.hn also supports non-QoS operation by means of “Contention-based Time Slots”.
- Audio Video Bridging

QoS solutions

The research project "Multi Service Access Everywhere" (MUSE)[5] defined a QoS concept in Phase I which was further worked out in another research project PLANETS. The new idea of this solution is to agree on a discrete jitter value per QoS class which is imposed on network nodes. Including best effort, four QoS classes were defined, two elastic and two inelastic. The solution has several benefits:

- End-to-end delay and packet loss rate can be predicted
- It is easy to implement with simple scheduler and queue length given in PLANETS
- Nodes can be easily verified for compliance
- End users do notice the difference in quality

The MUSE project finally elaborated its own QoS solution which is primarily based in:

- The usage of traffic classes
- Selective CAC concept
- Appropriate network dimensioning] Quality of service procedures

Unlike the Internet2 Abilene Network, the Internet is actually a series of exchange points interconnecting private networks and not a network in its own right.[6] Hence the Internet's core is owned and managed by a number of different network service providers, not a single entity. Its behavior is much more stochastic or unpredictable. Therefore, research continues on QoS procedures that are deployable in large, diverse networks.

There are two principal approaches to QoS in modern packet-switched IP networks, a parameterized system based on an exchange of application requirements with the network, and a prioritized system where each packet identifies a desired service level to the network.

- Integrated services ("IntServ") implements the parameterized approach. In this model, applications use the Resource Reservation Protocol (RSVP) to request and reserve resources through a network.
- Differentiated services ("DiffServ") implements the prioritized model. DiffServ marks packets according to the type of service they desire. In response to these markings, routers and switches use various queueing strategies to tailor performance to expectations. DiffServ Code Point

(DSCP) markings use the first 6 bits in the ToS field of the IP(v4) packet header.

At the MAC layer, VLAN IEEE 802.1Q and IEEE 802.1p can be used to carry essentially the same information as used by DiffServ.

Cisco IOS NetFlow and the Cisco Class Based QoS (CBQoS) Management Information Base (MIB) can both be leveraged within a Cisco network device to obtain visibility into QoS policies and their effectiveness on network traffic. [7]

Non-IP protocols, especially those intended for voice transmission, such as ATM or GSM, have already implemented QoS in the core protocol and don't need additional procedures to achieve it.

End-to-end quality of service

End-to-end quality of service usually requires a method of coordinating resource allocation between one autonomous system and another. Research consortia such as EuQoS[8] and fora such as IPsphere[9] have developed mechanisms for handshaking QoS invocation from one domain to the next. IPsphere defined the Service Structuring Stratum (SSS) signaling bus in order to establish, invoke and (attempt to) assure network services. EuQoS conducted experiments to integrate Session Initiation Protocol, Next Steps in Signaling and IPsphere's SSS.

The Internet Engineering Task Force (IETF) defined the Resource Reservation Protocol (RSVP) for bandwidth reservation. RSVP is an end-to-end bandwidth reservation protocol that is also useful to end-to-end QoS. The traffic engineering version, RSVP-TE, is used in many networks today to establish traffic-engineered MPLS label-switched paths.

The IETF also defined NSIS[10] with QoS signalling as a target. NSIS is a development and simplification of RSVP.

Quality of service circumvention

Strong cryptography network protocols such as Secure Sockets Layer, I2P, and virtual private networks obscure the data transferred using them. As all electronic commerce on the Internet requires the use of such strong cryptography protocols, unilaterally downgrading the performance of encrypted traffic creates an

unacceptable hazard for customers. Yet, encrypted traffic is otherwise unable to undergo deep packet inspection for QoS.

Doubts about quality of service over IP

Gary Bachula, Vice President for External Affairs for Internet2, asserts that specific QoS protocols are unnecessary in the core network as long as the core network links are "over-provisioned" to the point that network traffic never encounters delay. In "quality of service" engineering, this formulation is guaranteed by the *admission control* feature. It is important to note that this only refers to core networks and not end-to-end connections. Recent studies point to a relatively low end-to-end bandwidth availability even on Internet2.

The Internet2 QoS Working Group concluded that increasing bandwidth is probably more practical than implementing QoS.[11][12]

The Internet2 project found, in 2001, that the QoS protocols were probably not deployable inside its Abilene network with equipment available at that time. While newer routers are capable of following QoS protocols with no loss of performance, equipment available at the time relied on software to implement QoS. The Internet2 Abilene network group also predicted that "logistical, financial, and organizational barriers will block the way toward any bandwidth guarantees" by protocol modifications aimed at QoS.[11][12] In essence, they believe that the economics would be likely to make the network providers deliberately erode the quality of best effort traffic as a way to push customers to higher priced QoS services.

The Abilene network study was the basis for the testimony of Gary Bachula to the Senate Commerce Committee's Hearing on Network Neutrality in early 2006. He expressed the opinion that adding more bandwidth was more effective than any of the various schemes for accomplishing QoS they examined.

Bachula's testimony has been cited by proponents of a law banning quality of service as proof that no legitimate purpose is served by such an offering. This argument is dependent on the assumption that over-provisioning isn't a form of QoS and that it is always possible. Cost and other factors affect the ability of carriers to build and maintain permanently over-provisioned networks.

- of developing or enhancing standards related to QoS and provide concepts and terminology that will assist in maintaining the consistency of related standards.

- The main QoS-related IETF RFCs are Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC 2474), and Resource ReSerVation Protocol (RSVP) (RFC 2205); both these are discussed above. The IETF has also published two RFCs giving background on QoS: RFC 2990: Next Steps for the IP QoS Architecture, and RFC 3714: IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet.

8.Explain the Backward Explicit Congestion Notification techniques.

Backward Explicit Congestion Notification

Set BECN bit in reverse traffic or send Consolidated Link-Layer Management (CLLM) message to source
On first BECN bit: Set R = CIR
On further "S" BECNs: R=0.675 CIR, 0.5 CIR, 0.25 CIR
On S/2 BECNs clear: Slowly increase R = 1.125 R
If idle for long, R = CIR

For window based control:
S = One frame interval
Start with W=1
First BECN W = max(0.625W,1)
Next S BECNs W = max(0.625W,1)
S/2 clear BECNs $\Rightarrow$ W = max(W+1, Wmax)
CLLM used if no reverse traffic
CLLM = XID message on maintenance
DLCI = 1007 (decimal)
CLLM contains a list of congested DLCIs

Implicit Congestion Control

Decrease window on frame loss
Increase window slowly
Decrease by 1, Decrease to Wmin, Decrease by a factor α
Increase by 1 after N frames

8.Explain the Operation of Leaky Bucket

Operation of Leaky Bucket

The choice of **R**, token generation rate is crucial and so is the size of the token buffer **BL**

The higher **R** the smaller **BL**. For network, smaller **BL** is better, less bursty source. However, for a fixed **R**, a larger **BL** means a smaller **BI**, i.e., lower delays.

The user specifies: **Peak Cell Rate** (PCR) (minimum spacing between cells when coming from the source), **Sustainable Cell Rate** (SCR) and **Maximum Burst Size** (MBS).

The token generation rate **R = SCR**. (Note SCR is not necessarily the source's average rate)

The burst tolerance is defined by:

BT = BL = (MBS - 1) (1/SCR + 1/PCR)

UNIT IV INTEGRATED AND DIFFERENTIATED SERVICES

Integrated services architecture – Approach, components, services – Queuing discipline,FQ – PS – BRFQ – GPS – WFQ – Random early detection, differentiated services.

PART-A(2 marks)

1. What are the two types of traffic on internet?
Traffic on network or internet is classified into two broad categories:
1. Elastic
2. Inelastic

2. Define Elastic traffic.
Elastic traffic is that which can adjust to changes in delay and throughout across an internet and still meet the needs of its applications.

3. Mention some of the applications that are classified as elastic.
The applications that operate over
i. File transfer (FTP)
ii. Electronic mail (SMTP)
iii. Remote logon (TELNET)
iv. Network management (SNMP)
v. Web access (HTTP)

4. Define Inelastic Traffic.
Inelastic traffic does not easily adapt to changes in delay and throughput across the internet.

5. What are the requirements for inelastic traffic?
i. Throughput
ii. Delay
iii. Jitter
iv. Packet loss

6. What are the problems in inelastic traffic?
i. Difficult to meet requirements on network with variable queuing delays and congestion
ii. Need preferential treatment
iii. Applications need to state requirements
1. Ahead of time (preferably) or on the fly

2. Using fields in IP header
3. Resource reservation protocol
iv. Must still support elastic traffic
1. Deny service requests that leave too few resources to handle
elastic traffic demands

7. What is the need of ISA?
The purpose of ISA is to enable the provision of QoS support over IP-based internets. The central design issue of ISA is how to share the available capacity in times of congestion

8. What are the tools used by a router for controlling congestion in IP networks?
i. Routes can be selected to minimize the delay.
ii. When a buffer overflows, it discards the packets

9. What are the functions used by ISA for controlling congestion and provide QoS transport?
i. Admission control
ii. Routing algorithm
iii. Queuing discipline
iv. Discard policy

10. What are the components of ISA?
i. Reservation protocol
ii. Admission protocol
iii. Management agent
iv. Routing protocol

11. What is a packet scheduler?
Packet scheduler function manages one or more queues for each output port. It determines the order in which queued packets are transmitted and the selection of packets for discard. Decisions are made based on a packet's class, the contents of the traffic control database and the current and past activity on this outgoing port.

12. What are the services provides by ISA?
i. Guaranteed
ii. Controlled load
iii. Best effort

13. What is token bucket traffic specification?
Token bucket traffic specification is a way of characterizing traffic.

14. What are the advantages of Token-Bucket scheme?
i. Many traffic sources can be defined by token bucket scheme
ii. Provides concise description of load imposed by flow
iii. Easy to determine resource requirements
iv. Provides input parameters to policing function

15. What are the key elements of guaranteed service?
i. Assured capacity level or data rate
ii. Specific upper bound on queuing delay through network which is added to propagation delay or latency to get total delay
iii. No queuing losses i.e. no buffer overflow

17. What are the key elements of controlled load?
i. Tightly approximates to best efforts under unloaded conditions
ii. No upper bound on queuing delay.
1. High percentage of packets do not experience delay over minimum transit delay
iii. Very high percentage of transmitted packets will be delivered
iv. Almost no queuing loss

18. What is meant by Fair-queuing?
i. In fair queuing each incoming packet is placed in the appropriate queues.
ii. Queues are serviced in round robin fashion, taking one packet from each queue.
iii. Each busy queue (flow) gets exactly one packet per cycle
iv. Short packets are penalized as each queue sends one packet per cycle

19. Write about BRFQ.
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. This bit-by-bit approach is called processor sharing **(PS).**

20. What is Generalized Processor sharing technique?
In GPS each flow is assigned a weight that determines how many bits are transmitted from that queue during each round. If a weight for a given flow is 5, then during each round that the queue is non-empty, 5 bits will be transmitted

.

22. Mention the RED design goals.
i. Congestion avoidance

ii. Global synchronization avoidance
iii. Avoidance of bias against bursty traffic.
iv. Bound on average queue length.

24. What are differentiated services?
The differentiated services architecture is designed to provide a simple, easy-to implement, low overhead toll to support a range of network services that are differentiated on the basis of performance.

PART-B

1.Explain the Integrated and differentiated services approach in detail.

- Modern Internet applications demand services not provided by a best-effort service model
- Two complementary, yet fundamentally different, traffic management frameworks have evolved:
  - Integrated Services (IS, ISA, IntServ): reserve resources per session and limit total demand to the capacity that can be handled by the network
  - Differentiated Services (DS, DiffServ): classify traffic into a number of traffic groups and handle traffic based on its group
- Traffic control mechanisms: queuing discipline, packet discard policy
- Services are specified within a given domain

Internet Traffic

- *Elastic* Traffic
  - traffic that can adapt, over a wide range, to delay and throughput changes
  - typically TCP/UDP
  - QoS perceived based on application
- *Inelastic* Traffic
  - traffic does not adapt well
  - requires guarantees on: throughput, delay, jitter, packet loss
  - e.g. traffic generated by real-time applications

IntServ Approach

- Two key features form core of architecture
  - Resource reservation – routers must maintain state of available resource reserved for each “session”
  - Call/session setup – each router on the session’s path must verify availability of required resources for a session and admit sessions only if requirements can be met
- Call Admission process (more later)
  - Traffic characterization (Tspec)
  - Desired QoS caharterizatio (Rspec)
  - Reservation signaling (RSVP, RFC 2210)
  - Per-element call admission per Tspec and Rspec

IntServ Implementation

- Associate each packet with a “flow”
  - a distinguishable stream of related IP packets that result from a single user activity and demand the same QoS *(per RFC 1633)*
  - unidirectional, can have multiple recipients
  - typically identified by: source & destination IP addresses, port numbers and protocol type
- Provide for enhanced router functions to manage flows:
  - Admission control based on requested QoS and availability of required network resources
  - Routing protocol based on QoS (like OSPF/MOSPF)
  - Queuing/scheduling disciplines based on QoS
  - Packet discard policy based on QoS

ISA: 3 Categories of Service

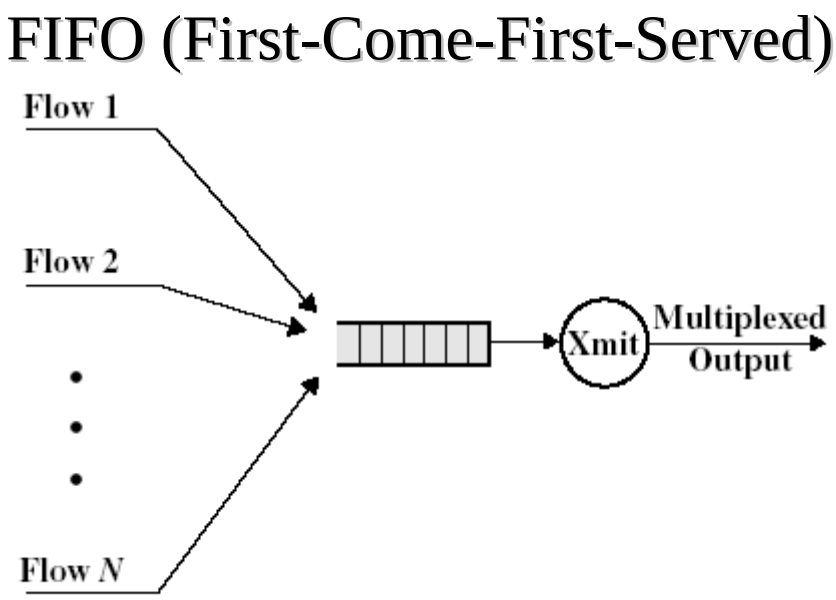
- Guaranteed Service
  - assured capacity (data rate)
  - specified upper bound on queuing delay through the network
  - no queuing loss (i.e., no buffer overflow)
- Controlled Load
  - roughly equivalent to best-effort under no-load conditions (dprop + dtrans)
  - no specified upper bound on queuing delay, but will approximate minimum expected transit delay
  - almost no queuing loss
- Best Effort

2.Describe the types of Queuing Disciplines.

Queuing Disciplines

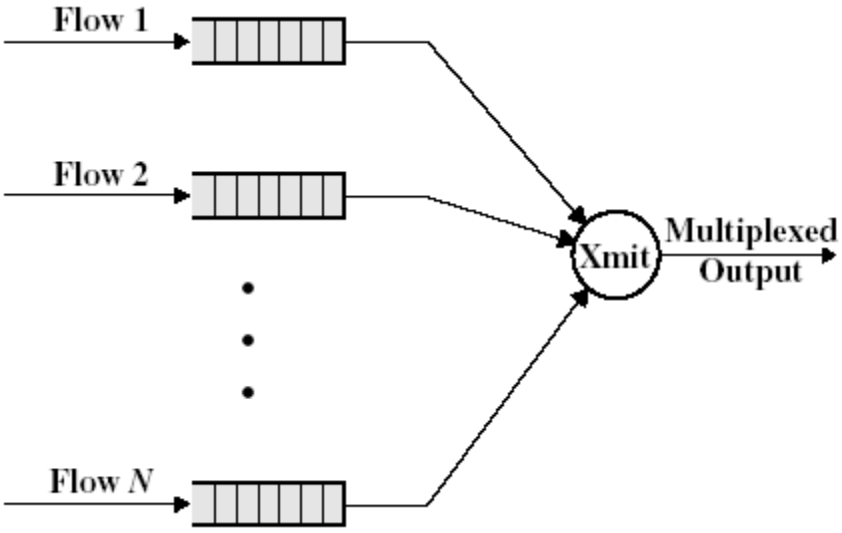
- Single FIFO queues have numerous drawbacks relative to QoS demands
  - no special treatment based on priority
  - larger packets get better service
  - connections can get an unfair share of resources
- IntServ allows for multiple queues
  - one per flow
  - separate discipline per flow
  - fair queuing policy

Queuing Disciplines (Scheduling)



- Flows with busy (greedy) sources crowd out others
- Flows with shorter packets are penalized

Round Robin (Fair Queuing)



Flows with shorter packets are penalized

Processor Sharing Approach

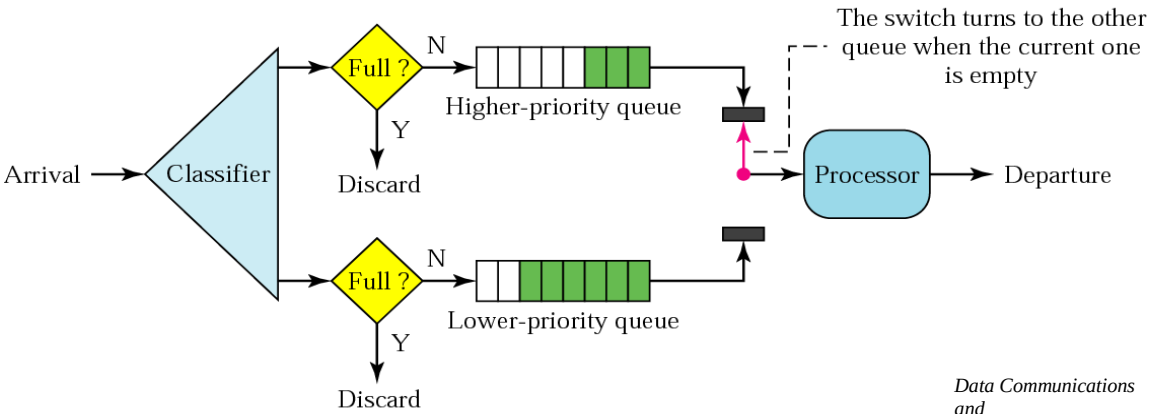
- Processor Sharing (PS)
  - ideal, but not a practical policy
  - transmit only one bit per round per queue
  - with N queues, each queue receives exactly 1/N of the available capacity
  - consider each queue independently to calculate "virtual" start and finish times for each transmission

EXAMPLE	QUEUE α		QUEUE β		QUEUE γ
	Packet 1	Packet 2	Packet 1	Packet 2	Packet 1
Real arrival time, τi	0	2	1	2	3
Transmission time, Pi	3	1	1	4	2
Virtual start time, Si	0	3	1	2	3
Virtual finish time, Fi	3	4	2	6	5

Bit-Round Fair Queuing

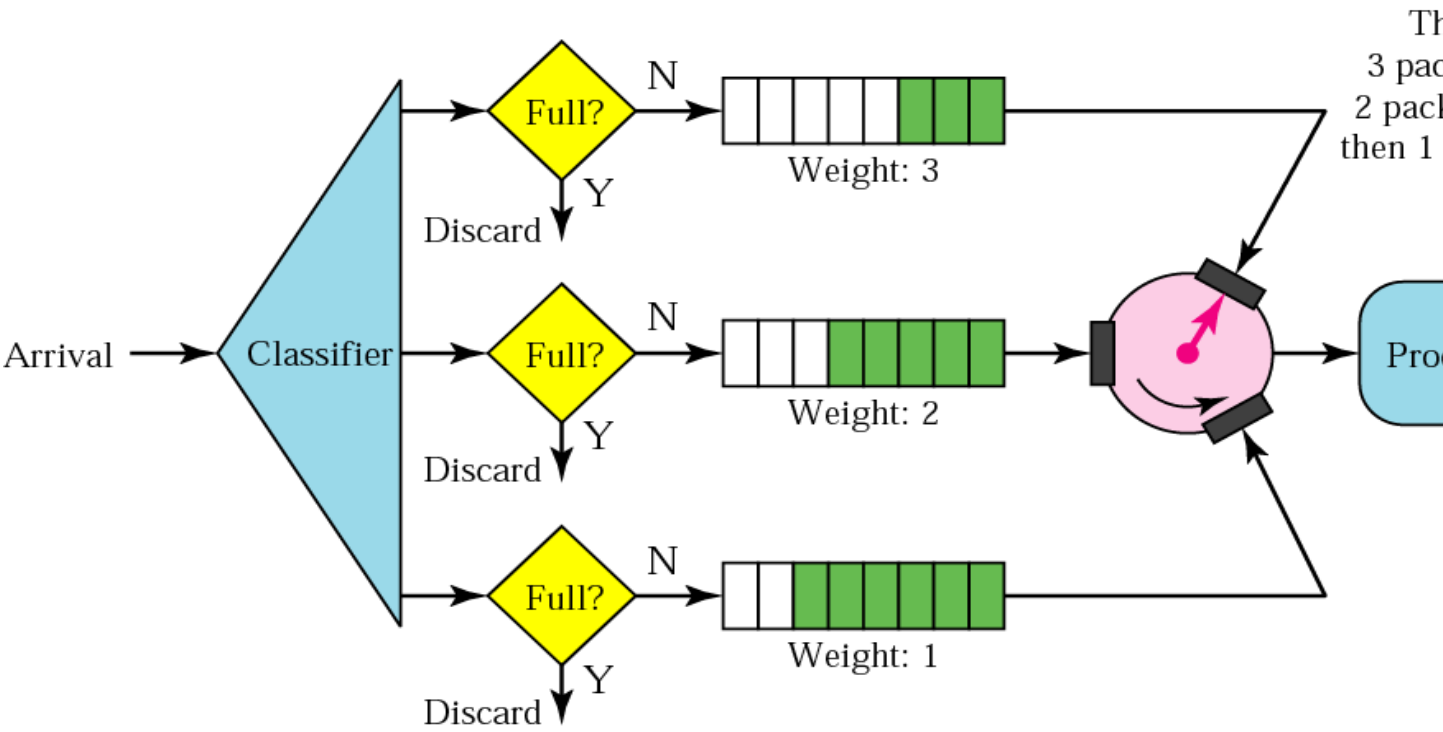
- Bit-Round Fair Queuing (BRFQ)
  - emulates PS round-robin approach for packets and multiple synchronous queues
  - uses packet length and flow identification (queue) to schedule packets
  - calculate *Si* and *Fi* as though PS were running
  - when a packet finishes transmission, send next packet based on smallest value of *Fi* over all queues
  - algorithm is fair on the basis of amount of data transmitted instead of number of packets

Queuing Discipline – Priority Queuing



Data Communications and

Queuing Discipline – Weighted Fair Queuing



Scheduling vs. Queue Management (see RFC 2309)

- Closely related, but different performance issues…
- Scheduling: managing allocation of bandwidth between flows by determining which packet to send next (*queuing discipline*)
- Queue Management: managing the length of packet queues by proactively dropping packets when necessary (*packet discard policy*)

3.Explain Random Early Detection in detail.

Random Early Detection (RED)

Random early detection (RED), also known as **random early discard** or **random early drop** is an active queue management algorithm. It is also a congestion avoidance algorithm.[1]

In the traditional tail drop algorithm, a router or other network component buffers as many packets as it can, and simply drops the ones it cannot buffer. If buffers are constantly full, the

network is congested. Tail drop distributes buffer space unfairly among traffic flows. Tail drop can also lead to TCP global synchronization as all TCP connections "hold back" simultaneously, and then step forward simultaneously. Networks become under-utilized and flooded by turns. RED addresses these issues.

RED monitors the average queue size and drops (or marks when used in conjunction with ECN) packets based on statistical probabilities. If the buffer is almost empty, all incoming packets are accepted. As the queue grows, the probability for dropping an incoming packet grows too. When the buffer is full, the probability has reached 1 and all incoming packets are dropped.

RED is more fair than tail drop, in the sense that it does not possess a bias against bursty traffic that uses only a small portion of the bandwidth. The more a host transmits, the more likely it is that its packets are dropped as the probability of a host's packet being dropped is proportional to the amount of data it has in a queue. Early detection helps avoid TCP global synchronization.

Problems with Classic RED

According to Van Jacobson, "there are not one, but two bugs in classic RED."[2] Improvements to the algorithm were developed, and a draft paper[3] was prepared, but the paper was never published, and the improvements were not widely disseminated or implemented.

Pure RED does not accommodate quality of service (QoS) differentiation. weighted RED (WRED) and RED with In and Out (RIO)[4] provide early detection with QoS considerations.

Other variants

In *Weighted RED* you can have different probabilities for different priorities (IP precedence, DSCP) and/or queues.[5]

The *Adaptive / Active RED* (ARED) algorithm[6] infers whether to make RED more or less aggressive based on the observation of the average queue length. If the average queue length oscillates around *min* threshold then early detection is too aggressive. On the other hand if the average queue length oscillates around *max* threshold then early detection is being too conservative. The algorithm changes the probability according to how aggressive it senses it has been discarding traffic.

See Srikant[7] for an in-depth account on these techniques and their analysis.

[RRED: Robust RED

Main article: Robust random early detection

The existing Random Early Detection (RED) algorithm and its variants are found vulnerable to emerging attacks, especially the Low-rate Denial-of-Service (LDoS) attacks. Experiments have confirmed that the existing RED-like algorithms are notably vulnerable under LDoS attacks due

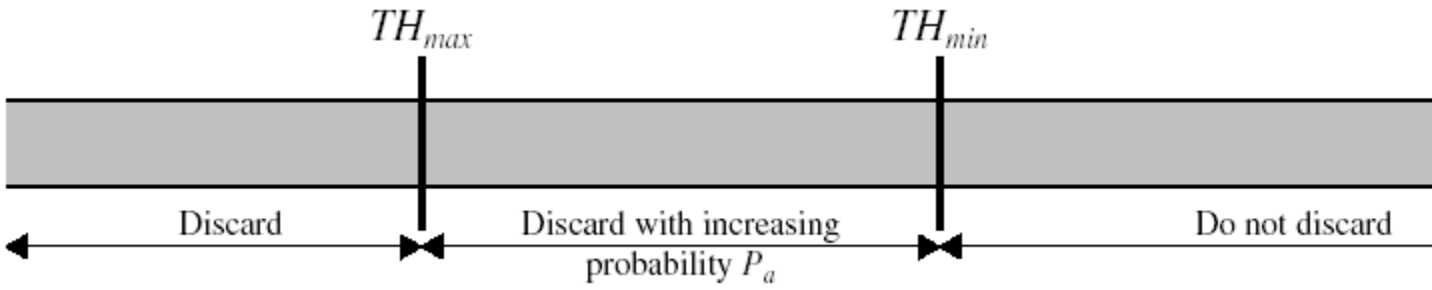
to the oscillating TCP queue size caused by the attacks. Recent Publications in low-rate Denial-of-Service (DoS) attacks

A Robust RED (RRED) algorithm was proposed to improve the TCP throughput against LDoS attacks. The basic idea behind the RRED is to detect and filter out attack packets before a normal RED algorithm is applied to incoming flows. RRED algorithm can significantly improve the performance of TCP under Low-rate Denial-of-Service attacks.

- Queuing discipline with proactive packet discard
  - anticipate congestion and take early avoidance action
  - improved performance for elastic traffic by not penalizing bursty traffic
  - avoids "global synchronization" phenomenon at congestion onset
  - control average queue length (buffer size) within deterministic bounds… therefore, control average queuing delay

4.Explain RED Buffer Management and Generalized RED Algorithm.

RED Buffer Management



Discard probability is calculated for each packet arrival
at the output queue based on:

- the current weighted average queue size, and
- the number of packets sent since the previous packet discard

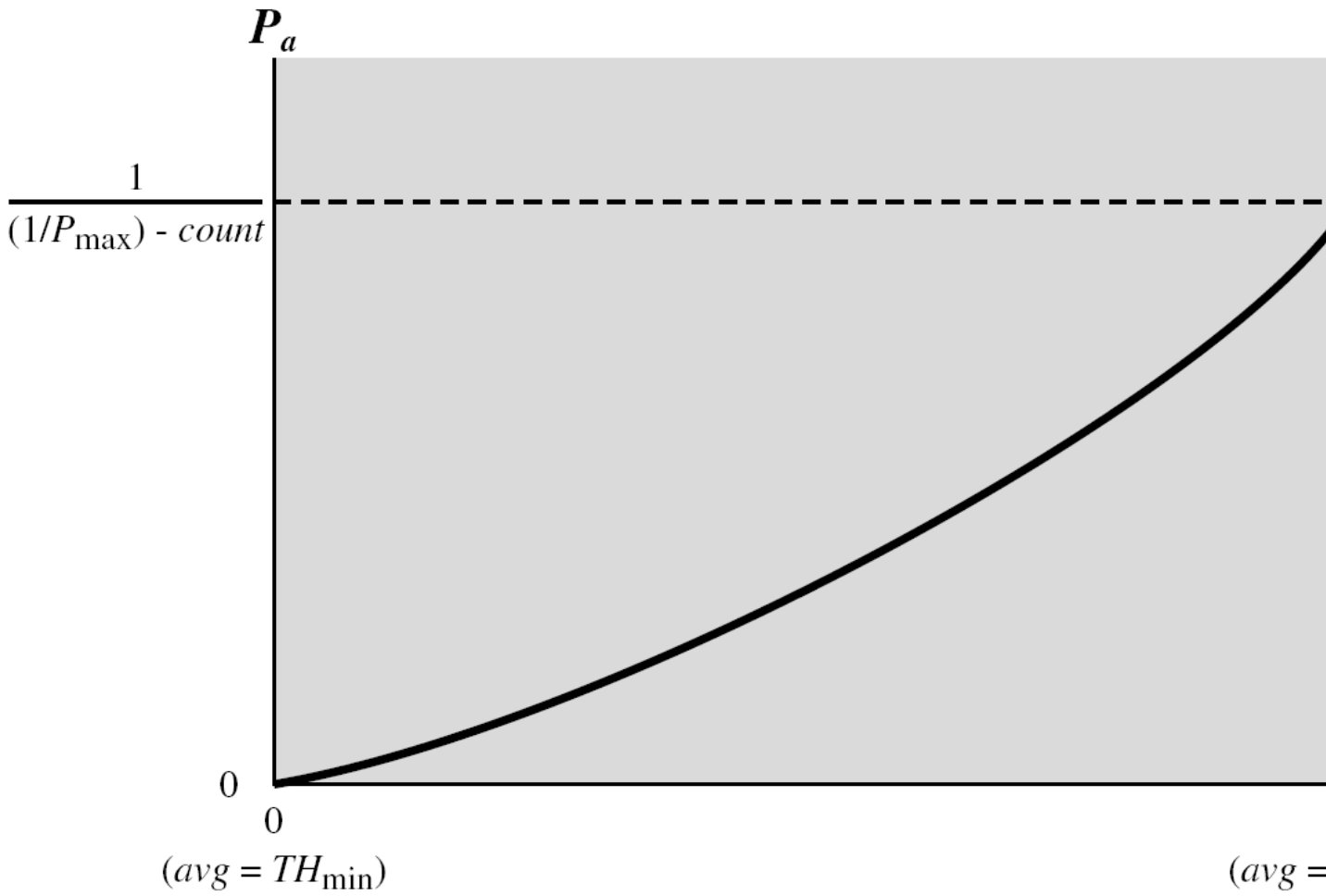
Generalized RED Algorithm

calculate the average queue size, *avg*

if *avg* < *THmin*
    queue the packet
else if *THmin* ≤ *avg* < *THmax*
    calculate probability *Pa*
    with probability *Pa*
        discard the packet
    else with probability 1 – *Pa*
        queue the packet
else if *avg* ≥ *THmax*
    discard the packet

RED Algorithm

- *avg* lags considerably behind changes in actual queue size (weight, *wq*, is small… typ. 0.002)
  - avg ← (1 – wq)avg + wqq
  - prevents reaction to short bursts
- *count*, number of packets passed without discard, increases incrementally while Thmin < avg < Thmax
  - probability of discard, Pa, increases as count increases
  - helps ensure fairness across multiple flows



5.Write short notes on Weighted fair queuing.

Weighted fair queuing

Weighted fair queuing (WFQ) is a data packet scheduling technique allowing different scheduling priorities to statistically multiplexed data flows.

WFQ is a generalization of fair queuing (FQ). Both in WFQ and FQ, each data flow has a separate FIFO queue. In FQ, with a link data rate of *R*, at any given time the *N* active data flows (the ones with non-empty queues) are serviced simultaneously, each at an average data rate of *R* / *N*. Since each data flow has its own queue, an ill-behaved flow (who has sent larger packets or more packets per

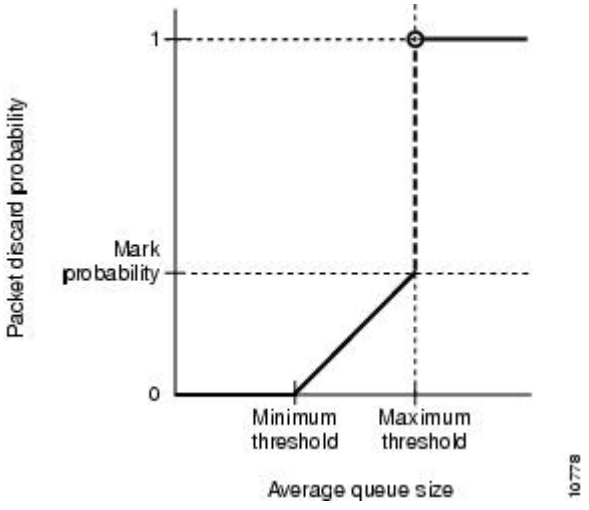
second than the others since it became active) will only punish itself and not other sessions.

Contrary to FQ, WFQ allows different sessions to have different service shares. If N data flows currently are active, with weights w_1,w_2...w_N, data flow number i will achieve an average data rate of

$$\frac{Rw_i}{(w_1 + w_2 + ... + w_N)}$$

It can be proven [1] that when using a network with WFQ switches and a data flow that is leaky bucket constrained, an end-to-end delay bound can be guaranteed. By regulating the WFQ weights dynamically, WFQ can be utilized for controlling the quality of service, for example to achieve guaranteed data rate.

Proportional fairness can be achieved by setting the weights to $w_i = 1 / c_i$, where c_i is the cost per data bit of data flow i. 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 can not use the same frequency channel, in view to avoid co-channel interference



UNIT V PROTOCOLS FOR QOS SUPPORT

RSVP – Goals and characteristics – data flow – RSVP operations – Protocol mechanisms – Multi protocol label switching – Operations – Label stacking – Protocol details – RTP – Protocol architecture – Data transfer protocol – RTCP.

PART-A (2 marks)

1. What is soft state?
A soft state is a set of state information at a router that expires unless regularly refreshed from the entity that requested the state. If a route for a given transmission changes, then some soft states will expire and new resource reservations will invoke the appropriate soft states on the new routers along the route.

2. What are the goals of RSVP?
RSVP- Resource Reservation Protocol
i. Enable receivers to make reservations
ii. Deal gracefully with changes in group membership
iii. Aggregate for group should reflect resources needed
iv. Receivers can select one of multiple sources (channel selection)
v. Deal gracefully with changes in routes
vi. Control protocol overhead
vii. Independent of routing protocol

3. **What are the characteristics of RSVP?**
i. Unicast and Multicast
ii. Simplex
iii. Receiver initiated-Receiver knows which subset of source transmissions it wants
iv. Maintain soft state in internet
v. Providing different reservation styles
vi. Transparent operation through non-RSVP routers
vii. Support IPv4 (ToS field) and IPv6 (Flow label field)

4. What is the basis of RSVP operation?
i. Session
ii. Flow specification
iii. Filter specification

5. What is a data-flow session?
i. A session is a data flow identified by destination
ii. Once the reservation is made at a router, the router considers this as a session and Resources are allocated by router for duration of session
iii. A session is defined by

1. Destination IP address
2. IP protocol identifier
3. Destination port

6. What is a flow descriptor?

i. Reservation Request issued by a destination end system is called flow descriptor.
ii. It consists of:
1. Flow spec
a. It specifies a desired QoS
b. Used to set parameters in node's packet scheduler
2. Filter spec
a. Defines the set of packets for this reservation

7. What are the different types of reservation styles in RSVP?

i. Wild-card filter style-- Single resource reservation shared by all senders to this address
ii. Fixed-filter style-- Distinct reservation for each sender
iii. Shared explicit (SE) style.-- Single reservation shared among specific list of senders

8. What are the message types used by RSVP?

i. Resv
1. Resv messages originate at multicast group receivers and Propagate upstream
2. It allow host to set up traffic control for first hop
ii. Path
1. Used to Provide upstream routing information.
2. Issued by sending hosts that wishes to participate in a multicast group.
3. Path message is transmitted through distribution tree to all Destinations

.

9. What is traffic engineering?

The ability to dynamically define routes, plan resource commitments based on known demands and optimize network utilization is referred to as traffic engineering.

10. Write about the universal nature of MPLS.

MPLS can be used on different network technologies like
i. IP
ii. ATM
iii. Frame relay
iv. Mixed network

11. Write about MPLS operation.

MPLS network of internet consists of a set of nodes called 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.

12. What is label stacking?

A labeled packet may carry a number of labels, organized as a last-in-first-out stack. Processing is based on the top label. At any LSR, a label may be added to the stack or removed from the stack. Label stacking allows the aggregation of LSP's into a single LSP for a portion of a route through the network creating a tunnel.

13. How route selection is made in MPLS?

Route selection refers to the selection of LSP for particular FEC.

Two options:

i. **Hop-by-hop**--LSR independently chooses next hop

ii. **Explicit**--LSR (usually ingress or egress) specifies some or all LSRs in LSP for given FEC

1. For strict explicit routing , an LSR specifies all of the LSR's on an LSP
2. For loose explicit routing, only some of the LSR's are specified.

14. What is constraint based routing algorithm?

A routing algorithm that takes into account the traffic requirements of flows and the resources available along hops and through various nodes is referred to as constraint based routing algorithm

15. How you can set the LSP?

i. Assign label to LSP

ii. Inform all potential upstream nodes of label assigned by LSR to FEC

iii. Learn next hop for LSP and the label that downstream node has assigned to FEC which allows LSR to map incoming label to outgoing label

16. What is RTP data transfer protocol?

RTP supports the transport of real time data among number of participants in a session. A session is a logical association among two or more RTP entities that is maintained for the duration of the data transfer. A session is defined by:

a. RTP Port number

i. UDP destination port number if using UDP

b. RTP Control Protocol (RTCP) port number

i. Destination port address used by all participants for RTCP transfer

c. IP addresses

i. Multicast or set of unicast.

17. What are the two types of relays in RTP?

i. Translators

ii. Mixers

18. Define a mixer.
A mixer is an RTP relay that receives streams of RTP packets from one or more sources, combines streams and forwards a new RTP packet stream to one or more destinations.

19. Define Translator.
A translator is a simpler device that produces one or more outgoing RTP packets for each incoming RTP packet. The translator may change the format of the data in the packet or use a different lower-level protocol suite to transfer from one domain to another.
E.g. convert video to lower quality

20. Mention the functions of RTCP.
i. QoS and congestion control
ii. Identification
iii. Session size estimation and scaling
iv. Session control

PART-B

1.Explain the RSVP protocols briefly.

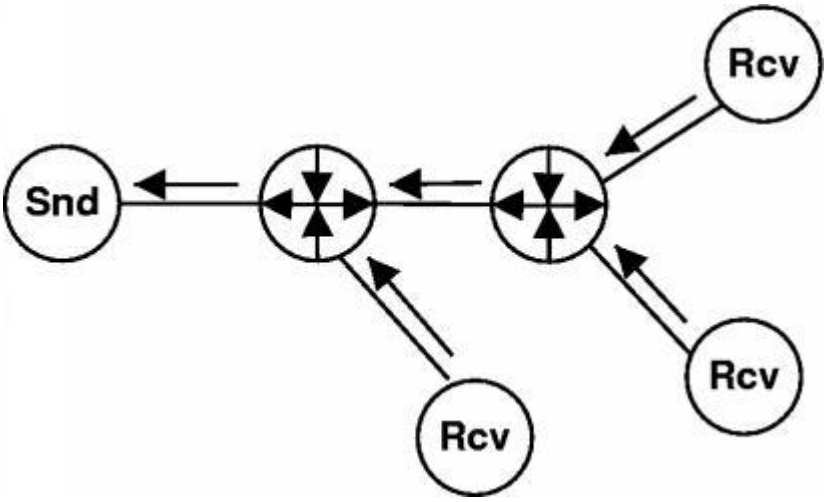
RSVP

RSVP is the network control protocol that allows data receiver to request a special end-to-end quality of service for its data flows. Real-time applications use RSVP to reserve necessary resources at routers along the transmission paths so that the requested bandwidth can be available when the transmission actually takes place. RSVP is a main component of the future Integrated Services Internet which can provide both best-effort and real-time service.

RSVP is used to set up reservations for network resources. When an application in a host (the data stream receiver) requests a specific quality of service (QoS) for its data stream, it uses RSVP to deliver its request to routers along the data stream paths. RSVP is responsible for the negotiation of connection parameters with these routers. If the reservation is setup, RSVP is also responsible for maintaining router and host states to provide the requested service.

The reservation requests are initiated by the receivers. They do not need to travel all the way to the source of the sender. Instead, it travels upstream until it meets another reservation request for the same source stream, then merges with that reservation. The figure below shows how the reservation requests merge as they progress up the multicast tree.

Figure A-10. RSVP merge



This reservation merging leads to the primary advantage of RSVP: scalability---a large number of users can be added to a multicast group without increasing the data traffic significantly. So RSVP can scale to large multicast groups and the average protocol overhead decreases as the number of participants increases.

The reservation process does not actually transmit the data and provide the requested quality of service. But through reservation, RSVP guarantees the network resources are available when the transmission actually takes place.

RTSP

RTSP, the Real-Time Streaming Protocol, is a client-server multimedia presentation protocol to enable controlled delivery of streamed multimedia data over IP network. It provides "VCR-style" remote control functionality for audio and video streams, like pause, fast forward, reverse, and absolute positioning. Sources of data include both live data feeds and stored clips.

RTSP is an application-level protocol designed to work with lower-level protocols like RTP, RSVP to provide a complete streaming service over Internet. It provides means for choosing delivery channels (such as UDP, multicast UDP and TCP), and delivery mechanisms based upon RTP. It works for large audience multicast as well as single-viewer unicast.

RTSP aims to provide the same services on streamed audio and video just as HTTP does for text and graphics. It is designed intentionally to have similar syntax and operations so that most extension mechanisms to HTTP can be added to RTSP.

In RTSP, each presentation and media stream is identified by an RTSP URL. The overall presentation and the properties of the media are defined in a presentation description file, which may include the encoding, language, RTSP URLs, destination address, port, and other parameters. The presentation description file can be obtained by the client using HTTP, email or other means.

But RTSP differs from HTTP in several aspects. First, while HTTP is a stateless protocol, an RTSP server has to maintain "session states" in order to correlate RTSP requests with a stream. Second, HTTP is basically an asymmetric protocol where the client issues requests and the server responds, but in RTSP both the media server and the client can issue requests. For example the server can issue an request to set playing back parameters of a stream.

2. Explain the RTP Protocol Architecture in detail.

RTP Protocol Architecture

Protocol layering

RTP is an application-level,datagram protocol

Traditional transport services
such as:
» addressing,
» segmentation/reassembly,
» quality-of-service, and
» delivery semantics
are all provided by a lower level protocol

Sessions

An RTP *session* is the sending and receiving of RTP
data by a group of participants

For each participant a session is a (pair of) transport addresses
used by a participant to communicate with the group

If multiple media types are communicated by the group,the transmission of each medium constitutes a session

3.Describe the operation of MPLS.

Multiprotocol Label Switching (MPLS) is a Layer-2 *switching* technology. MPLS-enabled routers apply numerical **labels** to packets, and can make forwarding decisions based on these labels. The MPLS architecture is detailed in RFC 3031.

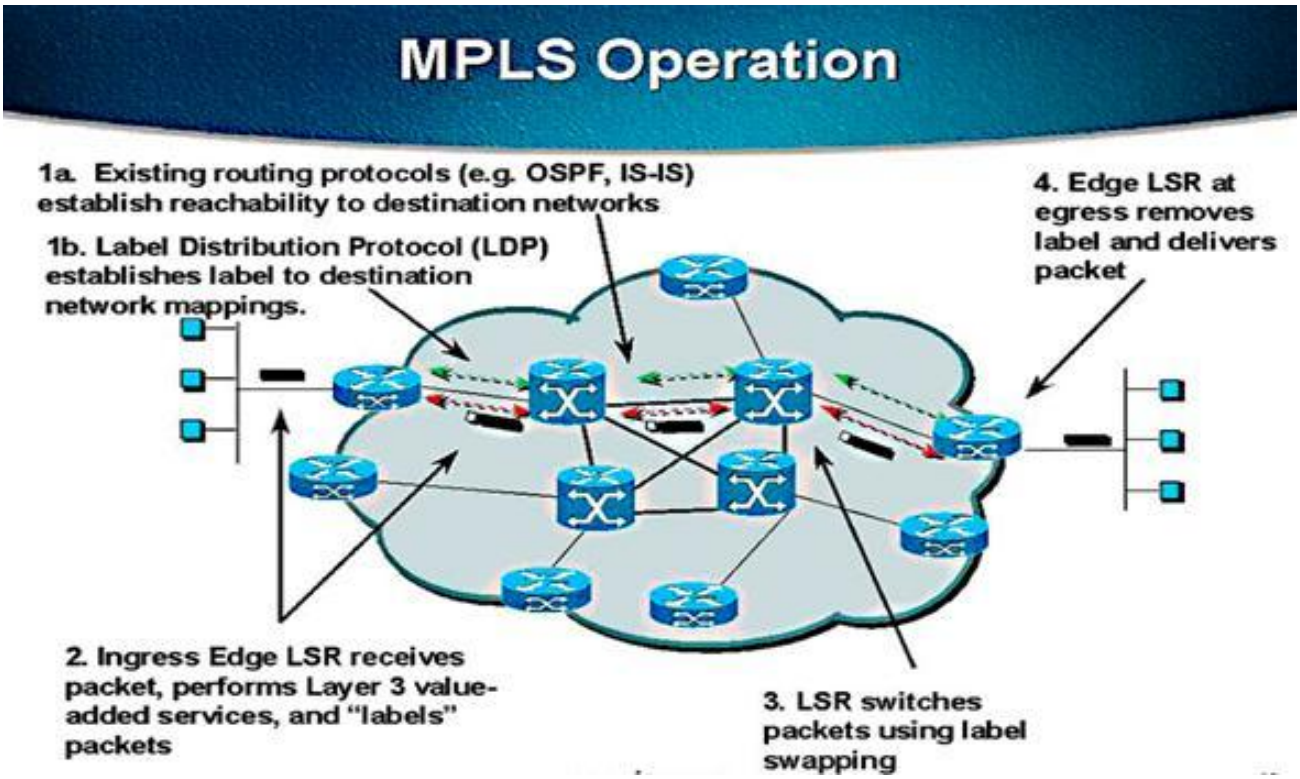
MPLS reduces CPU-usage on routers, by allowing routers to make forwarding decisions *solely* on the attached label, as opposed to parsing the full routing table.

Labels can based on a variety of parameters:
- Destination IP network
- Source IP address
- QoS parameters
- VPN destination
- Outgoing interface
- Layer-2 circuit

MPLS is not restricted to IP, or any specific Layer-2 technology, and thus is essentially **protocol-independent**.

Labels are applied to and removed from packets on **edge Label Switch Routers (edge LSRs)**. Only edge routers perform a route-table lookup on packets. All **core routers (**identified simply as **LSRs**) in the MPLS network forward solely based on the label.
As a packet traverses the core MPLS network, core routers will swap the label on hop-by-hop basis.

MPLS is completely dependent on **Cisco Express Forwarding (CEF)** to determine the next hop.



4.Describe the Real-Time Control Protocol in detail.

RTCP - Real-Time Control Protocol

Introduction

We have already mentioned that RTCP extends the RTP with a control functionality. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

Five different packets have been defined for carrying control information.

SR

Sender report, for transmission and reception statistics from session participants that are active senders.

RR

Receiver report, for reception statistics from session participants, that are not active senders.

SDES

Source description items, including CNAME

BYE

Indicates end of participation

APP

Application specific functions

Through these control information packets, RTCP provides the following functions:

The primary function of RTCP is to provide Quality of Service monitoring and congestion control. The control information is useful to the senders, the receivers and third-party monitors. The sender can adjust its transmission based on the receiver report feedback. This is similar to the flow and congestion control in other transport protocols. The receivers can determine whether a congestion is local, regional or global. This feedback function is performed by the RTCP sender and receiver reports described below.

RTCP carries a persistent transport-level identifier for an RTP source called the canonical name or CNAME. Since the SSRC identifier may change if a conflict is discovered or a program is restarted, receivers require the CNAME to keep track of each participant. Receivers also require the CNAME to associate multiple data streams from a given participant in a set of related RTP sessions, for example to synchronize audio and video.

The first two functions require that all participants send RTCP packets, therefore the rate must be controlled in order for RTP to scale up to a large number of participants. By having each participant send its control packets to all the others, each can dependently observe the number of participants. This number is used to calculate the rate at which the packets are sent.

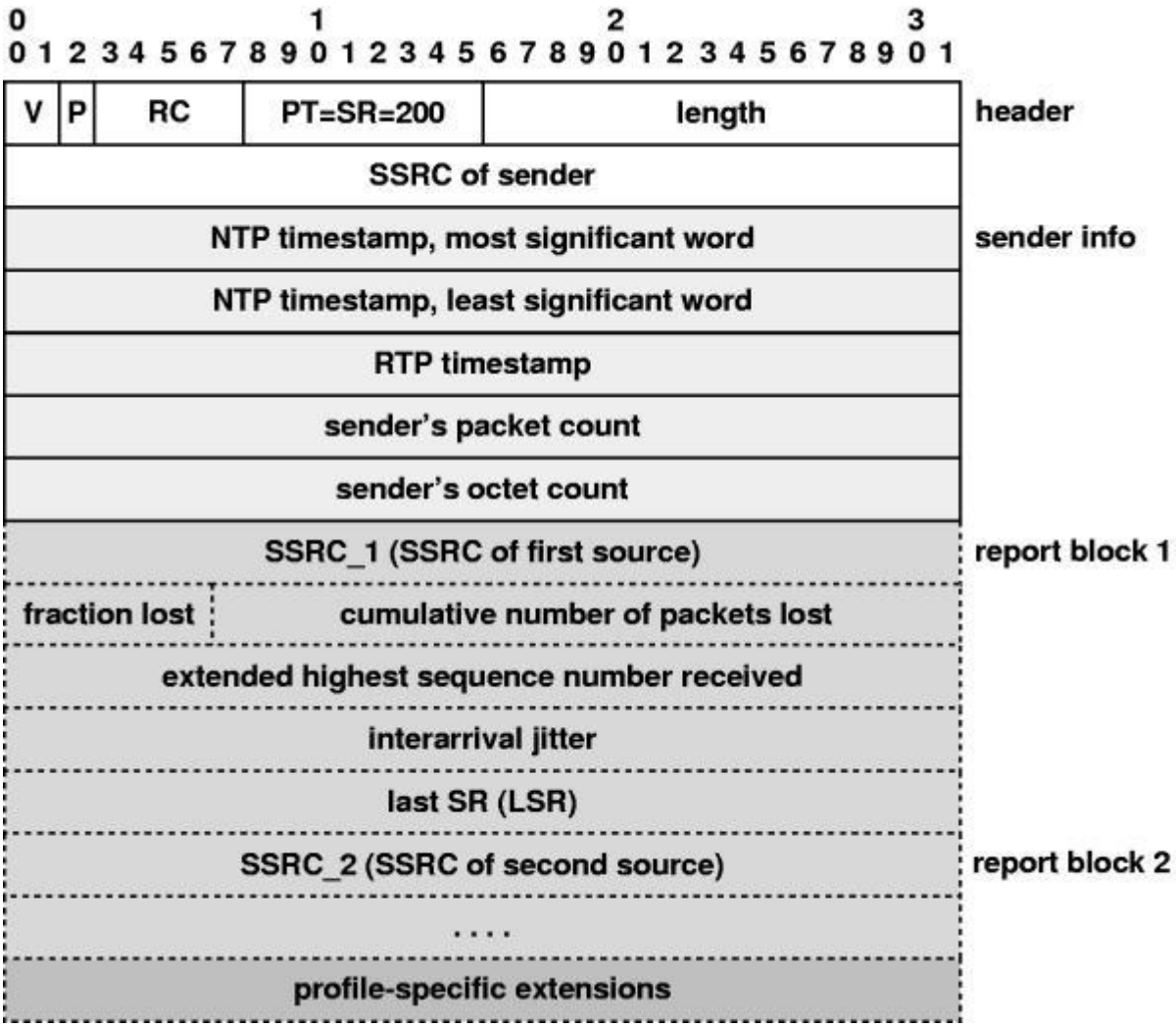
Now, let us have a closer look at the format of the different RTCP packets. Each RTCP packet begins with a fixed header part similar to that of RTP data packets, followed by structured elements that may be of variable length according to the packet type. Each packet ends on a 32-bit boundary. Multiple RTCP packets may be concatenated without any intervening separators to form a compound RTCP packet that is sent in a single packet of the lower layer protocol.

SR - Sender Report

The sender report packet consists of three sections, possibly followed by a fourth profile-specific extension section if defined.

5.Draw and explain RTCP SR Header and RTCP RR Header in detail.

Figure - RTCP SR Header



SR - Section one. The first section is 8 octets long

Version (V): 2 bits

> Identifies the version of RTP, which is the same in RTCP packets as in RTP data packets. The current version is two (2).

Padding (P): 1 bit

> If the padding bit is set, this RTCP packet contains some additional padding octets at the end which are not part of the control information. That last octet of the padding is a count of how many padding octets should be ignored. Some encryption algorithms with fixed block sizes may need padding. In a compound RTCP packet, padding should only be required on the last individual packet because the compound packet is encrypted as a whole.

Reception count: 5 bits

> The number of reception report blocks contained in this packet. A value of zero is also valid.

Packet type: 8 bits

> Contains the constant 200 to identify this as an RTCP SR packet.

Length: 16 bits

> The length is the RTCP packet in 32 bit words minus one, including the header and any padding.

SSRC: 32 bits

> The synchronization source identifier for the originator of this SR packet.

SR - Section two. The second section, the sender information, is 20 octets long and is presented in every sender report packet. It summarizes the data transmissions from this sender.

NTP timestamp: 64 bits

> Indicates the wall clock time when this report was sent so that it may be used in combination with timestamps returned in reception reports from other receivers to measure round-trip propagation to those receivers. A sender that has no notion of wall clock or elapsed time may set the NTP timestamp to zero.

RTP timestamp: 32 bits

> Corresponds to the same time as the NTP timestamp, but in the same units and with the same random offset as the RTP timestamps in the data packets.

Sender PKT count: 32 bits

> The total number of RTP data packets by the sender since starting transmission up until the time this SR packet was generated. The count is reset if the sender changes its SSRC identifier.

Sender octet count: 32 bits

> The total number of payload octets transmitted in RTP data packets by the sender since starting transmission. The count is reset if the sender changes its SSRC identifier. This field can be used to estimate the average payload data rate.

SR - Section three. The third section contains zero or more reception report blocks depending on the number of other sources heard by this sender since the last report. Each reception report block conveys statistics on the reception of RTP packets from a single synchronization source. Receivers do not carry over statistics when a source changes its SSRC identifier due to a collision.

SSRC_n (src ident): 32 bits

> The SSRC identifier of the source to which the information in this reception report block pertains.

Fraction lost: 8 bits

> The fraction of RTP data packets from source SSRC_n lost since the previous SR or RR packet was sent, expressed as a fixed point number with the binary point at the left edge of the filed. That is equivalent to taking the integer part after multiplying the loss fraction by 256. This fraction is defined to be the number of packets lost divided by the number of packets expected, as defined in the next paragraph.

Total packets lost: 24 bits

> Total number of RTP data packets from the source SSRC_n that have been lost since the beginning of reception. This number is defined to be the number of packets expected less the number of packets actually received, where the number of packets received includes any which are late or duplicates. Thus packets that arrive late are not counted as lost, and the loss may be negative if there are duplicates. The number of packets expected is defined to be the extended last sequence number received, as defined next, less the initial sequence number received.

Last sequence #: 32 bits

> The low 16 bits contain the highest sequence number received in an RTP data packet from source SSRC_n, and the most significant 16 bits extend that sequence number with the corresponding count of sequence number cycles. Note that different receivers within the same session will generate different extensions to the sequence number if their start times differ significantly.

Inter arrival jitter: 32 bits

> An estimate of the statistical variance of the RTP data packet inter-arrival time, measured in timestamp units and expressed as an unsigned integer. The inter-arrival jitter J is defined to be the mean deviation of the difference D in packet spacing at the receiver compared to the sender for a pair of packets. As shown in the equation below, this is equivalent to the difference in the "relative transit time" for the two packets (i and j). The relative transit time is the difference between a packets RTP timestamp Si and the receiver's clock at the time of arrival, Ri measured in the same units.

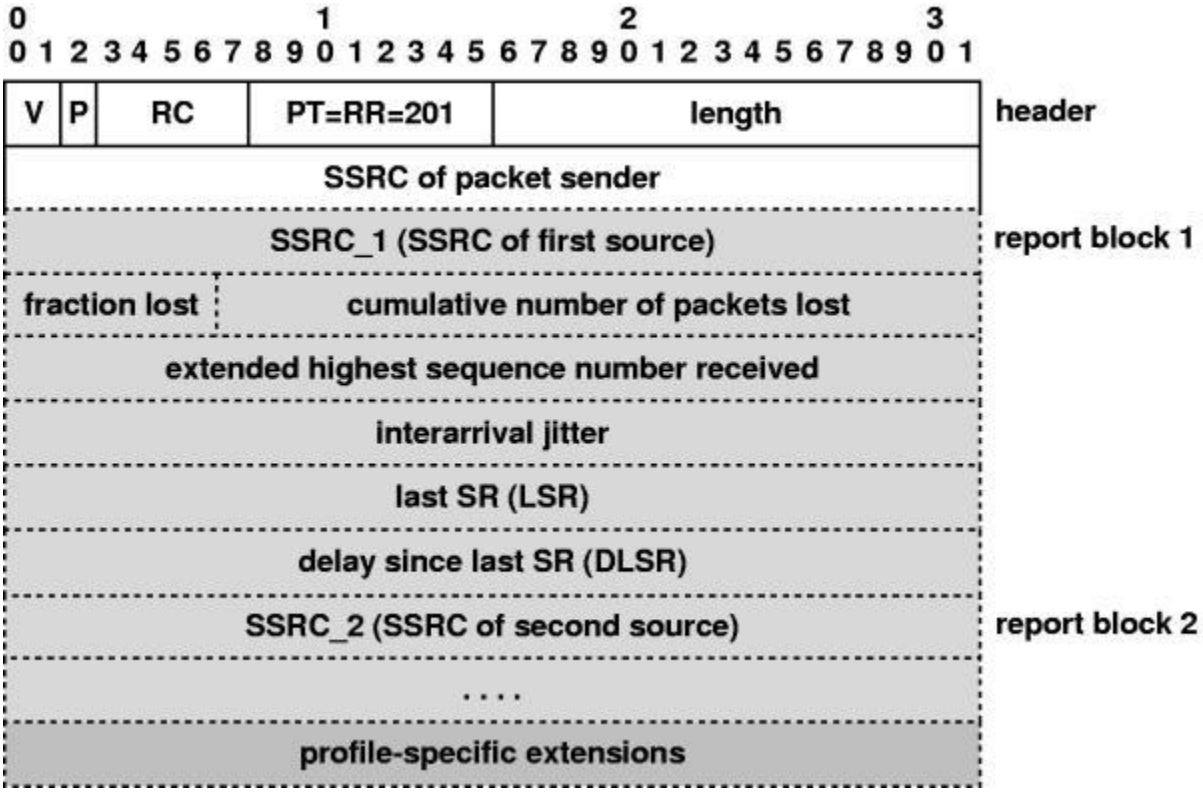
$$D(i,j) = (Rj - Sj) - (Ri - Si)$$

$$J = J + \frac{|D| - J}{16}$$

RR - Receiver

Report The format of the receiver report (RR) packet is the same as that of the SR packet except that the packet type field contains the constant 201 and the five words of sender information are omitted (these are the NTP and RTP timestamps and senders packet and octet counts). The remaining fields have the same meaning as for the SR packet.

Figure RTCP RR Header

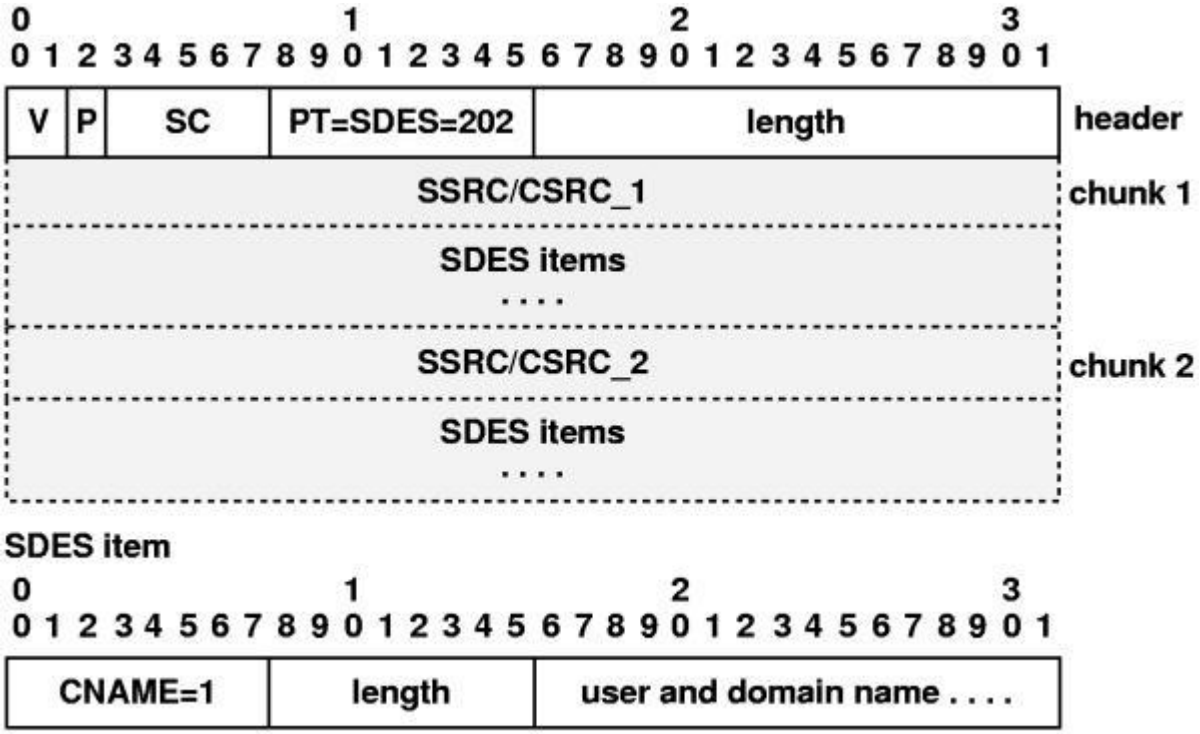


An empty RR packet (RC=0) is put at the head of a compound RTCP packet when there is no data transmission or reception to report.

SDES - Source description

The SDES packet is composed of a header and zero or more chunks, each of which is composed of items describing the source identified in that chunk.

Figure . RTCP SDES Header



RTCP SDES Header Description

Version (V), SSRC, Padding (P), length:

see SR packet description

Packet type (PT): 8 bits

Contains the constant 202 to identify this as an RTCP SDES packet.

Source Count (SC): 5 bits

The number of SSRC/CSRC chunks contained in this SDES packet. A value of zero is valid but useless.

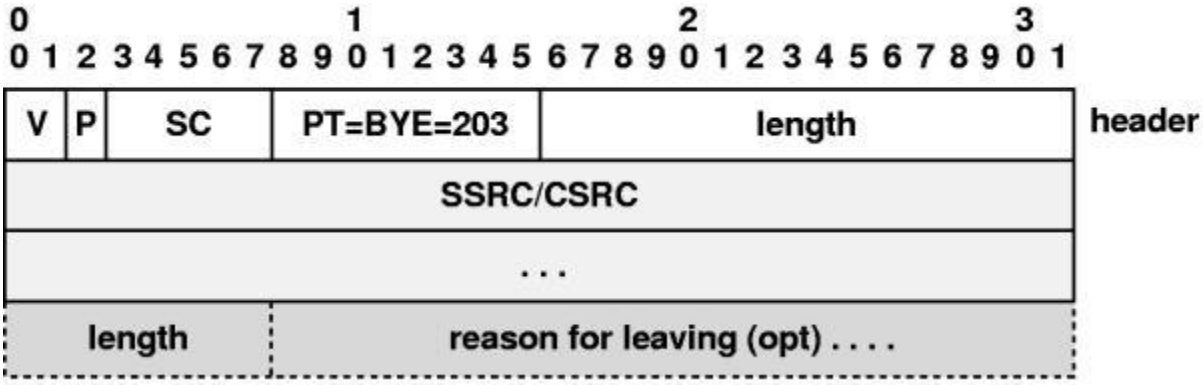
SDES item: n bits

The source description item has to be unique among all session participants, one good choice is to use the canonical name of the source.

BYE - The Goodbye

The BYE packet indicates that one or more sources are no longer active. The format of the BYE packet is the following:

Figure A-9. RTCP BYE Header



RTCP BYE Header

Version (V), SSRC, Padding (P), length:

see SR packet description.

Packet type (PT): 8 bits

Contains the constant 203 to identify this as an RTCP BYE packet.

Source count (SC): 5 bits

The number of SSRC/CSRC identifiers included in this BYE packet.

6.Explain the RSVP Goals and its characteristics.

RSVP Goals

- Used on connectionless networks.

    - Should not replicate routing functionality.
    - Should co-exist with route changes.
- Support for multicast.
    - Different receivers have different capabilities and want different QOS.
    - Changes in group membership should not be expensive.
    - Reservations should be aggregate – I.e. each receiver in group should not have to reserve.
    - Should be able to switch allocated resource to different senders.
- Limit control overhead.
- Modular design – should be generic "signaling" protocol.
- Result:
    - Receiver-oriented
    - Soft-state

Receiver-Initiated Reservation

- Receiver initiates reservation by sending a reservation over the sink tree.
    - Assumes multicast tree has been set up previously.
        - Also uses receiver-initiated mechanism.
    - Hooks up with the reserved part of the tree.
    - How far the request has to travel to the source depends on the level of service requested.
    - Uses existing routing protocol, but routers have to store the sink tree (reverse path from forwarding path).
- Properties:
    - Scales well: can have parallel independent connect and disconnect actions – single shared resource required.
    - Supports receiver heterogeneity: reservation specifies receiver requirements and capabilities.

Soft State

- Routers keep state about reservation.
- Periodic messages refresh state.
- Non-refreshed state times out automatically.
- Alternative: Hard state
    - No periodic refresh messages.
    - State is guaranteed to be there.
    - State is kept till explicit removal.
    - Why could there be a problem?
- Properties of soft state:
    - Adapts to changes in routes, sources, and receivers.
    - Recovers from failures

    - Cleans up state after receivers drop outs
- Philosophy: reservation is an optimization.

7.Explain the RSVP Service Model and the reservations.

RSVP Service Model

- Make reservations for simplex data streams.
- Receiver decides whether to make reservation
    - Control messages in IP datagrams (proto #46).
- PATH/RESV messages sent periodically to refresh soft state.
- One pass:
    - Failed requests return error messages - receiver must try again.
    - No end to end ack for success
    -

Basic Message Types

- PATH message
- RESV message
- CONFIRMATION message
    - Generated only upon request.
    - Unicast to receiver when RESV reaches node with established state.
- TEARDOWN message
- ERROR message (if PATH or RESV fails)

PATH Messages

- PATH messages carry sender's T-spec.
    - Token bucket parameters
- Routers note the direction PATH messages arrived and set up *reverse path* to sender.
- Receivers send RESV messages that follow reverse path and setup reservations.
- If reservation cannot be made, user gets an error.

RESV Messages

- RESV messages carry receiver's R-spec.
- Forwarded via reverse path of PATH.
- Queuing delay and bandwidth requirements.
- Source traffic characteristics (from PATH).
- Filter specification
    - Which transmissions can use the reserved resources?
    - Reservation style.
- Router performs admission control and reserves resources.
-

Router Handling of RESV Messages

- If new request rejected, send error message.
- If admitted:
    - Install packet filter into forwarding dbase.
    - Pass flow parameters to scheduler.
    - Activate packet policing if needed.
    - Forward RESV message upstream.

RSVP reservations

- Reservations from multiple receivers for a single sender are merged together at branching points.
- Reservations for multiple senders may be added up:
    - Video conference
- Reservations for multiple senders may not be added up:
    - Audio conference, not many talk at same time.
    - Only subset of speakers (filters).

Reservation Styles

- Three styles
    - Wildcard/No filter – does not specify a particular sender for group.
    - Fixed filter – sender explicitly specified for a reservation.
        - Video conference
    - Dynamic filter – valid senders may be changed over time.
        - Audio conference