EGS Pillay Engineering College, Nagapattinam

Department of Electronics & Communication Engineering

**Anna University – Solved 16 Marks Q&A**

**CS2060-High Speed Networks**

Prepared by **M.Nuthal Srinivasan**

**Unit -1**

1. **Explain the call control procedure in frame relay networks.**

Frame Relay often is described as a streamlined version of X.25, offering fewer of the robust capabilities, such as windowing and retransmission of last data that are offered in X.25.

**Frame Relay Devices**

Devices attached to a Frame Relay WAN fall into the following two general categories:

•blankData terminal equipment (DTE) •blankData circuit-terminating equipment (DCE)

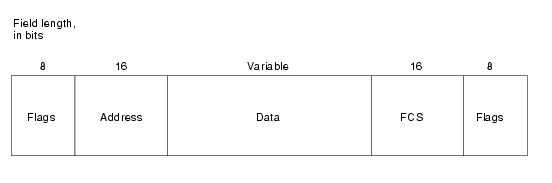
DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches. Figure 10-1 shows the relationship between the two categories of devices.

### Standard Frame Relay Frame

Standard Frame Relay frames consist of the fields illustrated in Figure 10-4.

Figure  Five Fields Comprise the Frame Relay Frame



Each frame relay [PDU](http://en.wikipedia.org/wiki/Protocol_data_unit) 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 either 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 comprising the EA=ADDRESS FIELD EXTENSION BITS and the C/R=COMMAND/RESPONSE BIT.
3. 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](http://en.wikipedia.org/wiki/Multiplexing) several different virtual connections.
4. FECN, BECN, DE bits. These bits report congestion:
   * FECN=Forward Explicit Congestion Notification bit
   * BECN=Backward Explicit Congestion Notification bit
   * DE=Discard Eligibility bit
5. 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.

***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 erred frames. The error detection mechanism used in frame relay uses the*** [***cyclic redundancy check***](http://en.wikipedia.org/wiki/Cyclic_redundancy_check) ***(CRC) as its basis.***

1. **Explain the various ATM service categories in detail.**

**ATM Classes of Services**

ATM is connection oriented and allows the user to specify the resources required on a per-connection basis (per SVC) dynamically. There are the five classes of service defined for ATM (as per ATM Forum UNI 4.0 specification). The QoS parameters for these service classes are summarized in Table 1.

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

|  |  |
| --- | --- |
| **Technical Parameter** | **Definition** |
| cell loss ratio (CLR) | CLR is the percentage of cells not delivered at their destination because they were lost in the network due to congestion and buffer overflow. |
| cell transfer delay (CTD) | The delay experienced by a cell between network entry and exit points is called the CTD. It includes propagation delays, queuing delays at various intermediate switches, and service times at queuing points. |
| cell delay variation (CDV) | CDV is a measure of the variance of the cell transfer delay. High variation implies larger buffering for delay-sensitive traffic such as voice and video. |
| peak cell rate (PCR) | The maximum cell rate at which the user will transmit. PCR is the inverse of the minimum cell inter-arrival time. |
| sustained cell rate (SCR) | This is the average rate, as measured over a long interval, in the order of the connection lifetime. |
| burst tolerance (BT) | This parameter determines the maximum burst that can be sent at the peak rate. This is the bucket-size parameter for the enforcement algorithm that is used to control the traffic entering the network. |

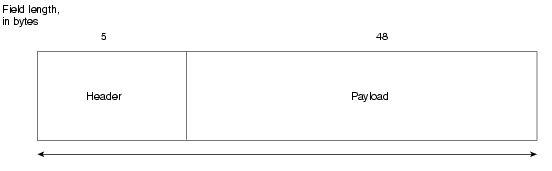
1. **Explain the architure of ATM?**

*Asynchronous Transfer Mode (ATM)* is an International Telecommunication Union-Telecommunications Standards Section (ITU-T) standard for cell relay wherein information for multiple service types, such as voice, video, or data, is conveyed in small, fixed-size cells. ATM networks are connection-oriented.

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (Gbps). Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as *time-division multiplexing (TDM)*.

With TDM, each user is assigned to a time slot, and no other station can send in that time slot. If a station has much data to send, it can send only when its time slot comes up, even if all other time slots are empty. However, if a station has nothing to transmit when its time slot comes up, the time slot is sent empty and is wasted. Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell.

ATM transfers information in fixed-size units called *cells*. Each cell consists of 53 octets, or bytes. The first 5 bytes contain cell-header information, and the remaining 48 contain the payload (user information). Small, fixed-length cells are well suited to transferring voice and video traffic because such traffic is intolerant of delays that result from having to wait for a large data packet to download, among other things. Figure illustrates the basic format of an ATM cell. Figure :An ATM Cell Consists of a Header and Payload Data



## ATM Protocol architecture:

ATM is almost similar to cell relay and packets witching using X.25and framerelay.like packet switching and frame relay,ATM involves the transfer of data in discrete pieces.also,like packet switching and frame relay ,ATM allows multiple logical connections to multiplexed over a single physical interface. in the case of ATM,the information flow on each logical connection is organised into fixed-size packets, called cells. ATM is a streamlined protocol with minimal error and flow control capabilities :this reduces the overhead of processing ATM cells and reduces the number of overhead bits required with each cell, thus enabling ATM to operate at high data rates.the use of fixed-size cells simplifies the processing required at each ATM node,again supporting the use of ATM at high data rates. The ATM architecture uses a logical model to describe the functionality that it supports. ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model. . the protocol referencce model shown makes reference to three separate planes:

**user plane** provides for user information transfer ,along with associated controls (e.g.,flow control ,error control).

**control plane** performs call control and connection control functions.

**management plane** includes plane management ,which performs management function related to a system as a whole and provides coordination between all the planes ,and layer management which performs management functions relating to resource and parameters residing in its protocol entities .

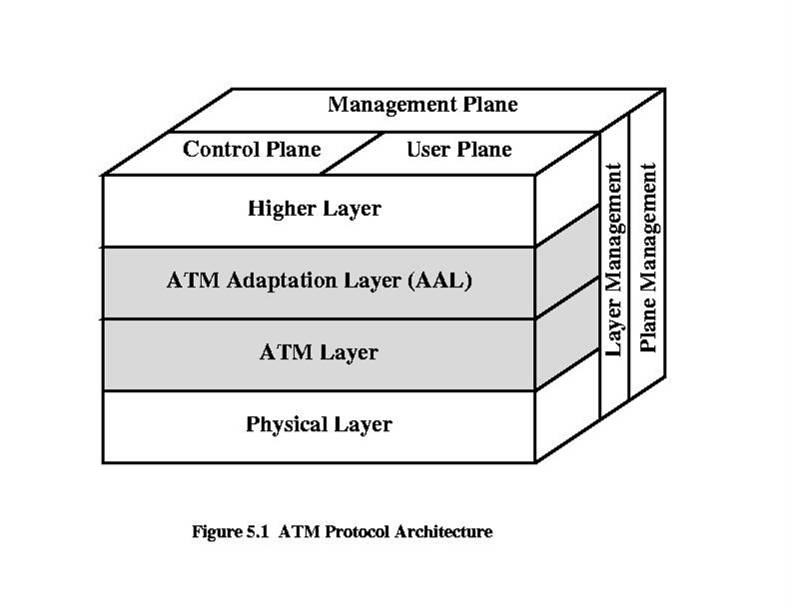
The ATM reference model is composed of the following ATM layers:

•blank**Physical layer**—Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.

•blank**ATM layer**—Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.

•blank**ATM adaptation layer (AAL)**—Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads.

Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL. Figure :illustrates the ATM reference model.



1. **Explain the IEEE802.11 architecture in detail. Illustrate the functions and combined operation of various protocol in MAC sub layer.**

**Classical Ethernet**

* Bus topology LAN
* 10 Mbps
* CSMA/CD medium access control protocol
* 2 problems:
* A transmission from any station can be received by all stations
* How to regulate transmission

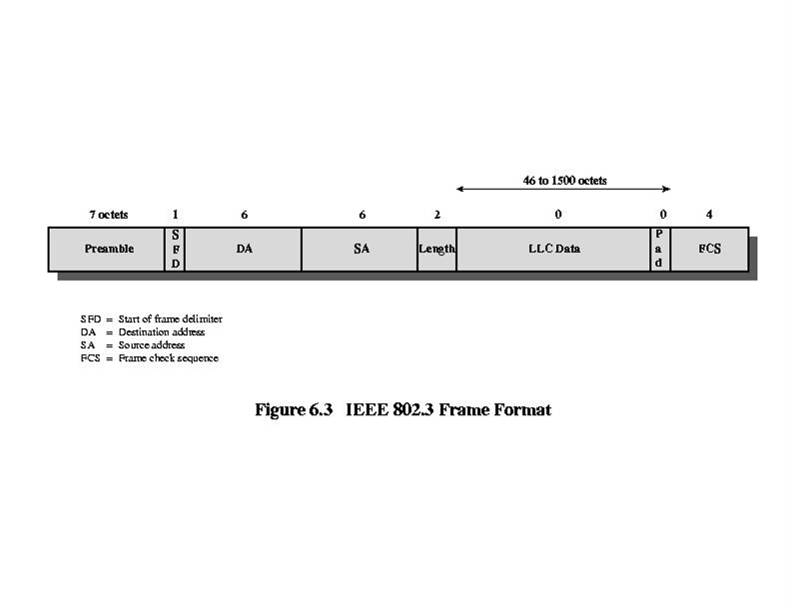
Solution to First Problem

* Data transmitted in blocks called frames:
* User data
* Frame header containing unique address of destination station

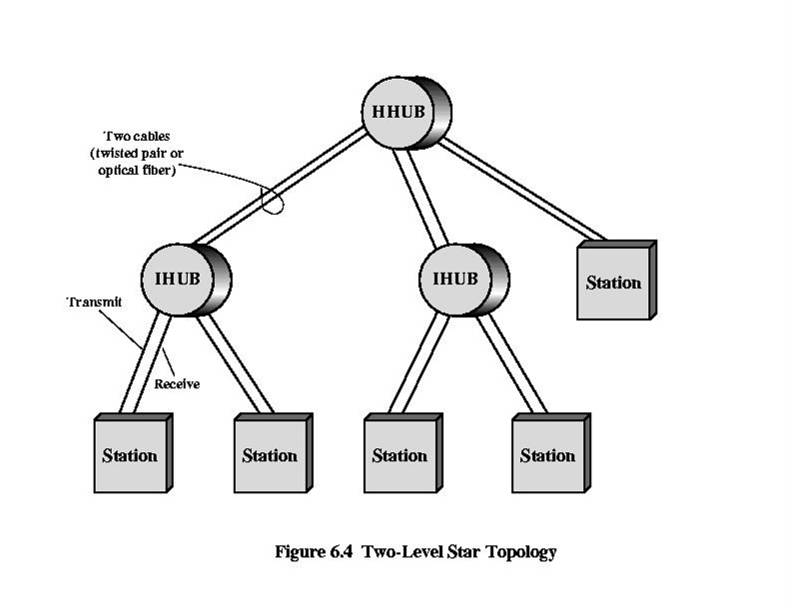
CSMA/CD

Carrier Sense Multiple Access/ Carrier Detection

* If the medium is idle, transmit.
* If the medium is busy, continue to listen until the channel is idle, then transmit immediately.
* If a collision is detected during transmission, immediately cease transmitting.
* After a collision, wait a random amount of time, then attempt to transmit again (repeat from step 1).



Medium Options at 10Mbps

* <data rate> <signaling method> <max length>
* 10Base5
* 10 Mbps
* 50-ohm coaxial cable bus
* Maximum segment length 500 meters
* 10Base-T
* Twisted pair, maximum length 100 meters
* Star topology (hub or multipoint repeater at central point)

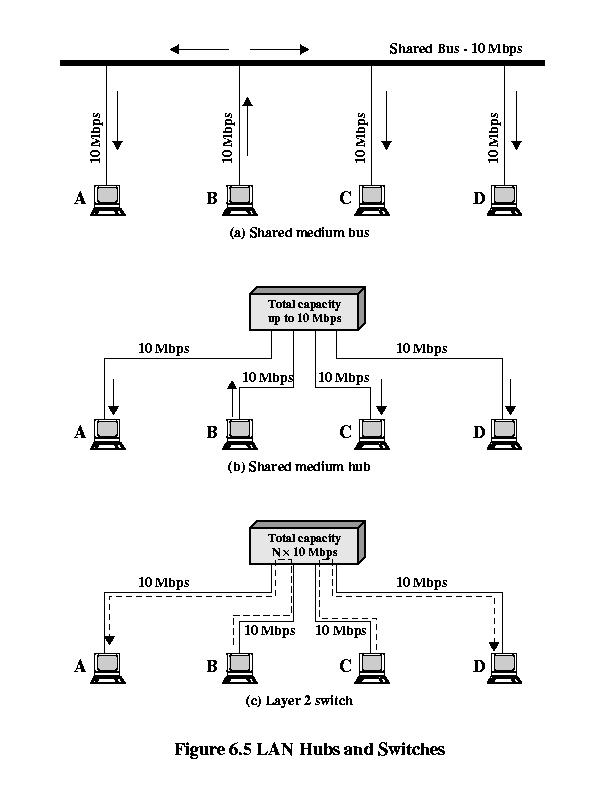
Hubs and Switches

Hub

* Transmission from a station received by central hub and retransmitted on all outgoing lines
* Only one transmission at a time

Layer 2 Switch

* frame switched to one outgoing line
* Many transmissions at same time



Bridge

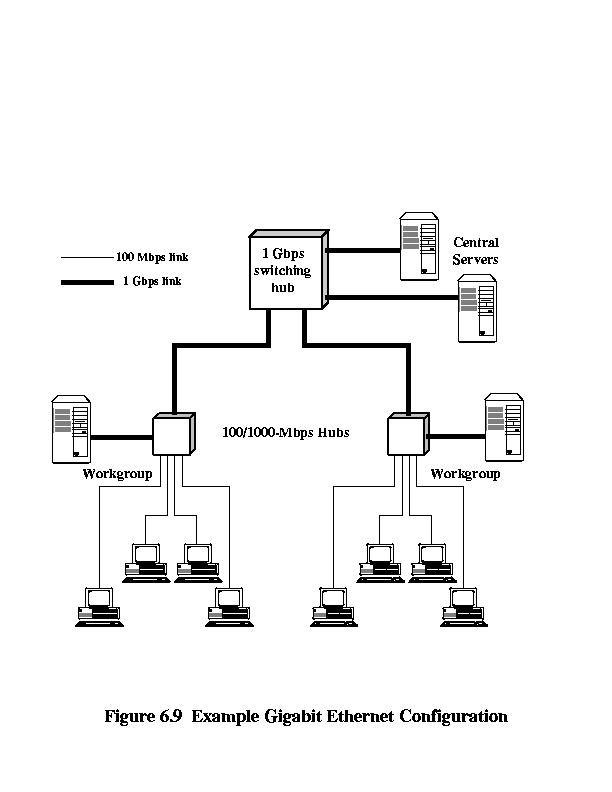
* Frame handling done in software
* Analyze and forward one frame at a time
* Store-and-forward

Layer 2 Switch

* Frame handling done in hardware
* Multiple data paths and can handle multiple frames at a time
* Can do cut-through

Layer 2 Switches

* Flat address space
* Broadcast storm
* Only one path between any 2 devices
* Solution 1: subnetworks connected by routers
* Solution 2: layer 3 switching, packet-forwarding logic in hardware

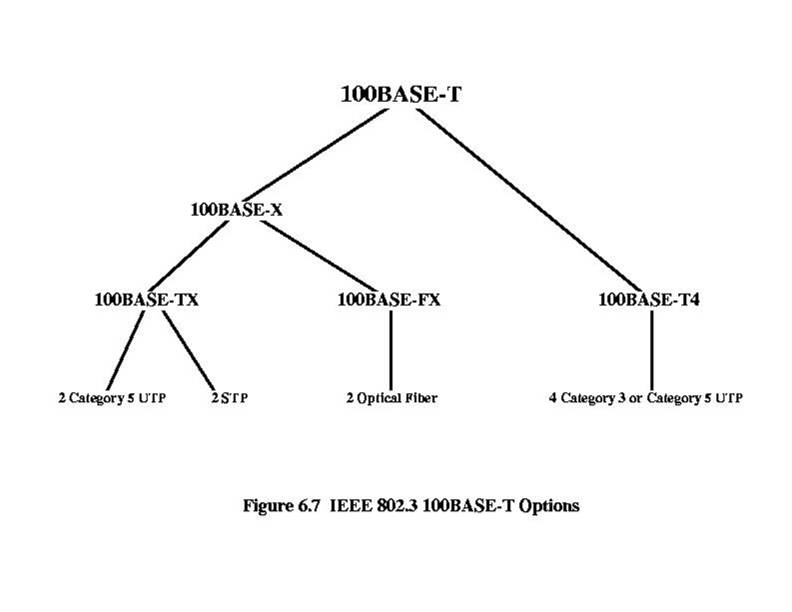


Benefits of 10 Gbps Ethernet over ATM

* No expensive, bandwidth consuming conversion between Ethernet packets and ATM cells
* Network is Ethernet, end to end
* IP plus Ethernet offers QoS and traffic policing capabilities approach that of ATM
* Wide variety of standard optical interfaces for 10 Gbps Ethernet

Fibre Channel

* 2 methods of communication with processor:
* I/O channel
* Network communications



**Unit-2**

1. **Explain with an example the implementation of single server queues.**

Single-server queues are, perhaps, the most commonly encountered queueing situation in real life. One encounters a queue with a single server in many situations, including business (e.g. sales clerk), industry (e.g. a production line), transport (e.g. a bus, a taxi rank, an intersection), telecommunications (e.g. Telephone line), computing (e.g. processor sharing). Even where there are multiple servers handling the situation it is possible to consider each server individually as part of the larger system, in many cases. (e.g A supermarket checkout has several single server queues that the customer can select from.) Consequently, being able to model and analyse a single server queue's behaviour is a particularly useful thing to do.

#### Poisson arrivals and service

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

This is fortunate because, an M/M/1 queuing model can be used to approximate many queuing situations.

#### Poisson arrivals and general service

**M/G/1/∞/∞** represents a single server that has unlimited queue capacity and infinite calling population, while the arrival is still Poisson process, meaning the statistical distribution of the inter-arrival times still follow the exponential distribution, the distribution of the service time does not. The distribution of the service time may follow any general statistical distribution, not just exponential. Relationships are still able to be derived for a (limited) number of performance measures if one knows the arrival rate and the mean and variance of the service rate. However the derivations a generally more complex.

A number of special cases of M/G/1 provide specific solutions that give broad insights into the best model to choose for specific queueing situations because they permit the comparison of those solutions to the performance of an M/M/1 model.

1. **Explain the effects of Congestion in Packet switching networks.**

## Effects of Congestion

## F4‘

## Congestion-Control Mechanisms

## Backpressure

## Request from destination to source to reduce rate

## Useful only on a logical connection basis

## Requires hop-by-hop flow control mechanism

## Policing

## Measuring and restricting packets as they enter the network

## Choke packet

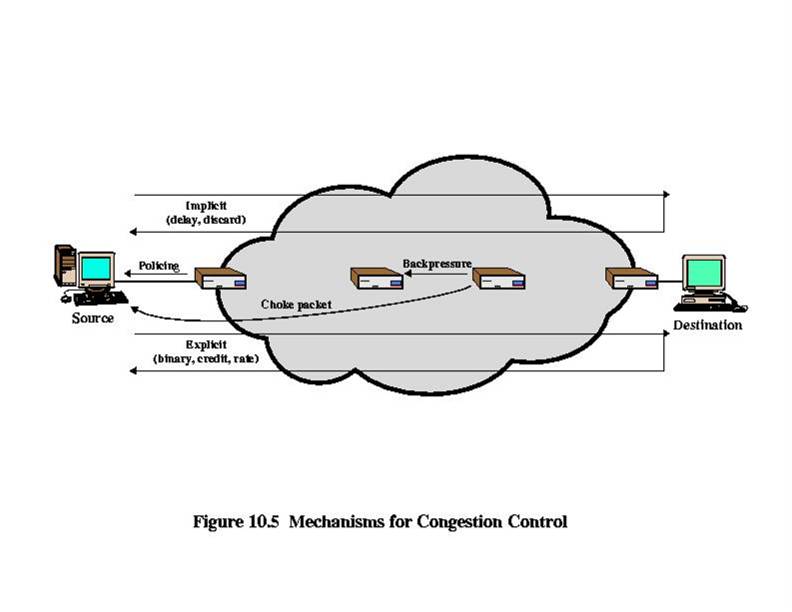
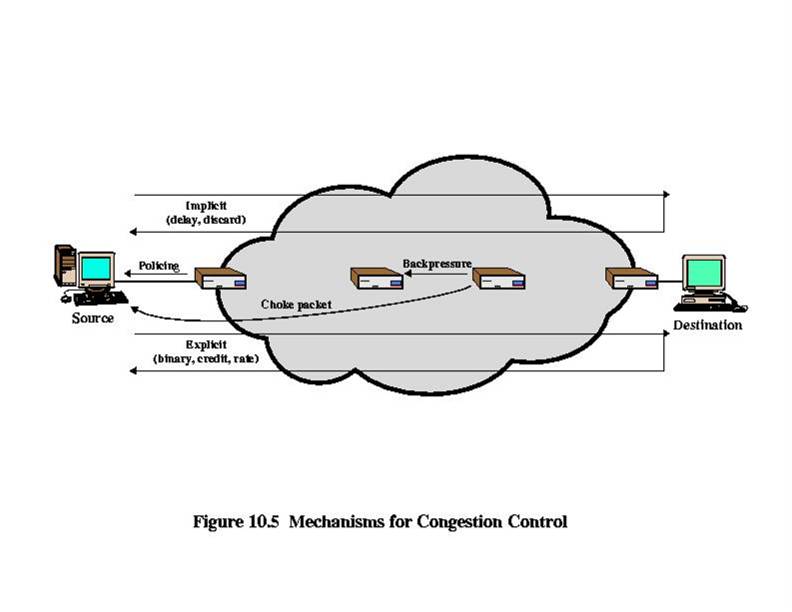
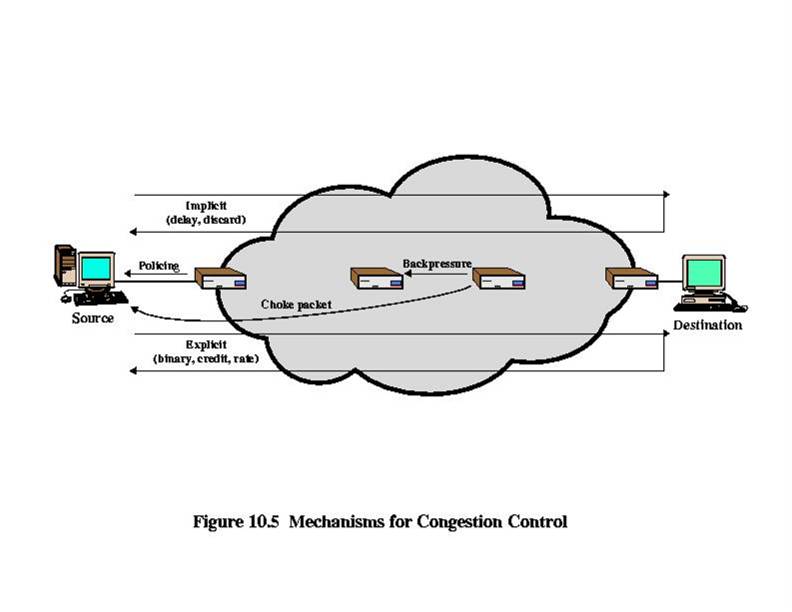
## Specific message back to source

## E.g., ICMP Source Quench

## Implicit congestion signaling

## Source detects congestion from transmission delays and lost packets and reduces flow

## Explicit congestion signaling



Frame Relay reduces network overhead by implementing simple congestion-notification mechanisms rather than explicit, per-virtual-circuit flow control. Frame Relay typically is implemented on reliable network media, so data integrity is not sacrificed because flow control can be left to higher-layer protocols. Frame Relay implements two congestion-notification mechanisms:

•blankForward-explicit congestion notification (FECN)

•blankBackward-explicit congestion notification (BECN)

FECN and BECN each is controlled by a single bit contained in the Frame Relay frame header. The Frame Relay frame header also contains a Discard Eligibility (DE) bit, which is used to identify less important traffic that can be dropped during periods of congestion.

The *FECN bit* is part of the Address field in the Frame Relay frame header. The FECN mechanism is initiated when a DTE device sends Frame Relay frames into the network. If the network is congested, DCE devices (switches) set the value of the frames' FECN bit to 1. When the frames reach the destination DTE device, the Address field (with the FECN bit set) indicates that the frame experienced congestion in the path from source to destination. The DTE device can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow control may be initiated, or the indication may be ignored.

The *BECN bit* is part of the Address field in the Frame Relay frame header. DCE devices set the value of the BECN bit to 1 in frames traveling in the opposite direction of frames with their FECN bit set. This informs the receiving DTE device that a particular path through the network is congested. The DTE device then can relay this information to a higher-layer protocol for processing. Depending on the implementation, flow-control may be initiated, or the indication may be ignored.

1. **Explain the congestion control mechanism used in frame relay and in TCP.**

### Frame Relay Discard Eligibility

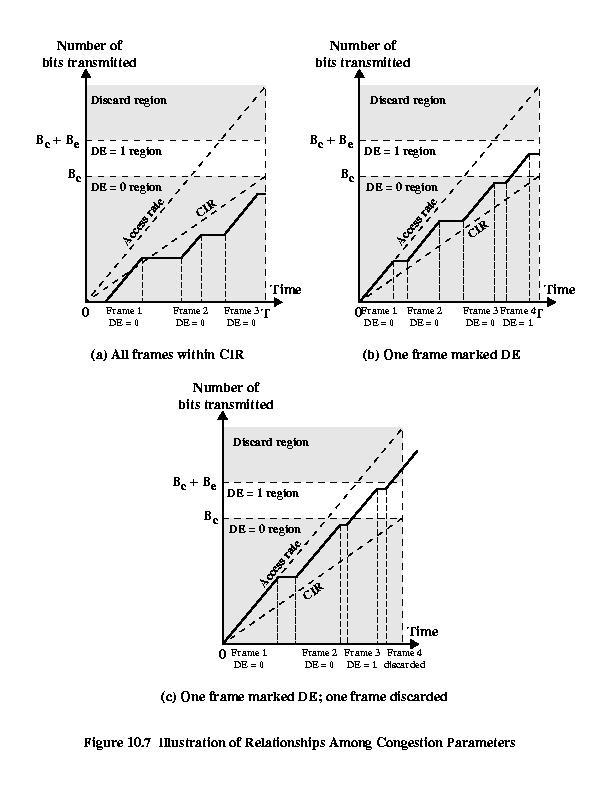
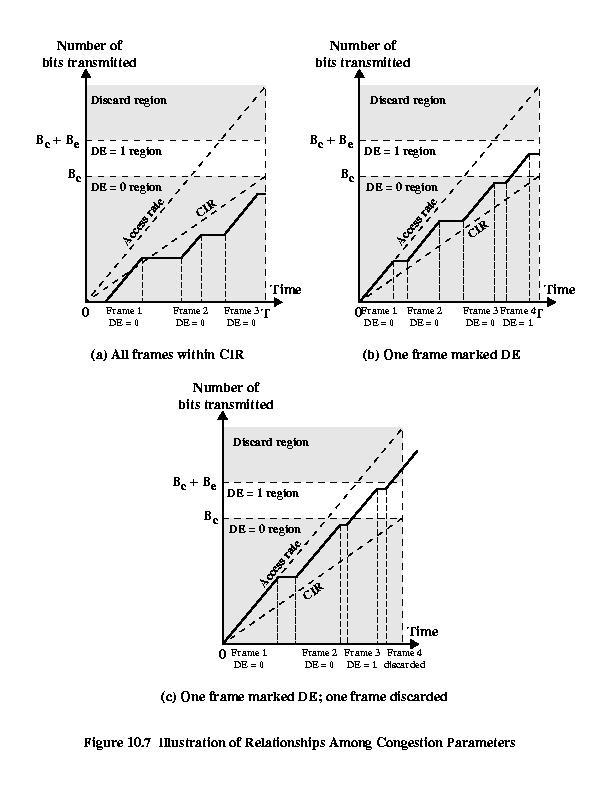
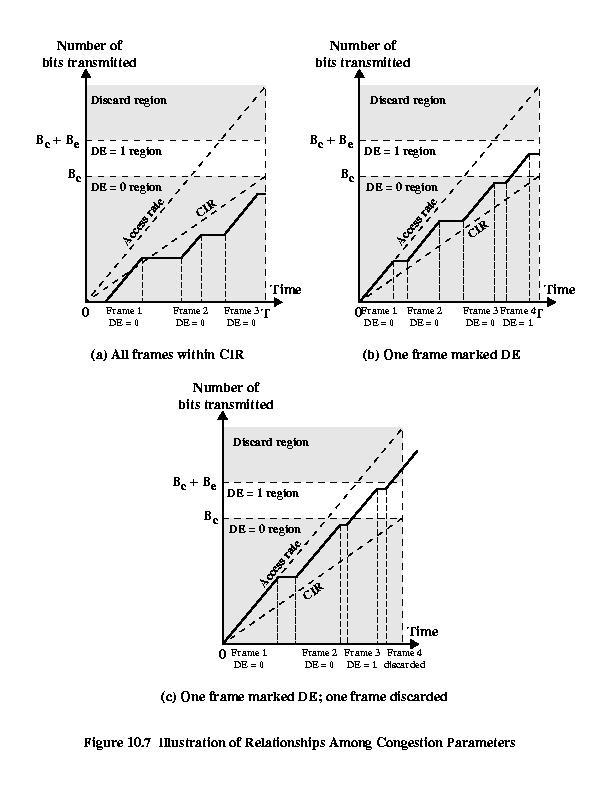
The *Discard Eligibility (DE) bit* is used to indicate that a frame has lower importance than other frames. The DE bit is part of the Address field in the Frame Relay frame header.

DTE devices can set the value of the DE bit of a frame to 1 to indicate that the frame has lower importance than other frames. When the network becomes congested, DCE devices will discard frames with the DE bit set before discarding those that do not. This reduces the likelihood of critical data being dropped by Frame Relay DCE devices during periods of congestion.

### Frame Relay Error Checking

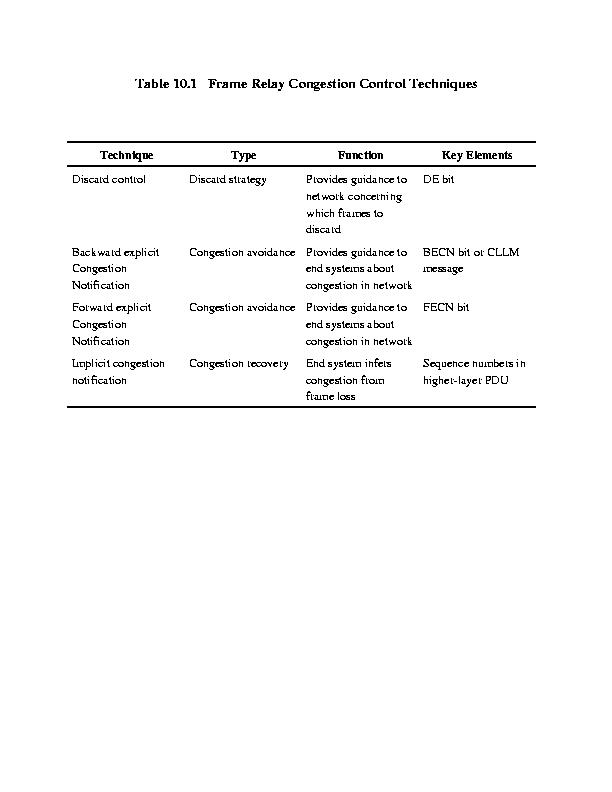
Frame Relay uses a common error-checking mechanism known as the *cyclic redundancy check (CRC)*. The CRC compares two calculated values to determine whether errors occurred during the transmission from source to destination. Frame Relay reduces network overhead by implementing error checking rather than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

**Traffic Management in Congested Network – Some Considerations**

* Fairness
  + Various flows should “suffer” equally
  + Last-in-first-discarded may not be fair
* Quality of Service (QoS)
  + Flows treated differently, based on need
  + Voice, video: delay sensitive, loss insensitive
  + File transfer, mail: delay insensitive, loss sensitive
  + Interactive computing: delay and loss sensitive
* Reservations
  + Policing: excess traffic discarded or handled on best-effort basis
* 

**Frame Relay Congestion Control**

* Minimize frame discard
* Maintain QoS (per-connection bandwidth)
* Minimize monopolization of network
* Simple to implement, little overhead
* Minimal additional network traffic
* Resources distributed fairly
* Limit spread of congestion
* Operate effectively regardless of flow
* Have minimum impact other systems in network
* Minimize variance in QoS

****

**Congestion Avoidance with Explicit Signaling**

Two general strategies considered:

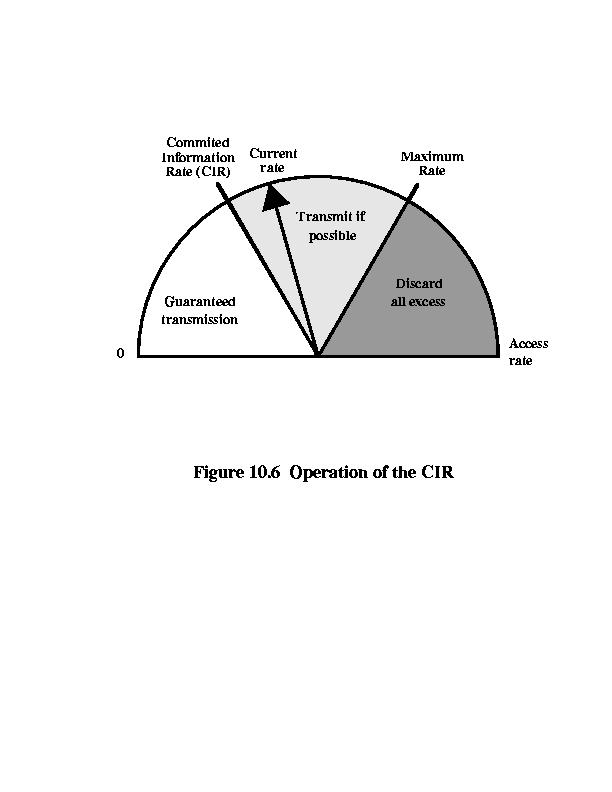
* Hypothesis 1: Congestion always occurs slowly, almost always at egress nodes
  + forward explicit congestion avoidance
* Hypothesis 2: Congestion grows very quickly in internal nodes and requires quick action
  + backward explicit congestion avoidance

**Explicit Signaling Response**

* **Network Response**
  + each frame handler monitors its queuing behavior and takes action
  + use FECN/BECN bits
  + some/all connections notified of congestion
* **User (end-system) Response**
  + receipt of BECN/FECN bits in frame
  + BECN at sender: reduce transmission rate
  + FECN at receiver: notify peer (via LAPF or higher layer) to restrict flow

**Frame Relay Traffic Rate Management Parameters**

* Committed Information Rate (CIR)
  + Average data rate in bits/second that the network agrees to support for a connection
* Data Rate of User Access Channel (Access Rate)
  + Fixed rate link between user and network (for network access)
* Committed Burst Size (Bc)
  + Maximum data over an interval agreed to by network
* Excess Burst Size (Be)
  + Maximum data, above Bc, over an interval that network will attempt to transfer



**Relationship of Congestion Parameters**

4.

****

**Queueing models** can be represented using [Kendall's notation](http://www.answers.com/topic/kendall-s-notation):

A/B/S/K/N/Disc

where:

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

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

* M for a [Markovian](http://www.answers.com/topic/markov-property) ([exponential](http://www.answers.com/topic/exponential-distribution)) distribution
* Eκ for an [Erlang distribution](http://www.answers.com/topic/erlang-distribution) with κ phases
* D for Deterministic (constant)
* G for General distribution
* PH for a [Phase-type distribution](http://www.answers.com/topic/phase-type-distribution)

### Single-server queue

Single-server queues are, perhaps, the most commonly encountered queueing situation in real life. One encounters a queue with a single server in many situations, including business (e.g. sales clerk), industry (e.g. a production line), transport (e.g. a bus, a taxi rank, an intersection), telecommunications (e.g. Telephone line), computing (e.g. processor sharing). Even where there are multiple servers handling the situation it is possible to consider each server individually as part of the larger system, in many cases. (e.g A supermarket checkout has several single server queues that the customer can select from.) Consequently, being able to model and analyse a single server queue's behaviour is a particularly useful thing to do.

#### Poisson arrivals and service

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

This is fortunate because, an M/M/1 queuing model can be used to approximate many queuing situations.

#### Poisson arrivals and general service

**M/G/1/∞/∞** represents a single server that has unlimited queue capacity and infinite calling population, while the arrival is still Poisson process, meaning the statistical distribution of the inter-arrival times still follow the exponential distribution, the distribution of the service time does not. The distribution of the service time may follow any general statistical distribution, not just exponential. Relationships are still able to be derived for a (limited) number of performance measures if one knows the arrival rate and the mean and variance of the service rate. However the derivations a generally more complex.

A number of special cases of M/G/1 provide specific solutions that give broad insights into the best model to choose for specific queueing situations because they permit the comparison of those solutions to the performance of an M/M/1 model.

### Multiple-servers queue

Multiple (identical)-servers queue situations are frequently encountered in telecommunications or a customer service environment. When modelling these situations care is needed to ensure that it is a multiple servers queue, not a network of single server queues, because results may differ depending on how the queuing model behaves.

One observational insight provided by comparing queuing models is that a single queue with multiple servers performs better than each server having their own queue and that a single large pool of servers performs better than two or more smaller pools, even though there are the same total number of servers in the system.

One simple example to prove the above fact is as follows: Consider a system having 8 input lines, single queue and 8 servers.The output line has a capacity of 64 kbit/s. Considering the arrival rate at each input as 2 packets/s. So, the total arrival rate is 16 packets/s. With an average of 2000 bits per packet, the service rate is 64 kbit/s/2000b = 32 packets/s. Hence, the average response time of the system is 1/(μ-λ) = 1/(32-16) = 0.0667 sec. Now, consider a second system with 8 queues, one for each server. Each of the 8 output lines has a capacity of 8 kbit/s. The calculation yields the response time as 1/(μ-λ) = 1/(4-2) = 0.5 sec. And the average waiting time in the queue in the first case is ρ/(1-ρ)μ = 0.25, while in the second case is 0.03125.

### Infinitely many servers

While never exactly encountered in reality, an *infinite-servers* (e.g. **M/M/∞**) model is a convenient theoretical model for situations that involve storage or delay, such as parking lots, warehouses and even atomic transitions. In these models there is no queue, as such, instead each arriving *customer* receives service. When viewed from the outside, the model appears to delay or store each *customer* for some time.

## Queueing System Classification

With Little's Theorem, we have developed some basic understanding of a queueing system. To further our understanding we will have to dig deeper into characteristics of a queueing system that impact its performance. For example, queueing requirements of a restaurant will depend upon factors like:

* How do customers arrive in the restaurant? Are customer arrivals more during lunch and dinner time (a regular restaurant)? Or is the customer traffic more uniformly distributed (a cafe)?
* How much time do customers spend in the restaurant? Do customers typically leave the restaurant in a fixed amount of time? Does the customer service time vary with the type of customer?
* How many tables does the restaurant have for servicing customers?

The above three points correspond to the most important characteristics of a queueing system. They are explained below:

|  |  |
| --- | --- |
| **Arrival Process** | * The probability density distribution that determines the customer arrivals in the system. * In a messaging system, this refers to the message arrival probability distribution. |
| **Service Process** | * The probability density distribution that determines the customer service times in the system. * In a messaging system, this refers to the message transmission time distribution. Since message transmission is directly proportional to the length of the message, this parameter indirectly refers to the message length distribution. |
| **Number of Servers** | * Number of servers available to service the customers. * In a messaging system, this refers to the number of links between the source and destination nodes. |

Based on the above characteristics, queueing systems can be classified by the following convention:

**A/S/n**

Where A is the arrival process, S is the service process and n is the number of servers. A and S are can be any of the following:

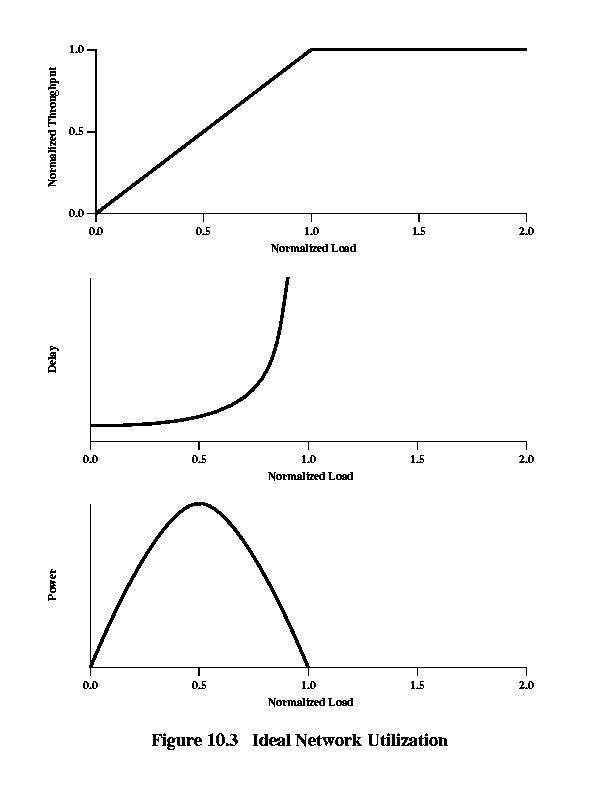
|  |  |
| --- | --- |
| M (Markov) | Exponential probability density |
| D (Deterministic) | All customers have the same value |
| G (General) | Any arbitrary probability distribution |

Examples of queueing systems that can be defined with this convention are:

* **M/M/1:** This is the simplest queueing system to analyze. Here the arrival and service time are negative exponentially distributed (poisson process). The system consists of only one server. This queueing system can be applied to a wide variety of problems as any system with a very large number of independent customers can be approximated as a Poisson process. Using a Poisson process for service time however is not applicable in many applications and is only a crude approximation. Refer to [M/M/1 Queueing System](file:///D:\ash\m_m_1_queue.htm) for details.
* **M/D/n:** Here the arrival process is poisson and the service time distribution is deterministic. The system has n servers. (e.g. a ticket booking counter with n cashiers.) Here the service time can be assumed to be same for all customers)
* **G/G/n:** This is the most general queueing system where the arrival and service time processes are both arbitrary. The system has n servers. No analytical solution is known for this queueing system.

Markovian arrival processes

**Ideal Performance**



**Unit-3**

* 1. **Explain the retransmission timer management techniques used in TCP also Explain the window management techniques used in TCP for congestion control.**

**TCP Congestion Control**

* Dynamic routing can alleviate congestion by spreading load more evenly
* But only effective for unbalanced loads and brief surges in traffic
* Congestion can only be controlled by limiting total amount of data entering network
* ICMP source Quench message is crude and not effective
* RSVP may help but not widely implemented

**TCP Congestion Control is Difficult**

* IP is connectionless and stateless, with no provision for detecting or controlling congestion
* TCP only provides end-to-end flow control
* No cooperative, distributed algorithm to bind together various TCP entities

**TCP Flow and Congestion Control**

* The rate at which a TCP entity can transmit is determined by rate of incoming ACKs to previous segments with new credit
* Rate of Ack arrival determined by round-trip path between source and destination
* Bottleneck may be destination or internet
* Sender cannot tell which
* Only the internet bottleneck can be due to congestion

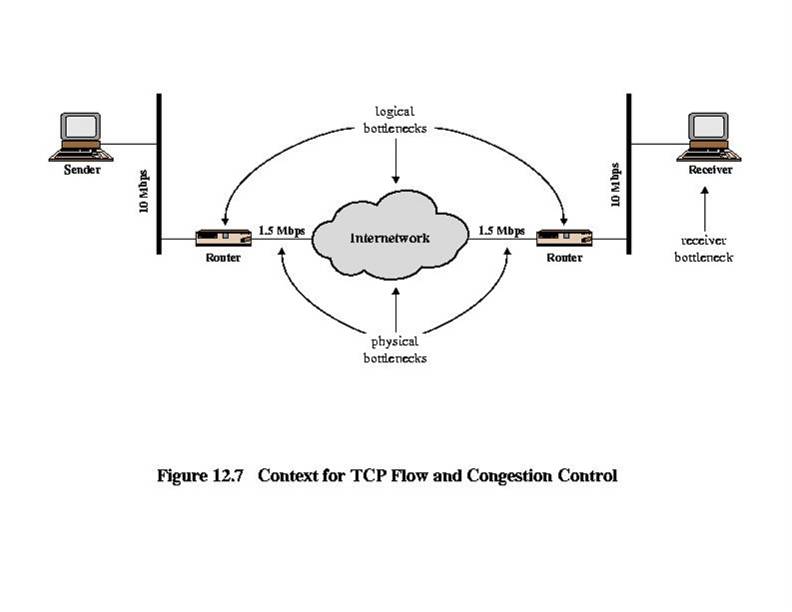
**Retransmission Timer Management**

Three Techniques to calculate retransmission timer (RTO):

* RTT Variance Estimation
* Exponential RTO Backoff
* Karn’s Algorithm

**TCP Segment Pacing**

**TCP Flow and Congestion Control**



* 1. **Explain about the Jacobson’s Algorithm.**

**Jacobson’s Algorithm**

SRTT(K + 1) = (1 – g) × SRTT(K) + g × RTT(K + 1)

SERR(K + 1) = RTT(K + 1) – SRTT(K)

SDEV(K + 1) = (1 – h) × SDEV(K) + h ×|SERR(K + 1)|

RTO(K + 1) = SRTT(K + 1) + f × SDEV(K + 1)

g = 0.125

h = 0.25

f = 2 or f = 4 (most current implementations use f = 4)

**Two Other Factors**

Jacobson’s algorithm can significantly improve TCP performance, but:

* What RTO to use for retransmitted segments?

ANSWER: exponential RTO backoff algorithm

* Which round-trip samples to use as input to Jacobson’s algorithm?

ANSWER: Karn’s algorithm

**Exponential RTO Backoff**

* Increase RTO each time the same segment retransmitted – backoff process
* Multiply RTO by constant:

RTO = q × RTO

* q = 2 is called binary exponential backoff

**Which Round-trip Samples?**

* If an ack is received for retransmitted segment, there are 2 possibilities:
* Ack is for first transmission
* Ack is for second transmission
* TCP source cannot distinguish 2 cases
* No valid way to calculate RTT:
* From first transmission to ack, or
* From second transmission to ack?
  1. **Briefly explain the types of traffic control functions used in ATM networks to maintain the promised QOS Parameter.**

**Traffic and Congestion Control in ATM Networks**

**Introduction**

* Control needed to prevent switch buffer overflow
* High speed and small cell size gives different problems from other networks
* Limited number of overhead bits
* ITU-T specified restricted initial set
  + I.371
* ATM forum Traffic Management Specification 41

**Overview**

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

**Requirements for ATM Traffic and Congestion Control**

* Most packet switched and frame relay networks carry non-real-time bursty data
  + No need to replicate timing at exit node
  + Simple statistical multiplexing
  + User Network Interface capacity slightly greater than average of channels
* Congestion control tools from these technologies do not work in ATM

**Problems with ATM Congestion Control**

* Most traffic not amenable to flow control
  + Voice & video can not stop generating
* Feedback slow
  + Small cell transmission time v propagation delay
* Wide range of applications
  + From few kbps to hundreds of Mbps
  + Different traffic patterns
  + Different network services
* High speed switching and transmission
  + Volatile congestion and traffic control

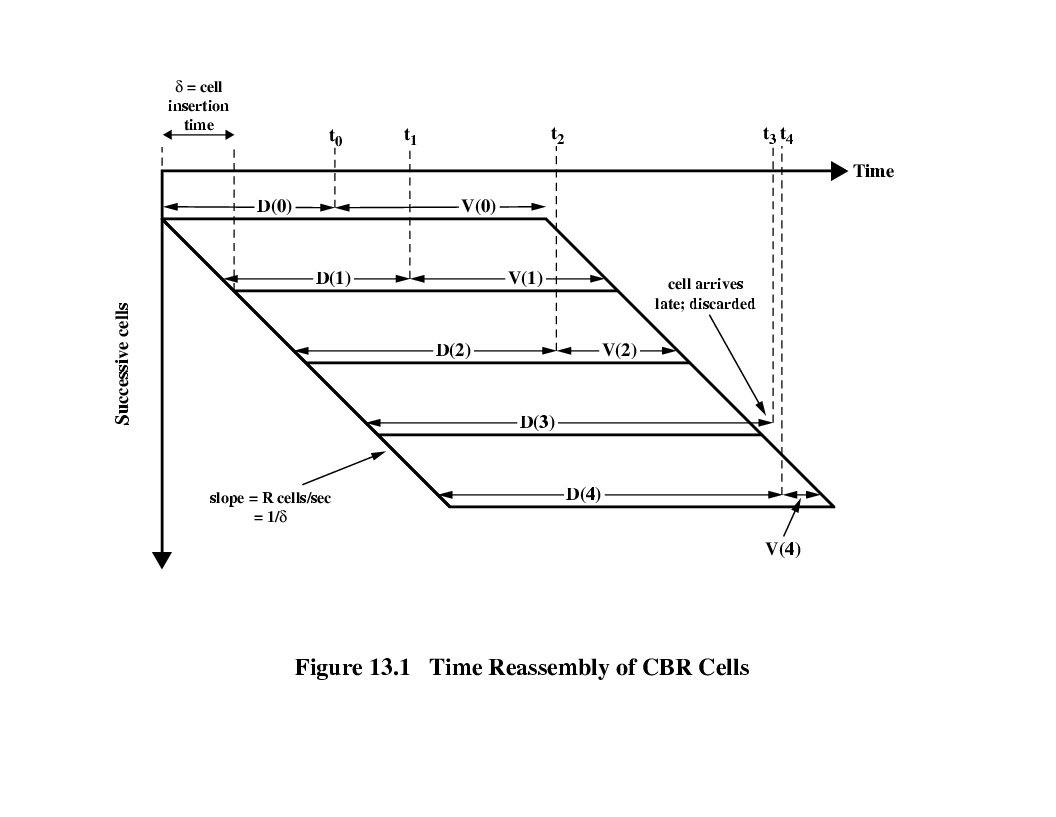
**Key Performance Issues-Latency/Speed Effects**

* E.g. data rate 150Mbps
* Takes (53 x 8 bits)/(150 x 106) =2.8 x 10-6 seconds to insert a cell
* Transfer time depends on number of intermediate switches, switching time and propagation delay. Assuming no switching delay and speed of light propagation, round trip delay of 48 x 10-3 sec across USA
* A dropped cell notified by return message will arrive after source has transmitted N further cells
* N=(48 x 10-3 seconds)/(2.8 x 10-6 seconds per cell)
* =1.7 x 104 cells = 7.2 x 106 bits
* i.e. over 7 Mbits

**Cell Delay Variation**

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

**Time Reassembly of CBR Cells**



**Network Contribution to Cell Delay Variation**

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

**Cell Delay Variation at UNI**

* Caused by processing in three layers of ATM model
  + See next slide for details
* None of these delays can be predicted
* None follow repetitive pattern
* So, random element exists in time interval between reception by ATM stack and transmission

**ATM Traffic-Related Attributes**

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

**Traffic Parameters**

* Traffic pattern of flow of cells
  + Intrinsic nature of traffic
    - Source traffic descriptor
  + Modified inside network
    - Connection traffic descriptor

**Source Traffic Descriptor**

* Peak cell rate
  + Upper bound on traffic that can be submitted
  + Defined in terms of minimum spacing between cells *T*
  + PCR = 1/*T*
  + Mandatory for CBR and VBR services
* Sustainable cell rate
  + Upper bound on average rate
  + Calculated over large time scale relative to *T*
  + Required for VBR
  + Enables efficient allocation of network resources between VBR sources
  + Only useful if SCR < PCR
* Maximum burst size
  + Max number of cells that can be sent at PCR
  + If bursts are at MBS, idle gaps must be enough to keep overall rate below SCR
  + Required for VBR
* Minimum cell rate
  + Min commitment requested of network
  + Can be zero
  + Used with ABR and GFR
  + ABR & GFR provide rapid access to spare network capacity up to PCR
  + PCR – MCR represents elastic component of data flow
  + Shared among ABR and GFR flows
* Maximum frame size
  + Max number of cells in frame that can be carried over GFR connection
  + Only relevant in GFR

**Connection Traffic Descriptor**

Includes source traffic descriptor plus:-

Cell delay variation tolerance

Amount of variation in cell delay introduced by network interface and UNI

Bound on delay variability due to slotted nature of ATM, physical layer overhead and layer functions (e.g. cell multiplexing)

Represented by time variable τ

Conformance definition

Specify conforming cells of connection at UNI

Enforced by dropping or marking cells over definition

**Quality of Service Parameters-maxCTD**

Cell transfer delay (CTD)

Time between transmission of first bit of cell at source and reception of last bit at destination

Typically has probability density function (see next slide)

Fixed delay due to propagation etc.

Cell delay variation due to buffering and scheduling

Maximum cell transfer delay (maxCTD)is max requested delay for connection

Fraction α of cells exceed threshold

Discarded or delivered late

**Peak-to-peak CDV & CLR**

Peak-to-peak Cell Delay Variation

Remaining (1-α) cells within QoS

Delay experienced by these cells is between fixed delay and maxCTD

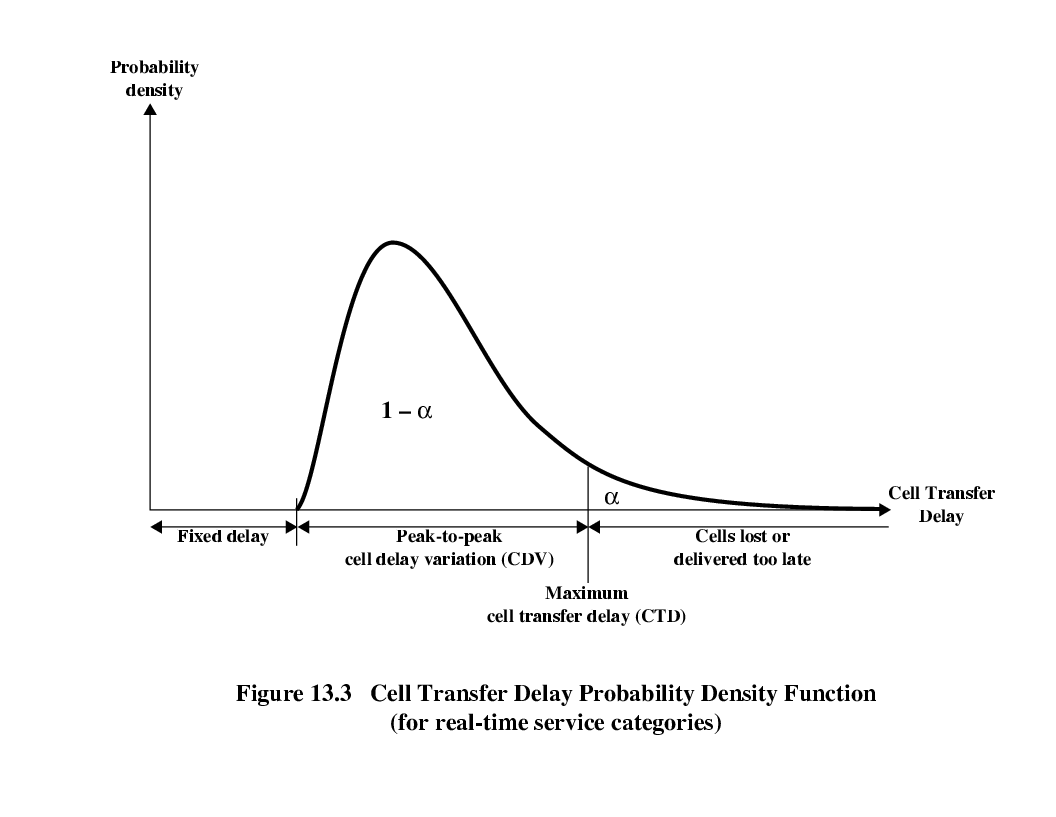
This is peak-to-peak CDV

CDVT is an upper bound on CDV

Cell loss ratio

Ratio of cells lost to cells transmitted

**Cell Transfer Delay PDF**



* 1. **Explain briefly ABR & GFR Traffic management in detail.**

**Congestion Control Attributes**

Only feedback is defined

ABR and GFR

Actions taken by network and end systems to regulate traffic submitted

ABR flow control

Adaptively share available bandwidth

**Other Attributes**

* Behaviour class selector (BCS)
  + Support for IP differentiated services (chapter 16)
  + Provides different service levels among UBR connections
  + Associate each connection with a behaviour class
  + May include queuing and scheduling
* Minimum desired cell rate

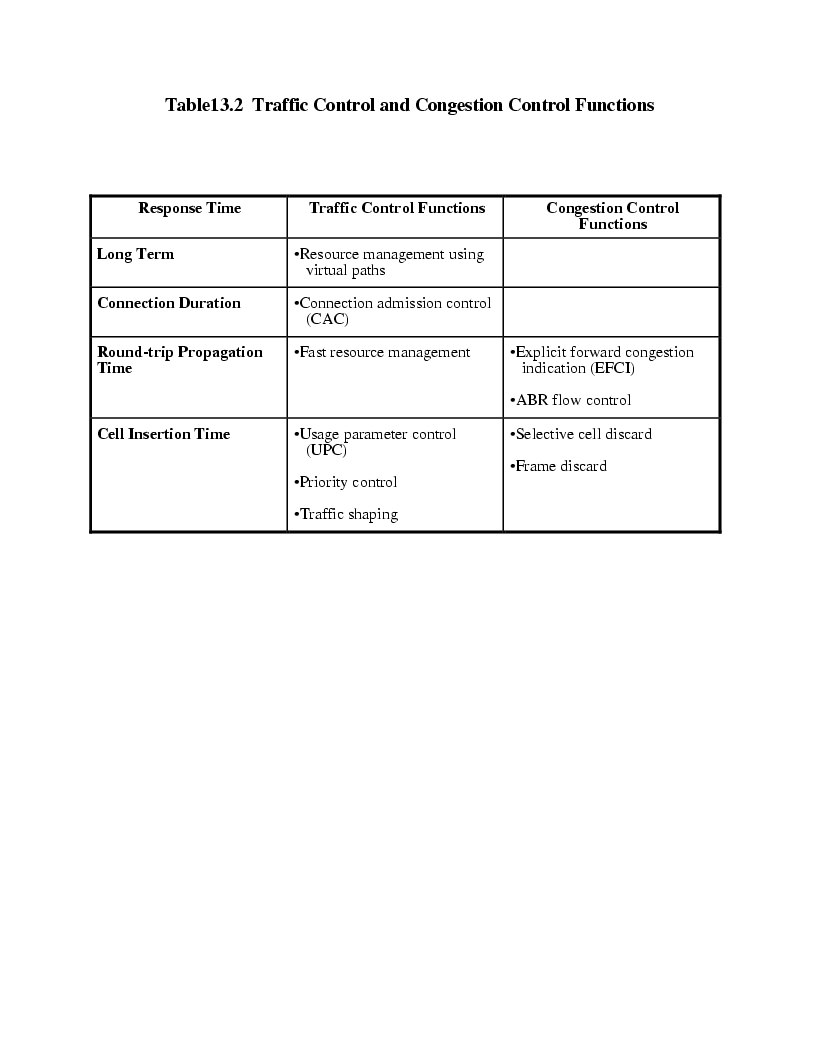
**Traffic Management Framework**

* Objectives of ATM layer traffic and congestion control
  + Support QoS for all foreseeable services
  + Not rely on network specific AAL protocols nor higher layer application specific protocols
  + Minimize network and end system complexity
  + Maximize network utilization

**Timing Levels**

* Cell insertion time
* Round trip propagation time
* Connection duration
* Long term

**Traffic Control and Congestion Functions**

****

**Traffic Control Strategy**

* Determine whether new ATM connection can be accommodated
* Agree performance parameters with subscriber
* Traffic contract between subscriber and network
* This is congestion avoidance
* If it fails congestion may occur
  + Invoke congestion control

**Traffic Control**

* Resource management using virtual paths
* Connection admission control
* Usage parameter control
* Selective cell discard
* Traffic shaping
* Explicit forward congestion indication

**Resource Management Using Virtual Paths**

* Allocate resources so that traffic is separated according to service characteristics
* Virtual path connection (VPC) are groupings of virtual channel connections (VCC)

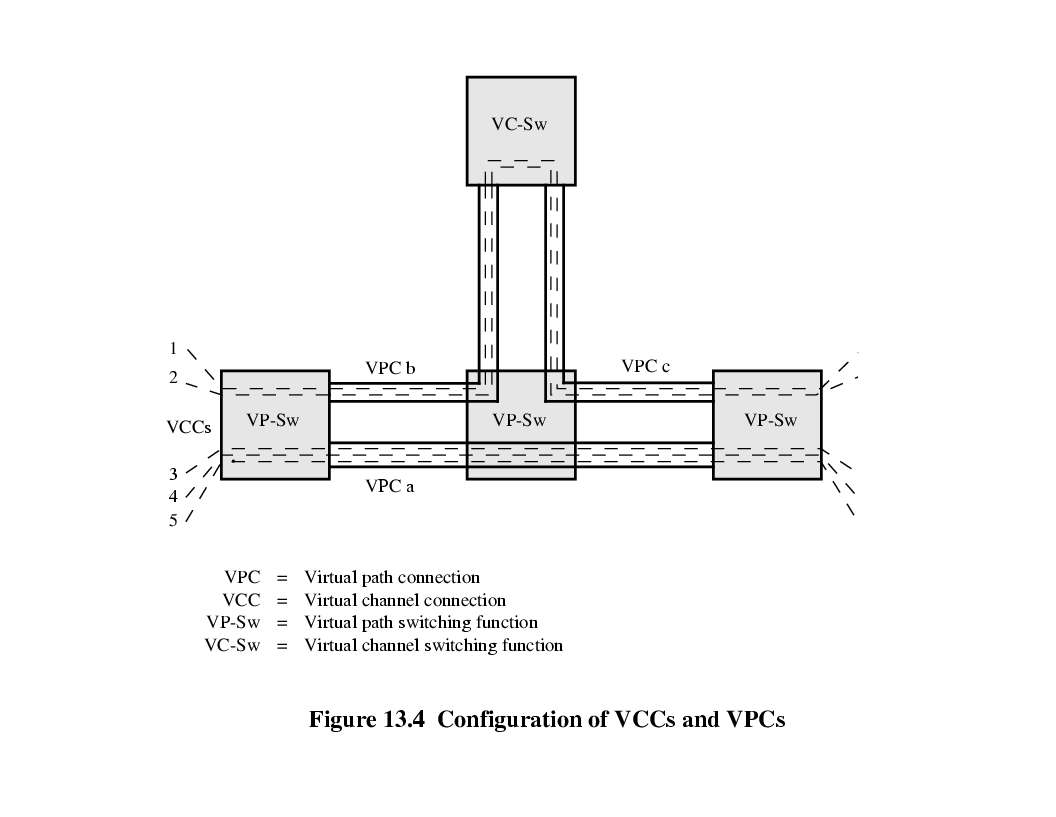
**Applications**

* User-to-user applications
  + VPC between UNI pair
  + No knowledge of QoS for individual VCC
  + User checks that VPC can take VCCs’ demands
* User-to-network applications
  + VPC between UNI and network node
  + Network aware of and accommodates QoS of VCCs
* Network-to-network applications
  + VPC between two network nodes
  + Network aware of and accommodates QoS of VCCs

**Resource Management Concerns**

* Cell loss ratio
* Max cell transfer delay
* Peak to peak cell delay variation
* All affected by resources devoted to VPC
* If VCC goes through multiple VPCs, performance depends on consecutive VPCs and on node performance
  + VPC performance depends on capacity of VPC and traffic characteristics of VCCs
  + VCC related function depends on switching/processing speed and priority

**VCCs and VPCs Configuration**



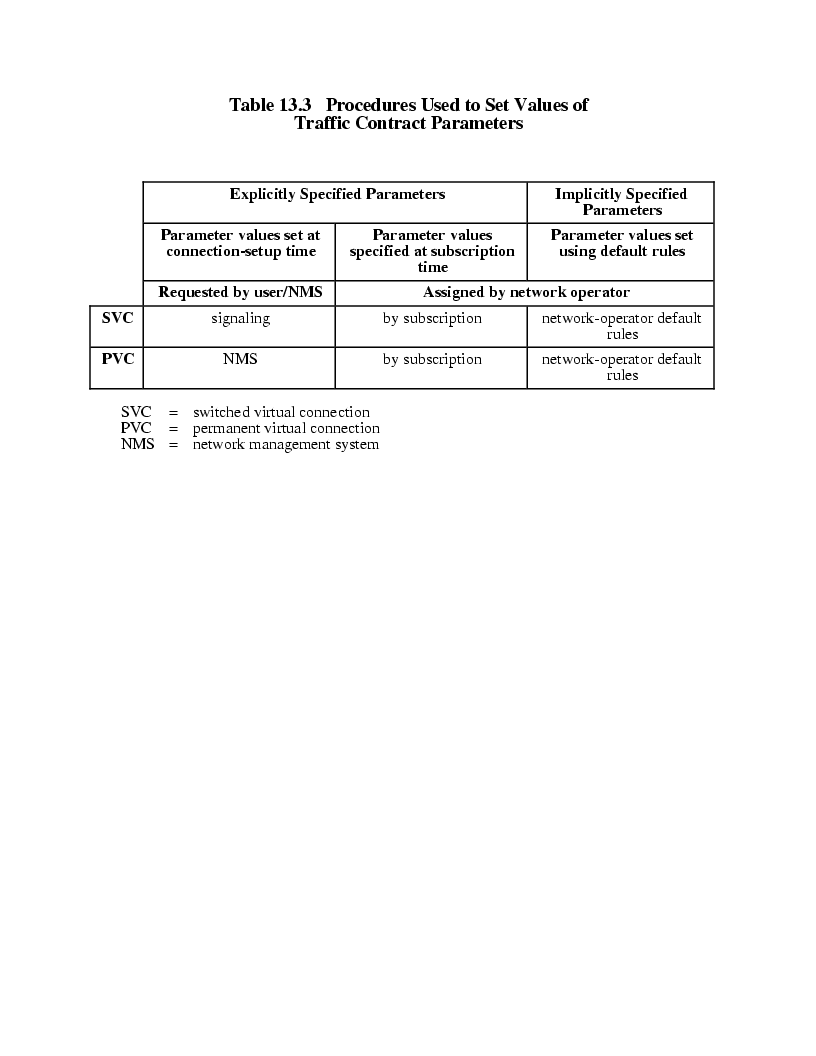
**Allocation of Capacity to VPC**

* Aggregate peak demand
  + May set VPC capacity (data rate) to total of VCC peak rates
    - Each VCC can give QoS to accommodate peak demand
    - VPC capacity may not be fully used
* Statistical multiplexing
  + VPC capacity >= average data rate of VCCs but < aggregate peak demand
  + Greater CDV and CTD
  + May have greater CLR
  + More efficient use of capacity
  + For VCCs requiring lower QoS
  + Group VCCs of similar traffic together

**Connection Admission Control**

* User must specify service required in both directions
  + Category
  + Connection traffic descriptor
    - Source traffic descriptor
    - CDVT
    - Requested conformance definition
  + QoS parameter requested and acceptable value
* Network accepts connection only if it can commit resources to support requests

**Procedures to Set Traffic Control Parameters**

****

**Cell Loss Priority**

* Two levels requested by user
  + Priority for individual cell indicated by CLP bit in header
  + If two levels are used, traffic parameters for both flows specified
    - High priority CLP = 0
    - All traffic CLP = 0 + 1
  + May improve network resource allocation

**Usage Parameter Control**

* UPC
* Monitors connection for conformity to traffic contract
* Protect network resources from overload on one connection
* Done at VPC or VCC level
* VPC level more important
  + Network resources allocated at this level

**Unit-4**

* 1. **Discuss the advantages and downsides of Integrated service architecture.**

**Integrated Services Architecture (ISA)**

* IPv4 header fields for precedence and type of service usually ignored
* ATM only network designed to support TCP, UDP and real-time traffic
* May need new installation
* Need to support Quality of Service (QoS) within TCP/IP
* Add functionality to routers
* Means of requesting QoS

**Internet Traffic – Elastic**

* Can adjust to changes in delay and throughput
* E.g. common TCP and UDP application
* E-Mail – insensitive to delay changes
* FTP – User expect delay proportional to file size
* Sensitive to changes in throughput
* SNMP – delay not a problem, except when caused by congestion
* Web (HTTP), TELNET – sensitive to delay
* Not per packet delay – total elapsed time
* E.g. web page loading time
* For small items, delay across internet dominates
* For large items it is throughput over connection
* Need some QoS control to match to demand

**Internet Traffic – Inelastic**

* Does not easily adapt to changes in delay and throughput
* Real time traffic
* Throughput
* Minimum may be required
* Delay
* E.g. stock trading
* Jitter - Delay variation
* More jitter requires a bigger buffer
* E.g. teleconferencing requires reasonable upper bound
* Packet loss

**Inelastic Traffic Problems**

* Difficult to meet requirements on network with variable queuing delays and congestion
* Need preferential treatment
* Applications need to state requirements
* Ahead of time (preferably) or on the fly
* Using fields in IP header
* Resource reservation protocol
* Must still support elastic traffic
* Deny service requests that leave too few resources to handle elastic traffic demands

**ISA Approach**

* Provision of QoS over IP
* Sharing available capacity when congested
* Router mechanisms
* Routing Algorithms
* Select to minimize delay
* Packet discard
* Causes TCP sender to back off and reduce load
* Enahnced by ISA

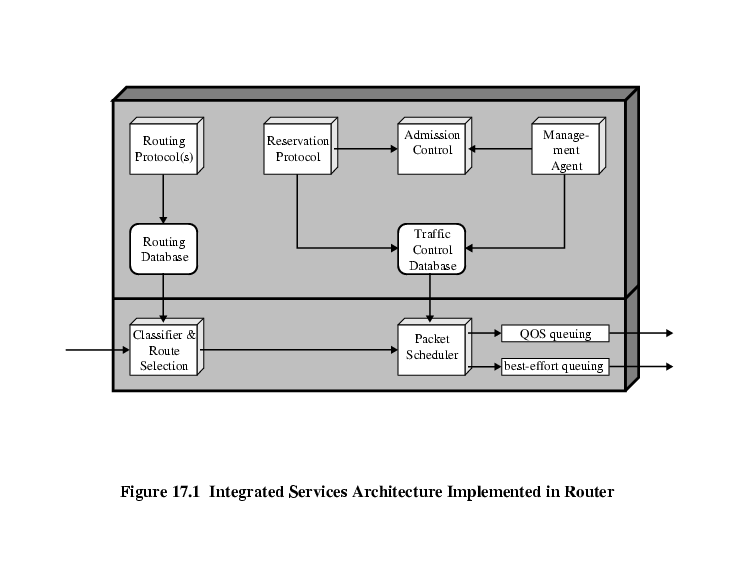
**Flow**

* IP packet can be associated with a flow
* Distinguishable stream of related IP packets
* From single user activity
* Requiring same QoS
* E.g. one transport connection or one video stream
* Unidirectional
* Can be more than one recipient
* Multicast
* Membership of flow identified by source and destination IP address, port numbers, protocol type
* IPv6 header flow identifier can be used but isnot necessarily equivalent to ISA flow

**ISA Functions**

* Admission control
* For QoS, reservation required for new flow
* RSVP used
* Routing algorithm
* Base decision on QoS parameters
* Queuing discipline
* Take account of different flow requirements
* Discard policy
* Manage congestion
* Meet QoS

**ISA Implementation in Router**

* Background Functions
*  Forwarding functions

**ISA Components – Background Functions**

* Reservation Protocol-RSVP
* Admission control
* Management agent-Can use agent to modify traffic control database and direct admission control
* Routing protocol

**ISA Components – Forwarding**

* Classifier and route selection
* Incoming packets mapped to classes
* Single flow or set of flows with same QoS
* E.g. all video flows
* Based on IP header fields
* Determines next hop
* Packet scheduler
* Manages one or more queues for each output
* Order queued packets sent
* Based on class, traffic control database, current and past activity on outgoing port
* Policing

**2.Briefly discuss the various Queuing disciplines of Integrated services.**

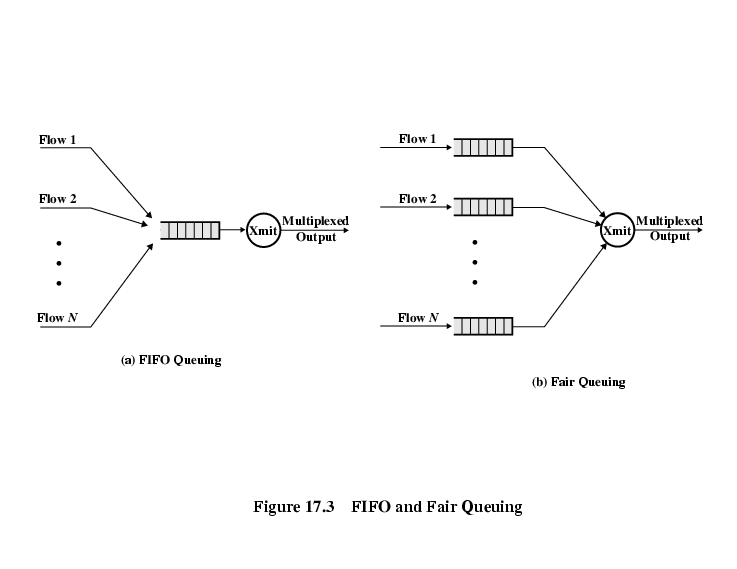
**Queuing Discipline**

* Traditionally first in first out (FIFO) or first come first served (FCFS) at each router port
* No special treatment to high priority packets (flows)
* Small packets held up by large packets ahead of them in queue
* Larger average delay for smaller packets
* Flows of larger packets get better service
* Greedy TCP connection can crowd out altruistic connections
* If one connection does not back off, others may back off more

**Fair Queuing (FQ)**

* Multiple queues for each port
* One for each source or flow
* Queues services round robin
* Each busy queue (flow) gets exactly one packet per cycle
* Load balancing among flows
* No advantage to being greedy
* Your queue gets longer, increasing your delay
* Short packets penalized as each queue sends one packet per cycle

**FIFO and FQ**



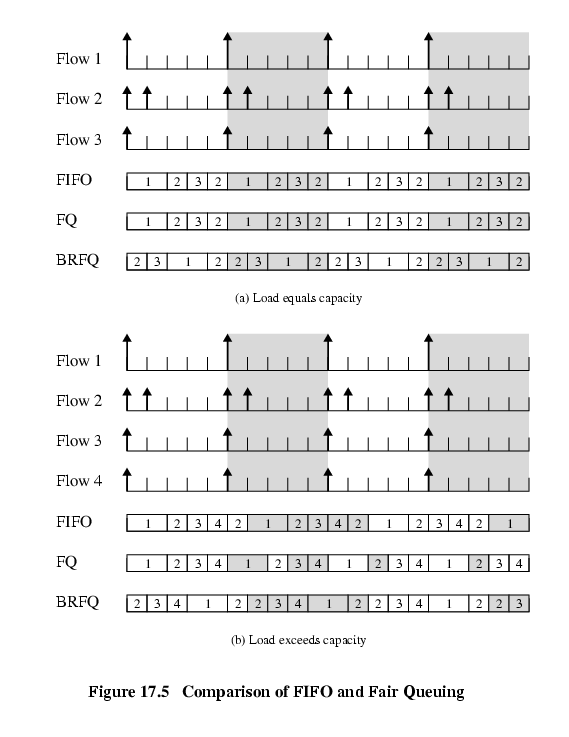
**Processor Sharing**

* Multiple queues as in FQ
* Send one bit from each queue per round
* Longer packets no longer get an advantage
* Can work out virtual (number of cycles) start and finish time for a given packet
* However, we wish to send packets, not bits

**Bit-Round Fair Queuing (BRFQ)**

* Compute virtual start and finish time as before
* When a packet finished, the next packet sent is the one with the earliest virtual finish time
* Good approximation to performance of PS
* Throughput and delay converge as time increases

**Comparison of FIFO, FQ and BRFQ**



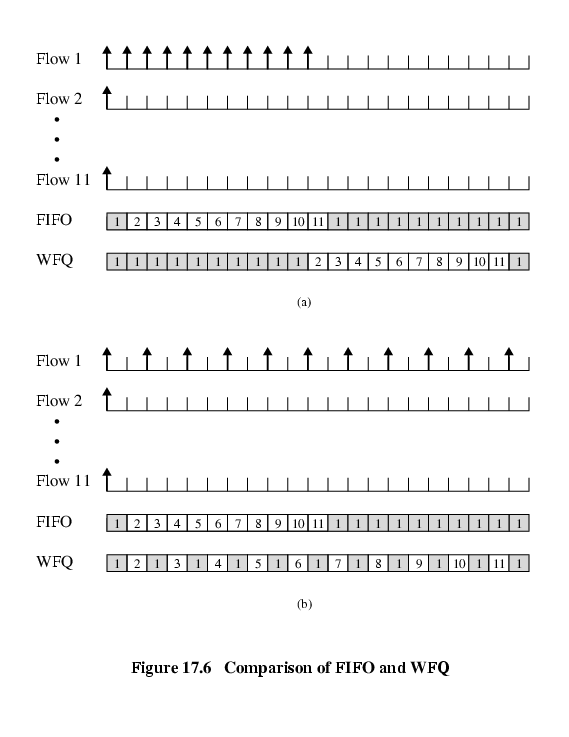
**Generalized Processor Sharing (GPS)**

* BRFQ can not provide different capacities to different flows
* Enhancement called Weighted fair queue (WFQ)
* From PS, allocate weighting to each flow that determines how many bots are sent during each round
* If weighted 5, then 5 bits are sent per round
* Gives means of responding to different service requests
* Guarantees that delays do not exceed bounds

**Weighted Fair Queue**

* Emulates bit by bit GPS
* Same strategy as BRFQ

**FIFO v WFQ**



1. **Discuss the benefits of Random Early Detection algorithm**

**Random Early Detection (RED)  
Motivation**

* Surges fill buffers and cause discards
* On TCP this is a signal to enter slow start phase, reducing load
* Lost packets need to be resent
* Adds to load and delay
* Global synchronization
* Traffic burst fills queues so packets lost
* Many TCP connections enter slow start
* Traffic drops so network under utilized
* Connections leave slow start at same time causing burst
* Bigger buffers do not help
* Try to anticipate onset of congestion and tell one connection to slow down

**RED Design Goals**

* Congestion avoidance
* Global synchronization avoidance
* Current systems inform connections to back off implicitly by dropping packets
* Avoidance of bias to bursty traffic
* Discard arriving packets will do this
* Bound on average queue length
* Hence control on average delay

**RED Algorithm – Overview**

Calculate average queue size avg

if avg < THmin

queue packet

else if THmin ≤ avg < Thmax

calculate probability Pa

with probability Pa

discard packet

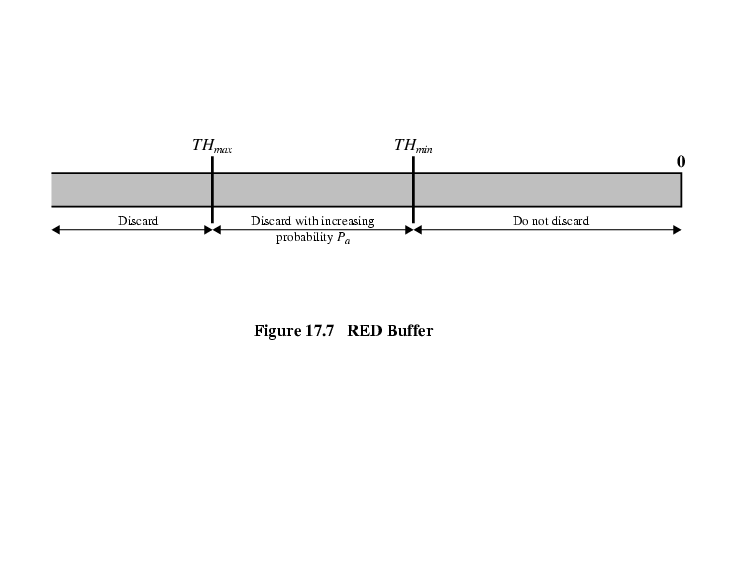
else with probability 1-Pa

queue packet

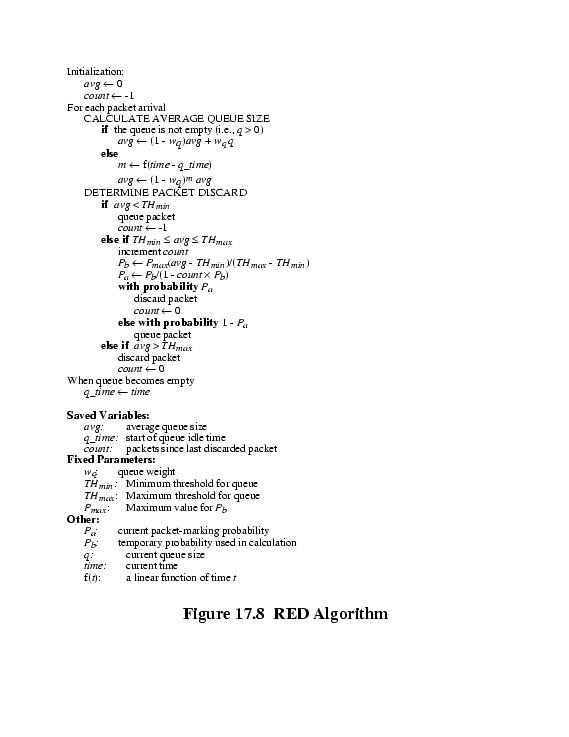
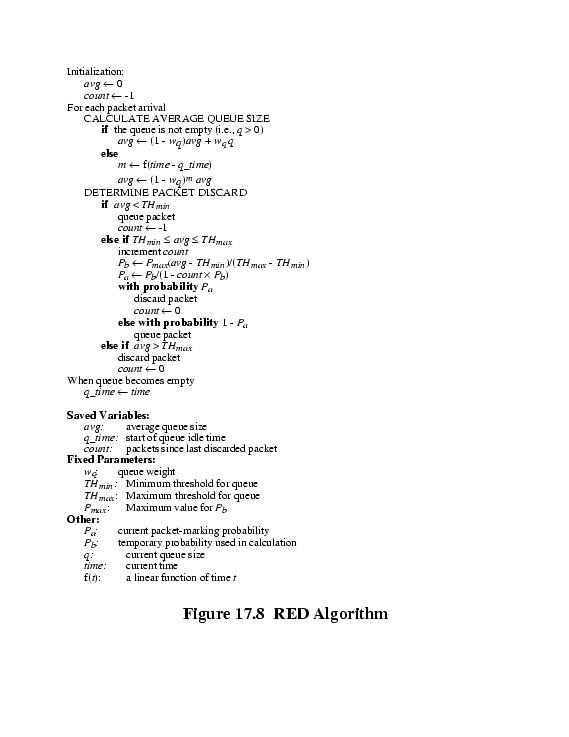
else if avg ≥ THmax

discard packet

**RED Buffer**



**RED Algorithm Detail**



1. **Explain the Differentiated service architecture in detail.**

**Differentiated Services (DS)**

* ISA and RSVP complex to deploy
* May not scale well for large volumes of traffic
* Amount of control signals
* Maintenance of state information at routers
* DS architecture designed to provide simple, easy to implement, low overhead tool
* Support range of network services
* Differentiated on basis of performance

**Characteristics of DS**

* Use IPv4 header Type of Service or IPv6 Traffic Class field
* No change to IP
* Service level agreement (SLA) established between provider (internet domain) and customer prior to use of DS
* DS mechanisms not needed in applications
* Build in aggregation
* All traffic with same DS field treated same
* E.g. multiple voice connections
* DS implemented in individual routers by queuing and forwarding based on DS field
* State information on flows not saved by routers

**Services**

* Provided within DS domain
* Contiguous portion of Internet over which consistent set of DS policies administered
* Typically under control of one administrative entity
* Defined in SLA
* Customer may be user organization or other DS domain
* Packet class marked in DS field
* Service provider configures forwarding policies routers
* Ongoing measure of performance provided for each class
* DS domain expected to provide agreed service internally
* If destination in another domain, DS domain attempts to forward packets through other domains
* Appropriate service level requested from each domain

**SLA Parameters**

* Detailed service performance parameters
* Throughput, drop probability, latency
* Constraints on ingress and egress points
* Indicate scope of service
* Traffic profiles to be adhered to
* Token bucket
* Disposition of traffic in excess of profile

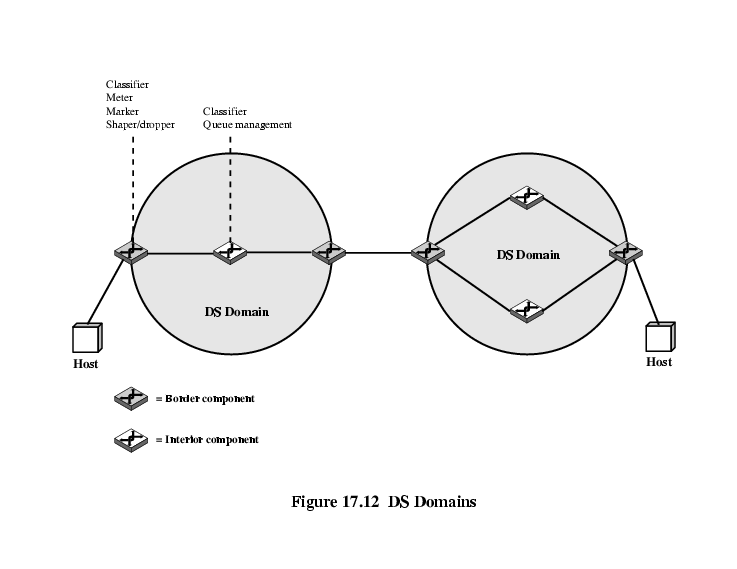
**Example Services**

* Qualitative
* A: Low latency
* B: Low loss
* Quantitative
* C: 90% in-profile traffic delivered with no more than 50ms latency
* D: 95% in-profile traffic delivered
* Mixed
* E: Twice bandwidth of F
* F: Traffic with drop precedence X has higher delivery probability than that with drop precedence Y

DS Field Detail

* Leftmost 6 bits are DS codepoint
* 64 different classes available
* 3 pools
* xxxxx0 : reserved for standards
* 000000 : default packet class
* xxx000 : reserved for backwards compatibility with IPv4 TOS
* xxxx11 : reserved for experimental or local use
* xxxx01 : reserved for experimental or local use but may be allocated for future standards if needed
* Rightmost 2 bits unused

**Configuration Diagram**

****

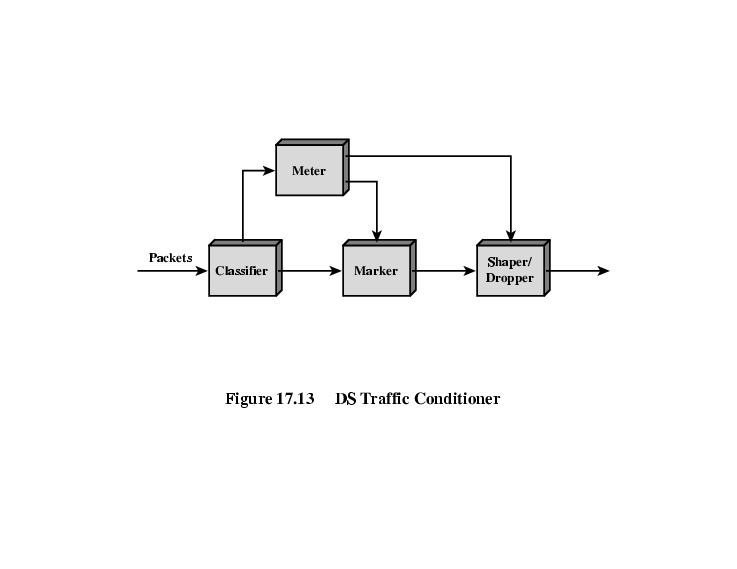
**Configuration – Interior Routers**

* Domain consists of set of contiguous routers
* Interpretation of DS codepoints within domain is consistent
* Interior nodes (routers) have simple mechanisms to handle packets based on codepoints
* Queuing gives preferential treatment depending on codepoint
* Per Hop behaviour (PHB)
* Must be available to all routers
* Typically the only part implemented in interior routers
* Packet dropping rule dictated which to drop when buffer saturated

**Configuration – Boundary Routers**

* Include PHB rules
* Also traffic conditioning to provide desired service
* Classifier
* Separate packets into classes
* Meter
* Measure traffic for conformance to profile
* Marker
* Policing by remarking codepoints if required
* Shaper
* Dropper

**DS Traffic Conditioner**

****

**Per Hop Behaviour –  
Expedited forwarding**

* Premium service
* Low loss, delay, jitter; assured bandwidth end-to-end service through domains
* Looks like point to point or leased line
* Difficult to achieve
* Configure nodes so traffic aggregate has well defined minimum departure rate
* EF PHB
* Condition aggregate so arrival rate at any node is always less that minimum departure rate
* Boundary conditioners

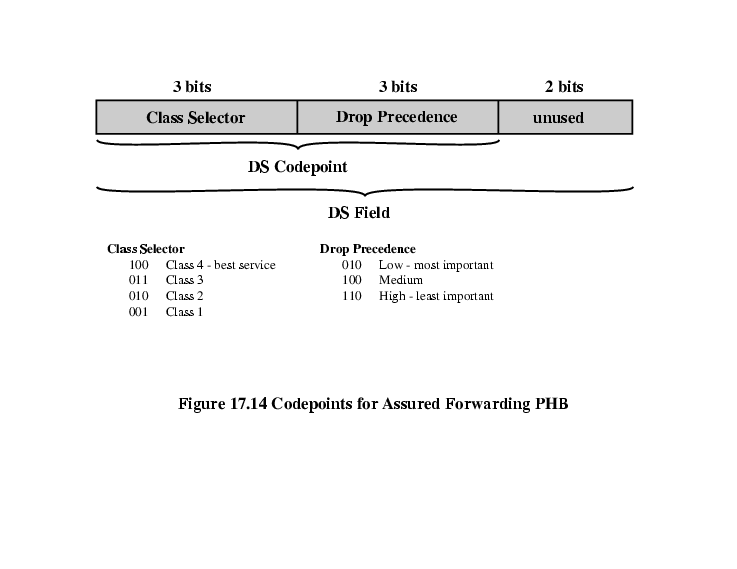
**Per Hop Behaviour –Explicit Allocation**

* Superior to best efforts
* Does not require reservation of resources
* Does not require detailed discrimination among flows
* Users offered choice of number of classes
* Monitored at boundary node
* In or out depending on matching profile or not
* Inside network all traffic treated as single pool of packets, distinguished only as in or out
* Drop out packets before in packets if necessary
* Different levels of service because different number of in packets for each user

**PHB - Assured Forwarding**

* Four classes defined
* Select one or more to meet requirements
* Within class, packets marked by customer or provider with one of three drop precedence values
* Used to determine importance when dropping packets as result of congestion

**Codepoints for AF PHB**

****

**Unit-5**

* 1. Explain the Following

**RSVP**

**Resource ReSerVation Protocol (RSVP) Design Goals**

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

**RSVP Characteristics**

* Unicast and Multicast
* Simplex
  + Unidirectional data flow
  + Separate reservations in two directions
* Receiver initiated
  + Receiver knows which subset of source transmissions it wants
* Maintain soft state in internet
  + Responsibility of end users
* Providing different reservation styles
  + Users specify how reservations for groups are aggregated
* Transparent operation through non-RSVP routers
* Support IPv4 (ToS field) and IPv6 (Flow label field)

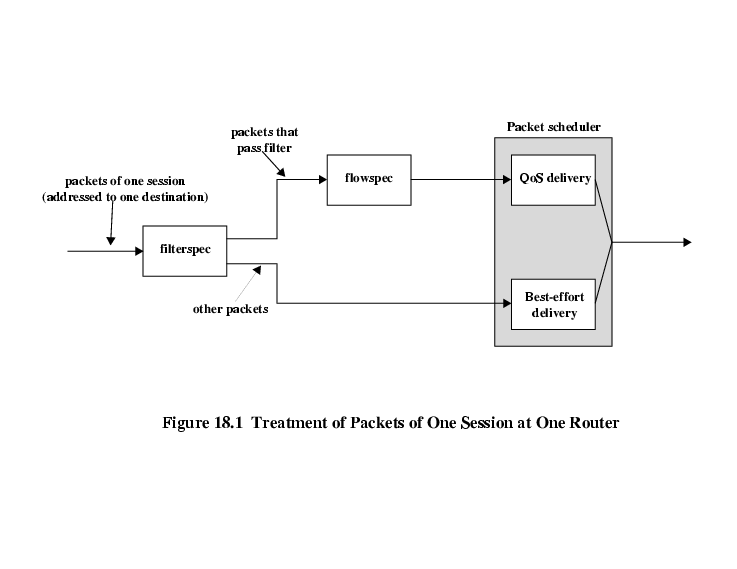
**Data Flows - Session**

* Data flow identified by destination
* Resources allocated by router for duration of session
* Defined by
  + Destination IP address
    - Unicast or multicast
  + IP protocol identifier
    - TCP, UDP etc.
  + Destination port
    - May not be used in multicast

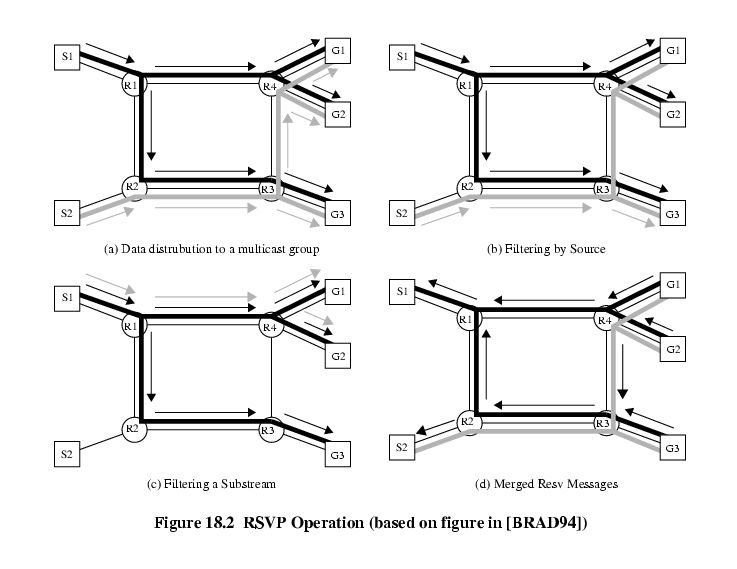
**Flow Descriptor**

* Reservation Request
  + Flow spec
    - Desired QoS
    - Used to set parameters in node’s packet scheduler
    - Service class, Rspec (reserve), Tspec (traffic)
  + Filter spec
    - Set of packets for this reservation
    - Source address, source prot

**Treatment of Packets of One Session at One Router**

****

**RSVP Operation Diagram**

****

**RSVP Operation**

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

**Filtering**

* G3 has reservation filter spec including S1 and S2
* G1, G2 from S1 only
* R3 delivers from S2 to G3 but does not forward to R4
* G1, G2 send RSVP request with filter excluding S2
* G1, G2 only members of group reached through R4
  + R4 doesn’t need to forward packets from this session
  + R4 merges filter spec requests and sends to R3
* R3 no longer forwards this session’s packets to R4
  + Handling of filtered packets not specified
  + Here they are dropped but could be best efforts delivery
* R3 needs to forward to G3
  + Stores filter spec but doesn’t propagate it
  1. **Explain the Following**

**MPLS**

**MPLS**

**Multiprotocol Label Switching (MPLS)**

* Routing algorithms provide support for performance goals
  + Distributed and dynamic
    - React to congestion
    - Load balance across network
  + Based on metrics
    - Develop information that can be used in handling different service needs
* Enhancements provide direct support
  + IS, DS, RSVP
* Nothing directly improves throughput or delay
* MPLS tries to match ATM QoS support

**Background**

* Efforts to marry IP and ATM
* IP switching (Ipsilon)
* Tag switching (Cisco)
* Aggregate route based IP switching (IBM)
* Cascade (IP navigator)
* All use standard routing protocols to define paths between end points
* Assign packets to path as they enter network
* Use ATM switches to move packets along paths
  + ATM switching (was) much faster than IP routers
  + Use faster technology

**Developments**

* IETF working group in 1997, proposed standard 2001
* Routers developed to be as fast as ATM switches
  + Remove the need to provide both technologies in same network
* MPLS does provide new capabilities
  + QoS support
  + Traffic engineering
  + Virtual private networks
  + Multiprotocol support

**Connection Oriented QoS Support**

* Guarantee fixed capacity for specific applications
* Control latency/jitter
* Ensure capacity for voice
* Provide specific, guaranteed quantifiable SLAs
* Configure varying degrees of QoS for multiple customers
* MPLS imposes connection oriented framework on IP based internets

**Traffic Engineering**

* Ability to dynamically define routes, plan resource commitments based on known demands and optimize network utilization
* Basic IP allows primitive traffic engineering
  + E.g. dynamic routing
* MPLS makes network resource commitment easy
  + Able to balance load in face of demand
  + Able to commit to different levels of support to meet user traffic requirements
  + Aware of traffic flows with QoS requirements and predicted demand
  + Intelligent re-routing when congested

**VPN Support**

* Traffic from a given enterprise or group passes transparently through an internet
* Segregated from other traffic on internet
* Performance guarantees
* Security

**Multiprotocol Support**

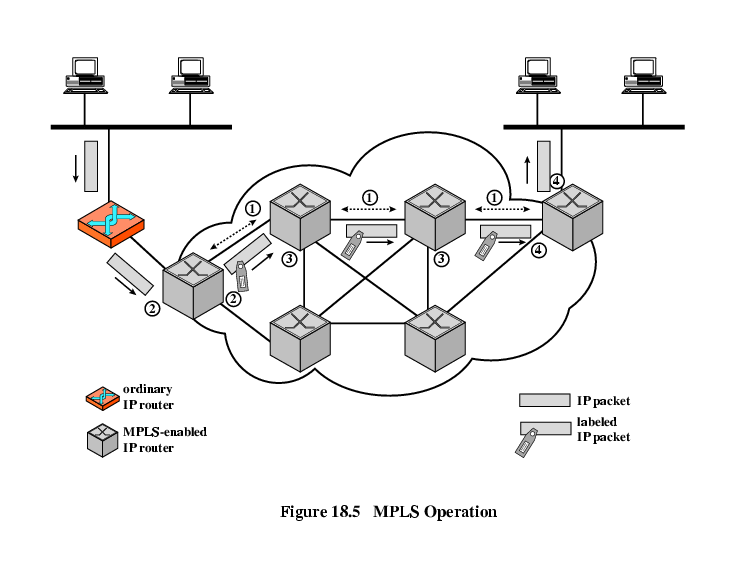
* MPLS can be used on different network technologies
* IP
  + Requires router upgrades
    - Coexist with ordinary routers
* ATM
  + Enables and ordinary switches co-exist
* Frame relay
  + Enables and ordinary switches co-exist
* Mixed network

**MPLS Terminology**

**MPLS Operation**

* Label switched routers capable of switching and routing packets based on label appended to packet
* Labels define a flow of packets between end points or multicast destinations
* Each distinct flow (forward equivalence class – FEC) has specific path through LSRs defined
  + Connection oriented
* Each FEC has QoS requirements
* IP header not examined
  + Forward based on label value

**MPLS Operation Diagram**

****

**Explanation – Setup**

* Labelled switched path established prior to routing and delivery of packets
* QoS parameters established along path
  + Resource commitment
  + Queuing and discard policy at LSR
  + Interior routing protocol e.g. OSPF used
  + Labels assigned
    - Local significance only
    - Manually or using Label distribution protocol (LDP) or enhanced version of RSVP

**Explanation – Packet Handling**

* Packet enters domain through edge LSR
  + Processed to determine QoS
* LSR assigns packet to FEC and hence LSP
  + May need co-operation to set up new LSP
* Append label
* Forward packet
* Within domain LSR receives packet
* Remove incoming label, attach outgoing label and forward
* Egress edge strips label, reads IP header and forwards

**Notes**

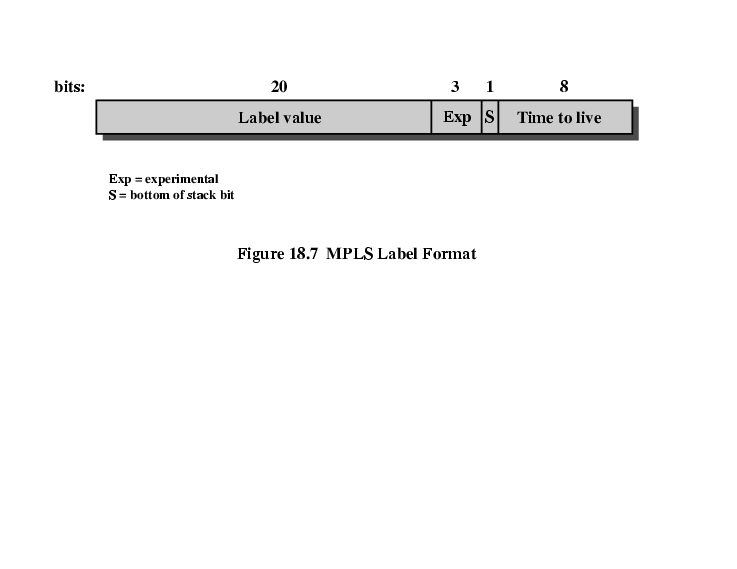
* MPLS domain is contiguous set of MPLS enabled routers
* Traffic may enter or exit via direct connection to MPLS router or from non-MPLS router
* FEC determined by parameters, e.g.
  + Source/destination IP address or network IP address
  + Port numbers
  + IP protocol id
  + Differentiated services codepoint
  + IPv6 flow label
* Forwarding is simple lookup in predefined table
  + Map label to next hop
* Can define PHB at an LSR for given FEC
* Packets between same end points may belong to different FEC

**MPLS Packet Forwarding**

**Label Stacking**

* Packet may carry number of labels
* LIFO (stack)
  + Processing based on top label
  + Any LSR may push or pop label
    - Unlimited levels
  + Allows aggregation of LSPs into single LSP for part of route
  + C.f. ATM virtual channels inside virtual paths
  + E.g. aggregate all enterprise traffic into one LSP for access provider to handleReduces size of tables

**Label Format Diagram**

****

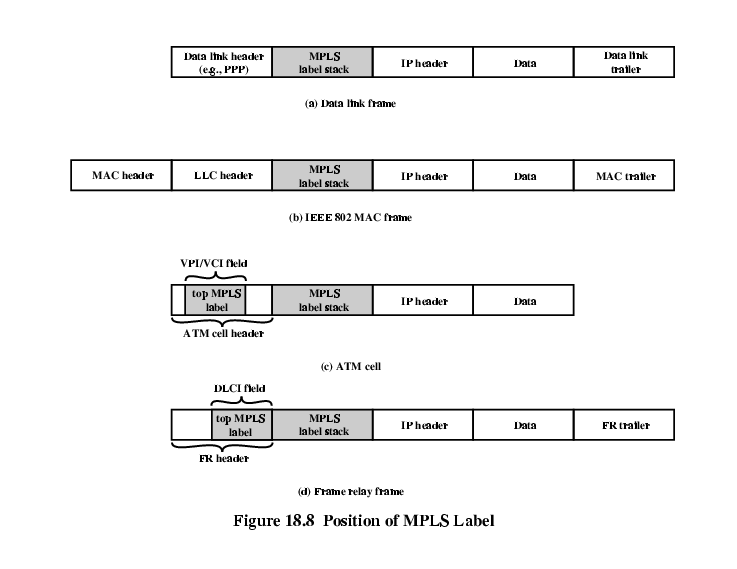
**Time to Live Processing**

* Needed to support TTL since IP header not read
* First label TTL set to IP header TTL on entry to MPLS domain
* TTL of top entry on stack decremented at internal LSR
  + If zero, packet dropped or passed to ordinary error processing (e.g. ICMP)
  + If positive, value placed in TTL of top label on stack and packet forwarded
* At exit from domain, (single stack entry) TTL decremented
  + If zero, as above
  + If positive, placed in TTL field of Ip header and

**Label Stack**

* Appear after data link layer header, before network layer header
* Top of stack is earliest (closest to network layer header)
* Network layer packet follows label stack entry with S=1
* Over connection oriented services
  + Topmost label value in ATM header VPI/VCI field
    - Facilitates ATM switching
  + Top label inserted between cell header and IP header
  + In DLCI field of Frame Relay
  + Note: TTL problem

**Position of MPLS Label Stack**



* 1. **Explain the Following**

**RTP**

**Real Time Transport Protocol**

* TCP not suited to real time distributed application
  + Point to point so not suitable for multicast
  + Retransmitted segments arrive out of order
  + No way to associate timing with segments
* UDP does not include timing information nor any support for real time applications
* Solution is real-time transport protocol RTP

**RTP Architecture**

* Close coupling between protocol and application layer functionality
  + Framework for application to implement single protocol
* Application level framing
* Integrated layer processing

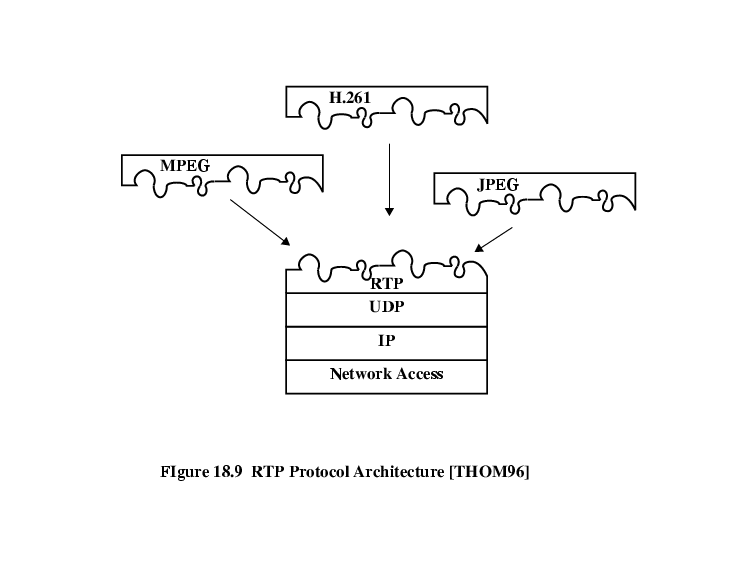
**Application Level Framing**

* Recovery of lost data done by application rather than transport layer
  + Application may accept less than perfect delivery
    - Real time audio and video
    - Inform source about quality of delivery rather than retransmit
    - Source can switch to lower quality
  + Application may provide data for retransmission
    - Sending application may recompute lost values rather than storing them
    - Sending application can provide revised values
    - Can send new data to “fix” consequences of loss
* Lower layers deal with data in units provided by application
  + Application data units (ADU)

**Integrated Layer Processing**

* Adjacent layers in protocol stack tightly coupled
* Allows out of order or parallel functions from different layers

**RTP Architecture Diagram**



**RTP Data Transfer Protocol**

* Transport of real time data among number of participants in a session, defined by:
  + RTP Port number
    - UDP destination port number if using UDP
  + RTP Control Protocol (RTCP) port number
    - Destination port address used by all participants for RTCP transfer
  + IP addresses
    - Multicast or set of unicast

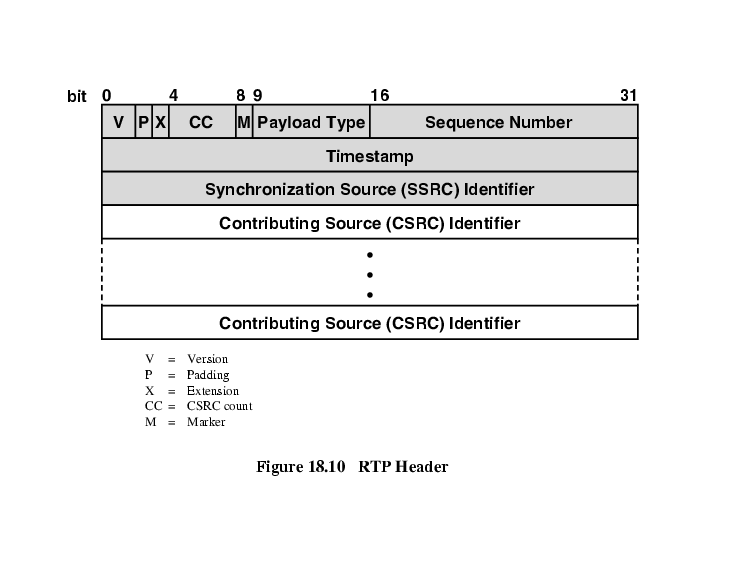
**Multicast Support**

* Each RTP data unit includes:
* Source identifier
* Timestamp
* Payload format

**Relays**

* Intermediate system acting as receiver and transmitter for given protocol layer
* Mixers
  + Receives streams of RTP packets from one or more sources
  + Combines streams
  + Forwards new stream
* Translators
  + Produce one or more outgoing RTP packets for each incoming packet
  + E.g. convert video to lower quality

**RTP Header**

****

* 1. **Explain in detail about RTCP.**

**RTP Control Protocol (RTCP)**

* RTP is for user data
* RTCP is multicast provision of feedback to sources and session participants
* Uses same underlying transport protocol (usually UDP) and different port number
* RTCP packet issued periodically by each participant to other session members

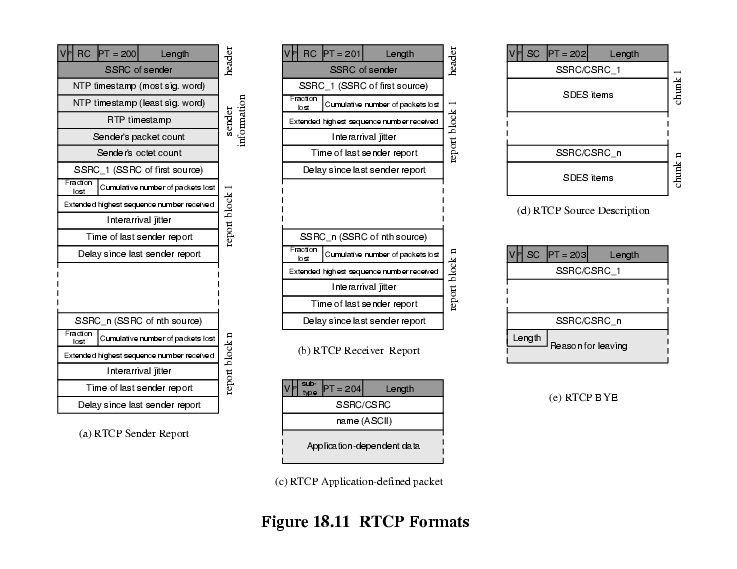
**RTCP Functions**

* QoS and congestion control
* Identification
* Session size estimation and scaling
* Session control

**RTCP Transmission**

* Number of separate RTCP packets bundled in single UDP datagram
  + Sender report
  + Receiver report
  + Source description
  + Goodbye
  + Application specific

**RTCP Packet Formats**



**Packet Fields (All Packets)**

* Version (2 bit) currently version 2
* Padding (1 bit) indicates padding bits at end of control information, with number of octets as last octet of padding
* Count (5 bit) of reception report blocks in SR or RR, or source items in SDES or BYE
* Packet type (8 bit)
* Length (16 bit) in 32 bit words minus 1
* In addition Sender and receiver reports have:
* Synchronization Source Identifier

**Packet Fields (Sender Report)  
Sender Information Block**

* NTP timestamp: absolute wall clock time when report sent
* RTP Timestamp: Relative time used to create timestamps in RTP packets
* Sender’s packet count (for this session)
* Sender’s octet count (for this session)

**Packet Fields (Sender Report)  
Reception Report Block**

* SSRC\_n (32 bit) identifies source refered to by this report block
* Fraction lost (8 bits) since previous SR or RR
* Cumulative number of packets lost (24 bit) during this session
* Extended highest sequence number received (32 bit)
* Least significant 16 bits is highest RTP data sequence number received from SSRC\_n
* Most significant 16 bits is number of times sequence number has wrapped to zero
* Interarrival jitter (32 bit)
* Last SR timestamp (32 bit)
* Delay since last SR (32 bit)

**Receiver Report**

* Same as sender report except:
* Packet type field has different value
* No sender information block

**Source Description Packet**

* Used by source to give more information
* 32 bit header followed by zero or more additional information chunks
* E.g.:
* 0 END End of SDES list
* 1 CNAME Canonical name
* 2 NAME Real user name of source
* 3 EMAIL Email address

**Goodbye (BYE)**

* Indicates one or more sources no linger active
* Confirms departure rather than failure of network

**Application Defined Packet**

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