CHAPTER 1
ATM TRAFFIC MANAGEMENT

Webster's New World Dictionary defines congestion as "filled to excess, or overcrowded; for example, highway congestion". Although, the best solution of congestion is to simply avoid situations where and when congestion is likely to occur, this strategy isn't always possible. Unfortunately, congestion occurs in many real world networking environments because there is always a bottleneck of some sort – a slow computer, a low-speed link, or an intermediate switch with low throughput.

First, this chapter introduces the definition, causes and effects of the network congestion. Congestion control and its categories are also discussed. Then, the details of ATM traffic management are presented. The chapter ends with a brief introduction to ATM service classes.

1.1 INTRODUCTION

1.1.1 Network Congestion: Definition, Causes and Effects

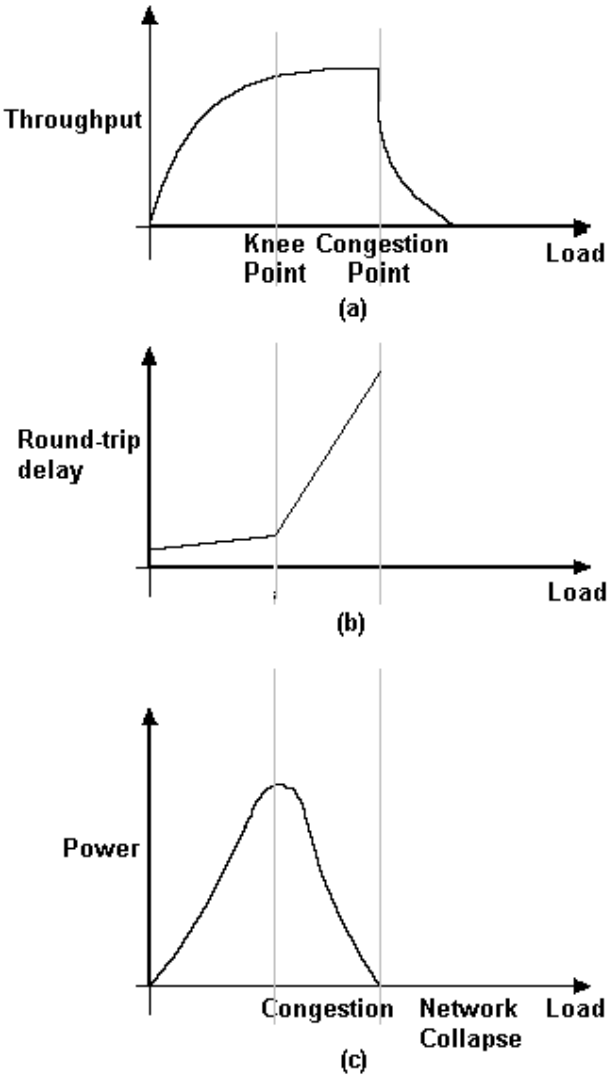

Figure 1.1: Network performance vs. offered traffic load.

(a) Throughput versus load, **(b)** Round-trip delay versus load, and **(c)** Power versus load.

Congestion in a network is a state in which performance degrades due to the saturation of network resources such as communication links, processor cycles, and memory buffers. Network congestion has been well recognized as a *resource-sharing problem*. In a packet-switched network, resources are shared among all the hosts attached to it, including switch processors, communication channels, and buffer spaces. These three driving forces of data transmission in network communication can also be potential bottlenecks that cause

congestion in the network. On the one hand, networks need to serve all user requests for data transmission, which are often unpredictable and bursty with regard to transmission starting time, rate, and size. On the other hand, any physical resource in the network has a finite capacity, and must be managed for sharing among different transmissions.

Consequently, network congestion will result if the resources in the network cannot meet all of the users' current demands. In simple terms, if, for any time interval, the total sum of demands on a resource is more than its available capacity, the resource is said to be congested for that interval. Mathematically speaking:

$$\text{Demand} > \text{Available Resources}$$

Adverse effects resulting from such congestion include the long delay of message delivery, waste of system resources, and possible network collapse, when all communication in the entire network ceases.

A more formal and quantitative definition for network congestion is based on the performance behavior of a network. Figure 1.1(a) shows the throughput-load relationship in a packet-switching network [1,2]. We see that, as the load is small and within the subnet carrying capacity, network throughput generally keeps up with the increase of the load until the offered load reaches to the knee point, where the increase of the throughput becomes much slower than the increase of the load. If the load keeps increasing up to the capacity of the network, the queues on switching nodes will build up, potentially resulting in packets being dropped, and throughput will eventually arrive at its maximum and then decrease sharply to a low value (possibly zero). It is at this point that the network is said to be congested. Figures 1.1(b) and 1.1(c) illustrate the relationships between the round-trip delay, and the resource power with respect to the offered load. The delay (or response time) curve follows a similar pattern as the throughput curve. At first, the response time rises slowly with the load due to the fast increment of the throughput. Then after the knee point is reached, the delay curve jumps significantly while the throughput stays flat. Finally, the delay grows indefinitely when the network becomes congested. The resource power is defined as the ratio of the throughput to the response time. The resource power gets to its maximum value at the knee point, where the average queue size is close to one, including the packet in service.

1.1.2 Congestion Control

Congestion control is concerned with allocating the resources in a network such that it can operate at an acceptable performance level when the demand exceeds or is near the capacity

of the network resources (i.e. to prevent it from operating in the congested region for any significant period of time).

Without proper congestion control mechanisms, the throughput (or net work) may be reduced considerably under heavy load.

Many congestion control algorithms have been proposed and developed, and may be divided into two categories: *congestion avoidance* and *congestion recovery*. The strategy of congestion avoidance is preventive in nature; it is aimed to keep the operation of a network at or near the point of maximum power, so that congestion will never occur. Whereas, the goal of congestion recovery is to restore the operation of a network to its normal state after congestion has occurred. Without a congestion recovery scheme, a network may crash entirely whenever congestion occurs. Therefore, even if a network adopts a strategy of congestion avoidance, congestion recovery schemes would still be required to retain throughput in the case of abrupt changes in a network that may cause congestion.

With the recent development of network technology and the growth of network-intensive applications, the issue of congestion control becomes even more urgent. A great number of congestion control algorithms and strategies have been reported in literature.

It is worth explicitly pointing out the difference between congestion control and flow control. To see this difference, consider a fiber optic network with a capacity of 1000 Gigabits/sec on which a supercomputer is trying to transfer a file to a personal computer at 1 Gbps, as shown in figure 1.2(a) [30]. Although, there is no congestion (the network itself is not in trouble), flow control is needed to force the supercomputer to stop frequently to give the PC a chance to breathe.

A the other extreme, consider a store-and-forward network with 1-Mbps lines and 1000 large computers, half of which are trying to transfer files at 100 Kbps to the other half, as shown in figure 1.2(b). Here the problem is not that of fast senders overpowering slow receivers, but simply that the total offered traffic exceeds what the network can handle. Therefore, the congestion control is needed.

Congestion control has to do with making sure that the subnet is able to carry the offered traffic. It is a global issue, involving the behavior of all the hosts, all the routers, the store-and-forwarding processing within the routers, and all the other factors that tend to affect the carrying capacity of the subnet.

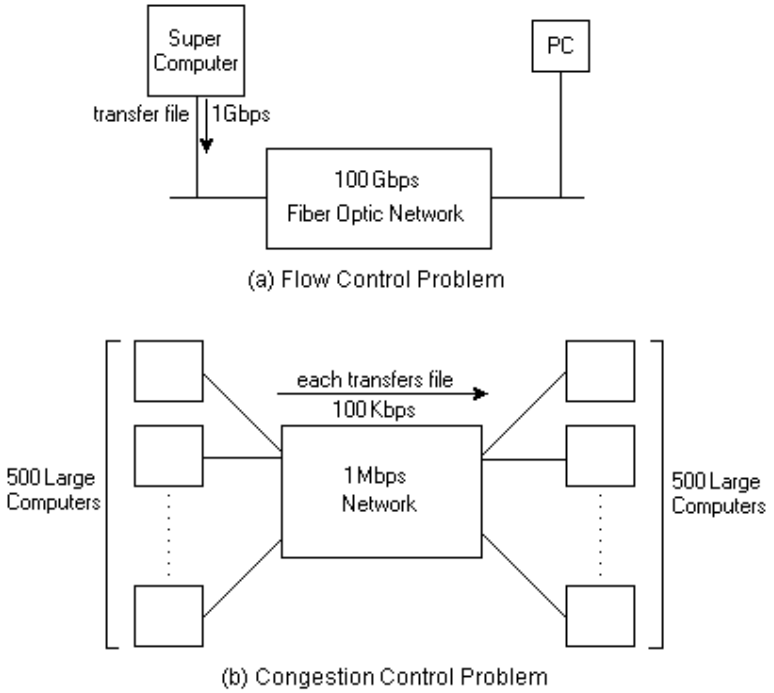

Figure 1**.2:** Difference between congestion control and flow control

Flow control, in contrast, relates to the point-to-point traffic between a given sender and a given receiver. Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver can absorb it. Flow control nearly always involves some direct feedback from the receiver to the sender to tell the sender how things are doing at the other end.

The reason congestion control and flow control are often confused is that some congestion control algorithms operate by sending messages back to the various sources telling them to slow down when the network gets into trouble. Thus a host can get a "slow down" message either because the receiver cannot handle the load, or because the network cannot handle it.

1.1.3 Myths about Congestion Control

Congestion occurs when the demand is greater than the available resources. Therefore, it is believed that as resources become less expensive, the problem of congestion will be solved automatically. This has led to the following myths:

1. *Congestion is caused by a shortage of buffer space* and will be solved when memory becomes cheap enough to allow infinitely large memories.

2. *Congestion is caused by slow links*. The problem will be solved when high-speed links become available.

3. *Congestion is caused by slow processors*. The problem will be solved when the speed of the processors is improved.

4. If not one, then all of the above developments will cause the congestion problem to go away.

On the contrary to these beliefs, without proper protocol redesign, the above developments may lead to more congestion and, thus reduce performance [3,31]. The following discussion explains why.

- **The congestion problem can not be solved with a large buffer space**

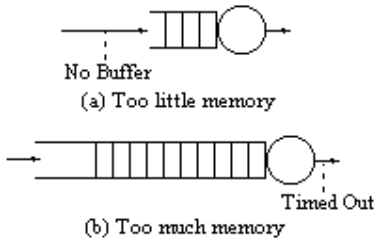

Figure 1.3: Too much memory in the intermediate nodes is as harmful as too little memory

With infinite-memory switches, as shown in Figure 1.3, the queues and the delays can get so long that by the time the packets come out of the switch, most of them have already timed out, dropped, and have been retransmitted by higher layers.

- **The congestion problem can not be solved with high-speed links**

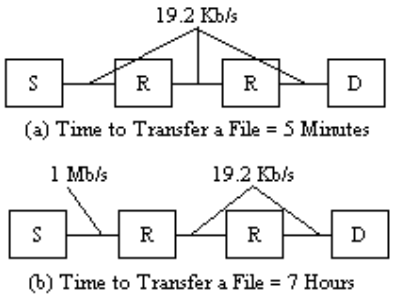

Figure 1.4: Introducing a high-speed link may reduce the performance.

In Figure 1.4, with the high-speed link, the arrival rate to the first router became much higher than the departure rate, leading to long queues, buffer overflows, and packet losses that cause the transfer time to increase.

The point is that high-speed links cannot stay in isolation. The low-speed links do not go away as the high-speed links are added to a network. The protocols have to be designed specifically to ensure that this increasing range of link speeds does not degrade the performance.

- **The congestion problem can not be solved with high-speed processors**

The argument for processors is similar to that for links. Introduction of a high-speed processor in an existing network may increase the mismatch of speeds and the chances of congestion.

- **Congestion occurs even if all links and processors are of the same speed**

Our arguments above may lead some to believe that a balanced configuration with all processors and links at the same speed will probably not be susceptible to congestion.

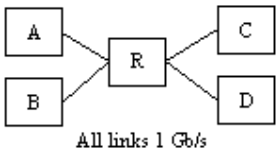

Figure 1.**5:** A balanced configuration with all processors and links at the same speed is also susceptible to congestion.

This is not true. Consider, for example, the balanced configuration shown in Figure 1.5. A simultaneous transfer of data from nodes A and B to node C can lead to a total input rate of 2 Gbits per second at the router R while the output rate is only 1 Gbits per second, thereby, causing congestion.

The *conclusion* is that congestion is a dynamic problem. It cannot be solved with static solutions alone. We need protocol designs that protect networks in the event of congestion. The explosion of high-speed networks has led to more unbalanced networks that are causing congestion. In particular, packet loss due to buffer shortage is a symptom not a cause of congestion

1.2 TRAFFIC MANAGEMENT

1.2.1 Role of Traffic Management

ATM technology is intended to support a wide variety of services and applications. The control of ATM network traffic is fundamentally related to the ability of the network to provide appropriately differentiated Quality of Service (QoS) for network applications. A primary role of traffic management is to protect the network and the end-system from congestion in order to achieve network performance objectives. An additional role is to promote the efficient use of network resources. Proper traffic management helps ensure efficient and fair operation of networks in spite of constantly varying demand and ensure that users get their desired quality of service.

One of the challenges in designing ATM traffic management was to maintain the QoS for various classes while attempting to make maximal use of network resources. This is what distinguishes traffic management from "congestion control" problem of the past. Congestion control deals only with the problem of reducing load during overload. Traffic management deals not only with load reduction under overload or load increase during underload but more importantly it tries to ensure that the QoS guarantees are met in spite of varying load conditions. Thus, traffic management is required even if the network is underloaded. The problem is especially difficult during periods of heavy load particularly if the traffic demands cannot be predicted in advance. This is why congestion control, although only a part of the traffic management issues, is the most essential aspect of traffic management.

A set of six service categories are specified and will be described in section 1.2.4. For each one, a set of parameters is given to describe both the traffic presented to the network, and the Quality of Service (QoS) which is required of the network. A number of traffic control mechanisms are defined, which the network may utilize to meet the QoS objectives [4].

1.2.2 Generic Functions

To meet the QoS objectives, the following functions form a framework for managing and controlling traffic and congestion in ATM networks and may be used in appropriate combinations depending on the service category.

- *Connection Admission Control (CAC)* is defined as the set of actions taken by the network during the call set-up phase in order to determine whether a connection request can be accepted or should be rejected.

• *Feedback controls* are defined as the set of actions taken by the network and by end-systems to regulate the traffic submitted on ATM connections according to the state of network elements. ATM Forum specification [4] defines one network feedback control mechanism: the ABR flow control. The ABR flow control may be used to adaptively share the available bandwidth among participating users. It will be discussed in details in the next chapter.

• *Usage Parameter Control (UPC)* is defined as the set of actions taken by the network to monitor traffic and enforce the traffic contract at the User Network Interface. Network Parameter Control (NPC) is a similarly defined set of actions at the Network Node Interface. The main purpose of UPC and NPC is to protect network resources from malicious as well as unintentional misbehavior, which can affect the QoS of other already established connections, by detecting violations of negotiated parameters and taking appropriate actions. Such actions may include cell discard and cell tagging.

• *Cell Loss Priority control*: For some service categories, the end system may generate traffic flows of cells with Cell Loss Priority (CLP) marking. The network may follow models which treat this marking as transparent or as significant. If treated as significant, the network may selectively discard cells marked with a low priority to protect, as far as possible, the QoS objectives of cells with high priority.

• *Traffic Shaping*: Traffic shaping mechanisms may be used to achieve a desired modification to the traffic characteristics of a connection. The objectives of this function are to achieve a better network efficiency whilst meeting the QoS objectives and/or to ensure connection traffic conformance at a subsequent interface.

• Network Resource Management: The service architecture allows logical separation of connections according to service characteristics. Although cell scheduling and resource provisioning are implementation and network specific, they can be utilized to provide appropriate isolation and access to resources. Virtual Paths are a useful tool for resource management.

• Frame Discard: A congested network that needs to discard cells may discard at the frame level rather than at the cell level.

1.2.3 Traffic Contract and Connection Parameters

The traffic contract is an agreement that specifies the characteristics of a connection between a subscriber and the ATM network. These characteristics are defined by two key elements: the Quality of Service (QoS) parameters and a Connection Traffic Descriptor. The

input traffic characteristics are enforced by the network at the network entry while QoS parameters provided by the network are measured at the network exit point.

1.2.3.1 QoS Parameters

A set of parameters are negotiated when a connection is set up on ATM networks. These parameters are used to measure the Quality of Service (QoS) of a connection and quantify end-to-end network performance at ATM layer. The network should guarantee the QoS by meeting certain values of these parameters:

- *Cell Loss Ratio (CLR)*: The percentage of cells that are lost in the network due to error and congestion and are not delivered to the destination.

$$\text{Cell Loss Ratio} = \frac{\text{Lost Cells}}{\text{Transmitted Cells}}$$

  Each ATM cell has a "Cell Loss Priority (CLP)" bit in the header. During congestion, the network first drops cells that have CLP bit set. Since the loss of CLP=0 cell is more harmful to the operation of the application, CLR can be specified separately for cells with CLP=1 and for those with CLP=0.

- *Cell Transfer Delay (CTD)*: The delay experienced by a cell between network entry and exit points is called the cell transfer delay. It includes propagation delays, queuing delays at various intermediate switches, and service times at queuing points.

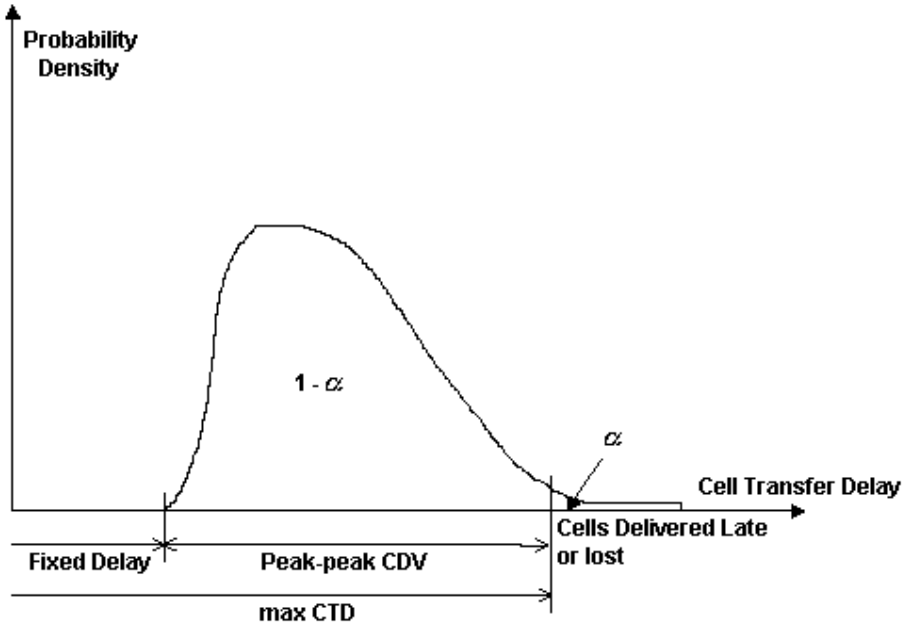

Figure 1.**6:** Cell transfer delay probability density model (for real-time service categories)

- *Cell Delay Variation (CDV)*: This is a measure of variance of CTD. High variation implies larger buffering for delay sensitive traffic such as voice and video. There are multiple ways to measure CDV. One measure called "peak-to-peak" CDV consists of computing the difference between the (1-α)-percentile and the minimum of the cell transfer delay for some small value of α as shown in figure 1.6.

1.2.3.2 Connection Traffic Descriptor

As long as the subscriber sends traffic across the UNI in conformance with the Connection Traffic Descriptor, the network will provide the negotiated QoS. The Connection Traffic Descriptor includes a Source Traffic Descriptor, the Cell Delay Variation Tolerance (CDVT), and a conformance definition.

1.2.3.2.1 Source Traffic Descriptor and Cell Delay Variation Tolerance

The Source Traffic Descriptor defines the characteristics of ATM traffic coming into the network and includes several negotiable traffic parameters. At the time of connection, the network determines if it can accept the connection and still meet QoS levels for all connections including the new one. These traffic parameters and CDVT are defined as follows:

- *Peak Cell Rate (PCR)*: The maximum instantaneous rate at which the user will transmit.
- *Sustained Cell Rate (SCR)*: The average rate as measured over a long interval.
- *Cell Delay Variation Tolerance (CDVT) and Burst Tolerance (BT)*: For sources transmitting at any given rate, a slight variation in the inter-cell time is allowed. For example, a source with a PCR of 10,000 cells per second should nominally transmits cells every 100 μs. A leaky bucket type algorithm called "Generalized Cell Rate Algorithm (GCRA)" is used to determine if the variation in the inter-cell times is acceptable. This algorithm has two parameters. The first parameter is the nominal inter-cell time (inverse of the rate) and the second parameter is the allowed variation in the inter-cell time. Thus, a GCRA(100μs, 10μs), will allow cells to arrive no more than 10 μs earlier than their nominal scheduled time. The second parameter of the GCRA used to enforce PCR is called Cell Delay Variation Tolerance (CDVT) and of that used to enforce SCR is called Burst Tolerance (BT).

- *Maximum Burst Size (MBS)*: The maximum number of back-to-back cells that can be sent at the peak cell rate but without violating the sustained cell rate is called maximum burst size (MBS). It is related to the PCR, SCR, and BT as follows:

$$\text{Burst Tolerance} = (\text{MBS} - 1)\left(\frac{1}{\text{SCR}} - \frac{1}{\text{PCR}}\right)$$

Since MBS is more intuitive than BT, signaling messages use MBS. This means that during connection setup, a source is required to specify MBS. BT can be easily calculated from MBR, SCR, and PCR.

- *Minimum Cell Rate (MCR)*: This is the minimum rate desired by a user.

1.2.3.2.2 Conformance Definition

The conformance definition unambiguously specifies conformance for connections of each service category. It is a theoretical description of how the traffic should behave to comply with the traffic descriptors [5]. It consists of a sequence of Generic Cell Rate Algorithms (GCRA), which are applied to each set of traffic descriptors. With the help of these algorithms each cell of an ATM cell flow is either defined as conforming or non-conforming.

1.2.4 Service Categories

The architecture for services provided at the ATM layer consists of six service categories. These service categories relate traffic characteristics and QoS requirements to network behavior. Functions such as routing, CAC, and resource allocation are, in general, structured differently for each service category. The QoS and traffic parameters for these categories are summarized in Table 1 and are explained below [4]:

Table 1.1: ATM Layer Service Categories

	Attributes	CBR	rt-VBR	nrt-VBR	UBR	ABR	GFR
Traffic Parameters	PCR and CDVT	specified					
	SCR, MBS, CDVT	n/a	specified		n/a		
	MCR	n/a				specified	n/a
QoS Parameters	Peat-to-Peak CDV	specified		unspecified			
	maxCTD	specified		unspecified			
	CLR	specified			unspecified	low	
	Feedback	unspecified				specified	unspecified

- **Constant Bit Rate (CBR) Service Category**

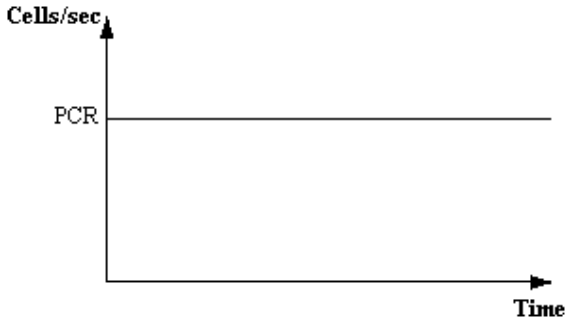

Figure 1.7: CBR uses a static amount of bandwidth

The CBR service category is used by connections that request a static amount of bandwidth that is continuously available during the connection lifetime. This amount of bandwidth is characterized by a PCR value. The source may emit cells at, or below the negotiated PCR (and may also even be silent), for any periods of time. CBR service is intended to support real-time applications requiring tightly constrained delay variation (e.g., voice, video, circuit emulation "leased-lines emulation") but is not restricted to these applications.

- **Variable Bit Rate Service Category**

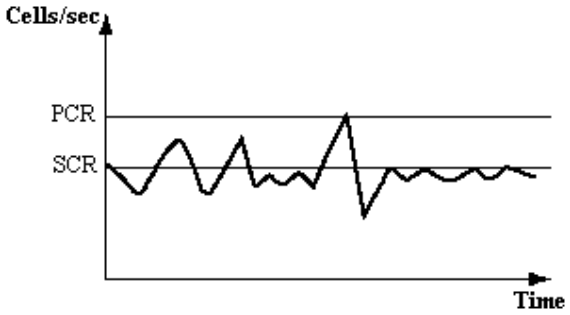

Figure 1.**8:** VBR traffic

The bandwidth requirements of VBR traffic (i.e. both rt-VBR and nrt-VBR) constantly changes. Sources are expected to transmit at a rate that varies with time. Equivalently the source can be described as "bursty". VBR connections define bandwidth requirements in terms of PCR, MBS and SCR. Cells can enter the network at the PCR for a period of time (i.e. MBS) but on average must be emitted at the SCR for the duration of the connection. The variation in cell input rate enables multiple VBR sources to be statistically multiplexed over the same physical connection to maximize network resources.

Depending upon whether or not the application is sensitive to cell delay variation, this category is subdivided into two categories: Real time VBR and Non real time VBR.

- *Real-Time Variable Bit Rate (rt-VBR) Service Category*

The real-time VBR service category is intended for real-time applications, i.e., those requiring tightly constrained delay and delay variation, as would be appropriate for voice and video applications. A peak to peak CDV and a max CTD are specified for rt-VBR traffic. An example of rt-VBR is interactive compressed video.

- *Non-Real-Time (nrt-VBR) Service Category*

The non-real-time VBR service category is intended for non-real-time applications which have bursty traffic characteristics. No delay bounds are associated with this service category. Typical applications include critical-response-time transaction processing (airline reservations, banking transactions) [6].

- **Available Bit Rate (ABR) Service Category**

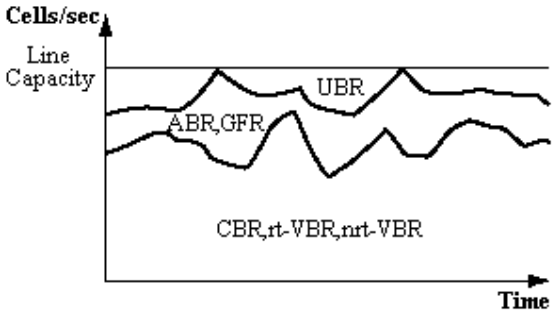

Figure 1.**9:** ABR, GFR and UBR traffic

This category is designed for normal data traffic such as file transfer and email. 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 the delay and loss as much as possible.

A flow control mechanism is specified that supports several types of feedback to control the source rate in response to changing ATM layer transfer characteristics. The source shall specify to the network both PCR and MCR. The MCR may be specified as zero. The bandwidth available from the network may vary, but shall not become less than MCR. Further information on the ABR flow control model and service model can be found in the next chapter.

- **Guaranteed Frame Rate (GFR) Service Category**

The GFR service category is intended to support non-real-time applications. It is designed for applications that may require a minimum rate guarantee and can benefit from accessing additional bandwidth dynamically available in the network. It does not require adherence to a flow control protocol. The source specifies a PCR, and a MCR that is defined along with a MBS and a Maximum Frame Size (MFS). Under congestion conditions, the network attempts

to discard complete Frames instead of discarding cells. The user may always send cells at a rate up to PCR, but the network only commits to carry cells in complete frames at MCR. Traffic beyond MCR will be delivered within the limits of available resources. There are no delay bounds associated with this service category.

- **Unspecified Bit Rate (UBR) Service Category**

This category is designed for those data applications that want to use any left-over capacity and are not sensitive to cell loss or delay. Such connections are not rejected on the basis of bandwidth shortage (no CAC) and not policed for their usage behavior. During congestion, the cells are lost but the sources are not expected to reduce their cell rate. Instead, these applications may have their own higher-level cell loss recovery and retransmission mechanisms. Examples of applications that can use this service are email, file transfer, news feed, etc. Of course, these same applications can use the ABR service, if desired.