

NIST PUBLICATIONS

NISTIR 5000

Study of Traffic Control and Congestion Control in Broadband ISDN

Yoon D. Chang David H. Su

U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology Computer Systems Laboratory Advanced Systems Division Gaithersburg, MD 20899

QC 100 .U56 5000 1992





Study of Traffic Control and Congestion Control in Broadband ISDN

Yoon D. Chang David H. Su

U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology Computer Systems Laboratory Advanced Systems Division Gaithersburg, MD 20899

December 1992



U.S. DEPARTMENT OF COMMERCE Barbara Hackman Franklin, Secretary

TECHNOLOGY ADMINISTRATION Robert M. White, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY John W. Lyons, Director

STUDY OF TRAFFIC CONTROL and CONGESTION CONTROL IN BROADBAND ISDN

Yoon D. Chang

David Su

ABSTRACT

In Broadband Integrated Services Digital Network (B-ISDN), the Asynchronous Transfer Mode (ATM) network architecture has been adopted as the switching and multiplexing scheme. One of the important ATM architectural issues is traffic and congestion control. Many schemes, algorithms and theories have been studied for network flow control, congestion control, and traffic control in order to find suitable techniques to manage network traffic effectively to meet the quality of service requirement for network users.

Among B-ISDN terminals in a Customer Premises Network (CPN) domain, a new flow control concept refered to as Generic Flow Control (GFC), has been adopted and its protocol standardization is under study. The main purpose of GFC is to control and to schedule the local traffic flow at the Broadband Terminal Equipment (B-TEs) at an early stage before the traffic is transmitted into the network. This will have a significant role in the overall performance of high speed network traffic management.

This paper presents a general overview of traffic control as well as congestion control, related topics and issues currently under study. It is also a survey of publicly addressed techniques and algorithms used in B-ISDN networks, and report on status of the ANSI Accredited Standards Committee T1S1 and CCITT standardization activities. The objective of this paper is to provide concrete concepts of ATM layer traffic/congestion control and to contribute technical studies to the standardization efforts in the traffic control and congestion control areas, particularly in ATM layer traffic and congestion control issues in B-ISDN.

CONTENTS

1.	INTRODUCTION	•	•	•	•	•	1
2.	OVER VIEW OF CONGESTION CONTROL, FLOW CONTROL AND TRAFFIC CONTROL2.1 Overview of Congestion Control2.2 Overview of Flow Control2.3 Overview of Traffic Control2.4 Overview of Generic Flow Control	C	• • •	• • •	• • •	• • •	3 3 3 4 5
3.	 MULTIMEDIA TRAFFIC ENVIRONMENT	•	•	•	•	•	6 7 7 7 9 9 10
4.	 TRAFFIC CONTROL FRAMEWORK IN ATM NETWORKS	•	•	•	•	•	13 14 14 15 15 16 16
5.	 TRAFFIC CONTROL and CONGESTION CONTROL FUNCTIONS in B-ISDN 5.1 Traffic Control Functions		•	•	•	•	18 18 19 19 20 21 22 22 22 22 22
6.	5.2.3 Explicit Backward Congestion Notification (EBCN) 5.2.4 Reaction to UPC/NPC Failures 5.3 Items/Issues under Study in CCITT IMPLICATIONS OF TRAFFIC CONTROL IN B-ISDN 6.1 Traffic Management Strategies 6.2 Requirements for Traffic Control Techniques in B-ISDN 6.3 Traffic Control Techniques in B-ISDN	· ·	•	•	• • •	• • •	23 24 24 26 26 26 26 27
7	6.4 Standardization of frame Control Procedures	•	•	•	•	•	28 30
A	PPENDIX OUEUEING MODELS		•	•	•		33

1. INTRODUCTION

In Broadband Integrated Services Digital Network (B-ISDN), the Asynchronous Transfer Mode (ATM) network architecture has been adopted as the switching, multiplexing and transport scheme[1] by international standards groups. One of the important ATM architectural issues is traffic and congestion control in ATM networks. Many schemes, algorithms and theories have been studied for network flow control, congestion control and traffic control in order to find suitable techniques to manage network traffic effectively to meet the quality of service requirement for network users. Some of these schemes of traditional networks are not quite appropriate in the high-speed ATM environment since the majority of traffic is not flow-controllable¹. This problem requires a new concept of traffic and congestion control in an ATM network environment due to difficulties of ATM requirements such as wide range of bandwidth applications, supporting both delay sensitive and loss sensitive services and very high speed switching and transmission².

Among B-ISDN terminals in a Customer Premises Network (CPN) domain a new flow control concept, referred to as Generic Flow Control (GFC), has been adopted and its protocol is under study with the expectation that future users of B-ISDN equipment will incorporate high speed LAN-like switching capabilities at the customer premises. The main purpose of GFC is to control and to schedule the local traffic flow at the Broadband Terminal Equipment (B-TEs) at an early stage before the traffic is transmitted into the network. This will contribute significantly to the overall performance of high speed network traffic management.

In the LAN/MAN (Metropolitan Area Network) environment, there are two main categories of industrial standards, bus based and ring based protocols. The relatively low speed (4 Mbps - 16 Mbps) Ethernet (IEEE 802.3) and Token Ring (IEEE 802.5) protocols, and the relatively high speed DQDB (IEEE 802.6, Distributed Queue Dual Bus) and FDDI (ANSI X3T9.5) protocols are widely prevailing standards. Due to the ATM GFC requirements for supporting various network topologies, these conventional protocols are not quite suitable for a GFC protocol. Currently there are two GFC protocol proposals under study:

- a slotted ring based proposal from British Telecom (BT) and Nippon Telegraph and Telephone (NTT)
- a DQDB-like dual bus protocol from AT&T, the Swiss PTT and QPSX, an Australian firm.

The terms flow control, traffic control and congestion control are widely discussed in the literature[3][4][9][12][17][24][28][31]. Congestion control[33][37] refers to a set of reactive actions taken to minimize the intensity, spread and duration of congestion when congestion occurs. Flow control and traffic control[37] are preventive actions taken to avoid congestions by restricting, monitoring and smoothing traffic. These controls generally apply both at the lower network layers (Layers 2 and 3) and at the higher layers (Layer 3 or above)³ in OSI layer terms.

This paper presents the general overview of traffic control as well as congestion control, related topics and issues currently under study. It is also a survey of publicly addressed techniques and algorithms used in B-ISDN networks, and a report on status of the ANSI Accredited Standards Committee T1S1 and CCITT standardization activities. The traffic flow control issues of GFC between multiple B-TEs with different network topologies and some results of simulation work done for proposed GFC protocols are discussed in a paper[50]. The objective of this paper is to provide concrete concepts of ATM layer

^{1.} For example, with the 622 Mbps User Network Interface (UNI) interface rate for a distance of 1,000 miles, the source transmits 6.2 Mbits during the round-trip delay time of approximately 10 mili-second

^{2.} With the 622 Mbps rate, one ATM cell switching of 0.7x 10⁻⁶ second compared to 5x10⁻³ second propagation delay of approximate 1,000 miles at light speed, and medium propagation delay of 5x 10⁻³/Km in B-ISDN GFC test parameters

^{3.} Routing is usually performed at layer 3 (network layer) in traditional packet switching network versus the ATM layer (relatively lower layer compared to traditional packet switching) using VPI/VCI in the header of an ATM cell in ATM networks. B-ISDN standards define routing as part of connection admission control (CAC) actions and CAC as one of the traffic control functions.

traffic/congestion control and to contribute to the standardization efforts in the traffic control and congestion control areas, particularly the ATM layer traffic and congestion control issues in B-ISDN. Various schemes, algorithms and protocols that have been proposed in the standard committees and many related issues are evaluated via simulations to seek most the appropriate methods to achieve network performance objectives in the future.

2. OVERVIEW OF CONGESTION CONTROL, FLOW CONTROL AND TRAFFIC CONTROL

2.1 Overview of Congestion Control

Congestion control⁴ is a mechanism to deal with the situations where the total offered traffic exceeds the capacity of the network. In CCITT Recommendation I.371[37], ATM layer congestion control refers to the set of actions taken by the network to minimize the intensity, spread and duration of congestion. Congestion can occur in the situation where a user can send a burst of packets at the channel rate in a network and when a number of B-TEs simultaneously transmit bursts of data on the same link in the network.

In B-ISDN I.371 Recommendation[37], congestion is defined as a state of NEs (Network Elements, e.g. switches, transmission links, concentrators, multiplexers) in which, due to traffic overload and/or control resource overload, the network is not able to meet the negotiated quality of service (QOS) objectives for the already established connections and/or for the new connection requests.

In general, congestion can be caused by:

- Unpredictable statistical fluctuations of traffic flows due to the nature of network burstiness
- Fault or malfunctioning conditions within the network

A typical way of reducing traffic congestion is to use buffers that can absorb sudden surges of traffic. Because the buffer size is limited, the network may have to shut off any bursty data source or drop the incoming packets when the buffer reaches its maximum capacity. If the network remains without such controls for some time, the overflow of internal buffer queues are being dropped. Since discarded data are eventually retransmitted, the entering traffic tends to grow. A vicious circle of instability can then be entered where more traffic brings more retransmission which brings more traffic and eventually it may end up the in ultimate congestion state of "deadlock", also called a "lockup". That is the state when virtually any data or traffic flow is impossible in the network.

Bursty communication requires dynamic bandwidth allocation to prevent short-term or long-term traffic congestion in the network. In practice, bandwidth may be difficult to allocate dynamically. However, ATM can adjust bandwidth dynamically based on incoming cell rates because bandwidth is not preallocated and dedicated; this is one of the major advantages of an ATM network. Even though ATM can handle bursty traffic with higher efficiency, congestion can occur at any cell level or call level for any of the reasons described above and its impact is quite serious due to the high data rate. Therefore, once congestion occurs, the network requires appropriate congestion control to alleviate the situation and to prevent further damage, degrading the level of QOS for ATM network users.

In conjunction with flow control, back-pressure schemes can be used to resolve a network congestion. The node sends the congestion information to other nodes or a source so that the notified nodes or sources can control their traffic, possibly via traffic shaping (a form of flow control) or other disciplinary actions.

2.2 Overview of Flow Control

Flow control is defined in various ways in the literature. In one reference[12], flow control is a technique for assuring that a transmitting entity does not overload a receiving entity with data. In another reference[38], flow control is the method whereby a network can exercise a back-pressure (feedback-based mechanism, e.g., EBCN in B-ISDN) or necessary actions on a data source, selectively for each of its flows of data. In a text reference[8], flow control is described as the solution to all problems related to congestion and is a protocol, or more generally, a set of protocols whose goals are 1) to maintain efficient network operations, 2) to guarantee fairness in resource sharing and 3) to protect the network from congestion.

^{4.} Sometimes it's referred to as as "overload control"

Typically flow control techniques are used in a traditional end-to-end⁵ manner, aiming to control one end rate, thus preventing overflow at the other end. Such techniques are used in low speed packet-switched data networks that mostly carry non-real time data. This non-real time data traffic can be flow controlled to prevent congestion. In that regard, various flow control mechanisms have been used effectively for preventing congestion in conventional packet networks. In order to prevent network congestion, flow control schemes usually utilize various techniques to keep a data source node from overflowing a network. The receiving node typically allocates a data buffer with some maximum length. These flow control schemes include stop-and-go, sliding window (such as in X.25 packet networks), feedback-based mechanism with choking and other derivatives of window control mechanisms.

The stop-and-go[12] scheme is the simplest form of flow control where the destination node indicates its willingness to accept another frame by sending back an acknowledgement when a frame is received from a source node. The source must wait until it receives an acknowledgement for the next frame from a destination node. By doing this, the destination node can stop the flow of data traffic by simply withholding acknowledgement. Thus, the send, stop, wait, and go steps can recursively cycle between a source and a destination node.

In sliding window[12] schemes, a source node sends multiple frames called a window of frames, within the limit of buffer sizes allocated in a destination node and the schemes keep track of the number of frames pending in the network for each virtual circuit using some acknowledgement mechanism. Thus, a destination node controls multiple window frames by withholding acknowledgement instead of a single frame at a time. There are many variations of these window schemes, which can be mainly categorized by two schemes, acknowledgement-based and rate-based.

In an ATM network, there will be two flow control levels; Node-to-Node and End-to-End. Nodeto-Node flow control controls the flow of traffic between adjacent nodes and reduces the cell loss on the ATM layer. This method is generally considered to be undesirable in an ATM network due to delays of high speed data rate. End-to-End flow control is to match the speeds of the end entities and this control scheme could be provided by the ATM Adaptation Layer (AAL) or higher layers. The ATM network adopts a simplified transport protocol based on hardware cell switching without any conventional window-based flow control and without retransmission in a network. Instead of conventional per-packet window based flow control, the ATM network flow control is based on a connection call-oriented arrangement by allocating network resources or by traffic shaping.

2.3 Overview of Traffic Control

Often traffic control is referred to as traffic management because it involves multiple actions of controlling network traffic that flows globally for the purpose of preventing and alleviating congestion, and of meeting network performance objectives. Thus, traffic control may involve congestion preventive actions such as flow control, disciplinary restrictive actions like connection admission control and monitoring and policing functions, reactive actions like early warning congestion notifications and packet discarding. It may also involve network resource management as a way to effectively avoid network congestion. Some literature[12] includes congestion control as part of traffic control functions. This is because the congestion control is partially understood as a way of managing traffic flows in overflow situations in a network.

The goal of traffic control is to provide a guaranteed quality of service to network users by means of controlling network traffic flows effectively. In the CCITT Draft Recommendation I.371, ATM layer traffic control refers to the set of actions taken by the network to avoid congested conditions.

In general, there are several methods for controlling traffic to avoid congestion and to minimize the congestion state spreading. These controls involve: 1) allocating resources in advance (e.g., bandwidth allocation, buffer allocation), 2) restricting the number of cells in the network, 3) effective routing of

^{5.} Some techniques are using Node-to-Node (point-to-point) flow control (e.g., DEC's Autonet)

traffic, 4) using flow control to avoid congestion, 5) allowing cells to be selectively discarded when they can not be processed, 6) choking off input⁶ when the network is overloaded, 7) deadlock prevention methods, and others.

The traffic control levels consist of mainly call level and cell level controls⁷. Based on widely accepted terminologies by standards bodies, (CCITT and T1S1), traffic control involves preventive actions to avoid congested conditions. This is clearly distinguished from congestion control which involves reactive actions for congested conditions in a network. The functions of traffic control may include a connection admission control, routing, monitoring, flow control mechanisms, policing, QOS control, traffic shaping, network resource management, and any other functions that prevent congestion. Flow control involves preventive actions from overflow of traffic in a network and therefore it is a part of traffic control mechanisms.

2.4 Overview of Generic Flow Control

At the CCITT Study Group XVIII Party 8 meeting of B-ISDN in January 1990, it was agreed that some B-TEs will have two Physical Layer ports or Transmitter/Receiver pairs in order to support a large variety of broadband terminal equipment configurations. However, there was no agreement on the use of these two ports at the next higher layer (ATM Layer).

One possible way of using these ports is to create a shared medium (local area network architectures) on various network topologies such as a bus, ring, star or star-bus structure at customer premises. The current agreement (Melbourne and Matsuyama meeting results in 1991) concerning the B-TE reference configurations appear in CCITT Draft Recommendation I.413 Section 2 "Reference configuration at the user- network interface (Figures 1/I.413, 2/I.413 and 3/I.413)". In order to support this feature, it may be necessary to have an ATM layer protocol which controls the transmission of cells from B-TEs and communicates its information between B-TEs, using the Generic Flow Control (GFC) field.

GFC is a shared medium flow control of ATM traffic connections among B-TEs in a customer premises network at each User Network Interface (UNI) reference point[34]. It schedules transmission to network among multiple B-TE sources. It coordinates and mediates media access among multiple B-TEs at the customer premises. For network providers, it is quite necessary to control user's traffic so that network resources can be utilized efficiently and fairly by all the network users while satisfying individual QOS requirements. Also, an ATM network does not store cells over a long period of time, so there are no conventional flow control mechanisms inside the ATM networks. Thus, the GFC role of controlling input traffic sources with various QOS before they are transmitted into the network can have significant impact on overall traffic control management in ATM networks. The four-bit GFC field in the ATM cell header is used to perform these roles. The GFC field has two sets of procedures[35][36], controlled-transmission procedures and uncontrolled-transmission procedures. The GFC function is used only in controlled-transmission procedures. The standards bodies of CCITT and T1S1 are currently working on the standardization of GFC protocol.

^{6.} Such as additional call admission denial or even existing call release in certain circumstances

^{7.} Interim levels can be added, such as burst level and dialog level

3. MULTIMEDIA TRAFFIC ENVIRONMENT

As specified in principles and concepts of B-ISDN in a reference[45], B-ISDN service will support a wide range of data, video and voice (multimedia) applications and will support both switched and nonswitched connections requiring both circuit-mode and packet-mode information transfer capabilities. This section briefly studies these multimedia traffic types and the modeling of traffic flows from one end point to the other end point in a network. These modeling and traffic types can be used to analyze and simulate the characteristics of traffic for real service implementations.

3.1 Asynchronous Transfer Mode Overview

Asynchronous Transfer Mode (ATM) is a variation of fast packet switching technology that has been the subject of research since the early 1980s. In 1990 the CCITT adopted the ATM approach for the emerging Broadband ISDN[48] standard. Since then CCITT approved fifteen sets of Recommendations on B-ISDN and many other set of Recommendations are under study. The B-ISDN protocol reference model is shown in I.321[49].

In ATM, all user information is segmented into short, fixed-size packets called cells. This is contrast to other fast packet switching technologies, such as Frame Relay, which handle variable-size packets. Short cells were chosen to reduce the transfer delay to accommodate a wide range of services like voice and video in real-time. The fixed size format was chosen to allow better hardware performance. The cell sequence integrity is guaranteed by ATM connections across each ATM switch.

Each ATM cell consists of a 5-octet header as shown in Figure 1, and a 48-octet information field called a payload[35].

5 Octet ATM Cell Heade	er at UNI	
Generic Flow Control (GFC 4-bit)	VPI (4-bit)	
Virtual Path Identifier (VPI) (4-bit)	VCI (4-bit)	
Virtual Channel Identifier (VCI) (8-bit)		
VCI (4-bit)	Payload Type (3-bit)	Cell Loss Priority (1-bit)
Header Error Check (HEC 8-bit)		

Figure 1 ATM Cell Structure (CCITT Figure 2/1.361)

The ATM cell routing information is contained in the header and is the concatenation of the VPI and the VCI. ATM is connection oriented. The VPI and VCI fields are identifying labels used only for local links in the virtual connection between ATM switch nodes. The ATM cell routing is performed at an ATM layer which is considered to be a lower layer than the traditional packet switching routing performed at layer three (in the OSI model). The fixed size ATM cells and the virtual circuit routing in switches can be implemented in hardware more easily than conventional layer 3 routing, resulting in lower delay at each intermediate switching mode.

The ATM cells can be transported by any physical medium. The B-ISDN standards has standardized to use the optical transmission system, Synchronous Digital Hierarchy (SDH) and Synchronous Optical Networks (SONET in ANSI) as a physical layer to carry ATM information.

Overall, ATM provides some specific, advantageous facilities:

- High network access flexibility compared to the Synchronous Transfer Mode (STM) in circuit switching. In ATM, each cell identified by the header is associated with a specific virtual channel at any position and hence can be sent at any frequency. In STM, the transmission bandwidth is divided into fixed-rate channels and each channel is dedicated to the predefined channel bit rate of the call.
- Flexible service capability allocation and easy provision of semi-permanent connections due to the virtual path (grouping several virtual channels) concept.

• Dynamic bandwidth allocation on demand with a fine degree of granularity.

3.2 ATM Traffic Types and Flow Models

3.2.1 Traffic Types

In CCITT Draft Recommendation I.211[39], the types of information are categorized as Moving Pictures (Video) and Sound, Data, Documents, Text, Graphics, Still Images and Moving Pictures.

The traffic type of an ATM network can be categorized based on bit rate characterized by traffic descriptors (e.g., average rate, peak rate), connection mode and distribution characteristics of interburst-time and burst length.

3.2.2 Service Classes

In order to minimize the number of ATM Adaptation Layer (AAL) protocols, a service classification which categorizes the type of information into services is defined based on the following parameters:

- · Timing relation between source and destination
- Bit rate such as Constant Bit Rate (CBR) or Variable Bit Rate (VBR)
- Connection Mode such as Connection Oriented (CO) or Connectionless (CL)

Details of service classification are described in CCITT Draft Recommendation I.362 (B-ISDN AAL Functional Description).

The services of an ATM network are generally divided into two categories, Constant Bit Rate (CBR) and Variable Bit Rate (VBR), which are sub-divided into two sub-categories, Bursty VBR and Stream VBR. The details of service type descriptions are described in Broadband Aspects of ISDN Baseline Document (I.121R, Section 3 - Table 3.1).

3.2.3 Queuing Flow Models

Queueing theory is one of the most powerful mathematical tools[43] widely used for making quantitative analyses of networks. This technique was originally developed to analyze the statistical behavior of randomly arising demands[44] and was used in the early telephone traffic congestion problems studied by the Danish scientist, A. Erlang. Since then, it has been applied to many networking problems as well.

Queueing system can be generally characterized by six components:

1. The Interarrival-time Probability Density Function (Arrival Pattern of Data):

The arrival pattern or input to a queueing system is often measured in terms of the mean arrival rate (the average number of arrivals per unit of time) or mean interarrival time (the average time between successive arrivals). Similarly, the service pattern can also be measured by a rate (number of inputs served per unit of time) or a time (time required to service an input). Arrivals and services are generally mutually independent and occur at irregular intervals. Hence, the process follows a probability distribution for queue lengths.

Numerous papers[6][27][46][47] have studied traffic models in terms of probability distributions and some of the details are well studied in [27]. A brief summary of a set of models is listed in the Appendix.

- 2. The Service-time Probability Density Function (Service Pattern of Servers): The PDF of the service pattern of servers can be similar to the PDF of the arrival pattern.
- 3. The Number of Servers (Number of Service Channels): There are two variations of multiple server systems. One may have a single queue and the other has a queue for each server. It is generally assumed that the service mechanisms of multiple channels operate independently of each other. Using multiple servers as a queueing server model is quite complex. In a simulation study of B-ISDN traffic control, congestion control and generic flow control, a single server model is used as a simplified server model.

- 4. The Queueing Disciplines: Various queueing disciplines are well described in [22] and a brief summary abstracted from the reference literature is listed in Appendix.
- 5. The Amount of Buffer Space in the Queues (System Capacity): In many simulation studies, an infinite buffer size is assumed for simplicity. In some queueing processes (and in reality) there is a limitation on buffer size for physical and economic reasons; this is referred to as a finite queueing situation. If the queue size is at its limit when input data arrives, the data will be lost due to overload of the buffer. Hence, within the QOS requirement, cell loss probability versus buffer size has to be carefully balanced.
- 6. The Number of Service Stages

The notation below (Kandall's denomination) is widely used in the queueing literature[12][51][52] for these systems.

X/Y/m (or X/Y/m/D, when a buffer size k is described)

where,

- X the interarrival-time probability density,
- Y the service -time probability density,
- m the number of servers and buffer size k is either finite or infinite,
- C the queueing discipline
- D the buffer capacity.
- E the number of service stages

When the denomination of a queue is in the form of "X/Y/m/C/D/E", in many situations only the first three symbols (X/Y/m) are used and the next three symbols (/C/D/E) are understood as (FIFO/infinity/infinity).

When m=1 (single server), a queueing model of single server is drawn as in Figure 2.



Figure 2 Queueing Model of Single Server

A general n-state Markovian representation (Markov Chain) of an ATM source has been identified[6] which could be used to approximate a wide range of traffic flows. The graphical description of n-state is depicted in Figure 3. The n=2 state model has been widely used as a simplified traffic source state (Figure 4) in B-ISDN standards bodies.



Figure 3 General n-state Markov Chain Diagram



Average Burst Length B = 1/bAverage Cell Rate A = aP/a+b

Figure 4 Two-state ATM Traffic Flow Model

3.3 Scopes and Levels of Traffic Control

Traffic control techniques can be categorized by the scope of their applications and the control functions can be mainly carried out at two levels, the call process level and the cell transfer level.

3.3.1 Scopes of Flow Control

The flow control levels are closely related to network protocol levels. The various ranges of flow control are shown in Figure 5. This is a typical protocol level structure implemented in a packet network[8][12][19].

- Node-to-Node Control (Hop-to-Hop): This controls the flow of traffic between adjacent nodes. This
 control is supported by the network access link protocol through a mechanism of NPC (Network
 Parameter Control) when the network is congested.
- End-to-End Control (CPE-to-CPE⁸): Control the flow of traffic between End Systems. This control
 could be provided by the AAL or higher layers. The end-to-end control schemes can function in
 significant roles such as:
 - regulate the flow between the end points (for example, at $T_{\rm B}^{9}$ reference points)
 - prevent the excess data of the faster end point from entering the network
 - keep the excess data at the customer premises (out of the network)
 - help preserve the network bandwidth resources
- Local CPE-to-CPE Control: Controls the flow of local traffic within the customer premises network. It is an end-to-end control but it is governed by a group of local CPEs in a CPN. This level of control is defined as Generic Flow Control in B-ISDN.
- 4. CPE-to-Node (Network Access) Control: This method has the objective of regulating the input of packets into the network based on local or global congestion status. The UPC (usage Parameter Control) function will provide some degree of flow control at this level with the help of GFC.
- 5. Entry-to-Exit Control: This method has the objective of avoiding the overflow of exit buffers by regulating inputs at the entry node and to guarantee reassembly space at the exit node (e.g., by allocating exit buffers as needed). If message reassembly and sequencing is not required, this scheme is not necessary because other node-to-node and network access schemes cover these objectives.

^{8.} Customer Premises Equipment

^{9.} T_B is the boundary between B-ISDN Network Termination 1 (B-NT1) and B-ISDN Network Termination 2 (B-NT2) of a Customer Premises Network. S_B is the boundary between B-TEs and B-NT2 of a Customer Premises Network. The subscript "B" stands for 'Broadband'.



Figure 5 Various Scopes of Flow Control

3.3.2 Levels of Traffic Control

It is essential for ATM systems to control the characterized types of traffic streams. The ATM traffic processes are quite different and more complex compared to conventional telephony, whose model is well known as continuous stream with Poisson processes.

In general, levels of traffic control can be categorized as two levels, a longer duration time level (call level) and a shorter duration time level (cell level). The burst level can be characterized as an intermediate level in between cell level and call level. The literature[2] characterizes the burst level even further into two sub levels; dialog burst level and burst level. Figure 6 depicts four types of traffic stream models by means of discrete-time processes that are based on a block of cell transmission time.





1. Call Connection Level:

Traffic controls of call level include connection admission control and routing control for selecting a route from available end-to-end routes.

The virtual channels are set up before the cell transfer phase begins for each call. Bandwidth for all links on a route can be allocated via a bandwidth allocation function. If some links on a route do not have sufficient capacity to guarantee the QOS, the call is subject to rejection. The call admission decisions are based on a set of parameters called traffic descriptors. Components of traffic descriptors may be the average bit rate, the bit rate variance, the peak bit rate, and the maximum number of cells transmitted within a short duration (burst length). However, it is difficult to determine an appropriate minimum set of traffic descriptors and an effective bandwidth. In the future neural networks may offer a new technique for connection admission control.

2. Burst Level:

At burst level, traffic control may involve blocking or throttling of new bursts based on available buffer and bandwidth, monitoring of virtual connections to determine whether bursts are active or not and renegotiating bandwidth management parameters such as described in [7][16].

3. Cell Transfer Level:

At the cell level, traffic control may involve policing control, priority cell tagging, quality control and congestion control. It may also involve congestion notification and limiting cell flows into networks in case of overflow.

Once a connection has been admitted to the network, the traffic flow of the connection should be monitored and enforced according to its traffic descriptors, by a Usage Parameter Control/Network Parameter Control (policing) function. It consists of n-state Markov chain and each state is grouped into two states, active and inactive (idle) state. In an active state a cell is generated, and the state transition after each time slot of cell duration takes place without generating a cell in an idle state. Hence, it can characterize quite complex processes but the number of states at the cell level will be very large in most of the traffic streams. So the control mechanism at the cell level will be quite complex due to the complication of describing an analytical cell traffic model.

3.4 Reference Configuration for Traffic Control and Resource Management

The following reference configuration is used for traffic control and resource management (Figure 7, derived from Figure 1/I.371).



* Refer to Figure 5 (Broadband Reference Configuration) for CPN architecture.

Rodrawn from Figure 3.c/L413

Figure 7 Reference Configuration for Traffic Control & Resource Management

The reference configuration comprises customer premises networks and service-provided public networks. At customer premises, multiple B-TEs configured with various topologies are linked to a Broadband Network Termination Type 2 (B-NT2) via an interface reference point S_B . The B-NT2 is linked to a Broadband Network Termination Type 1 (B-NT1) via a reference point T_B . GFC mechanisms function between multiple B-TEs and a B-NT2 in an upstream direction. The user network is connected to a service provided network via a User Network Interface (UNI) applying primarily to the T_B reference point. User traffic is controlled by the Usage Parameter Control (UPC) mechanisms at the entrance to a network. The network performs various traffic control functions such as CAC, RM, CC, PC and others. Public networks are connected via a Network-Network Interface (NNI) and input and output traffic is controlled by Network Parameter Control (NPC) mechanisms.

4. TRAFFIC CONTROL FRAMEWORK IN ATM NETWORKS

An Asynchronous Transfer Mode is a standard transfer mode¹⁰ solution for implementing a broadband ISDN. An ATM network is a high speed multimedia network which handles various classes of traffic with different bit rates and with different QOS requirements. The ultimate goal of ATM traffic control is to ensure that B-ISDN services will be provided with guaranteed QOS. The ATM layer provides two types of service; deterministic (CBR) and statistical (stream VBR and bursty VBR) service. Since ATM networks do not know the AAL and higher layer protocols employed in a user's Customer Premises Equipment, ATM traffic controls should not rely on these higher layer protocols. The ATM Adaptation Layer performs necessary functions to ensure that the QOS of a B-ISDN service will be guaranteed based on the QOS provided by the ATM layer.

ATM networks assume a reliable fiber optics data transport service. In order to achieve guaranteed user throughput in a high speed multimedia network, the ATM network adopts a simplified transport protocol based on hardware cell switching without any conventional flow control and without retransmission in the network. Therefore, some traditional network overhead burdens¹¹ can be eliminated and network performance (e.g., guaranteed user throughput required by some voice and video communications) improved.

Instead of conventional per-packet window based flow control, the ATM network flow control can be based on a connection call oriented arrangement by allocating network resources or bandwidth management (BWM)[3] to each call according to its QOS requirements. The necessary number of cells are allocated on traffic transfer demand, so bursty data would be statistically multiplexed. However, some ATM network design methods, including call/cell arrival process modeling and traffic control of call/cell levels, require further study.

The CCITT and the T1 committee efforts to standardize B-ISDN have defined the objectives of ATM layer traffic controls for B-ISDN[18]. These are:

- ATM layer traffic controls should support a set of ATM layer QOS classes sufficient for all foreseeable B-ISDN services. The specification of these QOS classes should be consistent with network performance in CCITT Recommendation I.35B (Broadband ISDN Performance).
- ATM layer traffic control should not rely on AAL protocols which are B-ISDN service specific, nor
 on higher layer protocols which are application specific. Protocol layers above the ATM layer may
 make use of information provided by the ATM layer to improve the utility those protocols can
 derive from the network.
- The design of an optimum set of ATM layer traffic controls should trade-off minimizing network and End System (ES) complexity for maximizing network utilization.
- ATM layer traffic controls include actions taken to prevent congestion as well as actions taken to relieve congestion. Under congestion conditions, ATM layer congestion controls react to limit the intensity, spread and duration of control.

The generic functions have been worked to meet the objectives in need of standardization such as network resource management, connection admission control, feedback control, UPC/NPC, priority control and congestion control. These functions and other possible control functions can be used in appropriate combinations to manage and control traffic and congestion in ATM networks.

An informal framework for managing traffic and handling congestion in the ATM layer was developed based on the technical contributions presented at the October 1990 B-ISDN meeting of T1S1 in Boca Raton, Florida. The initial framework elements were included such as:

^{10.} The term "transfer" comprises both transmission and switching aspects, and so a transfer mode is a specific way of transmitting and switching information in a network

^{11.} Packet-by-packet based sliding window flow control in current X.25 packet networks

- SCD (selective cell discard) on the basis of CLP (cell loss priority) at NEs
- UPC (usage parameter control) at the edge of the network
- CVT (cell violation tagging) of excess traffic at the edge of network
- FCN (forward congestion notification) set by the NEs
- BCN (backward congestion notification)
- BMCS (buffer management and cell service) policies at NEs to provide service discrimination and help congestion control
- ES (end system) reactions in response to network congestion

In order to investigate various traffic management strategies and the performance of presented algorithms and to make a fair comparison, a test scenario has been developed and used as the basis of the evaluation.

4.1 Modeling the ATM Network

This section describes a simplified ATM network developed at the January 1991 meeting of T1S1 in Houston, Texas. It was developed to help create a common environment in which various traffic control and congestion control mechanisms can be evaluated as a part of the standardization process[18]. In that work, a generic Poisson-type traffic source model, which may be adequate only for academic purposes, was used for simplistic modeling of the ATM network. Later, more details for the control evaluation framework, such as a set of reference network topologies and more detailed descriptions of how the proposed control capabilities can be used to support mixes of traffic types for B-ISDN, were added. However, more sophisticated models and performance metrics need to be developed to accurately simulate traffic sources in the real world. The continuing and more detailed works are yet to be studied in standards bodies.

4.1.1 Network Modeling

A general ATM network can be described as a group of interconnected nodes, with multiple input sources and multiple destination nodes connected with multiple levels of intermediate nodes. The simplest approximation of the network consists of just one hop between the sources and the destination node. The complexity can vary by varying the number of hops between the sources and the destinations. For the purpose of comparing different traffic control mechanisms, T1S1 has adopted a system comprised of multi-input nodes and a single output node with two hops in between (Figure 8).



Figure 8 Simplified Two Hops Network Diagram

4.1.2 Node Modeling

A network node can be any one of several physical devices such as a cross connect, packet switch, or multiplexer. For evaluation purposes a simplified node model has been defined. Each node is treated as a multiple-input, single-output system with a maximum output rate of the reference interface. Some of the control mechanisms such as resource allocation or a priority scheme may be implemented internally. The approximated node model is a FIFO queue disciplined with one buffered output queue (Figure 9).



Figure 9 Network Node Model

4.1.3 Traffic Source Modeling

The widely used two-state Markov chain model has been suggested in T1S1 as the traffic source. In the source modeling draft of the T1S1 work, the two active states are the nominal state and the burst state (Figure 10). While in the nominal state, the source emits cells with a given Poisson Process rate of R_n during a specified mean time (T_n) which is distributed exponentially. In the burst state, the source emits cells at a given burst rate (with deterministic cell inter-emission times) R_b . The length of the burst is random and is defiend by a probability distribution. The maximum burst length B_{max} may be specified. The source alternates between the active state (T_a) and the idle state (T_i) , with the time of a probability distribution. In the active state, the behavior may be modeled by the two-state Markovian process.



Figure 10 Two-state ATM Traffic Source Model

4.1.4 Evaluation Scenario Mechanisms

The one-hop tree approximation to the network has been used for the purpose of evaluating overall traffic control mechanisms. The various mechanisms that comprise the overall traffic control and congestion control framework are shown at the location where they may be implemented (Figure 11).



Poisson Process

Figure 11 Approximation Model of Control Schemes Scenario

4.2 Framework for Traffic Control and Congestion Control Functions

This section describes traffic control policies and the traffic management framework adopted as a draft recommendation at the December 1991 CCITT meeting at Melbourne, Australia and at the March 1992 meeting of T1S1.5 in Denver, Colorado. The initial framework was modified later and was approved by the CCITT XVIII Working Party 8 as I.371, "Traffic Control and Congestion Control in B-ISDN" at the recent June 1992 CCITT meeting in Geneva[33]. However, more sophisticated control mechanisms and algorithms need further development to accurately control real sources.

The following mechanisms form an initial framework for managing traffic in ATM networks and may be used in appropriate combinations in order to manage traffic and control congestion events.

- 1. Network Resource Management: It may make use of Virtual Paths and other networking techniques to manage network connections effectively.
- Connection Admission Control (CAC): A source requests a connection with given connection parameters such as QOS and a traffic descriptor. The network accepts or rejects the request for

Virtual Channel/Virtual Path (VC/VP) connection. CAC can combine common routing and priority control for services requiring a number of Virtual Circuit Connections (VCCs) with low differential delays and different cell loss ratios.

- 3. Usage/Network Parameter Control (UPC/NPC): The exchange termination monitors each connection to identify those cells that are not in compliance with the traffic descriptor. This network traffic descriptor is derived from the source descriptor agreed upon at connection establishment and may need to account for cell jitter that may be introduced by access multiplexing. When non-complying cells are detected, the exchange termination may take actions such as:
 - Violation Cell Tagging (Marking non-complying cells) and submitting them to the network
 - Discarding non-complying cells
 - Informing the source of the detection of non-complying cells
- 4. Congestion dependent network element (NE) cell processing: Congested NEs may take the following actions:
 - Selective Cell Discard: selectively discard explicitly identified non-complying cells and cells marked with CLP=1.
 - Explicit Forward Congestion Notification (EFCN): ATM NEs will set an EFCN indicator in the cell header PTI (Payload Type Identification) field of a service-user cell so that proper action may be taken at the End System (ES). When a NE is not in a congested state, it will not modify the EFCN indicator.
 - Backward Congestion Notification (BCN): A congested NE may send congestion notification in the backward direction.

This may be employed as a back-pressure mechanism. Due to the propagation times and switch processing loads involved, functionality should be limited to longer time scale prospects rather than instantaneous short reaction to frequent events (e.g., the control mechanism may be based on call levels rather than cell levels). The following actions may be considered when a given VC experiences congestion:

- An ATM switch can route back to the source with the message indicating the congestion. The source could then limit its use of bandwidth by way of traffic shaping.
- An ATM switch can broadcast back to certain VCs that their cell rates need to be adjusted.
- An ATM switch can broadcast back to the previous switch that violation tagged cells should be dropped immediately.
- An ATM switch can broadcast back to sources that no excess traffic should be allowed to enter the network.
- Exception/Failure handling: May require the ability to release connections; other handling may also be helpful.

5. TRAFFIC CONTROL and CONGESTION CONTROL FUNCTIONS in B-ISDN

This section describes control functions recently aproved by CCITT in June of 1992 as recommendation I.371, "Traffic Control and Congestion Control in B-ISDN". The following functions are described in this recommendation:

- Traffic Control Functions
 - 1. Network Resource Management
 - 2. Connection Admission Control
 - 3. Usage/Network Parameter Control
 - 4. Priority Control and Selective Cell Discarding
 - 5. Traffic Shaping
 - 6. Fast Resource Management
- Congestion Control Functions
 - 1. Selective Cell Discarding
 - 2. Explicit Forward Congestion Notification
 - 3. Reaction to UPC/NPC Failures
- Additional control functions that require further study
 - 1. Connection Admission Control that reacts to and takes account of the measured load on the network
 - 2. Variation of Usage monitored parameters by the network (e.g., reduction of the peak rate available to the user)
 - 3. Other traffic control techniques {e.g., re-routing, connection release, Operation, Administration and Maintenance (OAM) functions}

5.1 Traffic Control Functions

5.1.1 Network Resource Management

The current draft recommendation specifies the use of Virtual Paths (VPs) as an important component of resource management and other networking techniques are for further study. Virtual Path Connection can be used to:

- simplify Call Admission Control (CAC)
- implement a form of priority control by segregating traffic types requiring different QOS
- distribute messages efficiently for the operation of traffic control schemes such as to indicate congestion in the network by distributing a single message for all Virtual Channel Connections (VCCs) in a Virtual Path Connection (VPC)
- · aggregate user-to-user services such that UPC/NPC can be applied to the collective traffic
- · aggregate network capabilities such that NPC can be applied to the collective traffic

By reserving capacity on VPCs, the processing required to establish individual Virtual Channel Connections is reduced. Individual VCCs can be established by making simple connection admission decisions at nodes where VPCs are terminated.

Strategies for the reservation of capacity on VPCs will be determined by the trade-off between increased capacity costs and reduced control costs. These strategies then can be determined by service providers. When all virtual channel links within the VPC can tolerate the QOS resulting from the statistical multiplexing, statistical multiplexing of VC links within a VPC is possible. In this case the aggregate peak of all VC links may exceed the VPC capacity for short period of time. As a result, VPC

may be used to separate traffic in order to prevent its statistical multiplexing with other types of traffic when statistical multiplexing of VC links is required by the network operator.

5.1.2 Connection Admission Control (CAC)

A CAC is defined as the set of actions taken by the network at the call set-up phase (or during call re-negotiation phase) in order to establish whether a VCC or a VPC can be accepted or not. When a call is initiated, a connection request is accepted only when sufficient resources are available to establish a new call through the whole network at its required QOS and to maintain the agreed QOS of existing calls.

A call can require multiple connections in a B-ISDN environment and CAC procedures should be performed for each VCC or VPC in this case.

A user sends information with at least a source descriptor, OAM procedure (on-line or off-line based, in case of permanent or reserved service) and required QOS class provided by the network in order to establish a connection. CAC determines the following actions based on this information:

- whether the connection can be accepted or not
- traffic parameters (e.g., peak rate, average rate, burst length) needed by UPC
- routing and allocation of network resources

Different levels of network resources may be allocated for CLP = 0 and CLP = 1 traffic in order to insure network performance and to protect the network property. CAC may make use of the measured network load in addition to the information described above to achieve higher network utilization while still meeting the performance objectives. Routing is part of connection admission control actions.

5.1.3 Usage/Network Parameter Control (UPC/NPC)

UPC/NPC¹² is defined as the set of actions taken by the network to monitor and control traffic in terms of traffic volume and cell routing validity, at the user access and the network access respectively. The main purpose is to protect network resources from malicious as well as unintentional misbehavior which can affect the QOS of other already established connections by policing violations of negotiated parameters and taking appropriate actions. Connection monitoring includes all connections crossing the UNI or NNI. UPC and NPC apply to both user VCCs/VPCs and virtual signalling channels. UPC/NPC can perform various monitoring actions:

- checking the validity of VPI/VCI values.
- monitoring the traffic volume entering the network from active VPCs or VCCs in order to ensure that parameters agreed upon are not violated.

The specification for the UPC/NPC algorithm is currently under study by CCITT and T1S1 standard committees. Some details of UPC/NPC requirements need further study.

Which traffic parameters included in the source traffic descriptors are subject to control may vary, depending on CAC and UPC/NPC mechanisms. The following parameters may be included (common parameter to be controlled for all types of connections):

- peak cell rate
- average cell rate
- burstiness
- · peak rate duration
- source type

^{12.} Also referred to as bandwidth enforcement, or traffic policing

The objective of UPC/NPC is to insure that a user will not be able to exceed the negotiated traffic contract. To those compliant and non-compliant cells from ATM connections, actions of the UPC/NPC function at the cell level may be:

- cell passing
- cell re-scheduling (when traffic shaping and UPC are combined)
- cell tagging of violation (option to the network operator):
- cell discarding
- · releasing the connection

Research based on simulations[15] indicates that the submission of excess traffic (beyond negotiated parameters) may be useful. Statistical multiplexing may allow delivery of a managable fraction of the submitted tagged cells. The level of dropping for non-tagged traffic may also be managed with appropriate UPC/NPC mechanisms.

The leaky bucket policing mechanism[13] can be used to detect and tag excess traffic. Tagged cells submitted to the network may be discarded in an appropriate way if network or switch congestion becomes serious. Tagging and submitting excess cells has some positive and negative aspects. If sufficient network capacity is available, the cells may be delivered and thus it utilizes network bandwidth resources by taking advantage of statistical multiplexing. Although carrying tagged cells does place extra load on the network and can affect the QOS received by untagged priority cell streams, the QOS may still be acceptable if the network manages to accommodate the tagged load and if the discarding probability for priority cells can be made small.

The network operator has the choice of how the network will process traffic by providing the ability to handle cell tagging with potential discarding.

Cell sequence integrity is maintained on any ATM connection. Therefore, the UPC/NPC, including its optional cell tagging action, must operate in accordance with a single server and First In First Out (FIFO) service discipline for each ATM connection. UPC/NPC may provide OAM alarm indications to the user and to the network management when cell discarding occurrs on violated VCCs/VPCs.

5.1.4 Cell Loss Priority (CLP) Control and Selective Cell Discarding

Priorities for buffer access (also called space priorities) enable the ATM layer to adapt the quality of the cell transfer to the QOS requirements of the specific B-ISDN services to improve the utilization of the network resources. The peak rate bandwidth allocation per call does not take good advantage of the statistical multiplexing which enables a large number of B-ISDN services with a broad variety of traffic characteristics. In order to achieve high effciency in the use of network resources, especially bursty VBR traffic types in B-ISDN, suitable priority mechanism techniques have to be implemented. These must be able to guarantee the required cell transport performance without assigning the peak rate bandwidth to each call. The required cell loss probability of these traffic types may differ from one to another to guarantee an acceptable QOS. Thus, a suitable priority mechanism can take advantage of different levels of cell loss probability within the range of guaranteed QOS. In general, there are two types of priority mechanism policies; implicit and explicit[25]. The implicit assigns the same priority class to all cells of a service while the explicit alternates the choice of the priority class of each cell for each call.

Current priority control in B-ISDN addresses the priority mechanism based on cell loss by utilizing the CLP bit set to 0 or 1. As mentioned before, these two service capabilities can have different required cell loss probability.

Various implementation schemes[32] using priority control mechanisms for selective cell discarding in ATM networks which offer dedicated buffer access for each traffic class have been introduced:

1. Push-out scheme to increase the network utilization:

Cells of both priorities share a common buffer and if the buffer is full when a high priority cell arrives, a low priority cell will be pushed out and lost. A complicated buffer management mechanism may be necessary to guarantee the ATM cell sequence integrity.

2. Partial buffer sharing scheme:

Low priority cells can access the buffer only if the total buffer is filled to less than a preset threshold value. High priority cells can access the whole buffer all the time. The system can adapt to various load situations by adjusting the threshold value.

3. Separate routing scheme:

Different buffers are used for the two priorities. This is the simplest way to establish space priority capabilities within an ATM network. This mechanism[32] uses separate routes within the network. No special management actions are taken at the cell level, since the priority processing is performed at the call connection level by the routing function. This mechanism is only applicable if the priorities will be assigned on a connection basis, because the ATM network has to preserve the cell sequence.

The standards bodies define only the usage of CLP (two levels of priority) and do not restrict the priority control mechanisms at the customer premises. The network users may generate different priority traffic flows by using the CLP bit capability. Then the network may selectively discard cells of lower priority flows while maintaining network performance objectives on both flows. One reference[5] proposes two quality classes based on the virtual cell loss probability, deterministic class (CLP=0) and statistical class (CLP=1).

5.1.5 Traffic Shaping

A data traffic source generates messages of variable length that are usually longer than one ATM cell. It then has to be segmented into ATM cells such that AAL protocols and the ATM cell header have to be added before a message can be transported by the network. After a message is segmented into ATM cells, these cells are transmitted over a UNI interface with a payload capacity of 45 Mbps, 155 Mbps or 622 Mbps. The ATM cells belonging to the same message can be sent two different ways:

- back-to-back: the peak bit rate of the data application is the bit rate of the interface's payload such as 45 Mbps, 155 Mbps, or 622 Mbps.
- spacing: a number of unassigned cells (empty cells) can be inserted between two consecutive cells of the message. ATM cells assigned to other connections can be inserted if the interface is used by more than one connection, instead of inserting empty cells.

The peak bit rate equals 45 Mbps/(m+1), 155 Mbps/(m+1) or 622 Mbps/(m+1), respectively, with a uniform spacing of m cells. This means inserting a fixed number of m cells between each two consecutive cells of the message. Thus, with appropriate spacing, the peak bit rate of a data application can be adjusted to a value below the transmission rate of the broadband interface. The lowest possible value for the peak bit rate is the average bit rate of the application. The function performing the spacing is called traffic shaping or smoothing and its purpose is to ensure that the cell stream leaving the traffic shaper never exceeds the peak bit rate that has been negotiated between user and network at call set-up. The figure 12 shows a model of a flexible traffic shaper providing a cell stream at any peak bit rate r[42].



Figure 12 Traffic Shaper Model

In this operation, messages are sent into a buffer and are segmented into ATM cells. The ATM cells are then transmitted to a rate converter over an internal link operating at transmission bit rate r. The cells belonging to the same message are transmitted back-to-back on the internal link, and the speed converter automatically introduces a certain spacing on the payload capacity line if the transmission bit rate r of the internal link is lower than UNI reference rate of 155 Mbps (622 Mbps).

CCITT Draft Recommendation I.371 defines traffic shaping as a mechanism that alters the traffic characteristics of cell streams on VCC or a VPC to achieve a desired modification of those traffic characteristics. However, it must maintain cell sequence integrity on an ATM connection. It is an optional use to service providers in conjunction with suitable UPC functions, provided the additional delay remains within the acceptable QOS negotiated at call set-up. Some of these options for service providers are as follows:

- Re-shape the traffic at the entrance of the network and allocate resources regarding both the Cell Delay Variation (CDV)¹³ and the propagation delay allocated to the network.
- Dimension the network in order to accommodate the input CDV and provide for a shaper at the output.
- Dimension the network in order to accommodate the input CDV and comply with the output CDV without a shaping function.

A traffic shaper can be located at any place where an ATM connection for data applications is terminated such as B-TEs, terminal adapters, gateway in a CPN, entry node as an interworking unit or server of the B-ISDN network. Some literatures introduce a mechanism for average rate enforcement without using a traffic shaper, but in general, study results[29] show that traffic shaping improves network performance in bursty data services by decreasing cell loss ratio and cell queueing delay in multiplexers and switches. There will be a trade-off between these advantages and the extra delay due to traffic shaping functions are implemented in a CPN close to the traffic. However, the drawback is that it requires additional buffers to facilitate this and the end-to-end delay may be increased which may affect some delay-sensitive real-time services. The decision for service providers to implement traffic shaping may depend on the extra delay tolerance level of QOS requirements in the network.

5.1.6 Fast Resource Management (FRM)

The functions of FRM operate on the time scale of the round-trip propagation delay of the ATM connection. One of the functions can be that the network may allocate resource capacity (such as bandwidth and buffer space) for the duration of the burst if a user requests to send bursty traffic. When a source requests an increase of its Peak Cell Rate, it has to wait until resources have been reserved in all NEs along the ATM connection before the new Peak Cell Rate can be used; the UPC/NPC parameters would be adjusted accordingly. The functions of fast resource management are to be studied further.

5.2 Congestion Control Functions

5.2.1 Selective Cell Discarding

A congested Network Element (or Node) may selectively discard cells explicitly identified as a non-compliant ATM connection and/or those cells with higher cell loss priority (CLP=1). This is to protect low cell loss priority cell flows (CLP=0) as long as possible.

5.2.2 Explicit Forward Congestion Notification (EFCN)

The EFCN scheme is one in which the ATM node sends an explicit congestion indicating message to the end points of the congested route. It sets Payload Type Identifier (PTI) bits (Figure 13, Table 1 of [40]) of an ATM header cell and forwards the cell towards the network destination. Higher layer protocols of the receiving CPE may utilize this congestion indication so that CPE-to-CPE (end-to-end) protocols may then react by adjusting source traffic flow. Otherwise the source may send traffic in excess of negotiated rates to make effective use of idle network resources (especially during off-peak hours) until the network is

^{13.} Cell Delay Variation [40]: a quantification of variability in cell delay for a connection. Figure 3/L371 depicts the origins of cell delay variation and corresponding network performance parameters are specified in ANSI ASC T1.1

informed of the congestion via the EFCN function. The study[15] shows that the EFCN mechanism improves the effective use of idle network bandwidth. The T1S1 committee has adopted this mechanism.

PTI Field and Coding						
PTI coding	Interpretation					
000	Congestion not experienced, User data cell, ATM_user_to_ATM_user = 0					
001	Congestion not experienced, User data cell, ATM_user_to_ATM_user = 1					
010	Congestion experienced, User data cell, ATM_user_to_ATM_user = 0					
011	Congestion experienced, User data cell, ATM_user_to_ATM_user = 1					
110	Reserved for fast resource management (Note 1)					
111	Reserved for future functions					

Note 1: Refers to future functions that operate on the same time scale of the round-trip propagation delay of the ATM connection

Note 2: ATM_user_to_ATM_user = 0 indicates the beginning of the cell stream ATM_user_to_ATM_user = 1 indicates the continuation of the cell stream Figure 13 PTI (Payload Type Identification) Coding and Field

The objective of the forward congestion notification is to carry the congestion information by setting PTI bits in the ATM header when the local information indicates existing or impending congestion to the far end of the VCC/VPC end system. This is fed back to the source CPE, which may adjust its data rate by a traffic shaping mechanism.

Because the notification cells are forwarded to the network destination, no additional cell traffic is generated. This can be advantageous compared to the backward congestion indication mechanism which may have to generate new notification cells in the backward direction to the network source. As a result, this mechanism may make more effective use of network resources.

This mechanism has been adopted to be one of the elements of the overall congestion control in CCITT at the meeting of June 1992. Details of the mechanism used by the higher layer protocols in the customer equipment and the impact on the traffic/congestion control functions are to be studied further.

5.2.3 Explicit Backward Congestion Notification (EBCN)

The objective of EBCN is the backward notification of relevant congestion conditions via network element originated ATM cells. The BCN may be used by a network element (NE) to inform a previous NE, or by an access NE to inform an end system (ES).

Many algorithms are possible for EBCN, ranging from a simple link-by-link stop/go control to ones using a per-VCI algorithm. (e.g., a point-to-point EBCN mechanism is implemented in DEC's Autonet[14]). As examples, the EBCN could be generated at all input ports of the NE, or at just those links with VCs that use the congested buffers, or at just those links with VCs of particular service classes that use the congested buffers. The threshold could apply to the number of CLP=0 cells that are queued, as opposed to all cells. Also, there could be separate thresholds for each VC or for each class of VCs. If a NE receives the EBCN, then the control action might be stop/go, or an adjustment to the transmission rate.

This mechanism can be used between B-NT2 and multiple B-TEs at the customer premises as an effective congestion control in conjunction with the GFC performing a traffic control. However, the impact of the result may require further study.

The current T1S1 draft standard does not recommend any particular algorithm for this mechanism and only suggests that the mechanism can be utilized as a congestion control method and leaves it as a subject for further study.

5.2.4 Reaction to UPC/NPC Failures

The controlled traffic characteristics at the UPC/NPC can be different from the values agreed upon during the call set-up due to equipment (e.g., UPC devices, NEs) mulfunctions. Specific procedures in the ATM management plane should be designed for these situations.

5.3 Items/Issues under Study in CCITT

Traffic control and resource management has been separated from CCITT Recommendation Draft I.311, expanded, and re-organized as I.371. Those items still under study are summarized as follows:

- 1. ATM peak cell rate granularity and its coding and other traffic parameters.
- 2. Definition of Error Types at the UPC/NPC.
- 3. Interworking issues when using CLP bit and Resource Allocation Options.
- 4. Classification of Traffic Sources and their Relationship to Multiplexing Schemes and Traffic Parameters.
- 5. Characterization of Multiplexing Schemes and Relevant Traffic Parameters.
- 6. Handling of the Cell Delay and Cell Delay Variation (CDV) Classes.
- 7. Other traffic and congestion control functions not defined by current agreement.
- 8. Cell Loss Ratio objectives.
- 9. The role of priority control in CAC (Connection Admission Control).
- 10. Specific Quality of Service Classes.
- 11. Re-negotiation procedure and the impact on Network Element complexity.
- 12. Resource Allocation Schemes.
- 13. Methods for monitoring meta-signalling channels and OAM flows.
- 14. Potential fast resource management functions.
- 15. Congestion Control functions other than functions defined, such as selective cell discard and EFCN.
- 16. Cell based reactive congestion control techniques.
- 17. The mechanism by which the EFCN is used by the higher layer protocols in the customer equipment.
- 18. The impact of EFCN on the traffic control and congestion control functions.
- 19. The impact of equipment mulfunctioning situations on the UPC.
- 20. NPC location and provision of UPC at other locations.
- 21. UPC/NPC Function in relation to OAM signaling.
- 22. The need for and the definition of a standardized UPC/NPC Monitoring Algorithms.
- 23. Throughput of the traffic from B-TE is defined as the number of cells per UPC flag interval. In that UPC flag interval, B-TEs can send cells up to the specified number of cells which is defined as a UPC window-size. The interval can be determined per UNI based on the considerations that shorter intervals support a smaller variety of throughput classes and the longer intervals allow delay sensitive bursty cell arrival.
- 24. UPC counts the number of cells transmitted between adjacent UPC flags.
- 25. Other traffic control functions not described in framework for controlling and managing traffic in ATM networks in Section 7.3 of I.371.
- 26. The exact definition of the source traffic descriptor used at the connection set-up to capture the intrinsic traffic characteristics of the ATM connection associated with CLP=0 and CLP=1 cell flows.

- 27. Standardization of a number of Cell Dealy Variation values less than the maximum allowable value of CDV to apply to certain interfaces (on a subscription basis or on a connection basis).
- 28. The impact on standardization of the use of additional traffic control techniques (e.g., the impact on ATM layer management, user-network signaling and control plane).
- 29. The impact of Cell Loss Priority on the management of the capacity of the VPC.
- 30. The way to manage the situation when the instanteneous total peak of all VC links exceeds the VPC capacity when all VC links within the VPC can tolerate the QOS resulting from the statistical multiplexing.
- 31. The role of priority control in Connection Admission Control.
- 32. The subject of specific QOS classes.
- 33. The re-negotiation procedure and the impact on Network Element complexity.
- 34. Resource Allocation Schemes.
- 35. The definition of tolerances of controlling performance parameters in UPC/NPC.
- 36. Methods for evaluating UPC/NPC performances and the need to standardize these methods.
- 37. Additional performance parameters other than those described in desirable UPC/NPC features.
- 38. The exact definition of Type A and Type B errors in relation to the traffic contract and whether values of types have to be standardized.
- 39. The identification of possibilities shown in location of the NPC function (Figure 8/I.371).
- 40. Provision of UPC locations other than the location described in location of UPC functions (Figure 7/I.371).
- 41. For OAM alarm indication provided by the UPC/NPC to initiate other enforcement actions such as connection release.
- 42. Fast allocation of resources in an ATM network.
- 43. Cell-based reactive congestion control techniques.
- 44. Other congestion control functions not described in the congestion control of the framework.
- 45. The mechanism by which the congestion indication is used by the higher layer protocols in the CPE.
- 46. The impact of EFCN on the resource management and traffic control functions.
- 47. The impact of UPC mulfunctioning situations.
- 48. The mechanisms by which protocols above the ATM layer may exploit the EFCN functionality.
- 49. The interactions of the EFCN functionality with other traffic management mechanisms.
- 50. Procedures for setting the EFCN indicator.
- 51. Connection Admission Control that reacts to and takes account of the measured load on the network.
- 52. Variation of Usage monitored parameters by the network (e.g., reduction of the peak rate available to the user).
- 53. Other traffic control techniques (e.g., re-routing, connection release, OAM functions).

6. IMPLICATIONS OF TRAFFIC CONTROL IN B-ISDN

It is quite obvious that efficient preventive traffic control is far better than reactive congestion control in a high speed ATM network due to the complexity of B-ISDN services, QOS requirements, characteristics of supporting traffic, and high speed ATM switching and transmission rates. Once the congestion occurs, the impact on the network would be quite considerable. The ultimate solution is the harmonized coordination and management of the source traffic.

In order to achieve that goal, the following processes may be desirable. The traffic control mechanisms force users to stay within the range of safe traffic. They continuously monitor network traffic and detect the warning level. They then resolve and mediate the traffic in an early stage of congestion, using all resources while meeting efficient bandwidth utilization and throughput, bounded by QOS requirements. When an unavoidable congestion occurs even with the best efforts, congestion control mechanisms must react quickly. They must be able to minimize the impact, avoid the wide spread of congestion throughout the network. These can be done by dynamic notification of congestion status to the source, and by dropping packets, or even by releasing some of the existing call connections if necessary.

When it comes to ATM transport systems[3] consisting of ATM nodes, ATM network ends and user's ends, there will be no ATM level flow control inside the ATM network. Thus, the only possible flow control is between B-TE ends and ATM network ends. The role of GFC function is quite important in that regard, because it contributes significant congestion preventive actions at the very early stage of emitting traffic into the network, and at the same time it tries to maximize the degree of network utilization.

For these reasons, classical flow control mechanisms have to be reinvestigated to be useful in ATM networks and customer premises networks. New traffic control and congestion control mechanisms need to be developed within or even beyond the boundaries of traffic/congestion control functions defined by international standards bodies.

6.1 Traffic Management Strategies

Based on the observation of the complex broadband network environment, some fundamental strategies for the traffic management, which involves congestion control and congestion preventive control, can be derived as follows:

1. Prevention of congestion:

Preventing congestion is more effective than reactive actions when in congestion. This may be even more effective when the congestion control mechanism is uncertain. Use of GFC is essential at local customer premises.

2. Managing local problems locally:

If congestion has occurred, local focused strategies utilizing local traffic descriptors, local traffic flow loads and local network topologies should be imposed to resolve focussed overloads. Use of EBCN may be effective at local customer premises.

3. Allowing flexible bandwidth:

The bandwidth should be transmission rate independent and flexible enough to handle various network link rates. In ATM networks, flexible bandwidth on demand is one of the advantageous features.

4. Distributed controlling networks and resources:

In a high speed network, delays often cause problems for reactive congestion control. Controlling local problems locally is more desirable and this requires more distributed network and other resources. Some dedicated bandwidth can be allocated to simplify network control functions.

6.2 Requirements for Traffic Control Techniques in B-ISDN

Traffic control mechanisms being developed for use in ATM networks may have to consider general requirements in terms of network utilization, provisioning of QOS, fairness, policing, overload warning notifications, and so on. The following summarizes those requirements that traffic control schemes should

take into account.

- 1. The bandwidth management and traffic control techniques should allow the users to utilize the entire capacity of the network efficiently. User may not use the network at the expense of the other users. However, a user has full network capacity available if no other user transmits data at the same time.
- 2. The available network capacity has to be shared fairly among the network users.
- 3. If a user subscribes to a sub-network, then a user must be allowed the prescribed bandwidth without interference from the other users.
- 4. In operating with high speed access links at or over 155 Mb/s, traffic control should put very little processing overhead on the network. Thus, traditional windowing flow control by the network as it is employed in narrowband networks may be inappropriate in a high speed network. A study[30] shows that a node-to-node flow control on a per-connection basis is an ineffective mechanism, due to the processing requirement and the buffering requirement imposed on the nodes. For real reason, an ATM network does not provide node-to-node flow control inside the network. However, some literature[30][31] shows that a node-to-node rate based control scheme performs better than the end-to-end scheme, if the traffic is controlled and monitored with appropriate mechanisms on a per connection basis. It is the trend that the price of microprocessors and memories continuously declines, with higher processing power and bigger capacity. This may ease the burden of stringent requirements of more processing and buffering as the trend heads in that direction. Such a new scheme needs to be investigated further for possible use in B-ISDN.
- 5. In the network under congestion, the carried overload should not decrease as a function of the offered load. Thus, such techniques dropping packets at congested facilities (decreasing overload) and causing retransmission by the user are not acceptable.
- 6. The congestion control scheme should not rely on the users to inform the network at the beginning of the call about the traffic statistics. Most users are not likely to know this. However, some traffic information is needed to estimate required bandwidth in the network.
- ATM layer traffic control and congestion control mechanisms should meet the goal of objectives[37] set by B-ISDN standards bodies.

6.3 Traffic Control Techniques in B-ISDN

After a connection has been set up, the usage parameter control function monitors and regulates the actual behavior of the source traffic to ensure that the usage parameters (source traffic descriptors) conform to the values negotiated during the connection set-up phase. This function will contribute to the prevention of network congestion and will provide QOS effectively for network users. Several mechanisms have been reported in the literature in recent years about these policing functions[13][20][21][23][26]. The following summarizes well known mechanisms; some of them were implemented as UPC/NPC algorithms and are currently being studied by standards groups.

1. Leaky Bucket Mechanism:

This is an end-to-end, simple, rate-based window open loop preventive control scheme. It accepts cells from the source and controls the average rate of flow in a session with a certain allowable burst rate. In general, a leaky bucket algorithm consists of a bucket capacity or threshold and a leak rate. Whenever the rate of flow coming into the bucket exceeds the leak rate for a sufficiently long period of time, the bucket will overflow and the overflowing cells are marked as a violation of the algorithm. The leaky bucket algorithms leak rate should be equal to the peak cell rate and its capacity, or threshold value, should be large enough to accommodate a specified amount of CDV (cell delay variation).

2. Dual Leaky Bucket Mechanism:

This uses two leaky buckets in cascade. One leaky bucket provides the peak rate value while the other provides the traffic descriptor parameters or the equivalent sustained average value. The scheme operates by identifying those cells on an ATM connection which exceed the value of either peak rate or average rate that is built into the dual leaky bucket algorithm; such identified cells can then be treated by a traffic enforcement procedure (Figure 2/XVIII/8-7, p14/20 of [41]).

3. Jumping Window:

In this scheme, the counter is incremented when a cell arrives within the window (fixed time interval) and resets to zero at the end of the window. When the counter exceeds a predetermined threshold, the cell is is either discarded or tagged for cell loss.

4. Triggered Jumping Window:

In this scheme, the time windows are triggered by the first arriving cell. This eliminates the ambiguity of source synchronization for the time window and windows are not consecutive.

5. Moving Window:

In this scheme, the maximum number of cell arrivals within a window (W time slots) is limited like the jumping window scheme. But the adjacent windows overlap by W-1 slots.

6. Exponentially Weighted Moving Average:

In this scheme, the threshold in the i-th window is a function of an exponentially weighed total of accepted cells in the preceding windows. If no weight is given to previous windows, it defaults to the jumping window scheme.

7. Spacer-Controller Algorithm:

This is a traffic shaping mechanism where incoming cells are actively spaced out when they are considered too close together, according to the negotiated peak rate. Cell clusters are strictly eliminated; this is performed by hardware device called the spacer-controller. It is located in the UPC and NPC which schedules the period during which any cell is admitted to the network according to some spacing algorithm (Figure 1/XVIII/8-7 p13/20 of [41]).

8. Dangerous Bridge Sliding Window Algorithm:

In this algorithm, the maximum number of cells for each VPC/VCC on the bridge is limited simultaneously and this will guarantee the minimum cell number in any time period for each VCC/VPC (Figure 1/XVIII/8-7 p16/20 of [41]). A variable length bridge using a multi-tap FIFO stores any traffic data during the peak rate period and a dual UPC scheme is required as in the dual leaky bucket algorithm.

9. Flag Algorithm:

In this algorithm, the network or B-TE issues UPC flags periodically and the B-TE can send cells up to the specified number of cells within the flag interval (UPC window-size) (XVIII/8-7 p17/20 of [41]).

6.4 Standardization of Traffic Control Procedures

Even if the traffic control functions are defined and the objectives are set, traffic control procedures for ATM networks are currently not standardized within CCITT. It is even under debate whether they should be standardized at all. It is argued that network providers may want flexible network tools to adequately handle users' needs. On the other hand, standard procedures for networks may be necessary for the benefit of users and equipment manufacturers simply because of cost effectiveness and interoperability.

The method of implementing traffic control strategies directly impacts on a network's resource allocation admission control strategy. For instance, considering only the peak rate for CAC and UPC can simplify running ATM networks. Because the peak rate bandwidth would have to be allocated to the connection, the network utilization would be quite inefficient most of the time if this connection had a low average rate. However, considering the fact that neither the source traffic characteristics nor the traffic type mixes on a link are quite clear, it may be a safe strategy to run this way even if the network capacity is under-utilized. It may even reduce the probability of network congestion with a peak rate reservation and a restricted network utilization. Nevertheless, network capacity is an expensive resourcesive resources, and ought be utilized as efficiently as possible. Therefore, more sophisticated control procedures and resource management need to be developed in a timely manner, and have to be seriously considered for standardization.

7. REFERENCES

- [1] CCITT Study Group XVIII Report R-34, pp 20-22, June 1990.
- [2] O. Gihr, "A Layered Description of ATM Cell Traffic Streams and Correlation Analysis", IEEE INFOCOM'91, pp 137-144.
- [3] A. Eckberg, "Meeting the Challenge: Congestion and Flow Control Strategies for Broadband Information Transport", *IEEE GLOBECOM*'89, pp 1769-1773.
- [4] A. Gersht, "A Congestion Control Framework for ATM Networks", *IEEE GLOBECOM*'89, pp 701-710.
- [5] H. Suzuki & S. Sato, "A Burst Traffic Control Strategies for ATM Networks", IEEE GLOBECOM'90, pp 874-878.
- [6] G. Woodruff, "Multimedia Traffic Management Principles for Guaranteed ATM Network Performance", *IEEE Journal on Selected Areas in Communications*, Vol. 8, No 3, pp 400-437.
- [7] R. Dighe, "Congestion Avoidance Strategies in Broadband Networks", *IEEE INFOCOM'91*, pp 295-303.
- [8] F. Kuo, "Protocols and Techniques for Data Communications Networks", Prentice Hall, pp 122-169,1981.
- [9] K. Bala, "Congestion Control for High Speed Packet Switched Networks", *IEEE INFOCOM'90*, pp 520-526.
- [10] Z. L. Budrikis, "A Generic Flow Control Protocol for B-ISDN", IEEE INFOCOM'92, pp 895-904.
- [11] H. Chao, "Architecture Design for Regulating and Scheduling User's Traffic in ATM Networks", ACM SIGCOMM'92, Vol. 22, No. 4, pp 77-86.
- [12] W. Stallings, "Data and Computer Communications", MacMillan Publishing Co., pp (155-163, 312-319), 3rd Edition, 1991.
- [13] A. Berger, A, Eckberh and others, "Performance Characterizations of Traffic Monitoring, and Associated Control, Mechanisms for Broadband Packet Networks", *IEEE GLOBECOM'90*, pp 350-354.
- [14] M. Schroeder et al., "Autonet: a High-speed, Self-configuring LAN Using Point-to-point Links", Digital SRC, pp 17-19, April 30, 1990.
- [15] B. Makrucki, "Forward Congestion Notification in ATM Networks", 3rd Annual Workshop on Very High Speed Networks, pp 137-148, March 9, 1992.
- [16] G. Ramamurthy and R. Dighe, "A Multidimensional Framework for Congestion Control in B-ISDN", *IEEE Journal on Seleceted Areas in Communications*, Vol. 9 No. 9, pp 1440-1451, December 1991.
- [17] K. Bala and K. Sohraby, "Congestion Control for High Speed Packet Switched Networks", *IEEE GLOBECOM*'90, pp 520-526, December 1990.
- [18] T1S1.5/92-009, "Traffic Management/Congestion Control", pp 79-80, January 20, 1992.
- [19] A. Vasilakos, "Variable Window Flow Control and ergodic discretized learning algorithms for adaptive routing in data Networks", *Computer Networks and ISDN Systems 22 (1991)*, pp 235-248.
- [20] L. Zhang, "A New Traffic Control Algorithm for Packet Switching Networks", Proceedings of SIGCOMM'90, pp 19-29, 1990.
- [21] L. Zhang, "A Comparison of Traffic Control Algorithm for High-Speed Networks", 2nd Annual Workshop on Very High Speed Networks, 1991.
- [22] S. Morgan, "Queueing Disciplines and Passive Congestion Control in Byte-Stream Networks", *IEEE INFOCOM*'89, pp 711-720.

- [23] E. Rathgab, "Modeling and Performance Comparison of Policing Mechanisms for ATM Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 9, No. 3, pp 325-334, April 1991.
- [24] D. Hong & T. Suda, "Congestion Control and Prevention in ATM Networks", *IEEE Network Magazine*, pp 10-16, July 1991.
- [25] G. Gallassi, "Bandwidth Assignment in Prioritized ATM Networks", IEEE GLOBECOM'90, pp 852-856, November 1990.
- [26] G. Gallassi, "ATM: Bandwidth Assignment and Bandwidth Enforcement Policies", IEEE GLOBECOM'89, pp 1788-1793, November 1989.
- [27] S. Kowtha and D. Vaman, "Realization of a Multimedia Traffic Generator based on (u,a) Buffer Occupancy Analysis", Stevens Inst. of Tech. Internal Memo, pp 1-21, April, 1992.
- [28] K. Kawashima, "Teletraffic Issues in ATM Networks", Computer Networks and ISDN Systems 20 (1990), pp 369-375.
- [29] T1S1.5/90-264 & 265, "Performance of a Traffic Shaper, Simulation Results", October 29, 1990.
- [30] W. Leland, "Window-based Congestion Management in Broadband ATM Networks", IEEE GLOBECOM'89, pp 1794-1800, November 1989.
- [31] P. Mishra and H. Kanakia, "A Hop by Hop Rate-based Congestion Control Scheme", ACM SIGCOMM'92, pp 112-123, August 17, 1992.
- [32] H. Kroner, "Comparative Performance Study of Space Priority Mechanisms for ATM Networks", IEEE INFOCOM'90, pp 1136-1143, 1990.
- [33] T1S1.5/92-270, "CCITT B-ISDN Recommendations June 1992", August 3, 1992.
- [34] CCITT B-ISDN Recommendation I.413 (B-ISDN UNI), pp 117-122, December 1991.
- [35] CCITT B-ISDN Recommendation I.361 (B-ISDN ATM Specification), pp 18, June 1992.
- [36] CCITT B-ISDN Recommendation I.150 (B-ISDN ATM Functional Characteristics), pp 13-14, June 1992.
- [37] CCITT B-ISDN Recommendation I.371 (Traffic Control and Congestion Control in B-ISDN), pp 3-6, June 1992.
- [38] R. Despres, "Global speed WAN architecture for the 90's", Computer Networks and ISDN Systems 23 (1991), pp 125-128.
- [39] CCITT B-ISDN Recommendation I.211 (B-ISDN Service Aspects), pp 32-38, December 1991.
- [40] T1S1/92-457, "T1-ATM-199X DRAFT, B-ISDN ATM Layer Functionality and Specification", pp 2, August 29, 1992.
- [41] T1S1.5/92-014, "CCITT SG XVIII WP 8 Meeting Report", pp 46-47, January 20, 1992.
- [42] T1S1.5/90-263, "Traffic Shaping", October 29, 1990.
- [43] A. Tanenbaum, "Computer Networks", *Prentice Hall*, pp 631-641, 2nd Edition, 1988.
- [44] D. Gross, "Fundamentals of Queueing Theory", John Wiley & Sons, pp 1-13, 2nd Edition, 1985.
- [45] T1S1, "Broadband Aspects of ISDN Baseline Document Review", pp 8-15, 1990.
- [46] F. Guillemin and A. Dupuis, "A Basic Requirement for the Policing Function in ATM Networks", Computer Networks and ISDN Systems 24 (1992), pp 311-320.
- [47] J. Boudec, "An efficient solution method for Markov models of ATM links with loss priorities", *IEEE Journal on Selected Areas in Communications*, Vol. 9, No. 3, pp 408-417, 1991.
- [48] CCITT B-ISDN Recommendation I.121R (Broadband Aspects of ISDN), June 1990.

- [49] CCITT B-ISDN Recommendation I.321 (B-ISDN Protocol Reference Model and its Application), June 1990.
- [50] Y. Chang & D. Su, "Study of Generic Flow Control (GFC) in B-ISDN", NIST Internal Report, December 1992.
- [51] L. Kleinrock, "Queueing Systems", John Wiley & Sons, Inc., pp 1-20, 1975
- [52] D. Gross, "Fundamentals of Queueing Theory", John Wiley & Sons, Inc., pp 1-13, 1985

APPENDIX QUEUEING MODELS

- A. Queueing Models of Traffic Source Types
 - M (Markov) or PP (Poisson Process): Exponential Probability Density. Markovian property of the exponential. Arrival and service stream forms a Poisson process. This model was used in early development of circuit switched networks to model call arrival and in the development of packet switched networks to approximate data traffic. It is the traditional traffic model and is characterized by an exponentially distributed interarrival-time.
 - D (Deterministic): All members have the same value
 - G (General): Arbitrary (general) Probability Density
 - GI: A general distribution with independent inter-arrival or service time
 - BPP (Batch Poisson Process): Poisson Process with a batch of cells on each arrival
 - ON/OFF Process: An alternating renewal process where the source alternates between ON and OFF states. Cells are entered at deterministic intervals in ON state and no cells in OFF state.
 - IPP (Interrupted Poisson Process): A special case of ON-OFF process. The packet arrival process is not deterministic but follows Poisson Process in ON state.
 - E_k (Erlang law of K order): The Erlang-k distribution. A gamma with an integral number of degrees of freedom.
 - K/ON/OFF (K-Superposition of Identical ON/OFF sources): Superposition of K identically distributed ON-OFF sources.
 - Absolute EX (Absolute Exponential Model): The probability density function of the bit rate for various sources such as CATV, High Definition TV, video conference and video phone, are approximated by an absolute exponential density function.
 - MMPP (Markov Modulated Poisson Process): Two state continuous time Markov chain where traffic in each state follows the Poisson Process. The duration time in each state is exponentially distributed. Poisson Process is a special case of MMPP where the sojourn time in one of the two states is zero and an ON-OFF process can be represented by MMPP when one of the two states has zero arrival rate.
 - MMBP, (n-stage Markov Modulated Bernoulli Process): A n-stage Markov Modulated Bernoullii process which parameter is governed by a Markov chain taking values in a finite phase space. It is a discrete-stochastic process and is constructed from the time-continuous Markov Modulated Poisson Process.
 - SBBP (Switched Bernoulli Process): A two state model where sojourn time in a state follows the geometric distribution. Messages arrive according to the Bernoulli process with probability of arrival in a slot depending on the state the process is currently in.
 - DMAP (Discrete Time Markovian Arrival Process): It is represented by a discrete time Markov chain and the chain consists of a finite number of states. The sojourn time in each state is one time slot and a transition occurs at the end of a slot time. MMPP is a special case of DMAP.
 - SMMP (Special Semi-Markov Process): It consists of m states. Interarrival time in state "i" is based on some distribution. State transition occurs upon arrival based on a probability transition matrix. It is a version of DMAP where a transition occurs after an arrival.
- B. Queueing Disciplines

The following queueing disciplines are widely used[22]:

1. Store and Forward:

Incoming information flows into a per-channel buffer, and when the last bit of the data has reached the buffer, the channel number is placed in a FIFO queue from which the trunk server draws channel numbers for service. When the channel number reaches the head of the queue, the entire message is transmitted into the trunk. Store and Forward is similar in most ways to Message FIFO.

2. Message FIFO:

Each incoming message flows into a per-channel buffer, and when the last bit of the first packet has reached the buffer, the channel number is placed in a FIFO queue from which the trunk server draws channel numbers for service. Service of a message is not interrupted once service is started until the last bit of the message has been put into the trunk.

3. Packet FIFO:

Messages arrive asynchronously from a number of sources in a packet FIFO. Each message is divided into packets of some maximum length. The packets are collected in a single FIFO from which they are transmitted over the trunk.

4. Packet FIFO with Priority:

This is derived from a Packet FIFO that reduces the queueing delay of single-packet messages. There are separate high priority and low priority queues in Priority with Packet FIFO. A packet that contains fewer than the maximum number of bytes permitted in a full length packet is assumed to represent a single packet message. Such a single packet message is placed at the end of the high priority queue (high priority FIFO). A full length packet is placed at the end of the low priority queue (low priority FIFO), as is a short packet if there are any other packets from the same channel currently in the system. The trunk server serves the high priority queue until the high priority queue is empty and then it serves the low priority queue, checking after each packet to see whether any new high priority FIFO queue.

5. Processor Sharing:

This is a mathematically defined queueing discipline in which, if there are a number of customers to be served in the system, each customer receives a proportional capacity of the server. It approximates Round Robin if the packet size is small compared to the message length and the trunk runs no faster than the access lines.

6. Round Robin:

Arriving messages are held in per-channel buffers and when a channel has data to transmit, its channel number is placed at the end of a FIFO list of channel numbers. When the channel number reaches the head of the list, the trunk server takes one packet from the given channel. If this does not empty the channel buffer, the channel number is returned to the end of the list. In general, many studies show that the the Round Robin disciplines have good fairness among light users and heavy users in the network.

7. Round Robin with Priority:

This is a derivative of Round Robin to reduce the queueing delay of short messages. As in Round Robin, arriving messages are held in per-channel buffers. When a channel has data to transmit, its channel number is added to a priority FIFO list of channel numbers. One packet is transmitted from the given channel. If this does not empty the per-channel buffer, the channel number is put at the end of the second list which runs the Round Robin discipline. After transmitting each packet the server checks whether there are any channel numbers waiting in the priority list, and if so the server serves them first. A new message is put into the priority FIFO and after it is served once it is put into the Round Robin queue; this expedites the short message queueing delay. Multiple priority levels may be useful in some situations.

8. Priority Round Robin with Hysteresis:

This avoids a difficulty of Priority Round Robin in high speed trunks. The first packet of a multi-packet message may be completely transmitted over the trunk before the second packet arrives from the access line if the trunk runs at high speed. In that case the channel number disappears from the system when the first packet is sent, and the second packet is given priority handling that it should not have. Simulations show that under heavy congestion the round robin queue can be frozen out, so that some messages wait in the round robin for a long time, while other messages get all their service from the priority queue and complete quickly. To avoid this situation, after a channel number passes through the priority queue it is automatically put at the end of the round robin queue, regardless of whether the channel buffer is emptied or not. If there is still no work waiting when the channel number reaches the head of the round robin queue, the channel number is deleted from the system. So channel numbers do not disappear until they have made at least one pass through the round robin.

ACRONYMS

	<u> </u>		
AAL	ATM Adaptation Layer	VBR	Variable Bit Rate
ANSI	American National Standards Institute	VCC(s)	Virtual Channel Connection(s)
ATM	Asynchronous Transfer Mode	VCI	Virtual Channel Identification
BCN	Backward Congestion Notification	VP(s)	Virtual Path(s)
B-ISDN	Broadband Integrated Services Digital Network	VPC(s)	Virtual Path Connection(s)
B-NT2	B-ISDN Network Termination 2	VPI	Virtual Path Identification
B-NT1	B-ISDN Network Termination 1		
B-TE(s)	Broadband ISDN Terminal Equipment		
CAC	Connection Admission Control		
CBR	Constant Bit Rate		
CC	Congestion Control		
CCITT	The International Telegraph and Telephon Consultative Committee		
CDV	Cell Delay Variation		
CL	Connectionless		
CLP	Cell Loss Priority		
CO	Connection Oriented		
CPE(s)	Customer Premises Equipment		
CPN(s)	Customer Premises Network(s)		
CVT	Cell Violation Tagging		1
DQDB	Distributed Queue Dual Bus		
EBCN	Explicit Backward Congestion Notification		
EFCN	Explicit Forward Congestion Notification		
ES(s)	End System(s)		
FCN	Forward Congestion Notification		
FDDI	Fiber Distributed Data Interface		
FRM	Fast Resource Management		
GFC	Generic Flow Control		
HEC	Header Error Check		
IEEE	Institute of Electrical and Electronics Engineers		
LAN	Local Area Network		
MAN	Metropolitan Area Network		
NE(s)	Network Element		
NNI	Network-Network Interface		
NPC	Network Parameter Control		
OAM	Operation, Administration and Maintenance		
OSI	Open Systems Interconnection		
PC	Priority Control		
PDF	Probability Density Function		
PP	Poisson Process		
PT	Payload Type		
PTI	Payload Type Identifier		
QOS	Quality Of Service		
RM	Resource Management		
SCD	Selective Cell Discard		
SDH	Synchronous Digital Hierarchy		
SONET	Synchronous Optical Network		
STM	Synchronous Transfer Mode		
UNI	User-Network Interface		
UPC	Usage Parameter Control		