Traffic Policing

Agilent Technologies Broadband Series Test System Application Note

Introduction

ATM networks have been touted as “one of the few networks that can provide the real-time and quality of service guarantees required for new multimedia data types”. However, as the networks become larger, busier and more complex, fulfilling this quality of service guarantee will not be a simple task. What are the end effects or the service layer effects if the quality of service (QoS) is less than expected? If cells are lost in a data communications application, retransmission may be required. If cells are delayed, timers may expire causing even more delays. In a video-on-demand service, if the cell delay variation in the ATM network increases due to congestion, the buffers in a set-top box may begin to underflow causing blanking or jagged movements.

Fortunately, there has been a great deal of forethought by members of the international standards bodies and industry forums to mitigate potential problems and to ensure that users of ATM networks get the QoS they expect.

ATM layer traffic control is designed to avoid network congestion — preventative traffic management. Network congestion is a state when the network cannot meet the negotiated network performance objectives for established connections or for new connection requests. The goal of traffic control is to protect the network, and other users of the network, so that everyone receives the performance that they pay for and depend on.

There are six traffic control functions that are important to maintaining network performance.

- Network resource management.
- Connection administration control.
- Selective cell discarding.
- Traffic shaping.
- Explicit forward congestion indication.
- Usage parameter control.

This paper focuses on one of the key ATM traffic control functions, Usage Parameter Control (UPC), commonly referred to as traffic policing.

To place UPC in the correct context this paper discusses traffic contracts which determine, for each connection, what requirements the UPC will uphold. The Generic Cell Rate Algorithm is discussed to understand what it means when a traffic contract specifies, for example, a peak cell rate. A significant portion of this paper considers the importance and the methods of testing UPC mechanisms. This paper finishes with a brief comment on some of the current standards activities in policing Available Bit Rate (ABR) services.

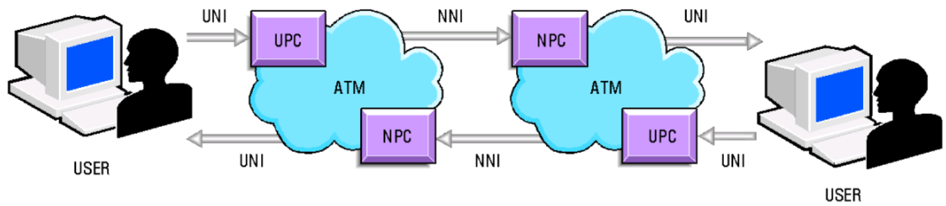

Figure 1: Location of policing mechanisms in an ATM network.

Usage Parameter Control

A key component of traffic control is Usage Parameter Control (UPC). UPC, often referred to as traffic policing, is a network mechanism which ensures that users do not violate their traffic contracts — accidentally or maliciously. Policing detects and stops contract violations so that the Quality of Service (QoS) of other connections are not effected by a traffic violator. As ATM networks mature, and especially as we begin to see switched virtual circuit (SVC) services appear, UPC mechanisms will become increasingly important. Figure 1 illustrates where the policing mechanisms are located in the network.

Usage Parameter Control and Network Parameter Control perform similar functions, but reside at different locations in the network. The UPC mechanism governs user-network interfaces (UNI) and the NPC mechanism governs at network-node interfaces (NNI). In the latest issue of ITU-I.371, UPC is recommended and NPC is optional. The UPC function is a requirement at the Public UNI in the ATM Forum UNI Specification. UPC is a network mechanism which monitors traffic submitted by a source at the public UNI.The main function of the UPC is to monitor the traffic cell rate for contract violations; however, the UPC also checks to ensure that the traffic submitted has a valid VPI/VCI. Cells with invalid VPI/VCI values could cause erroneous cells to be inserted into another connection — cell misinsertion.

Simply stated, UPC is like a policeman which monitors and enforces the law as defined by the traffic contract. If the UPC detects invalid or illegal traffic, it can discard the cell or it can optionally tag the cell by asserting the Cell Loss Priority (CLP) bit in the ATM header. Conversely, the UPC must pass or reschedule (traffic shape) conforming traffic. Any traffic that is shaped must still conform to the QoS objectives specified in the contract. By discarding or tagging illegal cells, UPC protects the network by ensuring that network resources are available for all users.

When connections are established (in the case of switched virtual circuits), a set of traffic contract parameters are negotiated prior to connection in the signalling procedures.

These parameters are collectively referred to as a connection traffic descriptor. In the case of permanent virtual circuits, the contract is agreed between the carrier and user. This negotiation is necessary to ensure that the network can support the QoS desired by the customer.

The connection traffic descriptor is used to parameterize the UPC mechanisms for that connection. Depending on the type of connection or service desired, different parameters are exchanged between the user and the network. The Peak Cell Rate(PCR) plus a Cell Delay Variation Tolerance (CDVT), and the Sustainable Cell Rate (SCR) plus a Maximum Burst Size (MBS), are two pairs of parameters currently defined in ATM Forum 3.x. These parameters are defined in relation to the Generic Cell Rate Algorithm (GCRA) which determines whether each cell is conforming or non-conforming.

According to the ATM Forum, it is a requirement to police the PCR, but policing the SCR is optional. Figure 2 is a simplified diagram of the decision-making process in a simple UPC mechanism. The decision boxes represent a GCRA.

In practice, UPC can be quite complex because of the different flows of traffic within a channel or path. The CLP bit in the ATM header creates a high and low priority flow for a connection. The PCR and SCR can separate monitoring of the CLP=0 flow and of the CLP=0+1 (aggregate of CLP=0 and CLP=1 streams) flow. Additionally, there is a separate set of parameters for each direction of cell flow! For a single bi-directional connection, there can be up to eight rate parameters which define cell flow conformance. Figure 3 illustrates a more complex UPC process.

In this discussion of UPC, we have briefly mentioned traffic contracts and the GCRA, two very important topics that will be covered in the following two sections.

Generic Cell Rate Algorithm

UPC implementations are vendor independent, which allows vendors to optimize their particular policing algorithms. However, this independence requires a common or reference definition of traffic parameters. The ATM Forum has defined the Generic Cell Rate Algorithm (GCRA) adopted from the Peak Cell Rate Reference Algorithm defined in ITU-I.371.

The GCRA is a reference algorithm for cell rate which determines if a cell is conforming. The GCRA is a relatively simple algorithm illustrated as a flow chart. There are two different but equivalent representations of the GCRA — the Virtual Scheduling Algorithm (less commonly known) and the Continuous-State Leaky Bucket Algorithm (commonly known). Figure 4 on previous page shows the two equivalent representations of the GCRA.

As shown in Figure 4, the GCRA requires only two parameters: I=increment and L=limit. GCRA(I,L) defines the cell rate conformance. The GCRA is commonly referred to as the Leaky Bucket Algorithm because of the visual analogy to a leaking bucket. The action of a leaky bucket can be dimensioned with two parameters, the drain rate of the bucket and the height of the bucket. The greater the drain rate, the faster the cells pour out of the bucket.

The greater the height of the bucket, the more cells the bucket can buffer. If the cells are pouring too quickly into the bucket, the bucket will overflow and cells will be lost.

The following example demonstrates the operation of the GCRA. Consider a video-on-demand service where the negotiated PCR = 50 kcells/s and the

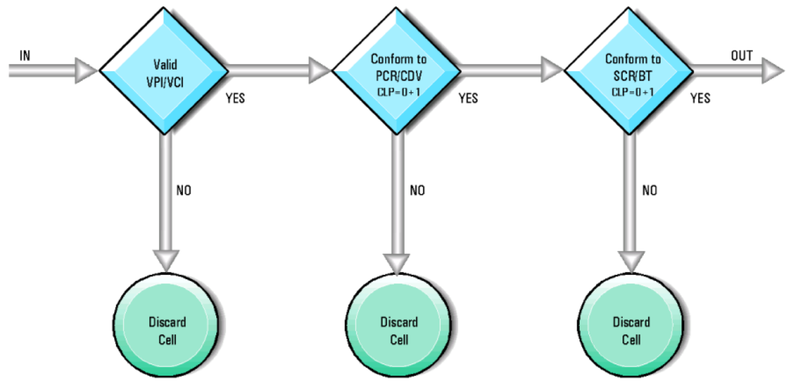

Figure 2: Decision process in a UPC mechanism.

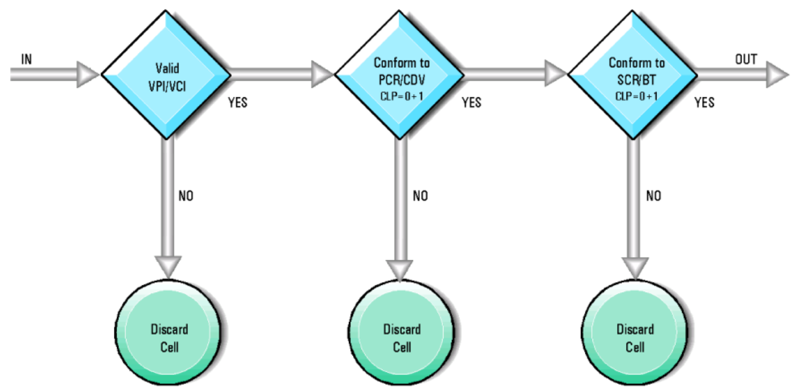

Figure 3: Complex UPC process.

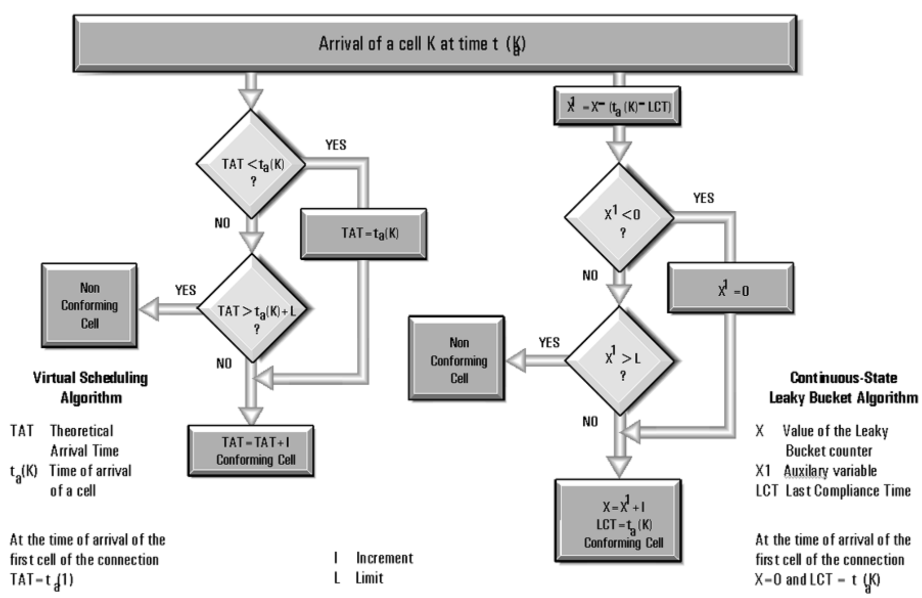

Figure 4: Equivalent representations of the generic cell rate algorithm

k	t_a(k)	LCT (k)	X (k)	X^1(k)	Conforming?
0	0 µs	0 µs	0 µs	0 µs	Yes
1	20 µs	0 µs	20 µs	0 µs	Yes
2	25 µs	20 µs	20 µs	15 µs	Yes
3	30 µs	25 µs	35 µs	30 µs	Yes
4	35 µs	30 µs	50 µs	45 µs	Yes
5	40 µs	35 µs	65 µs	60 µs	No
6	45 µs	35 µs	65 µs	55 µs	No
7	50 µs	35 µs	65 µs	50 µs	Yes
8	55 µs	50 µs	70 µs	65 µs	No
9	80 µs	50 µs	70 µs	40 µs	Yes
	100 µs	80 µs	60 µs	40 µs	Yes

Figure 5: Example of the GCRA.

CDV Tolerance = 50 us. The cells in this example arrive at the times as indicated by the t_a (k). (Note: GCRA (I,L) where L = T = 1/PCR = 20 µs/celland L = *t* = 50 µs.)

Although the user bursted cells at four times the specified PCR, the GCRA still judged the cells to be conforming because the CDV Tolerance allowed limited bursting. However, when k=5, excessive bursting caused a cell to be non-conforming. When the user throttled back the cell rate, the cells conformed.

As stated earlier, the GCRA is a reference algorithm for determining cell rate conformance. We have mentioned the different traffic parameters such as PCR, SCR and BT which are defined in relation to the GCRA. But how do you use the GCRA with these parameters?

Peak Cell Rate

The ATM Forum requires specification of a PCR parameter. The ATM Forum also requires that the user select a value for the CDV Tolerance from a set of values supported by the network. As discussed above, these two variables are sufficient to parameterize a GCRA to determine conformance.

The minimum cell interval (1/PCR), T, and the CDV Tolerance, *t*, are the increment and the limit for the GCRA and are denoted as GCRA(T, *t*). A different PCR can be stated for the CLP = 0 and the CLP = 0+1 streams which would be denoted as GCRA ($T_{0,t}$) and GCRA ($T_{0+1,t}$), respectively.

Sustainable Cell Rate and Burst Tolerance

SCR and BT are optional parameters that are jointly declared under the ATM Forum specification. The SCR specifies the average cell rate over the period of the connection. The BT, in conjunction with the SCR and the GCRA, determines the Maximum Burst Size (MBS) that can be submitted at the PCR.

The SCR for a connection only makes sense if it is less than the PCR. Specifying an SCR is a further restriction on the submitted traffic and should require less network resources. Specifying an SCR and BT would only make sense for VBR services. These two variables are sufficient to parameterize another GCRA.

The average cell interval (1/SCR), T_S, and the BT, t_S, are the increment and the limit for the GCRA and are denoted as GCRA(T_S, t_S). The SCR and BT for the CLP = 0 and CLP = 0+1 streams are denoted as GCRA(T_{S0}, t_{S0}) and GCRA (T_{S0+1}, t_{S0+1}). Since a CDV Tolerance effect the limit variable of the GCRA, it can be summed with the BT to account for this effect — GCRA(T_S, t_S+t).

Actually, the MBS (in cells) and not the BT is sent in the signalling message which must be translated into the BT parameter. This is done using the following equation: BT =t_S = (MBS-1) (T_S -T)

Traffic Contracts

A traffic contract is an agreement between the user and the network which is negotiated at connection time prior to traffic entering the network. For permanent circuits, the traffic contract is agreed upon when the circuit is provisioned. For switched virtual circuits, the traffic contract is negotiated in the signalling protocol during the call setup. Of particular relevance to traffic policing is the negotiation of the elements of the Connection Traffic Descriptor and the definition of a compliant connection.

As a cell flows through the UNI, cell conformance is determined by the conformance definition. The conformance definition is a defined combination of GCRAs or leaky buckets to which the cell must conform. However, a network operator must also define a compliant connection.

Even though some cells are non-conforming, they may still be deemed compliant depending on the compliant connection definition as defined by the network operator. In other words, the network operator may allow a number of non -conforming cells to pass up to some threshold.

Connection Traffic Descriptor

The Connection Traffic Descriptor specifies the traffic characteristics of a connection. The Connection Traffic Descriptor consists of the following:

- Source Traffic Descriptor
- CDV Tolerance
- Conformance Definition

Source Traffic Descriptor

The Source Traffic Descriptor is the subset of traffic parameters requested by the source (user) which characterizes the traffic that will (or should) be submitted during the connection. The Source Traffic Descriptor includes parameters such as the PCR, SCR and BT. In ATM Forum 3.x, the signalling message specifying parameters is the ATM User Cell Rate information element. This message is sent from the user to the network as an information element in a General Message Format. The ATM User Cell Rate message has fields for specifying the PCR, SCR and MBS for CLP = 0, CLP = 0+1 in both the forward and backward direction. Please refer to ATM Forum UNI 3.x section 5.4.5.6 for a full description of this message.

The rate parameters conveyed in the Source Traffic Descriptor also gives the network, information as to the additional amount and the type of load on the network which helps in setting up other traffic control functions such as Network Resource Management and Connection Admission Control.

QoS Class	Service	Example
1	Circuit emulsion, CBR video	CBR video conferencing
2	VBR audio & video	Video on demand
3	Connection-oriented data transfer	Frame relay
4	Connectionless data transfer	SMDS

Figure 6: Specified QoS Class Descriptions.

CDV Tolerance

The CDV Tolerance is specified indirectly by the QoS class which is another negotiated traffic contract parameter. The various QoS classes are differentiated by their performance parameters such as cell delay variation, cell transfer delay and cell loss ratio. The specific network provider quantifies these network performance parameters for each class. Currently there are five QoS classes defined — one unspecified class and four specified classes. The unspecified class (QoS Class 0) does not specify any parameters and is intended for “best effort” services. The specified QoS classes (QoS Classes 1-4) are defined in a manner such that they specify the type of service it can support.

Thus, for each Specified QoS Class, the network provider will specify the CDV objective as one of the performance parameters. This CDV Tolerance can then be used in relation to the GCRA with the PCR or SCR and BT to determine cell conformance in a UPC.

During the call setup procedure, the QoS class is requested (and indicated) in the Quality of Service Parameter information element. Please refer to the ATM Forum UNI 3.x section 5.4.5.18 for further details.

Conformance Definition

The Conformance Definition states the combination of GCRAs that define if a cell is conforming. For example, a Conformance definition could state that a cell that conforms to both a GCRA monitoring PCR of the CLP = 0+1 stream and a GCRA monitoring SCR of the CLP = 0 stream is a conforming cell.

In summary, a Traffic Contract, which includes the elements of a Connection Traffic Descriptor, are negotiated between the user and the network at connection time. The elements of the

Connection Traffic Descriptor include the CDV Tolerance, the Source Traffic Descriptor (PCR, SCR, BT) and Conformance Definition, which together, are sufficient to provision a UPC mechanism. However, depending on the network operator’s compliant connection definition, non-conforming cells may still be allowed to pass up to some threshold.

Testing Policing Implementations

A UPC mechanism which discards compliant traffic is violating the traffic contract and not delivering the expected QoS to the user. A UPC which does not discard non-compliant traffic could be jeopardizing the QoS of other users on the network by allowing a traffic violator to utilize more network resources than were originally provisioned. Needless to say, testing of traffic policing mechanisms is a very important process.

Testing UPC implementations is a challenging task because of the different types of traffic profiles that are possible. What type of traffic is appropriate for thoroughly testing a PCR leaky bucket? This section attempts to tackle these problems.

The two main aspects to testing policing algorithms are generation and analysis. The generation aspect consists of generating appropriate traffic to fully test the UPC implementation. Analysis consists of monitoring a cell stream and determining how many of those cells are non-conforming.

Generation

The traffic generation functionality required to test a UPC mechanism is to basically generate two types of traffic, conforming and non-conforming. It would be highly desirable feature on test equipment to generate conforming or non-conforming traffic by simply entering the traffic connection descriptor. However, there are many different traffic patterns that a developer may wish to generate in order to test the policing functions. Figures 7 through 12 illustrate each of these types of traffic patterns.

In these examples, PCR = 50 kcells/s and CDVT = 50µS.

The traffic profiles to the right have the same basic pattern, a burst of cells (possibly only one cell) followed by an idle time until the next burst. Therefore, using the following set of parameters, any of the above traffic profiles can be created to test a UPC implementation.

- Burst Length, J cells
- Burst Gap, K cells
- Number of non-conforming cells, M, occurring every N bursts
- Peak Emission Interval, T, and the CDV tolerance, *t*

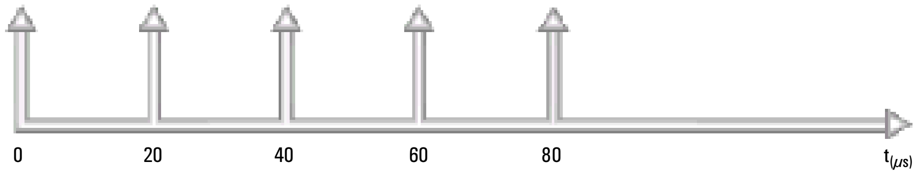

Figure 7: Conforming cell stream: each cell separated by 1/PCR.

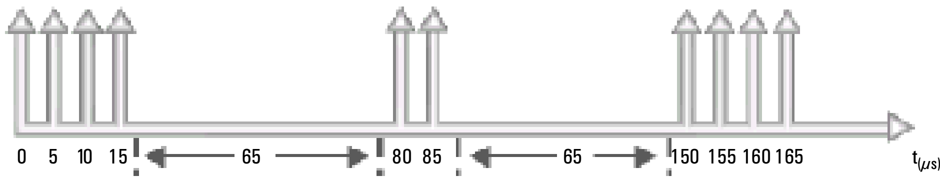

Figure 8: Conforming cell stream: bursted but meets CDV tolerance parameter.

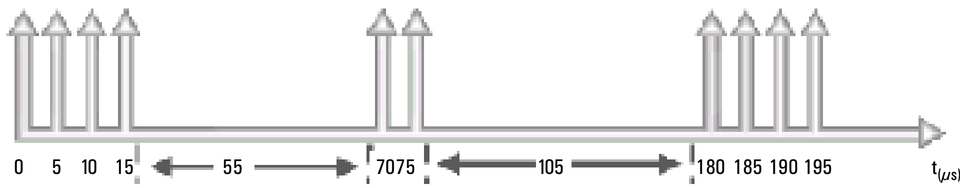

Figure 9: Conforming cell stream: bursts separated by random interarrival times.

Figure 10: Conforming cell stream: random cell arrival:

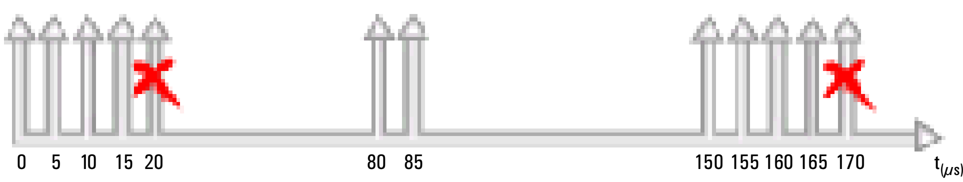

Figure 11: Non-conforming cell stream: bursted but some non-conforming.

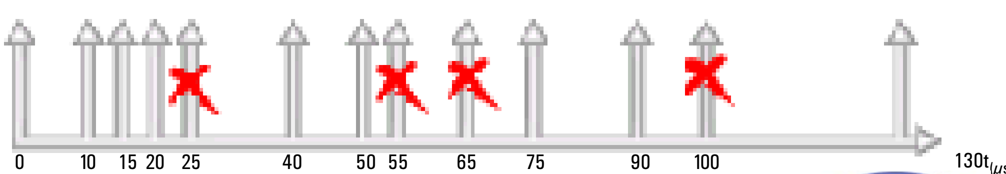

Figure 12: Non-conforming cell stream: random cell arrival.

Traffic Analysis

Analysis of data is a necessity in order to ensure that UPC implementations are correctly detecting and discarding non-conforming data and passing conforming data. As mentioned earlier, the actual UPC implementation is vendor dependent; however the implementation must not discard conforming cells.

The simplest method for analysing conformance is to simply monitor the channel, apply the GCRA to the cell stream and count the number of non-conforming cells. This number can subsequently be compared to the number of cells that the system under test discarded or tagged. This is a simple and straightforward test, however, this method does not truly indicate if the system under test is discarding only non-conforming cells.

A more accurate method is to actually control the contents of the cell stream. For example, by creating a CLP = 0 and a CLP = 1 cell sequence with each cell containing a sequence number, a flag indicating the original CLP value, the total number of cells in the sequence and a CRC field. Using this type of cell stream a tester can determine from the captured cells, what type of cells were discarded, how many cells were discarded and how many cells were tagged.

Policing ABR Services

Available Bit Rate (ABR) service is a new service definition where the cell rate provided by the network can change throughout the connection — the user gets what's available. It is expected that the cell loss ratio of ABR services is minimal provided that the user adapts to the networks feedback controls. After much discussion, the ATM Forum finally resolved that ABR services will be a rate-based service with resource management (RM) cells conveying rate and other information to the user. Undoubtedly, as the standard for this service type evolves, there will be a requirement to police ABR services.

Policing ABR service is still under discussion, however there have been several ideas that have been very popular. At connection time, the user will negotiate a Peak Cell Rate along with a Minimum Cell Rate (MCR, which can be zero). The current baseline text in the ATM Forum states that the user cannot exceed the PCR and the network guarantees the MCR. Both the PCR and MCR are defined in accordance to the GCRA.

What happens if a terminal does not obey the feedback controls (i.e. rate information) from RM cells? Will the network really provide the minimum usable bandwidth? There has been some preliminary discussion with regard to a dynamic UPC/NPC — however, nothing firm has yet to evolve. There are many questions to be answered and much testing to be performed.

Summary

Traffic control functions, including UPC, exist in ATM Networks to prevent network congestion — a highly undesirable state where the network is not achieving its QoS objectives. A UPC mechanism is responsible for checking the validity of traffic submitted on a connection at the UNI. The UPC polices the connection according to rules, including cell rates, which are set out in a traffic contract negotiated between the user and the network. There are two types of cell rates that can be policed and these rates are defined according to the GCRA. The first rate type is the Peak Cell Rate, a required traffic parameter, which specifies the upper bound on submitted traffic. The second rate type is the Sustainable Cell Rate, an optional traffic parameter jointly declared with a Burst Tolerance, which specifies the average cell rate over the duration of a connection. A UPC can monitor the Peak Cell Rate or it can police both the Peak and Sustainable Cell Rate of a connection.

Methodology for testing UPC mechanisms was discussed including traffic generation and traffic analysis. A key to testing a UPC mechanisms is in generating barely conforming and barely non-conforming traffic.

Acronyms

ABR	Available Bit Rate
ATM	Asynchronous Transfer Mode
BT	Burst Tolerance
CDVT	Cell Delay Variation Tolerance
CLP	Cell Loss Priority
GCRA	Generic Cell Rate Algorithm
ITU	International Telecommunications Union
MBS	Maximum Burst Size
NNI	Network-Node Interfaces
PCR	Peak Cell Rate
QoS	Quality of Service
SCR	Sustainable Cell Rate
SVC	Switched Virtual Circuit
UNI	User-Network Interfaces
UPC	Usage Parameter Control
VBR	Variable Bit Rate
VPI/VCI	Virtual Path Identifier/ Virtual Channel Identifier

Agilent Technologies Broadband Series Test System

The Agilent Technologies BSTS is the industry-standard ATM/BISDN test system for R&D engineering, product development, field trials and QA testing. The latest leading edge, innovative solutions help you lead the fast-packet revolution and reshape tomorrow's networks. It offers a wide range of applications:

- ATM traffic management and signalling
- Packet over SONET/SDH (POS)
- switch/router interworking and performance
- third generation wireless tesing
- complete, automated conformance testing

The BSTS is modular to grow with your testing needs. Because we build all BSTS products without shortcuts according to full specifications, you'll catch problems other test equipment may not detect.

www.Agilent.com/comms/BSTS

United States:
Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:
Agilent Technologies Canada Inc.
5150 Spectrum Way
Mississauga, Ontario
L4W 5G1
1-877-894-4414

Europe:
Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-9999

Japan:
Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura-Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:
Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #950
Miami, Florida 33126
U.S.A.
Tel: (305) 267-4245
Fax: (305) 267-4286

Asia Pacific:
Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 2599-7889
Fax: (852) 2506-9233

Australia/New Zealand:
Agilent Technologies Australia Pty Ltd
347 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

Specifications subject to change.

5963-7510E 04/00 Rev B

Agilent Technologies
Innovating the HP Way