EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 301

March 1995

Source: ETSI TC-NA

Reference: DE/NA-052801

ICS: 33.080

Key words: Broadband, ISDN, traffic, congestion

Broadband Integrated Services Digital Network (B-ISDN); Traffic control and congestion control in B-ISDN

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

The Broadband Integrated Services Digital Network (B-ISDN), which is based on the Asynchronous Transfer Mode (ATM) technique, is designed to transport a wide variety of traffic classes satisfying a range of transfer capacity needs and Network Performance (NP) objectives.

The primary role of traffic control and congestion control parameters and procedures is to protect the network and the user in order to achieve NP objectives. An additional role is to optimize the use of network resources.

The uncertainties of broadband traffic patterns, traffic control and congestion control complexity suggest a step-wise approach for defining traffic parameters and network traffic control and congestion control mechanisms. This ETS defines a restricted initial set of traffic control and congestion control capabilities, aiming at simple mechanisms and realistic network efficiency.

It may subsequently be appropriate to consider additional sets of such capabilities, for which additional traffic control mechanisms will be used to achieve increased network efficiency.

Transposition dates	
Date of latest announcement of this ETS (doa):	30 June 1995
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 December 1995
Date of withdrawal of any conflicting National Standard (dow):	31 December 1995

Blank page

1 Scope

This European Telecommunication Standard (ETS) describes traffic control and congestion control procedures for the Broadband Integrated Services Digital Network (B-ISDN):

- the main body describes the objectives and mechanisms of traffic control and congestion control (see CCITT Recommendation I.371 [1]);
- examples of application of monitoring functions are given in annex A.

In B-ISDN, congestion is defined as a state of network elements (e.g. switches, concentrators, cross-connects and transmission links) in which the network is not able to meet the negotiated NP 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;
- fault conditions within the network.

Congestion should be distinguished from the state where buffer overflow is causing cell losses, but still meets the negotiated Quality of Service (QoS).

Asynchronous Transfer Mode (ATM) layer traffic control refers to the set of actions taken by the network to avoid congested conditions.

ATM layer congestion control refers to the set of actions taken by the network to minimize the intensity, spread and duration of congestion. These actions are triggered by congestion in one or more network elements.

2 Normative references

This ETS incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] CCITT Recommendation I.371: "Traffic control and congestion control in B-ISDN".

[2] CCITT Recommendation I.150: "B-ISDN Asynchronous Transfer Mode functional characteristics".

[3] CCITT Recommendation I.311: "B-ISDN General Networks Aspects".

3 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

AAL	ATM Adaptation Layer
ATM	Asynchronous Transfer Mode
CAC	Connection Admission Control
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CEQ	Customer Equipment
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CRF	Connection Related Functions
CRF(VC)	Virtual Channel Connection Related Functions
CRF(VP)	Virtual Path Connection Related Functions
EFCI	Explicit Forward Congestion Indication
FIFO	First In First Out
FRM	Fast Resource Management
GFC	Generic Flow Control
NNI	Network-Network Interface
NP	Network Performance
NPC	Network Parameter Control
NRM	Network Resource Management
OAM	Operation And Maintenance
PC	Priority Control
PCR	Peak Cell Rate
PDU	Protocol Data Unit
QoS	Quality of Service
SAP	Service Access Point
SDU	Service Data Unit
UNI	User-Network Interface
VBR	Variable Bit Rate
VC	Virtual Channel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VPC	Virtual Path Connection
VP	Virtual Path
VPI	Virtual Path Identifier

4 General framework

4.1 General objectives

The objectives of ATM layer traffic control and congestion control for B-ISDN are as follows:

- ATM layer traffic control and congestion control 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 NP recommendations;

- ATM layer traffic control and congestion control should not rely on ATM Adaptation Layer (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 which may be provided by the ATM layer, in order to improve the utility that those protocols can derive from the network;

- the design of an optimum set of ATM layer traffic controls and congestion controls should minimize network and end-system complexity while maximising network utilization.

4.2 Generic functions

To meet these objectives, the following functions form a framework for managing and controlling traffic and congestion in ATM networks and may be used in appropriate combinations:

- Network Resource Management (NRM): provisioning may be used to allocate network resources in order to separate traffic flows according to service characteristics;

- Connection Admission Control (CAC): is defined as the set of actions taken by the network during the call set up phase (or during call re-negotiation phase) in order to establish whether a Virtual Channel (VC)/Virtual Path Connection (VPC) request can be accepted or rejected (or whether a request for re-allocation can be accommodated). Routeing is part of CAC actions;

- feedback controls are defined as the set of actions taken by the network and by the users to regulate the traffic submitted on ATM connections according to the state of network elements;

- Usage Parameter Control/Network Parameter Control (UPC/NPC) is defined as the set of actions taken by the network to monitor and control traffic, in terms of traffic offered and validity of the ATM connection, at the user access and the network access respectively. Their main purpose is to protect network resources from malicious, as well as unintentional, misbehaviour which can affect the QoS of other already established connections by detecting violations of negotiated parameters and taking appropriate actions;

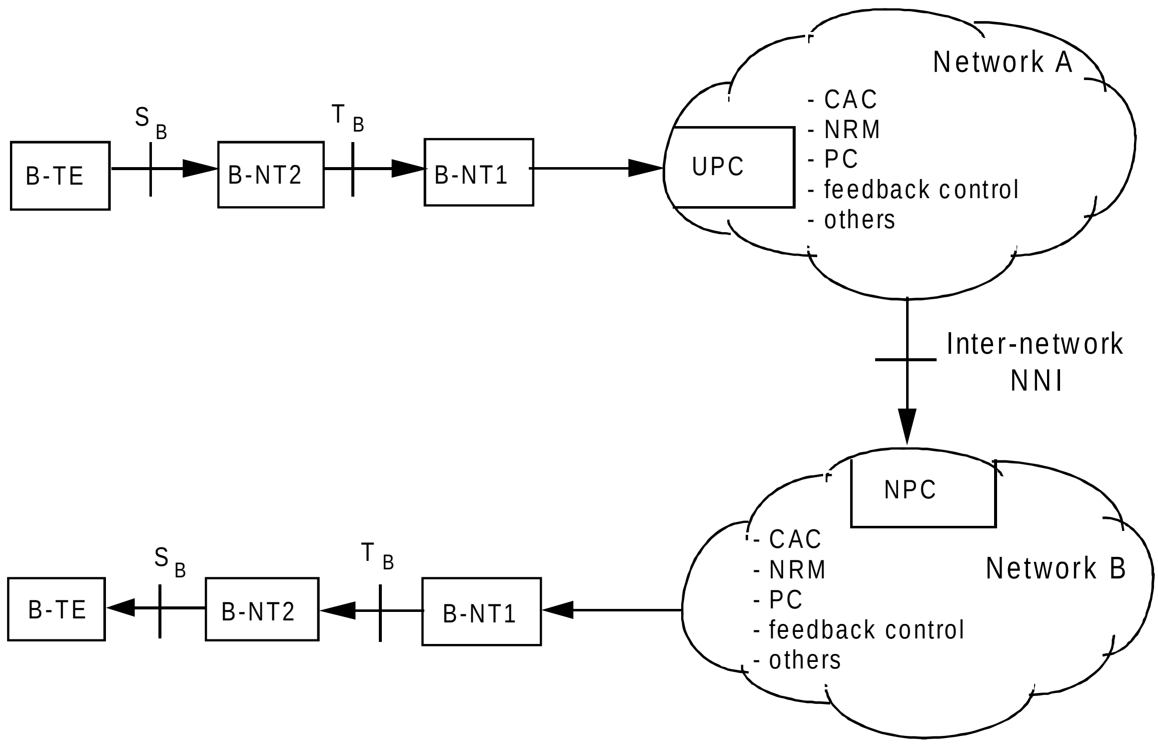
- Priority Control (PC): the user may generate different priority traffic flows by using the Cell Loss Priority (CLP) bit, see CCITT Recommendation I.150 [2]. A congested network element may selectively discard cells with low priority if necessary to protect, as far as possible, the NP for cells with high priority;

- other control functions are for further study.

As a general requirement, it is desirable that a high level of consistency be achieved between the above traffic control capabilities.

4.3 A reference configuration for traffic control and congestion control

The reference configuration used for traffic control and congestion control is given figure 1.



UPC: Usage Parameter Control
NPC: Network Parameter Control
CAC Connection Admission Control
NRM: Network Resource Management
PC: Priority Control
Others for further study

NOTE 1: NPC may also apply at some intra-network Network-Network Interfaces (NNIs).

NOTE 2: The arrows indicate the direction of the cell flow.

Figure 1: Reference configuration for traffic control and congestion control

4.4 Events, actions, time scales and response times

Figure 2 illustrates the time-scales over which various traffic control and congestion control functions operate. The response time defines how quickly the controls react. For example, cell discarding can react on the order of the insertion time of a cell. Similarly, feedback controls can react on the time scale of round-trip propagation times. Since traffic control and resource management functions are needed at different time-scales, no single function is likely to be sufficient.

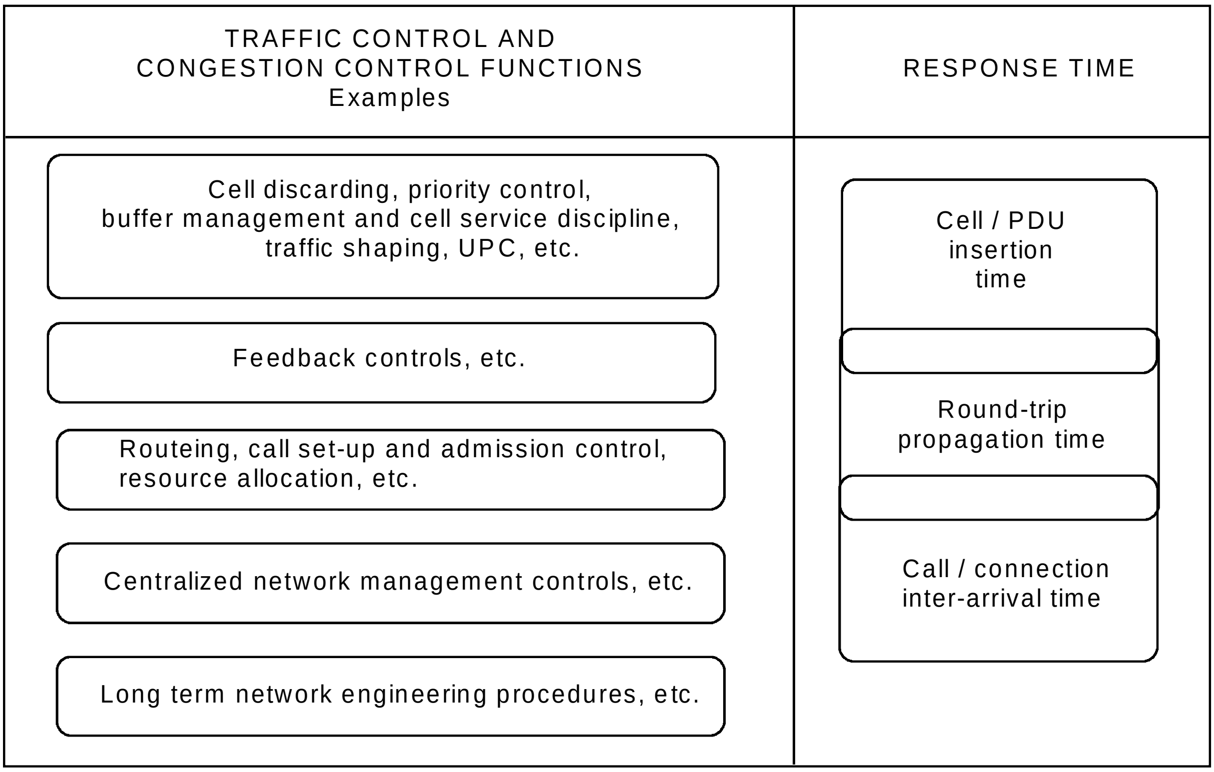


Figure 2: Control response times

4.5 QoS, NP and CLP

The ATM layer QoS is defined by a set of parameters such as delay and delay variation sensitivity, Cell Loss Ratio (CLR), etc. Other QoS parameters are for further study.

NOTE: In this case the Cell Delay Variation (CDV) effect applies to the network ---> user information traffic flow.

A user requests a specific ATM layer QoS from the QoS classes which a network provides. This is part of the traffic contract at connection establishment (see subclause 5.3.1). It is a commitment for the network to meet the requested QoS as long as the user complies with the traffic contract. If the user violates the traffic contract, the network need not respect the agreed QoS.

The selected QoS class may assign different objective values to the CLR computed on the CLP = 0 cell flow and on the aggregate CLP = 0+1 cell flow.

NP objectives at the ATM Service Access Point (SAP) are intended to capture the network ability to meet the requested ATM layer QoS. It is the role of the upper layers, including the AAL, to translate this ATM layer QoS to any specific application requested QoS.

5 Traffic descriptors and parameters

Traffic parameters describe traffic characteristics of an ATM connection. Traffic parameters are grouped into source traffic descriptors for exchanging information between the user and the network.

CAC procedures shall use source traffic descriptors to allocate resources and derive parameters for the operation of UPC/NPC.

5.1 Definitions

5.1.1 Traffic parameters

A traffic parameter is a specification of a particular traffic aspect. It may be qualitative or quantitative.

Traffic parameters may, for example, describe Peak Cell Rate (PCR), average cell rate, burstiness, peak duration, and source type (e.g. telephone, videophone).

Only PCR is presently defined in this ETS.

Some of the above mentioned parameters are mutually dependent (e.g. the burstiness with the average cell rate and PCR).

5.1.2 Traffic descriptors

The ATM traffic descriptor is the generic list of traffic parameters which can be used to capture the traffic characteristics of an ATM connection.

The introduction of additional parameters to enhance the NRM procedures or to capture traffic characteristics of a new type of connection is left open for further study.

A description of the characteristics of the traffic that any given requested connection may offer has to be provided by the user at the connection set-up.

A source traffic descriptor is the set of traffic parameters belonging to the ATM traffic descriptor used during the connection set-up to capture the traffic characteristics of the connection requested by the source.

5.2 Requirements

Any traffic parameter to be involved in a source traffic descriptor should:

- be understandable by the user or his terminal;
- enable conformance to be monitored by the network;
- be appropriate for use by the network in resource allocation schemes (e.g. CAC), to enable NP requirements to be met;
- be enforceable by the UPC and NPC functions, to enable NP requirements to be met, in case of non-compliant usage.

5.3 User-network traffic contract

5.3.1 Traffic contract definition

CAC and UPC/NPC procedures require the knowledge of certain parameters to operate efficiently: they should take into account the source traffic descriptor, the requested QoS and the CDV tolerance (see subclause 5.4) in order to decide whether the requested connection can be accepted.

NOTE 1: In this case the CDV effect applies to the user ---> network information traffic flow.

The source traffic descriptor, the requested QoS for any given ATM connection and the maximum CDV tolerance allocated to the Customer Equipment (CEQ) define the traffic contract at the T_B reference point. Source traffic descriptors and QoS are declared by the user at connection set-up by means of signalling or subscription. Whether the maximum allowable CDV tolerance is also negotiated on a subscription or on a per connection basis, is for further study.

The CAC and UPC/NPC procedures are operator specific. Once the connection has been accepted, the value of the CAC and UPC/NPC parameters shall be set by the network on the basis of the network operator's policy.

NOTE 2: All ATM connections handled by network Connection Related Functions (CRF) have to be declared and enforced by the UPC/NPC. ATM layer QoS can only be assured for compliant ATM connections. As an example, individual Virtual Channel Connections (VCCs) inside a user end-to-end VPC are neither declared nor enforced at the UPC and hence, no ATM layer QoS can be assured to them.

5.3.2 Source traffic descriptors, QoS and CLP

If a user requests two levels of priority for an ATM connection, as indicated by the CLP bit value, the intrinsic traffic characteristics of both cell flow components have to be characterized in the source traffic descriptor. This is by means of a set of traffic parameters associated with the CLP = 0 component and a set of traffic parameters associated with the CLP = 0+1 component.

As indicated in subclause 4.5, the network provides an ATM layer QoS for each of the components (CLP = 0 and CLP = 0+1) of an ATM connection. The traffic contract specifies the particular QoS choice (from those offered by the network operator) for each of the ATM connection components. There may be a limited offering of QoS specifications for the CLP = 1 component.

CLR objectives are for further study.

5.3.3 Impact of CDV on UPC/NPC and resource allocation

ATM layer functions (e.g. cell multiplexing) may alter the traffic characteristics of ATM connections by introducing CDV as illustrated in figure 3. When cells from two or more ATM connections are multiplexed, cells of a given ATM connection may be delayed while cells of another ATM connection are being inserted at the output of the multiplexer. Similarly, some cells may be delayed while physical layer overhead or Operation And Maintenance (OAM) cells are inserted. Therefore, some randomness affects the time interval between reception of ATM cell Data_Requests at the end-point of an ATM connection and the time that an ATM cell Data_Indication is received at the UPC/NPC. Additionally, AAL multiplexing may originate CDV.

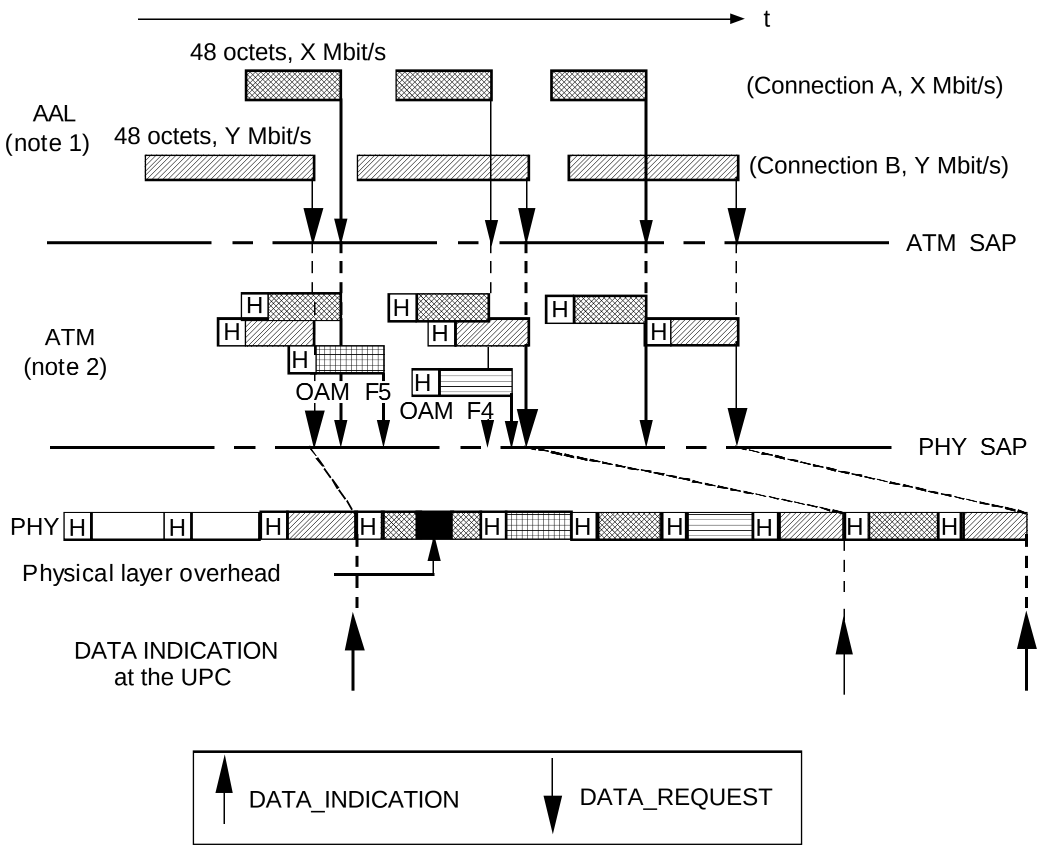
The UPC/NPC mechanism should not discard or tag cells in an ATM connection if the source conforms to the source traffic descriptor negotiated at connection establishment. However, if the CDV is not bounded at a point where the UPC/NPC function is performed, it is not possible to design a suitable UPC/NPC mechanism and to allocate resources properly. Therefore, it is required that a maximum allowable value of CDV be standardized edge-to-edge, e.g. between the ATM connection end-point and T_B, between T_B and an inter-network NNI and between inter-network NNIs (see figure 1).

Standardization of a number of CDV tolerance values, less than the maximum allowable value of CDV tolerance, to apply to certain interfaces (e.g. on a subscription basis or on a per connection basis) is for further study.

UPC/NPC should accommodate the effect of the maximum CDV allowed on ATM connections within the limit resulting from the accumulated CDV allocated to upstream subnetworks (including CEQ).

Traffic shaping partially compensates for the effects of CDV on the PCR of the ATM connection. Examples of traffic shaping mechanisms are re-spacing cells of individual ATM connections according to their PCR or suitable queue service schemes.

Values of the CDV are NP issues.



NOTE 1: ATM Service Data Units (SDUs) are accumulated at the upper layer service bit rate. Besides, CDV may also originate in AAL multiplexing.

NOTE 2: Generic Flow Control (GFC) delay and delay variation is part of the delay and delay variation introduced by the ATM layer.

NOTE 3: CDV may also be introduced by the network because of random queueing delays which are experienced by each cell in concentrators, switches and cross-connects.

Figure 3: Origins of CDV

The definition of a source traffic descriptor and the standardization of a maximum allowable CDV may not be sufficient for a network to allocate resources properly. When allocating resources, the network should take into account the worst case traffic passing through UPC/NPC in order to avoid impairments to other ATM connections. This worst case traffic depends on the specific implementation of the UPC/NPC. The trade-offs between UPC/NPC complexity, worst case traffic and optimization of network resources are made at the discretion of network operators. The quantity of available network resources and the NP to be provided for meeting QoS requirements can influence these trade-offs.

5.4 Traffic parameter specifications

PCR is a mandatory traffic parameter to be explicitly or implicitly declared in any source traffic descriptor. In addition to the PCR of an ATM connection, it is mandatory for the user to declare either explicitly or implicitly the CDV tolerance τ within the relevant traffic contract.

Additional standardized parameters beyond PCR which may be specified in the future should provide for a significant improvement of network utilization.

5.4.1 PCR

The following definition applies to ATM connections supporting both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) services.

The PCR in the source traffic descriptor specifies an upper bound on the traffic that can be submitted on an ATM connection. Enforcement of this bound by the UPC/NPC allows the network operator to allocate sufficient resources to ensure that the performance objectives (e.g. for CLR) can be achieved.

5.4.1.1 PCR for a VPC/VCC

Location: at the Physical layer SAP for an equivalent terminal representing the VPC/VCC (this is only a reference configuration, see figure 4).

Basic event: request to send an ATM Protocol Data Unit (ATM_PDU) in the equivalent terminal.

Definition: the PCR of the ATM connection is the inverse of the minimum inter-arrival time T between two basic events defined above. T is the peak emission interval of the ATM connection.

The source traffic descriptor of the ATM connection currently reduces to the PCR defined above.

It is noted that conformance control of the PCR by UPC/NPC requires that the CDV tolerance τ, allocated to the upstream portion of the ATM connection, be specified (see subclause 5.3.1). Whether additional parameters may be useful is for further study.

On a terminal with a single AAL and without ATM layer OAM flows, location and basic event are equivalent to the following.

Location: at the ATM layer SAP.

Basic event: request to send an ATM_SDU.

In order to properly allocate resources to a VPC/VCC, a PCR, as defined above, has to be defined for each component of the ATM connection, i.e. the CLP = 0 substream (not including the OAM), the aggregate (CLP = 0+1) substream (where appropriate) and the OAM substream. The CDV tolerance accounts for delay variation that will be present in respective cell substreams of the ATM connection. Their values and interpretation are defined by algorithms described in annex A.

5.4.1.2 PCR granularity specification

Network functions such as UPC/NPC cannot be requested to handle every specific PCR value but only a restricted, discrete and finite set of values. The ordered list of these values is referred to as the ATM PCR granularity.

As for the PCR definition, the PCR granularity specification should also be based on the peak emission interval.

The ATM PCR granularity and its coding are for further study.

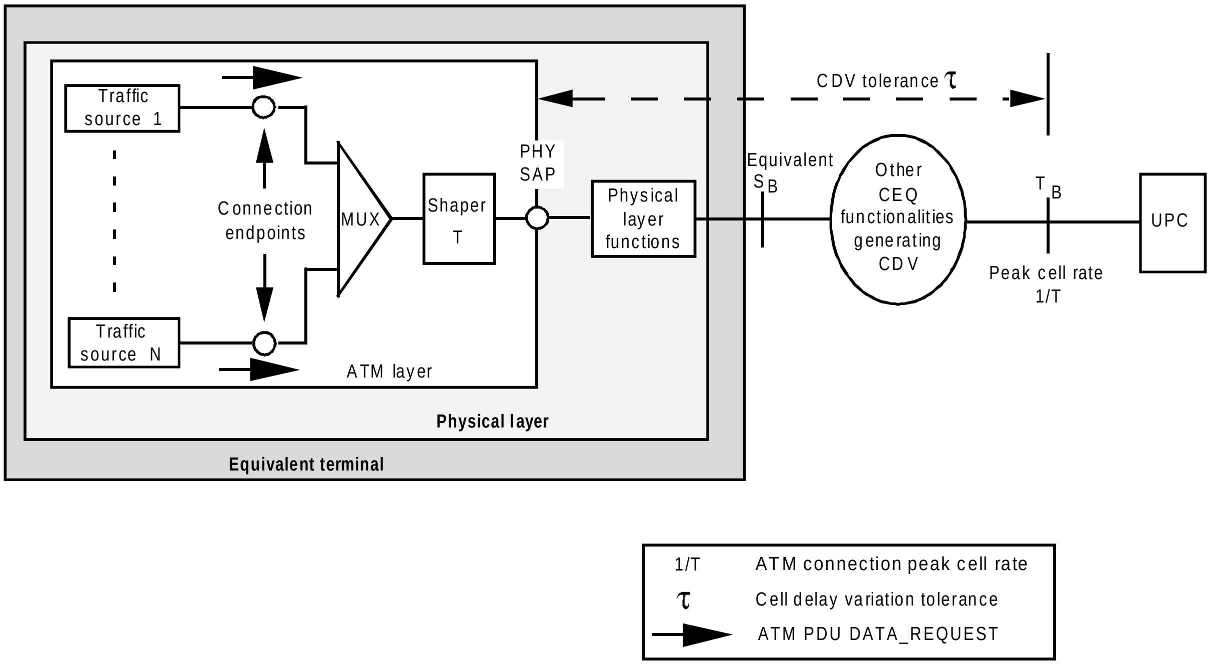


Figure 4: Reference configuration and equivalent terminal for the definition of the PCR of an ATM connection

5.4.2 Other traffic parameters

For further study.

6 Functions and procedures for traffic control and congestion control

6.1 Introduction

Generic traffic control and congestion control functions are defined as the set of actions respectively taken by the network in all the relevant network elements to avoid congestion conditions or to minimize congestion effects and to avoid the congestion state spreading, once congestion has occurred.

Under normal operation, i.e. when no network failures occur, functions referred to as traffic control functions in this ETS are intended to avoid network congestion.

However, congestion may occur, e.g. because of malfunctioning of traffic control functions caused by unpredictable statistical fluctuations of traffic flows, or of network failures. Therefore, additionally, functions referred to as congestion control functions in this ETS are intended to react to network congestion in order to minimize its intensity, spread and duration.

6.1.1 Traffic control and congestion control functions

A range of traffic and congestion control functions will be used in the B-ISDN to maintain the QoS of ATM connections.

The following functions are described in this ETS.

Traffic control functions

a) NRM (subclause 6.2.1);

b) CAC (subclause 6.2.2);

c) UPC/NPC (subclause 6.2.3);

d) PC and selective cell discarding (subclause 6.2.4);

e) traffic shaping (subclause 6.2.5);

f) Fast Resource Management (FRM) (subclause 6.2.6);

Congestion control functions:

g) selective cell discarding (subclause 6.3.1);

h) Explicit Forward Congestion Indication (EFCI) (subclause 6.3.2);

Additional control functions may be used. Possible useful techniques, which require further study to determine details, are:

j) CAC that reacts to and takes account of the measured load on the network;

k) variation of usage monitored parameters by the network. For example, reduction of the peak rate available to the user;

l) other traffic control techniques (e.g. re-routeing, connection release, OAM functions) are for further study.

The impact on standardization of the use of these additional techniques (e.g. the impact on ATM layer management, user-network signalling and control plane) requires further study.

Different levels of NP may be provided on ATM connections by proper routeing, traffic shaping, PC and resource allocation, to meet the required ATM layer QoS for these connections.

6.2 Traffic control functions

6.2.1 NRM

Use of Virtual Paths (VPs) is described below. Other networking techniques are for further study.

6.2.1.1 Use of VPs

VPs are an important component of traffic control and resource management in the B-ISDN. With relation to traffic control, VPCs can be used to:

- simplify CAC;
- implement a form of PC by segregating traffic types requiring different QoS;
- efficiently distribute messages for the operation of traffic control schemes (for example to indicate congestion in the network by distributing a single message for all VCCs comprising a VPC);
- aggregate user-to-user services such that the UPC/NPC can be applied to the traffic aggregate;
- aggregate network capabilities such that the NPC can be applied to the traffic aggregate.

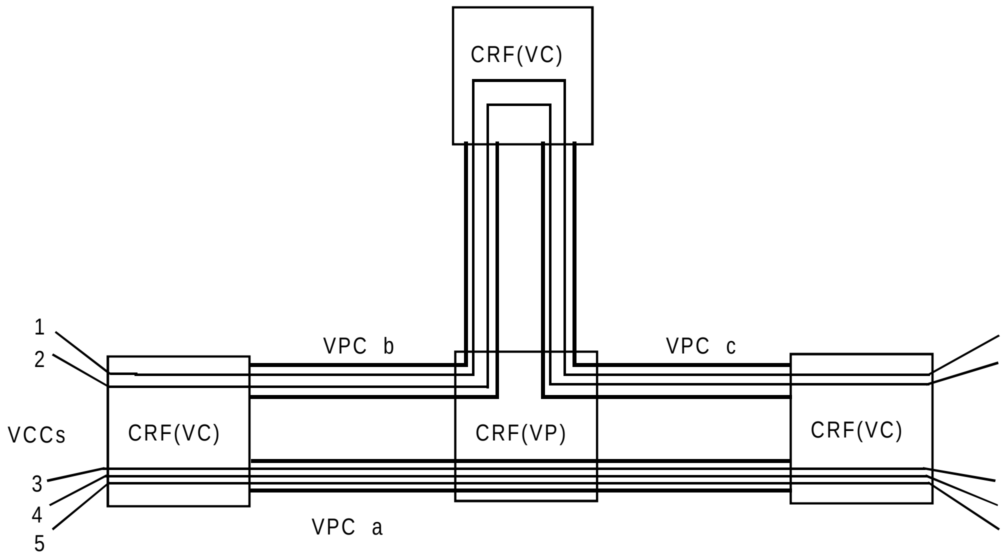
VPCs also play a key role in NRM. By reserving capacity on VPCs, the processing required to establish individual VCCs is reduced. Individual VCCs can be established by making simple connection admission decisions at nodes where VPCs are terminated. Strategies for the reservation of capacity on VPCs will be determined by the trade-off between increased capacity costs and reduced control costs. These strategies are left to operators' decision.

The peer-to-peer NP on a given VCC depends on the performances of the consecutive VPCs used by this VCC and on how it is handled in Virtual Channel Connection Related Functions (CRF(VC)s) (see figure 5).

If handled similarly by CRF(VC)s, different VCCs routed through the same sequence of VPCs, experience similar expected NP, e.g. in terms of CLR, cell transfer delay and CDV; along this route.

Conversely, when VCCs within a VPC require a range of QoS, the VPC performance objective should be set suitably for the most demanding VCC carried. The impact on resource allocation is for further study.

Combining common routeing and PC by CLP may be used by CAC for services requiring a number of VCCs with low differential delays and different CLRs (e.g. multimedia services).



NOTE 1: VCCs 1 and 2 experience a NP which depends on NP on VPCs b and c and on how these VCCs are handled by CRF(VC)s. It may differ from NP experienced by VCCs 3, 4 and 5, at least due to different network performances provided by VPCs.

NOTE 2: VCCs 3, 4 and 5 experience similar network performances in terms of cell delay and CDV if handled similarly by CRF(VC)s, whilst providing for two different CLRs by using the CLP bit.

NOTE 3: On a user-to-user VPC, the QoS experienced by individual VCCs depends on CEQ traffic handling capabilities.

Figure 5: Mapping CLRs for VCCs and VPCs

On the basis of the applications of VPCs contained in CCITT Recommendation I.311 [3], § 2.3.2, namely:

a) user-user application: the VPC extends between two T_B reference points;

b) user-network application: the VPC extends between a T_B reference point and a network node;

c) network-network application: the VPC extends between network nodes.

The above implies:

In case a: because the network has no knowledge of the QoS of the VCCs within the VPC, it is the user's responsibility to determine, in accordance with the network capabilities, the necessary QoS for the VPC.

In cases b and c: the network is aware of the QoS of the VCCs carried within the VPC and shall accommodate them.

Statistical multiplexing of VC links within a VPC where the aggregate peak of all VC links may exceed the VPC capacity, is only possible when all VC links within the VPC can tolerate the QoS that results from this statistical multiplexing. The way this is managed is for further study.

As a consequence, when statistical multiplexing of VC links is applied by the network operator, VPCs may be used in order to separate traffic, thereby preventing statistical multiplexing with other types of traffic. This requirement for separation implies that more than one VPC may be necessary between network origination/destination pairs to carry a full range of QoS between them. Implications of this are for further study.

6.2.1.2 Other networking techniques

For further study.

6.2.2 CAC

6.2.2.1 General

CAC is defined as the set of actions taken by the network at the call set-up (or during call re-negotiation phase) in order to establish whether a request for a VCC or a VPC can be accepted or rejected.

On the basis of CAC in an ATM based network, a connection request for a given call is accepted only if sufficient resources are available to establish the call through the whole network at its required QoS and to maintain the agreed QoS of existing calls. This also applies to re-negotiation of connection parameters within a given call.

In a B-ISDN environment, a call can require more than one connection (e.g. for multimedia or multiparty services such as videotelephony or videoconferencing). In this case, CAC procedures should be performed for each VCC or VPC.

PC using the CLP bit allows, at most, for two CLR objectives for ATM connections. Delay sensitivity is part of the required QoS.

In the case of an on-demand service, the connection establishment procedures shall enable CAC to derive at least the following information:

- source traffic descriptors;

- required QoS class.

In the case of permanent or reserved services (e.g. using a permanent VPC or a permanent VCC, this information is indicated with an appropriate OAM procedure, either on-line (e.g. signalling) or off-line (e.g. service order).

CAC makes use of this information to determine:

- whether or not, the connection request can be accepted;

- traffic parameters needed by UPC/NPC;

- routeing and allocation of network resources.

The role of PC in CAC is for further study. Further information on PC can be found in subclause 6.2.4.

6.2.2.2 Parameters for CAC

6.2.2.2.1 Required QoS class

For a single ATM connection, a user indicates at most two QoS classes from the QoS classes which the network provides, only differing by the CLR. Specific QoS classes are the subject for further study.

6.2.2.2.2 Negotiation of traffic characteristics

The user will negotiate the traffic characteristics of the ATM connections with the network at connection establishment. These characteristics may be re-negotiated during the lifetime of the connection at the request of the user. The network may limit the frequency of these re-negotiations.

The re-negotiation procedure and the impact on network element complexity require further study.

6.2.2.3 Resource allocation

In order to ensure NP and to protect the network, both CLP = 0 and CLP = 1 traffic flows shall be allocated resources.

Different strategies of network resource allocation may be applied for CLP = 0 and CLP = 1 traffic flows. In addition, information such as the measured network load may be used when performing CAC. This may allow a network operator to achieve higher network utilization, while still meeting the performance objectives.

Resource allocation schemes are for further study. They may be left to network operators' decision.

6.2.3 Usage parameter control and NPC

UPC and NPC perform similar functionalities at different interfaces: the UPC function is performed at the User-Network Interface (UNI), whereas the NPC function is performed at the inter-network NNIs.

The use of a UPC function is recommended, and the use of an NPC function is a network option. Whether or not the operator chooses to use the NPC function, the network-edge-to-network-edge and user-to-user performance objectives shall still be met.

6.2.3.1 UPC/NPC functions

UPC/NPC is defined as the set of actions taken by the network to monitor and control traffic in terms of traffic offered and validity of the ATM connection, at the user access and the network access respectively. Their main purpose is to protect network resources from malicious as well as unintentional misbehaviour which can affect the QoS of other already established connections by detecting violations of negotiated parameters and taking appropriate actions.

Connection monitoring encompasses all connections crossing the UNI or inter-network interface.

UPC and NPC apply to both user VCCs/VPCs and signalling VCs. Methods for monitoring meta-signalling channels and OAM flows is for further study.

The monitoring task for UPC and NPC is performed for VCCs and VPCs respectively by the following two actions:

a) checking the validity of Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) (i.e. whether or not VPI/VCI values are assigned), and monitoring the traffic entering the network from active VCCs in order to ensure that parameters agreed upon are not violated;

b) checking the validity of VPI (i.e. whether or not VPI values are assigned), and monitoring the traffic entering the network from active VPCs in order to ensure that parameters agreed upon are not violated.

6.2.3.2 UPC/NPC requirements

The need for and the definition of a standardized UPC/NPC algorithm requires further study. A number of desirable features of the UPC/NPC algorithm can be identified as follows:

- capability of detecting any illegal traffic situation;
- selectivity over the range of checked parameters (i.e. the algorithm could determine whether the user behaviour is within an acceptance region);
- rapid response time to parameter violations;
- simplicity of implementation.

There are two sets of requirements relating to the UPC/NPC:

- those which relate to the QoS impairments, the UPC/NPC could directly cause to the user cell flow;
- those which relate to the resource the operator should allocate to a given path/channel and the way the network intends to protect those resources against misbehaviour from the user side or another network (due to fault conditions or maliciousness).

There is a practical uncertainty in determining the values of the controlled parameters. Hence, in order to have adequate control performance, tolerances of controlling performance parameters need to be defined. The definition of these tolerances is for further study.

Two performance parameters have been identified. They shall be considered when assessing the performances of UPC/NPC mechanisms. Methods for evaluating UPC/NPC performance and the need to standardize these methods are for further study.

The two performance parameters are:

- response time: the time to detect a given non-compliant situation on a VPC/VCC under given reference conditions;
- transparency: for the same set of reference conditions, the accuracy with which the UPC/NPC initiates appropriate control actions on a non-compliant connection and avoids inappropriate control actions on a compliant connection.

Additional UPC/NPC performance parameters are for further study.

A specific UPC/NPC mechanism may commit errors by taking policing actions on a compliant connection, i.e. declaring a cell as non-compliant although the connection is actually compliant. It can also fail to take the appropriate policing actions on a non-compliant connection.

Inappropriate actions of the UPC/NPC on a compliant connection are part of the overall NP degradation. Safety margins may be provisioned, depending upon the UPC/NPC algorithm to limit the degradation introduced by the UPC/NPC.

Policing actions performed on the excess traffic in case of traffic contract violation shall not to be included in the NP degradation allocated to the UPC/NPC.

The impact of UPC/NPC on cell delay should also be considered. Cell delay and CDV introduced by UPC/NPC is also part of the delay and delay variation allocated to the network.

6.2.3.2.1 Performance of PCR UPC/NPC

A method to determine whether a traffic flow is conforming to a negotiated PCR at a given interface is currently considered for NP purposes. Non-conformance is measurable by a 1 point-measurement process in terms of the ratio γ_M between the number of cells exceeding the traffic contract and the total number of submitted cells.

An ideal UPC/NPC, implementing the 1 point-measurement process, would just take policing actions on a number of cells according to this ratio. Although the process allows for a cell-based decision, it is not possible to predict which particular cells of a non-compliant connection will suffer from the policing action (this is because of measurement phasing).

According to the definition of the conformance of a traffic flow to a PCR, the transparency of a UPC/NPC mechanism can be defined by the accuracy with which this mechanism approaches the ideal mechanism, i.e. the difference (δ) between the reference policing ratio γ_M and the actual policing ratio γ_P:

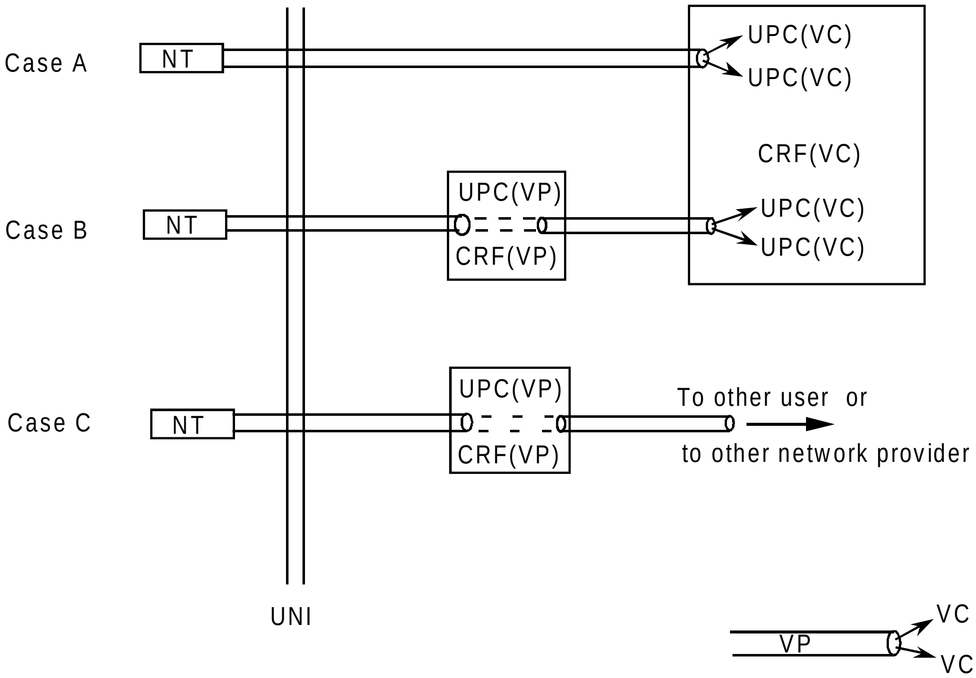
$$\delta = \gamma_M - \gamma_P$$

A positive δ means that the UPC/NPC is taking less policing action than a measurement process would do. A negative δ means that policing actions are unnecessarily taken by the UPC/NPC.

The exact way of measuring the transparency of a given mechanism for PCR UPC/NPC and its dependence on time requires further study.

6.2.3.3 UPC location

UPC is performed on VCCs or VPCs at the point where the first VP or VC links are terminated within the network. Three possibilities can be identified as shown in figure 6.



NT: Network Termination.
CRF: Connection Related Functions.
CRF(VC): Virtual Channel Connection Related Functions.
CRF(VP): Virtual Path Connection Related Functions.

NOTE 1: A CRF(VC) or a CRF(VP) may respectively be a VC or VP concentrator.

Case A: User connected directly to CRF(VC):
UPC is performed within the CRF(VC) on VCCs before the switching function is executed (action 1, subclause 6.2.3.1).

Case B: User connected to CRF(VC) via CRF(VP):
UPC is performed within the CRF(VP) on VPCs only (action 2, subclause 6.2.3.1) and within the CRF(VC) on VCCs only (action 1, subclause 6.2.3.1).

Case C: User connected to user or to another network provider via CRF(VP):
UPC is performed within the CRF(VP) on VPCs only (action 2, subclause 6.2.3.1). VCC UPC will be done by another network provider when CRF(VC) is present.

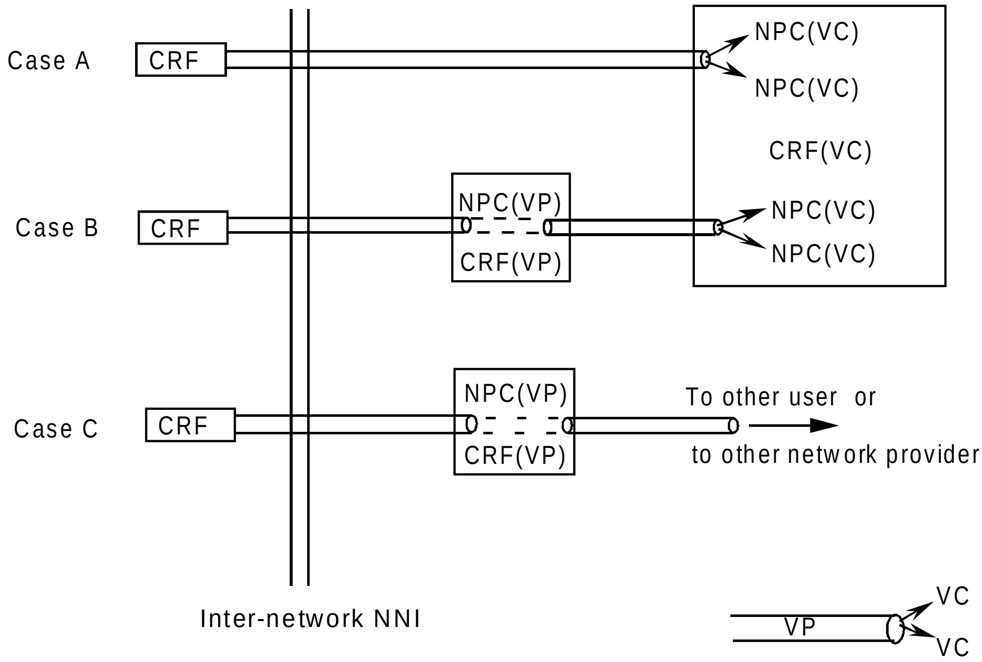
NOTE 2: In case A, the VPI value does not identify a negotiated VPC.

NOTE 3: Provision of UPC at other locations is for further study.

Figure 6: Location of the UPC functions

6.2.3.4 NPC location

NPC is performed on VCCs or VPCs at the point where they are first terminated within the network. Three possibilities can be identified, as shown in figure 7. This requires further study.



CRF: Connection Related Functions.
CRF(VC): Virtual Channel Connection Related Functions.
CRF(VP): Virtual Path Connection Related Functions.

Case A: Originating network connected directly to CRF(VC); NPC is performed within the CRF(VC) before the switching function is executed (action 1, subclause 6.2.3.1).

Case B: Originating network connected to the CRF(VC) via the CRF(VP): NPC is performed within the CRF(VP) on VPCs (action 2, subclause 6.2.3.1) only before the VP switching functions is executed and within the CRF(VC) on VCCs only (action 1, subclause 6.2.3.1) before the switching function is executed.

Case C: Originating network connected to user or another network provider via CRF(VP): NPC is performed within the CRF(VP) on VPCs only (bullet point 2 of subclause 6.2.3.1). VCC NPC is performed by another network provider when CRF(VC) is present.

NOTE: In case A, the VPI value does not identify a negotiated VPC.

Figure 7: Location of the NPC function

6.2.3.5 Traffic parameters subject to control at the UPC/NPC

Traffic parameters which may be subject to control are those included in the source traffic descriptor (see clause 5). Whether all of these parameters, or a subset of them are subject to control, depends upon CAC and UPC/NPC mechanism. The PCR shall be controlled for all types of connections.

6.2.3.6 UPC/NPC actions

The UPC/NPC is intended to control the traffic offered by an ATM connection to ensure compliance with the negotiated traffic contract. The objective is that a user shall never be able to exceed the traffic contract.

At the cell level, actions of the UPC/NPC function may be:

a) cell passing;

b) cell re-scheduling (when traffic shaping and UPC are combined, optional);

c) cell tagging (network operator optional): cell tagging operates on CLP = 0 cells only, by overwriting the CLP bit to 1;

d) cell discarding.

Cell passing and cell re-scheduling are performed on cells which are identified by a UPC/NPC as compliant. Cell tagging and cell discarding are performed on cells which are identified by a UPC/NPC as non-compliant.

Beside the above actions at the cell level, as an option, one other action performed at the connection level may be initiated by the UPC/NPC:

- releasing the connection.

6.2.3.7 Relationship between UPC/NPC and CLP

When an ATM connection utilizes the CLP capability on user request, network resources are allocated to CLP = 0 and CLP = 1 traffic flows as described in subclause 6.2.2.3. By controlling CLP = 0 and CLP = 0+1 traffic flows (see figure 8), allocating adequate resources and suitably routeing, a network operator may provide the two requested QoS classes for CLP = 0 and CLP = 0+1 cell flows.

If the tagging option is used by a network operator, CLP = 0 cells identified by the UPC/NPC function performed on CLP = 0 flow as non-compliant are converted to CLP = 1 cells and merged with the user-submitted CLP = 1 traffic flow before the CLP = 0+1 traffic flow enters the UPC/NPC mechanism.

A cell identified as non-compliant by the UPC/NPC function performed on the aggregate CLP = 0+1 flow is discarded.

When no additional network resource has been allocated for CLP = 1 traffic flow (either on user request or due to network provisioning), CLP = 0 cells identified by the UPC/NPC as not compliant are discarded. In this case, tagging is not applicable.

Since cell sequence integrity is maintained on any ATM connection, the UPC/NPC, including its optional tagging action, shall operate as a single server using First In First Out (FIFO) service discipline for each ATM connection.

Subclause 6.2.3.2 addresses undue UPC/NPC actions on compliant ATM connections. This is part of the NP degradation allocated to the UPC/NPC and should remain of a very low probability.

When the CLP capability is used by an ATM connection and the CLP = 0+1 aggregate flow is not complying to the traffic contract, the UPC/NPC function performed on the aggregate flow may discard CLP = 0 cells which were not considered in excess by the UPC/NPC function performed on the CLP = 0 cell stream.

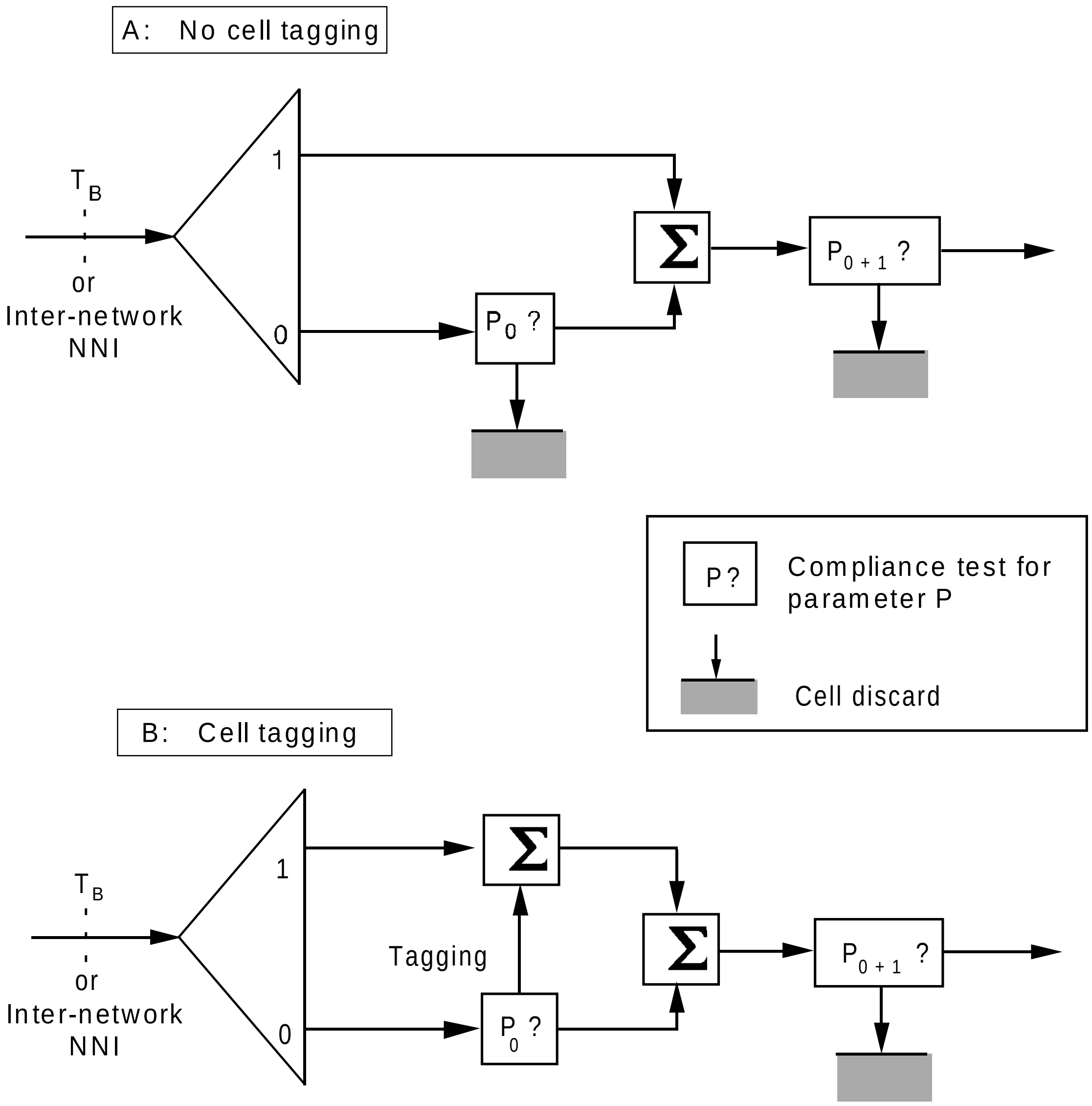


Figure 8: Possible actions of the UPC/NPC

6.2.3.8 Relationship between UPC/NPC, OAM and network management

OAM alarm indications may be provided by the UPC/NPC to the user and to the network management when enforcement actions occur on non-compliant VCCs/VPCs (e.g. cell discard). These alarm indications may initiate other enforcement actions (e.g. connection release). This is for further study.

As the output flow of any UPC should conform with the contract negotiated at connection set-up, alarms due to misbehaving users should not propagate through the network. This is for further study.

OAM information inserted at the ATM layer or above is part of the corresponding ATM connection. Therefore, it will be subject to enforcement at the UPC/NPC and needs properly allocated resources.

The use of OAM cells for traffic control and resource management purposes (e.g. to estimate delay and delay variation) is for further study.

6.2.4 PC and selective cell discard

Network elements may selectively discard cells of the lower priority flow while still meeting NP objectives on both flows.

6.2.5 Traffic shaping

Traffic shaping is a mechanism that alters the traffic characteristics of a stream of cells on a VCC or a VPC to achieve a desired modification of those traffic characteristics. Traffic shaping shall maintain cell sequence integrity on an ATM connection.

Examples of traffic shaping are PCR reduction, burst length limiting, reduction of CDV by suitably spacing cells in time, queue service schemes.

It is an option that the traffic shaping be used in conjunction with suitable UPC functions, provided the additional delay remains within the acceptable QoS negotiated at call set-up.

The options available to the network operator/service provider are the following:

- re-shape the traffic at the entrance of the network and allocate resources in order to respect both the CDV 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 both to accommodate the input CDV and comply with the output CDV without any shaping function.

Traffic shaping may also be used within the CEQ or the terminal to ensure that the traffic generated by the source or at the UNI is conforming to the traffic contract.

Traffic shaping is an option for network operators and users.

6.2.6 FRM

FRM functions operate on the time scale of the round-trip propagation delay of the ATM connection. Potential FRM functions are for further study.

One possible FRM function that has been identified is as follows: in response to a user request to send a burst, the network may allocate capacity (e.g. bandwidth, buffer space) for the duration of the burst. When a source requests an increase of its PCR, it has to wait until resources have been reserved in all network elements along the ATM connection before the new PCR can be used. UPC/NPC parameters would be adjusted accordingly.

6.3 Congestion control functions

For low priority traffic, some adaptive rate control facilities at the ATM layer or above may be used. Such cell-based reactive techniques are for further study.

The following congestion control functions have been identified. Other congestion control functions are for further study.

6.3.1 Selective cell discard

A congested network element may selectively discard cells explicitly identified as belonging to a non-compliant ATM connection and/or these cells with higher CLP = 1 cell loss priority. This is to primarily protect, as long as possible, high priority CLP = 0 flows.

6.3.2 EFCI

The EFCI is a congestion notification mechanism which may be used to assist the network in avoidance of and recovery from a congested state. Since the use of this mechanism by the CEQ is optional, the network operator should not rely on this mechanism to control congestion.

A network element in a congested state may set an EFCI in the cell header, so that this indication may be examined by the destination CEQ. For example, the end user's CEQ may use this indication to implement protocols that adaptively lower the cell rate of the connection during congestion. A network element that is not in a congested state shall not modify the value of this indication.

The mechanism by which a network element determines whether it is congested is an implementation issue and is not subject to standardization. The mechanism by which the congestion indication is used by the higher layer protocols in the CEQ is for further study.

The impact of EFCI on the traffic control and congestion control functions requires further study.

6.3.3 Reaction to UPC/NPC failures

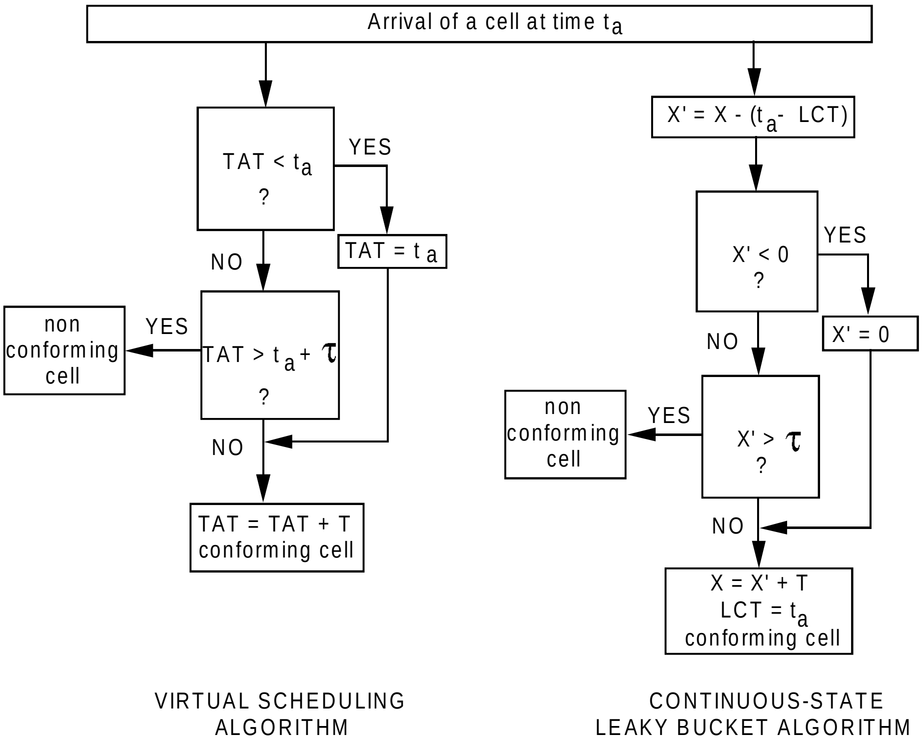
Due to equipment faults (e.g. in UPC/NPC devices and/or other network elements) the controlled traffic characteristics at the UPC/NPC could be different from the values agreed during the call set-up phase. To cope with these situations, specific procedures of the management plane should be designed (e.g. in order to isolate the faulty link). The impact of these malfunctioning situations on the UPC/NPC needs further study.

Annex A (informative): PCR monitor algorithms

A.1 Accounting for CDV tolerance

This annex provides two examples of algorithms that may be useful in monitoring the PCR 1/T of an ATM connection while taking into account a certain CDV tolerance τ. No recommendation is made that either of these algorithms be used for actual implementation.

A virtual monitor algorithm (which might be located within the equivalent terminal) determines whether or not ATM_PDU requests are conforming to the negotiated values of the PCR descriptor. It mirrors the measurement process of connection compliance currently considered for NP purposes.



TAT: Theoretical Arrival Time.
ta: Time of arrival of a cell.

At the time of arrival ta of the first cell of the connection, TAT = t_a.

X: Value of the leaky bucket.
X': Auxiliary variable.
LCT: Last Conformance Time.

At the time of arrival t_a of the first cell of the connection, X = 0 and LCT = t_a.

Figure A.1

Let T be the peak emission Interval and τ the CDV tolerance. τ corresponds to the amount of "distortion" introduced by, for example, either CEQ multiplexing before the T_B reference point or the mapping of ATM_PDU requests onto cell time slots. τ may be set to the difference between the maximum and minimum cell transfer delay throughout the CEQ.

T and τ are the only parameters needed to define the virtual monitor algorithm.

The virtual monitor algorithm is described in figure A.1. Two equivalent versions of this algorithm are shown: the virtual scheduling algorithm and the continuous state leaky bucket algorithm. In the first version, τ is expressed in units of time. In the second one, the leaky bucket capacity measured in units of time is equal to L_B = T + τ.

History

Document history	
March 1995	First Edition
December 1995	Converted into Adobe Acrobat Portable Document Format (PDF)

ISBN 2-7437-0089-0
Dépôt légal : Mars 1995