Manageable Parameters to Improve Access Control in ATM Networks[*]

Olivier Paul[†]*, Maryline Laurent, Sylvain Gombault*
ENST de Bretagne
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
Email : {paul|mlaurent|gombault}@rennes.enst-bretagne.fr

Abstract

In the recent years much attention has been paid to the way to develop security services for ATM networks. This has resulted in the creation of working groups within the standardization authorities to deal with this problem. The ATM-forum security working group is to the point to release its version 1.0 specification and other solutions have been widely exposed in several international conferences.
Most of these solutions rely on cryptography. Cryptography is a good way to provide security services such as confidentiality, integrity, authentication and some kind of access control. However it is possible to improve this access control.
In this paper we describe the reasons why cryptographic mechanisms have to be combined with non-cryptographic mechanisms in order to provide a full range of security services in ATM networks.
As an example we consider the case of access control. The currently proposed solutions use a combination of a cryptographic authentication based on ATM facilities' addresses and a security level indicator. We show that a simple analysis of the ATM flows provides information such as addresses, traffic descriptors or surrounding layers identifiers. This information can be used along with cryptographic information (Authentication results, Access control identifiers) or information not linked to the ATM model protocols (Time, Switch ports numbers) to improve currently proposed access control schemes.
A comparison between information provided by the ATM and the «internet» models shows that the security services usually supplied in internet networks could be provided quite easily, thus providing an alternative or further solution to the currently proposed solutions.

Keywords

Security, ATM, Access control, Manageable parameters.

*. In proceedings of the 5th Plenary Workshop of the HP OpenView University Association; ENST de bretagne, Rennes, France.
†. This work is funded by DRET

1 Introduction

In order to support future multimedia services, the ITU-T standardization organization adopted the Asynchronous Transfer Mode as the technique to implement B-ISDN.

In the recent past, much attention has been paid to develop security services for ATM networks. This is due to people believing that only a secured ATM model has a chance to attract end users. This resulted in the creation of many working groups within (and outside) the standardization authorities to deal with this problem.
At the ATM-forum a security working group was created in 1995 and is to the point to release its version 1.0 specifications. According to the ATM-forum web server, the security framework (Security Framework 1.0) should have been released in February and the security specification itself (Security 1.0) should be released in July.
At the ITU-T, a security working group has been created but the state of the standardization process is currently unknown. Moreover other solutions, coming from independent working groups have been widely exposed in several international conferences.

This paper will be composed of two parts. In the first part we show that non cryptographic security mechanisms have to be used along with cryptographic mechanisms in order to provide reliable security services in ATM networks. In the second part we take the example of access control to show our point of view.

2 Improving services relying on cryptography

2.1 Cryptographic mechanisms limits

Most of the solutions proposed to secure the ATM model rely on the use of cryptography. Cryptography is a very powerful tool to provide services like confidentiality, authentication, integrity and some kind of access control. However it is clear that cryptography suffers from many drawbacks:

- First of all cryptography implies the management of cryptographic tokens (keys). This problem has not been addressed by standardization authorities yet. This implies that only a small part of ATM users (mostly enterprises) will be able to use security services (inside their enterprise or with their major partners). This is a very big problem since the spread of the ATM security services will rely on their wide use (in order to provide interoperability since they require ATM facilities modifications).
- Differences in governmental regulations make it difficult to design security services common to all countries. Consequently even if the key management problem is to be solved, security services may be designed for each country. This will lead to non compatible implementations and/or restrictions to security services.
- The standard proposed by the ATM-forum security working group is quite complex since it offers many solutions for each security service. Since it is not possible to implement all the solutions to provide a single security service, this will result in non-compatible but specifications compliant implementations. This complexity is a great curb on the implementation of the security specifications.
- Services relying on cryptography may suffer from a performance bottleneck. Current implementations of security services over ATM networks are limited to OC3 speed (155 Mb/s) whereas products operating at OC12 speed (622 Mb/s) are available and proposals at OC192 speed (10 Gb/s) are in the standardization process. Moreover current products do not implement all the security services, most of them only provide confidentiality using (DES or Triple DES) encryption.
- Finally cryptography is a good tool to provide services such as confidentiality, authentication, integrity and some kind of access control. However security services such as denial of service detection and intrusion detection have not been addressed today.

From these statements we can conclude that the current specifications only target enterprises. This is in contradiction with the fact that ATM is also supposed to provide a full range of users including end users (at home) with multimedia services. This standardization process is partially flawed since it may result in various non-interoperable implementations.

2.2 The intrusion detection example

Even if cryptography had to be used to provide security services, it would be a good thing to provide the same services with other means. This would increase the overall security by controlling the results of the cryptographic mechanisms. To explain this point of view, we can re-use the reasons justifying the use of intrusion detection tools in secure operating systems [Muk94]:

- It is impossible to build a system which is completely secure. This is due to the fact that nobody can prove that an operational system is free of flaws. These flaws may result from misconception, flaws in the implementation process coming from the people implementing the system or coming from the tools used for its development. These flaws may also come from the hardware used or from misinteractions with other elements. Finally some flaws may come from the configuration process. This includes poor administrative policies and practices.
- Secure systems are always more constraining for users' activities. This often push administrators to let them operate in «open» mode.
- Secure systems rely on cryptographic tokens. These systems cannot defend against lost or stolen keys and/or cracked passwords.
- Finally a secure system can still be vulnerable to authorised users misusing their privileges.

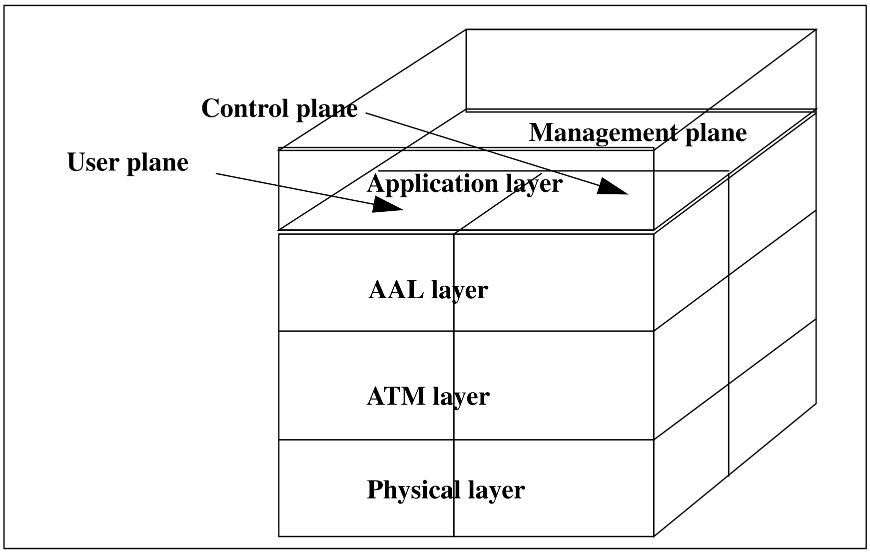
2.3 Conclusion

Cryptography is a good tool to provide some security services in some situations. However non-cryptographic mechanisms have to be widely used to provide or improve security services. In order to explain our point of view we take the example of access control. The currently proposed solutions to provide this service use a combination of a cryptographic authentication based on ATM facilities' addresses and a security level indicator. We'll show in the next section how a good management of information provided by an analysis of the ATM flows can improve access control.

3 Improving access control

In this part, we analyze the ATM model in order to find information that could be used to provide or improve access control, that is to say information that can be used to allow or deny ATM devices to communicate with one another. Before conducting this analysis, we provide a short description of the ATM technology.

Figure 1: The ATM model.



As shown in Figure 1 the ATM model is divided into three layers (Physical, ATM and AAL). The ATM model is also divided into three planes (user plane, control plane and management plane). In order to analyze the model, we

will follow this structure to organize this section.
The lowest layer in the ATM model is the physical layer. This layer's goal is to adapt the ATM flows to a specific physical media. This layer will not be described further since it doesn't transport end to end information. However all this information is not useless, but in this case this useful information is transmitted to the ATM layer or further. The analysis of the physical layer would thus be either useless or redundant.

This section will be divided into three main parts: The ATM layer, the AAL layer and the signalling. The signalling is located both in the ATM control plane and in the application layer above the ATM mode. In each section we give further information about the ATM model when needed.

3.1 The ATM Layer

All the information provided in this section are taken from the ATM-forum UNI3.1 [UNI31] specifications which are the most up-to-date in this field.
The ATM-PDUs, called cells are 53 bytes long. They may be divided into two parts:

- The control part is 5 bytes long. It contains information necessary for ATM switches to switch cells. It also indicates from which plane (User, Control, Management) the cell comes.
- The user part is 48 bytes long. It contains data originated from the AAL layer or the ATM management layer.

3.1.1. The control part

Figure 2: ATM cell header.

	GFC	VPI	VCI	PT	CLP	HEC
Bits	4	8	16	3	1	8

Note:
GFC: Generic Flow Control,VPI: Virtual Path Indicator, VCI: Virtual Channel Indicator.
PT: Payload Type, CLP: Cell Loss Priority, HEC: Header Error Control.

The control part (described in Figure 2) gives useful information:

- The type of the message is indicated by a combination of bits in the control part. This information can be used to control some flows. For example, this information can be used to block signalling information outside of office hours in order to prohibit dynamic connections outside of office hours (for security or financial reasons).
- The VPI/VCI fields are used to identify a connection. They can be used alone or along with other information such as date and time to prohibit some communications. For example it is possible to link a connection to a service such as a particular server when this connection has been set up permanently. The VPI/VCI fields may be used along with the date to prohibit the server's access at specific periods.

3.1.2. The User part.

The user and control planes

The specifications don't provide any information about the user and control data structure at the ATM level.

The management plane

The management plane produces three kinds of flows at the ATM level: ILMI flow, F4 flows and F5 flows. ILMI is an interface between two adjacent ATM devices (switches, end devices) used to provide management and automatic configuration services. Therefore information transported through ILMI are not very interesting since they have no global meaning (they are only valid between two adjacent devices).
F4 and F5 OAM cells include five fields: OAM type (4 bits), function type (4 bits), function specific (45 bits), Reserved field (6 bits), Error Detection Code (CRC-10) (10 bits).

The content of these fields can be used to refine the access control presented in section 3.1.1. For example it could be useful to stop AIS/RDI (Alarm Indication Signal/Remote Defect Indicator) traffic. AIS/RDI traffic is used to report errors occurring in the ATM network to end parties and network elements. Therefore it can be used to counter denial of service attacks realized by false AIS/RDI cells construction.

3.2 The AAL layer

The AAL layer is used to profile the ATM traffic for applications. Many AAL types have been designed for that purpose, each of them matches a specific application type and thus includes particular mechanisms. This results in differently structured AAL-PDUs, each structure corresponding to a single kind of AAL layer.

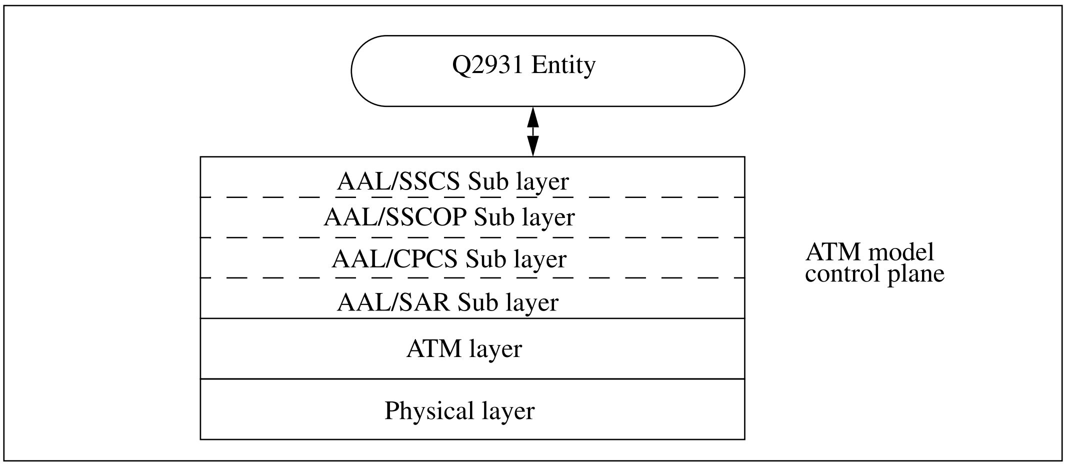
The structure of the PDUs provides information about the type of application used on top of the AAL layer, but this information is given more accurately within the signalling.
However, when no signalling is used (e.g. when permanent links are set up using management plane) this information could be used to forbid the use of some kind of applications between two ATM devices.

3.3 The signalling

Signalling is located both in the ATM control plane and in the application layer above the ATM model. We already presented the characteristics of the signalling flows at the ATM layer level in section 3.1.1. The signalling AAL layer (SAAL) may be divided into four sub-layers. As depicted in Figure 3 the first two sublayers (SAR and CPCS) are common to the AAL5 layer. The SSCOP sub-layer's aim is to provide a reliable transport service. The SSCF sub-layer provides an interface to the Q2931 entity. The Q2931 entity is responsible for the signalling messages construction. It uses these messages to establish, control and release ATM connections.
In this section we analyze the information provided by signalling messages in order to find information that could be used to improve access control. These messages were specified by two authorities: the ATM-forum who released its [UNI4.0] specification in 1996 and the ITU-T who released several standards in its Q signalling series ([Q2931], [Q2931add], [Q2932], [Q2933], [Q2951], [Q2959], [Q2961], [Q2962], [Q2963], [Q2971]).

As explained before, the ITU-T and the ATM-forum provide specifications for signalling. Since the ATM-forum's signalling specification has been released after the ITU-T's, the UNI4.0 specification is mostly compatible with the ITU-T standard. However the ITU-T released addendum and extra specifications after the release of the UNI4.0. This results in differences between these standards including several different messages and different information within the messages. Each message contains a specified amount of information. This information is structured in blocks called IEs (Information Elements) in the ATM terminology. An IE is a block of information relating to a single subject.

Figure 3: The control plane.



3.3.1. Messages' analysis

Before analyzing these IEs, we will refine our scope of research. Each of the messages specified in the standards has a scope. This scope can be local or global. This means that some messages are only meaningful to two adjacent network elements. Thus some of the IEs found within these messages have only a local meaning also. These IEs cannot be used to provide access control since they don't provide information about end parties.

The following list contains the messages with global scope:

- According to the ITU-T specifications: SETUP, CONNECT, ALERTING, RELEASE, PROGRESS, ADD PARTY, ADD PARTY ACK, PARTY ALERTING, ADD PARTY REJECT, DROP PARTY, MODIFY REQUEST, MODIFY ACK, MODIFY REJECT, CONNECTION AVAILABLE.
- According to the ATM-forum specification: SETUP, CONNECT, ALERTING, RELEASE, PROGRESS, ADD PARTY, ADD PARTY ACK, PARTY ALERTING, ADD PARTY REJECT, DROP PARTY, LEAF SETUP REQUEST, LEAF SETUP FAILURE.

From the previous list we can decide which IEs have a global meaning (all the abbreviations are given in the annex):

- According to the ITU-T specifications: NBC, C, PI, NI, ETD, CN, CSA, AALP, ATD, CI, QoSP, BHLI, BBC, BLLI, BSC, BRI, cPN, cPSA, CPN, CPSA, TNS, NLLC, NHLC, MATD, AATD, ER, BTR, LLCP, LLPP, OAMTD, pI.
- According to the ATM-forum specification: NBC, C, CS, PI, NI, ETD, CN, CSA, AALP, ATD, CI, QoSP, BHLI, BBC, BLLI, BSC, BRI, cPN, cPSA, CPN, CPSA, TNS, NLLC, NHLC, GIT, MATD, AATD, ASP, CSS, AAP, EQoSP, LIJCI, LIJP, LSN, ER.

3.3.2. IEs' analysis

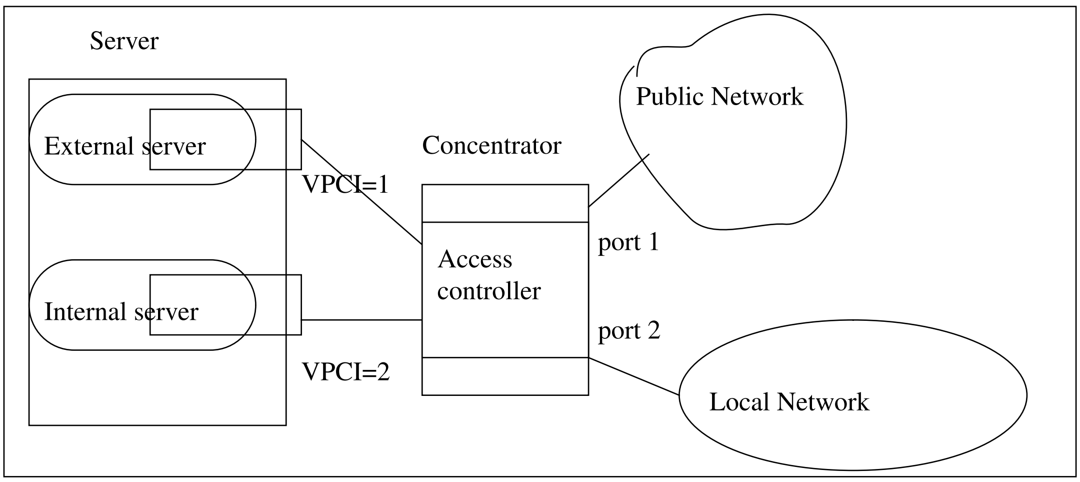
Some IEs contain poor information from an access control point of view. Some others relate to the same subject. For example the ABR Additional Parameters (AAP) IE, the Extended QoS Parameters (EQoSP) IE and the ABR Setup Parameters (ASP) all relate to traffic description. Therefore in order to analyze the IEs we will group them by subject.

End users' identifiers

- CPN, cPN, CPSA, cPSA: These IEs hold the addresses and sub-addresses of the calling and called parties.
- CN, CSA: These IEs contain the address and the sub-address of the connected party. This information may differ from the address and sub-address of the called party when this party is using services such as call redirection.
- ER: Endpoint Reference. This IE identifies an ATM device in a point to multipoint connection.
- LIJCI : Point to multipoint connection identifier. This IE is only specified in the UNI4.0 specification. It is similar to the ER IE but it is used to offer extra services.

These identifiers can be used to provide an address-based access control. This access control may take place between a local and a public ATM network to avoid «ATM spoofing».

Figure 4: VPCI based access control.



• CI: The VPCI information is included within the CI IE. The VPCI allows to distinguish ATM devices sharing the same address and the same signalling stack.

Figure 4 provides an example where VPCI access control can be used in association with the port number. In our example a server located inside our internal network provides two services, each service being provided by a software server. This server is connected to a specific ATM card. However the two software servers share the same ATM address and the same signalling stack which is located in the concentrator. In order to deny the access of external devices to the internal server, the concentrator has to block connection requests from the public network (port 1) to the server with a VPCI equal to 2.

• CS: The connection scope selection IE defines the area where the group addresses are valid. Group addresses may be defined at different levels (local/enterprise/organisation/region...). The meaning of a group address can vary with this level. Thus it is important to use this information to understand to which area group addresses relate.

Flow information

• BLLI, NLLC: These IEs provide information about the link and network layers when ATM is used as a physical or link layer. This information includes ISO or SNAP identifiers [X263], frame or packet sizes and windows sizes. These IEs also describe multiplexing capabilities. The difference between BLLI and NLLC is that BLLI relates to a Broadband use of the ATM network whereas NLLC relates to Narrowband emulation by the ATM network.

These information can be used to restrict access from a certain kind of network with a specified frame or packet size or with a specified window size.

• BHLI, NHLC: These IEs provide information about the applications used above the AAL layer. In the future these IEs are expected to describe applications in the same way as the protocol and port numbers do in an IP network.

When the content of the IE will have been standardized, it will allow application-based access control.

Table 1 : Relationships between applications and traffic classes

Application/Type of traffic	**CBR**	**rt-VBR**	**nrt-VBR**	**ABR**	**UBR**
LAN interconnection			x	X	x
Data transport			x	X	x
Circuit emulation (PABX)	X	x			
ISDN video conference	X				
Compressed audio data		X	x	x	
Video	X	x			
Interactive multimedia	X	X	x	x	
Critical data	x		X		

Note 1: X Optimum, x Fair.

Note 2: Relationships between AAL and traffic classes:

CBR: AAL1, rt-VBR: AAL2, nrt-VBR ABR UBR: AAL3/4 AAL5.

• AALP: This IE describes the AAL type and its parameters (for example the AAL1 CBR throughput).

• ATD, AATD, MATD, QoSP, BBC, ASP, EQoSP, AAP: These IEs describe the type of traffic and the traffic contract parameters. The traffic contract parameters vary with the type of traffic.

• LLCP, LLPP: These IEs are used to describe the traffic when the ATM network provides a frame relay service.

These IEs give some additional information about the service used. Table 1 (taken from [Atm97]) provides information about the links between applications and services classes.

This relationship can be refined by looking closer at the values of the traffic parameters. However there is no mandatory link between the traffic descriptor and the application. A malicious user could ask for FTP service over AAL2 or AAL1 with traffic parameters matching a video connection. This is one of the reasons why the security administrator has design properly the network to protect. A major aspect of this design is to build a unique relationship between each service and ATM address since this relationship can not be achieved through the signalling.

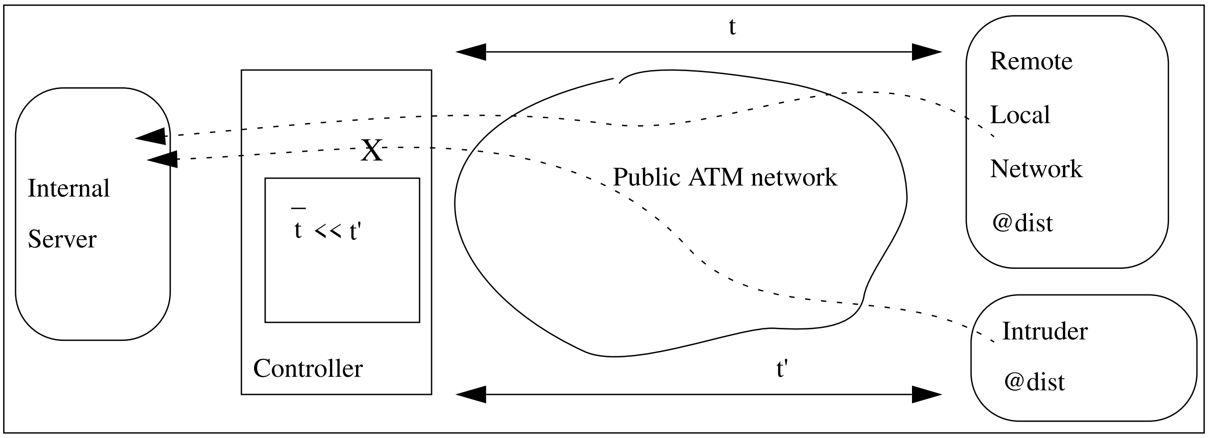
• GIT: The Generic Identifier Transport element describes the multimedia capabilities of the parties [H245].
This information can be used to restrict the range of flows that can be exchanged between two parties.

Other information

• TNS: The Transit Network Selection IE specifies the network that should be crossed during the connection set up.
This IE can be used to check which networks have been crossed during the connection setup. It can be useful to check that the connection request didn't passed through a sensible network (from a security point of view). It can also be used to verify that the list of the network crossed is compatible with the origin of the call.

• ETD: The End To end Delay describes the delay required by the signalling message to cross the network between the parties. This delay is calculated by the network.
Figure 5 provides an example where the transit delay is used to detect an intruder using address forgery to gain access to an internal server. In this example the transit delay at connection setup (t') is compared with the mean time for connection setup between the controller and the remote local network ($\bar{t}$). If t' is significantly different from $\bar{t}$, the connection setup is stopped.

Figure 5: Address forgery detection



4 Conclusion

As explained in section 2 non-cryptographic mechanisms have to be used to improve the overall security in ATM networks. In section 3 we provide parameters that could be managed to improve access control.
In order to evaluate the strengths and weaknesses of the access control service we can make a comparison between the information provided in the ATM model and the information used in the IP world to provide access control. This comparison is given in Table 2.

This comparison shows that parameters similar to those currently used to provide access control in the IP world could be used in ATM networks. Moreover since information provided by the ATM model is more accurate than information provided by the IP world, the access control could be thinner and more effective.
Therefore this information could be used today to achieve an access control level equivalent to the internet's one. It could also be used in the future to improve the access control specified in future standards since the use of our information can be used without standards modification.
An interesting continuation to this job would be the implementation of a controller to test performance and configuration issues.

Table 2 : Comparison between information provided by each world

Information/World	**IP**	**ATM**
Adresses	X/M	X/M
Sub adresses		X/O
Higher layers	X/M	X/O
Services	X/M	(1)
Traffic descriptor	x/O	X/M
Transit network selection	x/O	X/O
Performance information		X/O
Diagnostics	x/M	X/M
Security information	X/O	(1)

Note:

X: Major information. x: Minor information.

M: Mandatory information. O: Optional information.

(1): In standardization process.

5 References

[Atm97]: ATM in Europe: The User Handbook. European Market Awareness Committee. Version 1.0. The ATM forum. july 1997.

[H245]: Audiovisual and multimedia systems. Line transmission of non-telephone signals. Control protocol for multimedia communication. ITU-T recommendation H245. ITU-T. March 1996.

[I610]: Integrated services digital network, maintenance principles. B-ISDN operation and maintenance principles and functions. ITU-T recommendation I610. UIT-T. November 1995.

[Muk94]: Network Intrusion Detection. B. Mukherjee, L. T. Heberlein, K. N. Levitt. IEEE Network. May/June 1994.

[Q850]: Digital Subscriber Signalling System No. 1, General . Use of cause and location in the digital subscriber Signalling System No. 1 and the Signalling System No. 7. ITU-T recommendation Q850. UIT-T. March 1993.

[Q932]: Digital Subscriber Signalling System No. 1, Network Layer. Generic procedures for the control of ISDN supplementary services. ITU-T recommendation Q932. March 1993.

[Q2610]: Common aspects of B-ISDN application protocols for access signalling and network signalling and internetworking. Usage of cause and location in B-ISDN user part and DSS 2. ITU-T recommendation Q2610. February 1995.

[Q2931]: Broadband ISDN - B-ISDN application protocols for access signalling. B-ISDN application protocols for access signalling - Digital Subscriber Signalling System No. 2 - User-Network Interface (UNI) layer 3 specification for basic call/connection control. ITU-T recommendation Q2931. February 1995.

[Q2931add]: Broadband ISDN - B-ISDN application protocols for access signalling. B-ISDN application protocols for access signalling - Digital Subscriber Signalling System No. 2 - User-Network Interface (UNI) layer 3 specification for basic call/connection control. ITU-T recommendation Q2931 amendement 1. June 1997.

[Q2932]: Broadband ISDN - B-ISDN application protocols for access signalling. Digital subscriber signalling system No. 2 Generic functional protocol: Core functions. ITU-T recommendation Q2932. july 1996.

[Q2933]: Broadband ISDN - B-ISDN application protocols for access signalling. Digital subscriber Signalling System No. 2 (DSS 2) Signalling specification for Frame Relay service. ITU-T recommendation Q2933. july 1996.

[Q2951]: Broadband ISDN - B-ISDN application protocols for access signalling. Stage 3 description for number identification supplementary services using B-ISDN digital subscriber Signalling System No. 2 (DSS 2) Basic Call, Direct-Dialling-In (DDI), Multiple Subscriber Number (MSN), Calling Line Identification Presentation (CLIP), Calling Line Identification Restriction (CLIR), Connected Line Identification Presentation (COLP), Con-

nected Line Identification Restriction (COLR), Sub-addressing (SUB). ITU-T recommendation Q2951. February 1995.
[Q2959]: Broadband ISDN - B-ISDN application protocols for access signalling. Digital Subscriber Signalling System No. 2 - Call priority. ITU-T recommendation Q2959. july 1996.
[Q2961]: Broadband ISDN - B-ISDN application protocols for access signalling. B-ISDN application protocols for access signalling - Digital Subscriber Signalling System No. 2 - Additional traffic parameters. ITU-T recommendation Q2961. October 1995.
[Q2962]: Broadband ISDN - B-ISDN application protocols for access signalling. Digital Subscriber Signalling System No. 2 - Connection characteristics negotiation during call/connection establishment phase. ITU-T recommendation Q2962. july 1996.
[Q2963]: Broadband ISDN - B-ISDN application protocols for access signalling. Connection modification: Peak cell rate modification by the connection owner. ITU-T recommendation Q2963. july 1996.
[Q2971]: Broadband ISDN - B-ISDN application protocols for access signalling. B-ISDN application protocols for access signalling - Digital Subscriber Signalling System No. 2 - User-network interface layer 3 specification for point-to-multipoint call/connection control. ITU-T recommendation Q2971. October 1995.
[UNI3.1]:ATM User-Network Interface (UNI) specification. Version 3.1. The ATM-forum Technical Committee. September 1994.
[UNI4.0]: ATM User-Network Interface (UNI) Signalling Specification. Version 4.0. The ATM-forum Technical Committee. july 1996.

6 Annex : IEs abbreviations.

AALP: ATM Adaptation Layer Parameters.
AAP: ABR Additional Parameters.
AATD: Alternative Atm Traffic Descriptor.
ASP: ABR Setup Parameters.
ATD: ATM Traffic Descriptor.
BBC: Broadband Bearer Capability.
BHLI: Broadband High Layer Information.
BLLI: Broadband Low Layer Information.
BLS: Broadband Locking Shift.
BNLS: Broadband Non-Locking shift.
BRI: Broadband Repeat Indicator.
BSC: Broadband Sending Complete.
BTR: Broadband Type Report.
C: Cause.
CI: Connection Identifier.
CN: Connected Number.
cPN: Calling Party Number.
CPN: Called Party Number.
cPSA: Calling Party Subadress.
CPSA: Called Party Subadress.
CS: Call State.
CSA: Connected Subadress.
CSS: Connection Scope Selection.
EQoSP: Extended QoS Parameters.
ER: Endpoint Reference.
ES: Endpoint State.
ETD: End-to-End Transit Delay.
F: Facility.
GIT: Generic Identifier Transport.
LIJCI: Leaf Initiated Join Call Identifier.
LIJP: Leaf Initiated Join Parameters.
LLCP: Link Layer Core Parameters.
LLPP: Link Layer Protocol Parameters.
LSN: Leaf Sequence Number.
MATD: Minimum Acceptable Traffic Descriptor.
NBC: Narrowband Bearer Capability.
NHLC: Narrowband High Layer Information.
NI: Notification Indication.
NLLC: Narrowband Low Layer Information.
OAMTD: OAM Traffic Descriptor.
pI: Priority Information.
PI: Progress Indicator.
QoSP: QoS Parameters.
RI: Restart Indicator.
TNS: Transit Network Selection