Emerging Network Protocols

From IPv6 and RSVP to ATM

NR Norsk Regnesentral
ANVENDT DATAFORSKNING
Norwegian Computing Center/Applied Research and Development

NOTAT / NOTE

IMEDIA/04/98

Lars Aarhus
Jannicke Riisnæs

Oslo
April 1998

NR Norsk Regnesentral
ANVENDT DATAFORSKNING

Notat / Note

Tittel/Title:
Emerging Network Protocols
From IPv6 and RSVP to ATM

Dato/Date: April
År/Year: 1998
Notat nr/
Note no: IMEDIA/04/98

Forfatter/Author:
Lars Aarhus, Jannicke Riisnæs

Sammendrag/Abstract:

With the increasing use of real-time multimedia applications on the Internet a number of new network protocols have emerged. *IPv6*, which replaces the old Internet Protocol (IPv4) as the basic protocol in next generation IP networks. *ATM*, which is widely used as a link-layer protocol for high bandwidth traffic. *ISPN*, which is a proposed Internet architecture model, and an extension to traditional best-effort service. *RSVP*, which is a protocol for establishing and maintaining resource reservations on the Internet.

In this note, these emerging protocols are presented, and their characteristics are summarized. This work is based on a two hour seminar on the subjects, and is written as part of the IMiS Kernel project.

Emneord/Keywords: multimedia, IPv6, ATM, ISPN, RSVP, network protocols, QoS, resource reservation

Målgruppe/Target group: research institutions, NR

Tilgjengelighet/Availability: Open

Prosjektdata/Project data: IMiS Kernel

Prosjektnr/Project no: 28006

Antall sider/No of pages: 72

Norsk Regnesentral/Norwegian Computing Center
Gaustadalléen 23, Postboks 114 Blindern, N-0314 Oslo, Norway
Telefon (+47) 22 85 25 00, telefax (+47) 22 69 76 60

Emerging Network Protocols

From IPv6 and RSVP to ATM

Lars Aarhus
Jannicke Riisnæs

Norsk Regnesentral

April 15, 1998

Table of Contents

1 Introduction

This note is written as part of the IMiS Kernel project.

The goal of this project is to establish a national, experimental platform for infrastructure for multimedia services in seamless networks. Participants are Norwegian Computing Center (NR), UNINETT, Department of Informatics at the University of Oslo, and Ericsson.

1.1 Motivation

The subjects of study in this note are the new Internet Protocol (IPv6), the Asynchronous Transfer Mode (ATM) service and Integrated Service Packet Network (ISPN) with Resource Reservation Protocol (RSVP), part of the next generation Internet model.

IPv6 is chosen as it will be one of the basic protocols in next generation IP networks. The protocol will replace IPv4, adding an expanded address space and new functionality for multimedia communication. The IMiS Kernel infrastructure will support IPv6 communication.

ATM, or broadband ISDN, is emerging as a widely used link-layer protocol for high bandwidth traffic. The service is also defined for end-to-end communication, but this is rarely used. The IMiS Kernel infrastructure will use ATM as carrier in the core network.

ISPN is a proposed new packet-based Internet architecture model, and an extension to traditional best-effort Internet. The model defines a number of new service classes, and introduces the concept of quality of service (QoS) to the Internet.

RSVP is a protocol for establishing and maintaining resource reservations on the Internet. The protocol has attracted a lot of interest, despite a few shortcomings, which is why it is chosen as a subjcet of study. The IMiS Kernel infrastructure will implement RSVP.

1.2 Outline

After this short introduction, IPv6 is described in chapter 2. In chapter 3 ATM is presented, whereas ISPN and RSVP are the focus of chapter 4. The final chapter contains a short summary and a look ahead to future work on these issues as part of the IMiS Kernel project.

The content of this note is based on two one-hour lectures on the subjects of study, and will thus only provide an overview of the issues.

2 IPv6

The compelling reason for IPv6 is the need for a larger address space. It is estimated that 10^{15} computers will possibly be connected to the Internet by the year 2020 [4]! Additionally, as the protocol will replace the old one, a thorough revision of all parts was conducted, leading to improved support for the next generation Internet model.

The first two sections of this chapter present a brief overview of the differences in format and functionality between IPv4 and IPv6. Section 2.3 is concerned with the new addressing formats and types, whereas section 2.4 focuses on the new extension headers. In section 2.5 to 2.8 four important areas supported by new IPv6 functionality are presented in slightly more detail. Section 2.9 describes the transition mechanisms between the two protocols, before a short list of IPv6 testing and experimental environments is given in the last section.

2.1 Changes from IPv4

IPv6 was and is being developed by the IPng working group of the Internet Engineering Task Force (IETF), and is now an IETF proposed standard [2].

The main changes compared to IPv4 are [3]:

- Larger address space, as an IP address is now 128, not 32 bits long
- Header simplifications, as there is now a fixed format and no checksum.
- Better support for options, with the introduction of extension headers, and new functionality.

The IPv6 packet format is shown in figure 1. The header and payload are mandatory, whereas the extension header(s) is optional components.

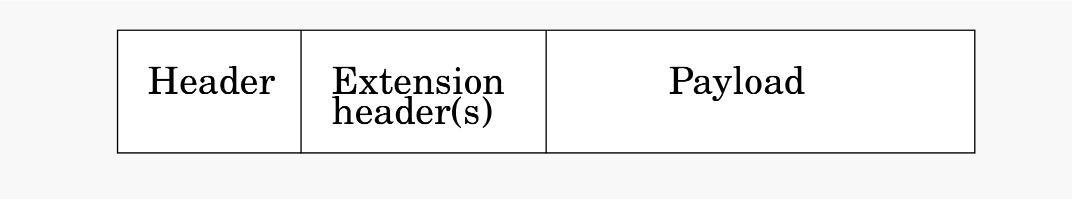


Figure 1 : *IPv6 packet format*

2.2 Funtionality in IPv6

The compostition of the IP header is the biggest difference between IPv4 and IPv6, when it comes to incorporating new functionality in the protocol.

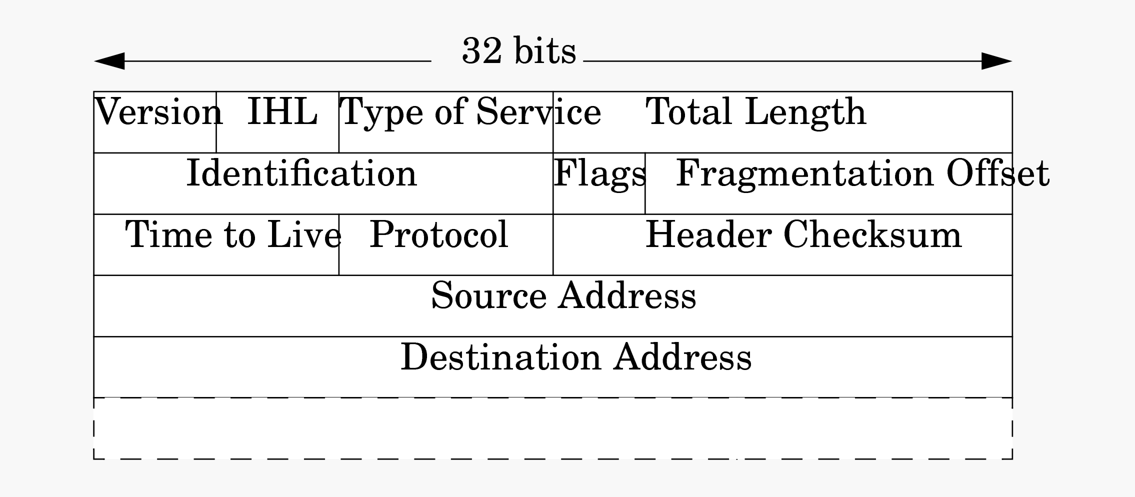


Figure 2 : *IPv4 header (~1975)*

The old IPv4 header is shown above in figure 2, and should be compared to the new IPv6 header presented below in figure 3.

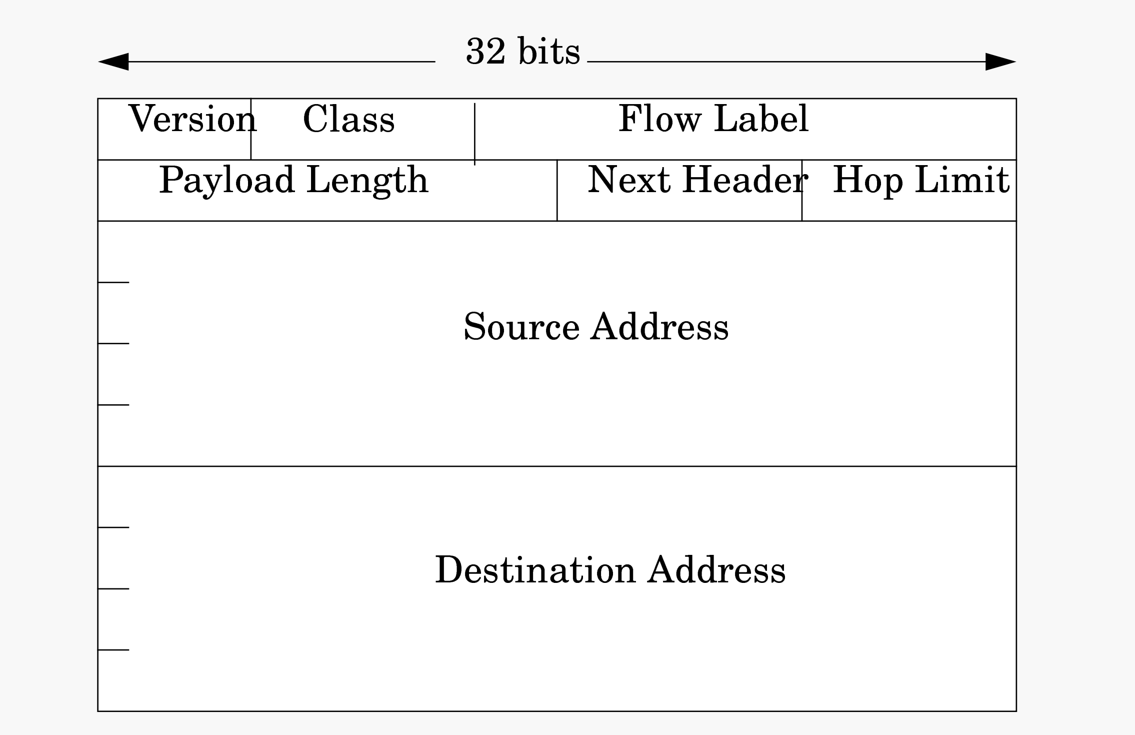


Figure 3 : *IPv6 header*

In short, new functionality in IPv6 include:

- Quality of service: support for flow and class differentiation
- Mobility: address auto configuration
- Security: support for authentication, integrity and confidensiality.

- Routing: neighbor discovery algorithm and DHCPv6

More details regarding each area are given in section 2.5 to 2.8.

2.3 Addressing

An IPv6 address is composed of 128 bits. The notation consists of eight 16-bit integers separated by colons. Each integer is represented by four hexadecimal digits. For convenience, a few abbreviations such as the double-colon convention (indicating a sequence of zeros) are allowed.

An example of an IPv6 address from NR is 3FFE:2A01::<64 bits interface identifier>.

The following address formats are defined:

- *aggregatable,* global addresses (with prefix 001), which consist of four fixed-sized components: TLA (top level aggregator, 13 bits), NLA (next level aggregator, 32 bits), SLA (site local aggregator, 16 bits) and interface identifier (64 bits).
- *special* addresses: link-local (with prefix FE80, only used within a single link), site-local (with prefix FEC0, only used within a single site), IPv4 (with 96 zero bits prefix), loopback (0:0:0:0:0:0:0:1) and unspecified (16 null bytes).

Three address types are defined:

- unicast (one to one interface)
- multicast (one to many interfaces)
- anycast (one to one-of-many interfaces)

Multicast is an integral part of IPv6, and not an extension as in IPv4. All routers should recognize the multicast address format, which includes a *scope* field for limited packet distribution. This scales better than the tuning of the Time to Live field in IPv4. Also, the Internet Group Management Protocol (IGMP) is now included in the new Internet Control Management Protocol (ICMP) v6, which is incompatible with the old ICMPv4.

Anycast is a new address type. Routers should deliver the packets to the “nearest” interface. One possible area of use is load balancing on a web site with several servers with replicated file systems [5].

There is no broadcast (one to all interfaces) address type in IPv6.

2.4 Options

In order to reduce complexity in the IP header, and increase effiiciency in routing, a number of *extension headers* are introduced in IPv6. In recommended order, for faster header processing, they are:

- hop-by-hop options (extra router information, jumbo payload)
- destination options (generic, additional functionality)
- routing (intermediate router “visits”)
- fragment (packet division)
- authentication (security)
- encrypted security payload (security)

For more details regarding the structure of these headers, see [4].

2.5 Quality of service

To support Quality of Service (QoS) two new fields are included in the IPv6 header:

- Class field (8 bits)
- Flow label (20 bits)

In the *class field*, the first bit, D, is set to indicate delay-sensitive (e.g. real-time) traffic. The next three bits specify global, networkwide priority level (traffic class), similar to the precedence bits in Type of Service field in IPv4 [1]. The last four bits are reserved for future use.

Incidently, there is now discussion going on in IETF about revising the use of the Type of Service (ToS) field for “differentiated service”. This work will have an impact on the exact specification of the class field, which is why the field is not yet defined.

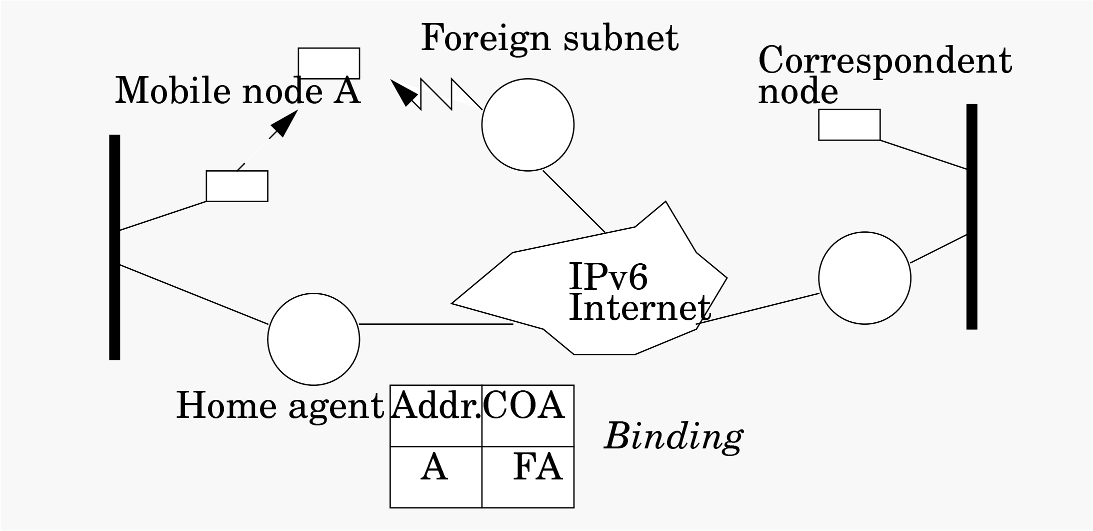
The flow label identifies a *flow* - a sequence of packets from the same sender, that “belong together” and demand special treamment. The intended use is when making resource reservations. Each flow will be assigned a (pseudo)random and uniform number from 1 to FFFFF, but routers and hosts without flow support will set the flow label to 0.

Until recently (fall 1997) there was a 4 bits drop priority field and a 24 bit flow label, but the notion of source-relative priorities that would differentiate packets belonging to the same flow is now abandoned, because of discouraging experimental results [4].

2.6 Mobility

In IPv6 there is better support for a mobile architecture, as proposed in MobileIP [6], and shown in figure 4. The mobile node needs a home agent in its own subnet, and a care-of-address (COA) in the foreign subnet. The *binding* between the home address (A) and the COA is maintained by the home agent.

Three destination options extension headers are defined in MobileIPv6 to support this architecture: Binding Update, Binding Acknowledgement and Binding Request.



Addr.	COA
A	FA

Figure 4 : Mobile IP architecture, from [5]

Address autoconfiguration is now an integral part of IPv6. Two modes are supported:

- *stateless*
- *stateful*

In stateless mode, the configuration of the host is automatic, without manual interaction, and based on some unique token (e.g. the Ethernet address). In stateful mode, the configuration requires a server, and a configuration protocol, Dynamic Host Configuration Protocol (DHCP) v6.

Also, a Neighbor Discovery procedure is developed in IPv6. The algorithm is an improvement of, and encompasses the funtions in the Address Resolution Protocol (ARPv4) and the ICMP Router Discovery. The new procedure identifies link-layer addresses of other nodes in the same subnet.

2.7 Security

IPv6 introduces built-in security mechanisms at the network level providing:

- Security associations
- Authentication
- Confidentiality

A unidirectional *security association* is established between a sender and a receiver. The association is identified by a Security Parameter Index (SPI) and the receiver address.

The authentication extension header offers both *autbelowhentication* and data integrity. The keyed MD5 cryptographic algorithm is specified as default when computing the checksum.

Confidentiality and data integrity is provided by the encapsulating security payload (ESP) extension header. The specified default encryption algorithm is Data Encryption Standard-Cipher Block Chaining (DES-CBC). Either the payload only or the entire IP packet is encrypted. Figure 5 below illustrates the packet format when only payload encryption (Transport mode ESP) is applied.

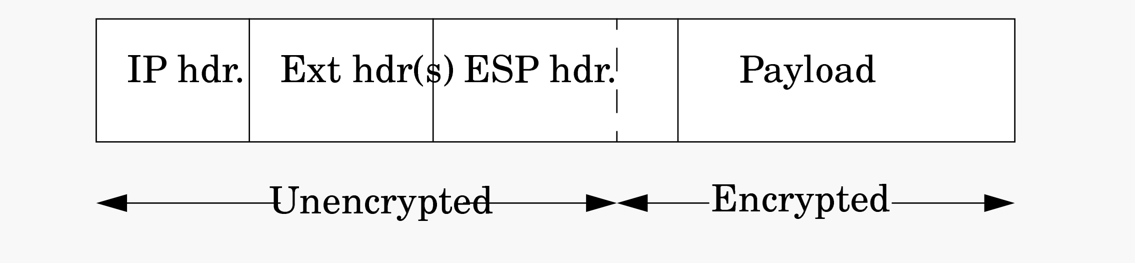


Figure 5 : *Transport mode ESP packet format, from [5]*

The secure key distribution method is likely to be Photuris. The method is based on the Diffie-Hellman key exchange algorithm, which uses the concept of private and public keys.

Although all the algorithms mentioned above are standardized in IPv6, a sender and a receiver can negotiate to apply others as part of a security association establishment.

2.8 Routing

By using the routing extension header, a sender can list one or more intermediate routers to be “visited” by the IPv6 packet before reaching its final destination. This functionality permits [3]:

- Provider selection (based on cost etc.)
- Host mobility (route to current location)
- Auto-readdressing (route to new address)

Else, routing in IPv6 is almost identical to IPv4 routing. All the same routing protocols, e.g. OSPF, RIF, are used, only upgraded to support IPv6.

2.9 Transition mechanisms

As the entire Internet can not be upgraded at once, interoperability between IPv4 and IPv6 nodes is the most important transition objective. This means a gradual upgrading and deploying of IPv6 routers and hosts, and ensuring backward compability with IPv4.

The transition mechanisms include:

- Domain Name Server (DNS) upgrade, by introducing AAAA resource records
- Dual protocol stacks, with parallel support for both IPv4 and IPv6
- Tunneling of IPv6 packets over IPv4 regions

A simple tunneling example of encapsulating IPv6 in IPv4 is given in figure 6.

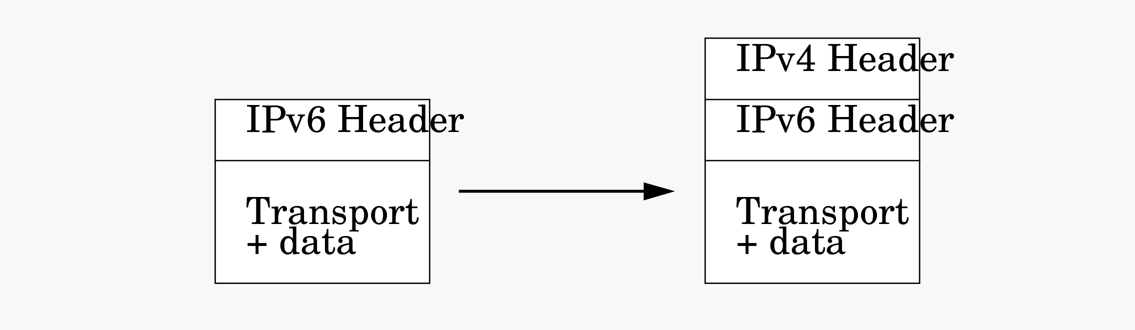


Figure 6 : *IPv6 in IPv4 encapsulation*

Also, to facilitate the upgrading of existing IPv4 applications and ease the development of new IPv6 applications, a standard IPv6 programming interface is defined.

2.10 Testing and experiments

More and more research- and development groups are establishing IPv6 test environments. A few examples, with corresponding web addresses:

- 6-bone: an open IETF forum, providing a worldwide IPv6 testbed
  `http://www-cnr.lbl.gov/6bone/`
- Digital IPv6 prototype: `http://www.digital.com/ipv6/`
- Lancaster University IPv6 project: `http://www.cs-ipv6.lancs.ac.uk/`
- Norwegian Computing Center (NR): IMiS Kernel - an experimental IPv6 network under establishment in cooperation with UNINETT and the Department of Informatics at the University of Oslo
  `http://www.nr.no/imis/imis-k/`

References

[1] Almquist, P., *Type of Service in the Internet Protocol Suite*, RFC 1349, 1992

[2] Deering, S. & Hinden, R., *Internet Protocol, Version 6 (IPv6), Specification*, RFC 1883, 1995

[3] Hinden, R., *IP Next Generation: Overview*, Communications of the ACM, vol.39, no.6, 1996

[4] Huitema, C., *IPv6: The New Internet Protocol*, 2nd edition, Prentice Hall, 1997

[5] Klovning, E., *IPv6 Overview*, Telektronikk, 2, 1997

[6] Perkins, C. & Johnson, D., *Mobility Support in IPv6*, ACM MobiCom'96, 1996

3 Asynchronous Transfer Mode (ATM)

ATM (Asynchronous Transfer Mode) is a result of the CCITT's (now ITU-T) attempt to standardize Broadband ISDN in the mid 1980s. It was originally closely bound up with the emerging Synchronous Digital Hierarchy (SDH) standards, and was first developed to provide communication channels with arbitrary bandwidth within a multiplexing hierarchy consisting of a defined set of fixed-bandwidth channels. The reason why ATM also can provide channels of variable bitrate, is a side-effect that emerged from its provision of arbitrary-capacity channels.

ATM started out as technology for the telecommunications community, but in the early 1990s the ATM standard was seen also by the data communications community as a promising candidate for networking in the local area as well as a replacement for TDM (Time Division Multiplexing) in transmission systems.

ATM has become a success as a link layer technology because it offers high-speed connections to routers and network through a flexible, high-speed, and scalable link layer.

Intergrated Services in the Internet is becoming a reality with ATM as the important backbone technology. "Classical" IP over ATM is now widely deployed, effectively solving the problem of "best effort service" in Internet with ATM links. An important problem is to integrate ATM networks with the Integrated Services Internet. RSVP (Resource ReSerVation Protocol) is the setup or signalling portion of the Internet Integrated Services model.

Another reason for using ATM is its possibility to integrate existing and/or new LANs and WANs since the same protocols can be used for both LANs and WANs.

ATMs biggest disadvantage though, is that its standardization is not complete, and that the standard is not precise and detailed enough when it comes to implementation issues. This makes it less seamless to integrate services, and also to integrate different ATM networks even though they are based on the same standard.

The ATM Forum

The ATM Forum is an international non-profit organization formed in 1991 with the objective of increasing the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness. Currently, The ATM Forum counts over 900 member companies, and it remains open to any organization that is interested in ATM-based solutions.

The ATM Forum [14] consists of a worldwide Technical Committee, three Marketing Committees for North America, Europe and Asia-Pacific as well as the Enterprise Network Roundtable, through which ATM end-users participate.

The ATM Forum Technical committee works with other worldwide standards bodies selecting appropriate standards, resolving differences among standards, and recommending new standards when existing ones are absent or inappropriate. The Technical Committee consists of several working groups, which investigate different areas of ATM technology [14].

The ATM Market Awareness Committees provide marketing and educational services designed to speed the understanding and acceptance of ATM technology [14].

The Enterprise Network Roundtable, formed in 1993, consists of ATM end-users. This group interacts regularly with the Market Awareness Committees to ensure that ATM Forum technical specifications meet real-world end-user needs [14].

The initial focus of the ATM Forum has been the development of specifications governing the use of ATM in a LAN environment. ATMs origin as a wide-area telecommunications standard and its rapid deployment in the LAN, MAN and WAN environments requires it to be simultaneously processed through multiple standards bodies (ITU-T, ANSI, IETF) [7].

This chapter started with an informal introduction to ATM and the ATM Forum, and will continue with a description of the basics of ATM (section 3.1) with focus on the cell structure with its different interfaces in section 3.2, two possible types of connections, virtual paths and virtual channels, in section 3.3, and signalling in ATM, described in section 3.4.

Section 3.5 introduces the ATM reference model, and describes in detail the structure of the different layers, both vertically and horizontally. Quality of service and traffic management in ATM is described in section 3.6, whereas section 3.7 is concerned with the use of ATM in networks. The whole chapter is concluded with two short sections on ATM and mobility (section 3.8), and ATM and multimedia (section 3.9).

3.1 ATM Basics

ATM - Asynchronous Transfer Mode - is the complement of, and was developed from Synchronous Transfer Mode

Synchronous Transfer Mode is a synchronous time multiplexed system where the packages are transferred in predefined 125 ms time slots. Synchronous time multiplexing (fixed cycle) lets the user have full access to the channel for a given time interval. This implies that the time slot will be empty if a user does not have anything to send [2].

Asynchronous Transfer Mode is on the other hand based on asynchronous time multiplexing. The basic theory behind ATM is that the packages sent is named according to the connection, and not a specified time. Asynchronous time multiplexing (on demand) allows the users to get arbitrary access to the channel whenever they have something to send, and they will then get full access to the channel throughout the whole transmission [2].

3.2 ATM Cells

The most important and most significant part of ATM is the packages, or cells as they are called in the world of ATM because they are of a fixed length of 53 bytes. The cells are small, which reflects the origin in telecommunication networks. The header constitutes 5 bytes, and the rest is reserved for data, 48 bytes. ATM was independently proposed by Bellcore, the research arm of AT&T in the US, and several giant telecommunications companies in Europe, and this is why they ended up with the compromise of 48 bytes of data (USA wanted 64 bytes, Europe 32 bytes).

The ATM cells have no explicit sender or receivers address because the combination of the connections VCI (Virtual Channel Identificator) and VPI (Virtual Path Identificator) is used instead. This makes the switching faster because you do the switching according to 28 bit VCI/VPI instead of 128 bit IP addresses (IPv6).

There are two types of cells defined in the ATM specification: one for the user-network interface (UNI), and one for the network-network interface (NNI) as pictured in figure 1.

.

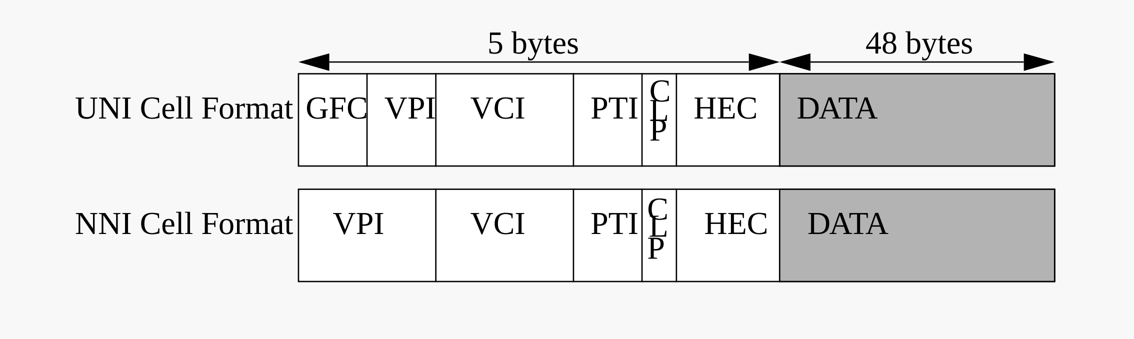


Figure 1 : *Specification of the cells in ATM, based on [4], where UNI is the cell for the user-to-network interface (host-to-switch), and NNI is the cell for the network-to-network interface (switch-to-switch).*

- GFC: generic flow control - 4 bits (only for UNI)
- VPI: virtual path identifier - 8 bits for UNI, and 12 bits for NNI
- VCI: virtual channel identifier - 16 bits
- PTI: payload type - 3 bits
- CLP: cell loss priority - 1 bit
- HEC: header error correction - 8 bits
- DATA: 48 bytes of data

The *generic flow control* (GFC) field does not appear in the cell header internal to the network, but only at the user-network interface. The field could be used to assist the customer in controlling the flow of traffic for different qualities of service. The *virtual path identifier* (VPI) constitutes a routing field for the network. It is 8 bits at the user-network interface, and 12 bits at the network-network interface, allowing for more virtual paths to be supported within the network. The *virtual channel identifier* (VCI) is used for routing to and from the end user, it functions much as a service access point. The *payload type* (PT) field indicates the type of information in the information field. A value of 0 in the first bit indicates user information, a value of 1 indicates that this cell carries network management or maintenance information. The *cell loss priority* (CLP) is used to provide guidance to the network in the event of congestion. A value of 0 indicates a cell of relatively higher priority which should not be discarded, and a value of 1 indicates that this cell is subject to discard within the network. Each ATM cell includes also an 8-bit *header error control* (HEC) that is calculated based on the remaining 32 bits of the header, and is used not only for error detection, but in some cases also for error correction ([1]).

The VPI and VCI will together be the unique identifier of the transmission or connection.

Most of the header information is generated in the ATM layer, but the payload data is generated by the ATM adaptation layer (AAL). HEC (Header Error Correction) is generated by the physical layer, and not by the ATM-layer. HEC is used to detect and/or correct header information. A single error can be detected and corrected, while several errors can only be detected. A cell with several errors will be discharged.

3.2.1 UNI and NNI

Virtual channel connections are set up between two endpoints which can be either end users, network entities, or an end user and a network entity [1].

An *end user to end user connection* is used to carry end-to-end user data, but can also be used to carry control signalling between end users. A VPC between end users provides them with an overall capacity; the VCC organization of the VPC is up to the two end users, provided the set of VCCs does not exceed the VPC capacity.

An *end user to network entity connection* is used for user-to-network control signaling. A VPC can be used to aggregate traffic from an end user to a network exchange or network server.

A *network entity to network entity connection* is used for network traffic management and routing functions. A VPC can be used to define a common route for the exchange of network management information.

The UNI (user-network interface) and NNI (network-network interface) are similar, the difference being that the UNI will connect customer equipment which could include broadband terminals, terminal adaptors, and cell-based LAN/MAN equipment as well as ATM switches. The NNI can only connect trunk ports of ATM switches and hence does not need the GFC field in the ATM cell header. It is intended to connect ATM subnetworks or networks and hence the GFC field has been subsumed into the VPI field, allowing 16 times as many virtual paths.

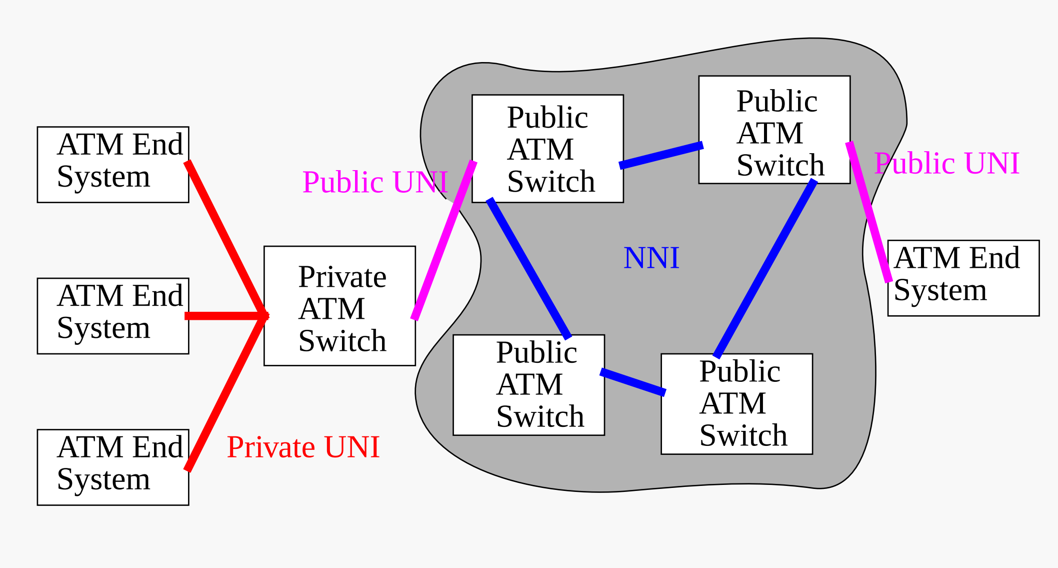


Figure 2 : *The difference between private and public UNI and NNI, from [5]*

The private UNI is used between ATM end systems in the private network and the switch that connects them. Public UNI is used to connect a component from the private network to the public network, see figure 2.

NNI is used between the switches in the public network, and since all flow control offered is the one by UNI, this means that a switch is only responsible for controlling the user data which has its origin in this same switch.

3.3 ATM Connections

ATM connections are characterized as

- *Permanent Virtual Connections* (PVC)
  - Established through an external mechanism, typically a network management station
  - All switches between the sender and the receiver is programmed with the correct values of VCI/VPI.
- *Switched Virtual Connections* (SVC)
  - Established by an application through signalling protocols.
  - Many higher layer protocols are based on the use of SVCs.

and also as

- *Point-to-point*
  - which can be either uni- or bidirectional.
- *Point-to-multipoint*
  - where a root node is connected to multiple leaf nodes
  - cell replication is done by the ATM switch in each branch
  - only unidirectional!

LAN technologies allow multipoint-to-multipoint connections, and support for this in ATM would have simplified LAN-LAN implementations. AAL 5 (ATM Adaptation Layer service protocol 5, described in more detail in subsection 3.5.3.2) which is often used for data communication has no possibility to distinguish between cells that belong to other data packets received on the same logical connection. This means that all the cells have to come in sequence for the packet to be reassembled. AAL 3/4 has this function in its MID (Message Identifier) field, but it is not desirable to use this protocol because it is far more complex than AAL 5.

The solution used in the ATM Forum’s LAN Emulation specification is a multicast server where you have uni-directional, point-to-point connections to the server, and the server has uni-directional point-to-multipoint connections out to everybody else.

3.3.1 Virtual Channels (VC) and Virtual Paths (VP)

ATM is connection-oriented and demands a virtual connection to be established by the use of management and automated call procedures. All traffic belonging to the same virtual connection is switched the same way through the net. ATM connections are of two types: Virtual Paths, and Virtual Channels.

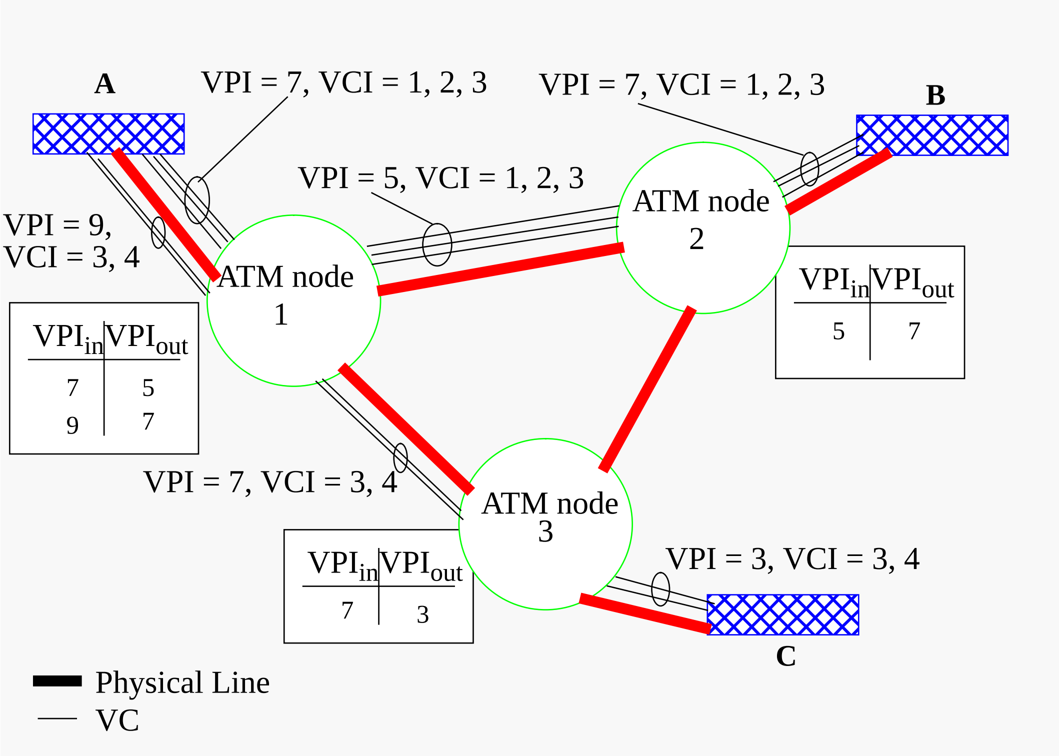


Figure 3 : *The relationship between VCs, VPs, and the physical line, from [5].*

Virtual channels (VC) are unidirectional logical ATM connections with some reserved resources. Virtual channel connections (VCCs) are the basic unit for switching in an ATM network. A Virtual Path (VP) is a number of virtual channels that have the same endpoints (see figure 3), and is considered as one unit for unidirectional traffic [5]. Thus, all the cells flowing over all the VCCs in a single VPC are switched together. Virtual paths are identified through the Virtual Path Identifier, and Virtual Channels through the combination Virtual Path Identifier/Virtual Channel Identifier.

The virtual-path technique helps contain the control cost by grouping connections that share common paths through the network into a single unit, see figure 4.

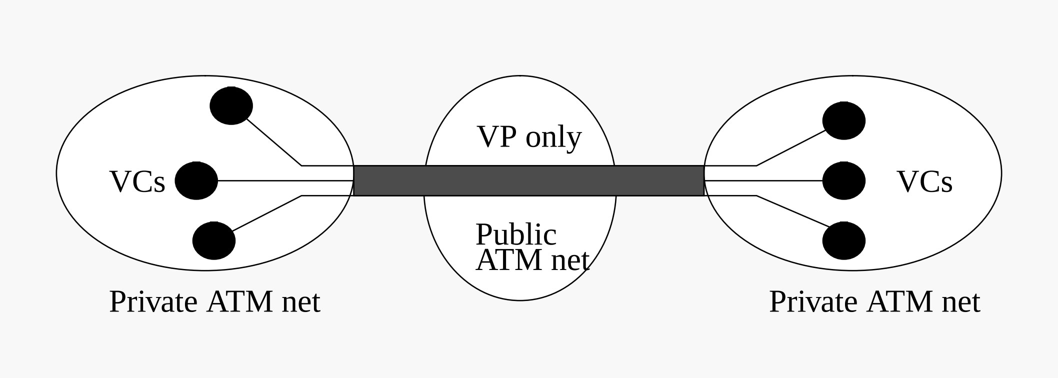


Figure 4 : *How private and public networks relate to VPs and VCs, from [5].*

The process of setting up a virtual path connection is decoupled from the process of setting up an individual virtual channel connection [1]:

- The virtual path control mechanisms include calculating routes, allocating capacity, and storing connection state information.
- To set up a virtual channel, there must first be a virtual path connection to the required destination node with sufficient available capacity to support the virtual channel, and with the appropriate quality of service. A virtual channel is set up by storing the required state information (virtual channel/virtual path mapping).

Once a VPC is set up, it is possible for the end users to negotiate the creation of new VCCs.

Table 1: A summary VP/VC terminology [1]

Virtual Channel	VC	A generic term used to describe a unidirectional transport of ATM cells associated by a common unique identifier value.
Virtual Channel Link		A means of unidirectional transport of ATM cells between a point where a VCI value is assigned and the point where that value is translated or terminated.
Virtual Channel Identificator	VCI	Identifies a particular VC link for a given VPC.
Virtual Channel Connection	VCC	A concatination of VC links that extends between two points where the adaptation layer is accessed. VCCs are provided for the purpose of user-user, user-network, or network-network information transfer. Call sequence integrity is preserved for cells belonging to the same VCC.
Virtual Path	VP	A generic term used to describe unidirectional transport of ATM cells belonging to virtual channels that are associated by a common unique identifier value.
Virtual Path Link		A group of CV links, identified by a common value of VPI, between a point where a VPI value is assigned and the point where that value is translated or terminated.
Virtual Path Identificator	VPI	Identifies a particular VP link.
Virtual Path Connection	VPC	A concatination of VP links that extends between the point where the VCI values are assigned and the point where those values are translated or removed, i.e., extending the length of a bundle of VC links that share the same VPI. VPCs are provided for the purpose of user-user, user-network, or network-network information transfer.

3.3.2 Switching in ATM

One of the advantages of using ATM, is that the switching is done in hardware since all cells have the same size. The switching function is rather simple in theory (but shows to be more complicated in practice!):

- A cell is received over a link with known VPI/VCI
- The switch finds the outgoing link with the new VPI/VCI by looking up a table
- The cell is then transmitted over the new link

Unlike Ethernet, the switches in ATM networks are involved in the connecting process by creating states and doing ackowledging between switches. If the connection is interrupted in one way or another, other switches have to remove the states. The ATM standard does not specify a routing protocol. The ATM switch works as a VP or a VC switch for each connection, see figure 5.

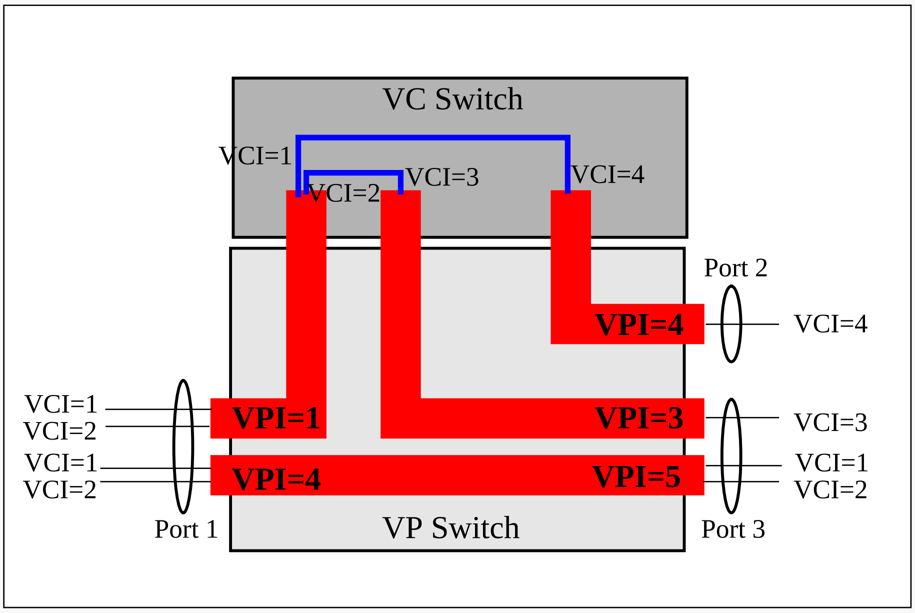


Figure 5 : *A typical VP/VC switch, from [9].*

3.4 Signalling in ATM

Signalling in ATM can be divided into three layers [5]:

- layer 1: signalling between physical hardware devices
- layer 2: interconnection of interworking units
- layer 3: establishment of calls and connections

For B-ISDN, the UNI signalling is located in layer 3. Signalling in ATM spans two different control areas:

- *Connection (Bearer) Control*: procedures to set-up or initialize features of user data connection, e.g., the ATM connection, the process of connecting.
- *Call Control*: procedures for maintaining the connection itself, e.g., associating specific VPIs and VCIs with a calling user, clearing VPI/VCI tables.

Two important tasks exist in any signalling scenario:

- *network-dependent* tasks:
  - set-up, maintenance, and clearance of VCCs and VPCs
  - negotiation of traffic characteristics
- *service-dependent* tasks:
  - independent of any specific network feature
  - not compulsory, but may be integrated
  - definition and support of multicast and multipeer
  - symmetric or asymmetric behavior of connections
  - QoS parameter negotiation

The last point of the network- and service-dependent tasks implies that QoS is related to the network and services through the traffic management concepts Peak Cell Rate (PCR), Minimum Cell Rate (MCR), and Sustainable Cell Rate (SCR), and the QoS Attributes Cell Loss Ration (CLR), Cell Transfer Delay (CTD), Cell Delay Variation (CDV), and Burst Tolerance (BT), all described in more detail in section 3.6.

3.5 The ATM Reference Model

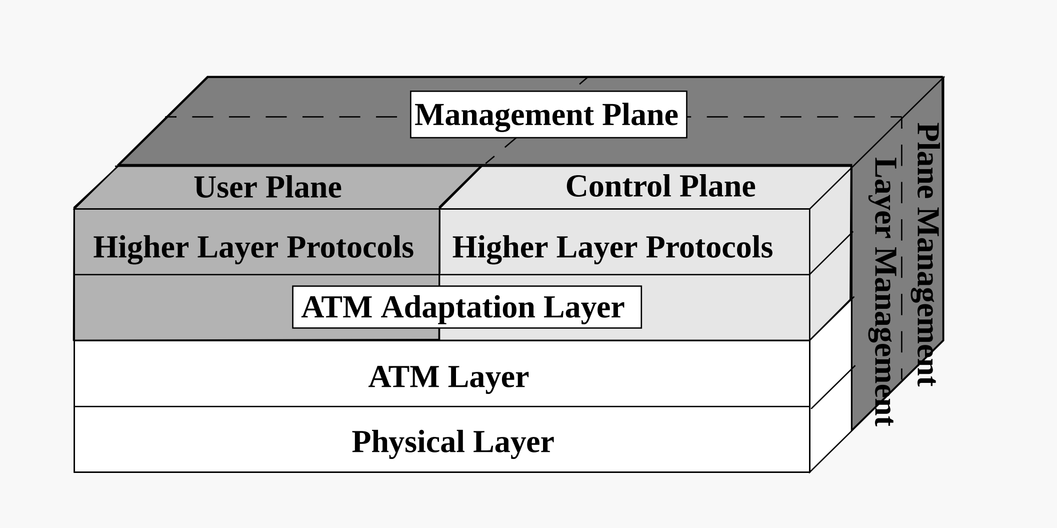


Figure 6 : *The ATM reference model, based on [5], [10],and [12].*

The ATM reference model has layers in two dimensions: horizontal and vertical, as can bee seen in figure 6. The horizontal layers correspond to the conventional network layers from the OSI model, including the physical layer, the ATM layer, the ATM adaptation layer, and other higher levels. The vertical layers function across all the horizontal layers, and are typically concerned with the interaction between the horizontal layers, and include the user plane, the control plane, and the management plane.

The *user plane* is concerned with the transmission of user data, and also provides associated controls like flow control and error control. The *control plane* performs call control and connection control functions. The *management plane* consists of functions used to interact and coordinate activities associalated with the user plane and the control plane**,** and includes *plane management*, which performs management functions related to a system as a whole and provides coordination between the planes, and *layer management*, which performs management functions relating to resources and parameters residing in its protocol entities [1].

3.5.1 Physical Layer

The physical layer controls the sending and receiving of bits over the physical medium. It also keeps track of the boundaries of the ATM cells, e.g., where a cell starts and where it ends. The physical layer is also responsible for plugging cells into the right frame type for the physical medium that is used.

The physical layer consists of two sublayers ([5] and [12]):

- *Physical Medium Sublayer (PM)* which is concerned with the transmission and reception of a continuous flow of bits with synchronize information. The signals are converted into electrical or optical signals suitable for transmission on optical fibre, coaxial cable, or radio links. It only covers the physical medium functions, and specifies for instance SDH/Sonet and FDDI.
- *Transmission Convergence Sublayer (TC)* which limits the cell size, generates and checks the HEC (a 8 bit header error control for correction of single bit errors, and detection of multiple bit errors), and inserts and removes empty ATM cells for transmission speed adaption. This sublayer also does frame generation and recovery, and mapping of cells into lower layer containers.

The B-ISDN (broadband ISDN) specifies that ATM cells are to be transmitted at a rate of 155.52 Mbps or 622.08 Mbps. As with ISDN, there is a need for specifying the transmission structure that will be used to carry this payload. For the 155.52 Mbps interface, two approaches has been defined, a cell based physical layer, and an SDH-based physical layer [1]. In addition, [5] recognizes two other standards for frame adaption: Plesiochronous Digital Hierarchy, and a FDDI option by the ATM forum.

3.5.2 ATM Layer

The ATM layer provides an interface between the AAL and the physical layer. This layer is responsible for relaying cells from the AAL to the physical layer for transmission, and from the physical layer to the AAL for use at the end systems.

The ATM Layer is primarily responsible for the generation of the cell Header and the functions associated with the Header, including the switching and routing of cells, flow control, congestion control, bit error detection in the Header, and cell delineation.

The ATM layer takes as input from higher layers streams of 48-octet cell payloads, performs cell header generation, and passes cells to the TC sublayer such that order is preserved within virtual circuits (VCs).

At the receiving end, it receives as input a stream of cells, for which it performs header extraction and delivers cells, in order, to the appropriate AAL service access point (SAP) using the virtual circuit identifier/virtual path identifier (VCI/VPI) values as identifiers.

At switching elements, the ATM layer uses the VCI/VPI to route the cells. The VPI and VCI values may change at each switching element, and the ATM layer does this translation. Interpretation of the values in the payload type (PT) and cell-loss priority (CLP) fields is done at the ATM layer in switching elements ([12]).

In other words, the ATM layer establishes the connection through the ATM network, and switches the ATM cells through the nodes based on VPI/VCI values.

The Physical Layer and the ATM Layer, taken together, provides the facilities for the connection-oriented transport of cells. These two protocol layers must be present in every ATM device, including end-user hosts and broadband switching systems, as shown in figure 7 below. The header of the ATM cells defines the functionality of the ATM layer since it can have two forms, UNI or NNI (see subsection 3.2.1).

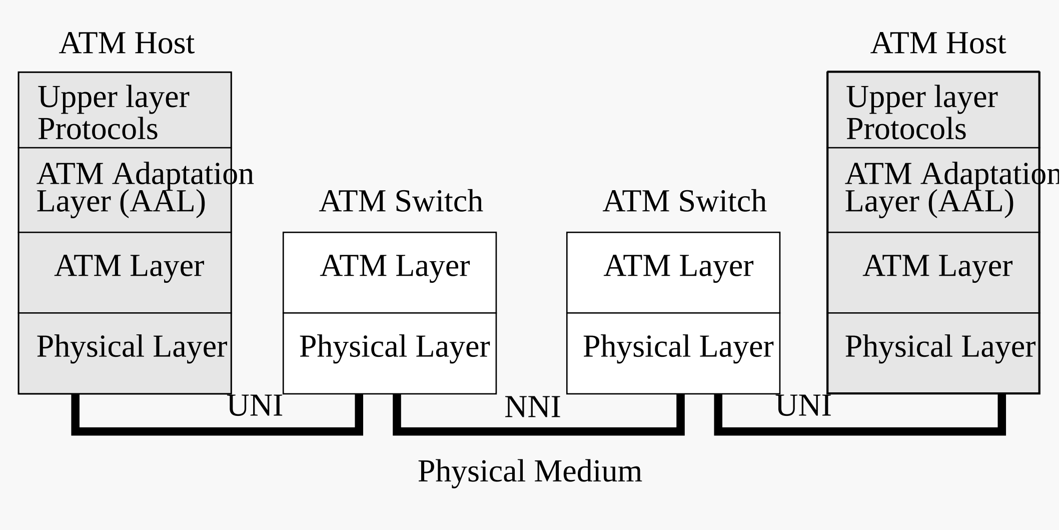


Figure 7 : *The protocol stack, and relationship between UNI and NNI, based on [5] and [11]).*

3.5.3 ATM Adaptation Layer

The main task of the ATM adaptation layer is to enhance the service of the ATM layer to the requirements of a specific service. This includes mapping of user/control/management PDUs (Protocol Data Units) into ATM cell payloads and vice versa.

When adapting the traffic from higher level protocols to the cell format, the ATM adaptation layer segments the traffic into 48 byte parts. All adaption between the different services and transmission is done in the adaptation layer. The ATM Adaptation Layer (AAL) is divided logically in two sublayers ([1] and [5]):

- *Convergence Sublayer (CS)* This sublayer contains different functions according to the AAL type of transmission protocol that is used. It offers functions which is needed to support special applications using the AAL. Each user connects to the AAL layer through a service access point (SAP) - typically the address to the application. This makes the layer service dependent.

- *Segmentation and Reassembly Sublayer (SAR)* This sublayer is responsible for packing information received from CS in cells for transmission, and to unpack the information at the other end. SAR must pack any SAR headers and trailers, plus CS information, into 48-octets since the ATM cell payload is of that size.

The use of ATM creates a need for an adaptation layer to support information transmission protocols not based on ATM. Two examples are the PCM (Pulse Code Modulation) voice and LAPF (Link Access Procedure for Frame mode bearer services). PCM voice is an application which produces a flow of bits from a voice signal, and LAPF ia a standard data link control protocol for frame relay [1].

Services offered by the AAL is typically [1]:

- Handling of transmission errors
- Segmentation and reassembling (to allow bigger data blocks to be contained in the information field of the ATM cells)
- Handling of lost and misinserted cell conditions.
- Flow control and timing control.
- Correction of single bit errors in payload
- Notification of lost cells or misordered cells

In order to minimize the number of different AAL protocols that must be specified to meet a variety of needs, CCITT defined four classes of service that cover a broad range of requirements.

3.5.3.1 ATM Adaptation Layer Service Classes

The classification is based on whether a timing relationship must be maintained between source and destination, whether the application requires a constant bit rate, and whether the transfer is connection-oriented or connectionless [1]. Originally the different types of traffic and transmission services supported by ATM were divided into four classes [10]:

- **Class A** demands (ex: circuit emulation):
  - a *timing relation* between the source and destination node
  - a *constant* bit rate
  - a connection-*oriented* transmission service
- **Class B** demands (ex: variable-bit-rate video, or video conferencing):
  - a *timing relation* between the source and destination node
  - a *variable* bit rate
  - a connection-*oriented* transmission service
- **Class C** demands (ex: data-transfer applications):
  - no timing relation between the source and destination node
  - a *variable* bit rate
  - a connection-*oriented* transmission service

- **Class D** demands (ex: data-transfer applications):
  - no timing relation between the source and destination node
  - a *variable* bit rate
  - a connection-*less* transmission service

These service classes have now been abandoned, but four types of service protocols for the ATM adaptation layer has been recommended by the CCITT based on these original service classes.

3.5.3.2 ATM Adaptation Layer Service Protocols

Initially, CCITT (now ITU-T) defined one protocol type for each class of service, named Type 1 through Type 4. Actually each protocol type consists of two protocols, one at the CS sublayer and one at the SAR sublayer. More recently, types 3 and 4 were merged into a Type 3/4, and a new type, Type 5, was defined [1].

- **AAL 1** corresponds to the service class A and are designed to transport CBR (constant bit rate) data streams in such a way that clock information can be recovered at the receiving end [12]. Examples of use are the telephone and uncompressed video. The payload consists of sampled, synchronous data. SN (sequence number) and SNP (sequence number protection) confirms that the receiver has received the packages in the right order. This protocol demands a medium which can transfer clocking.

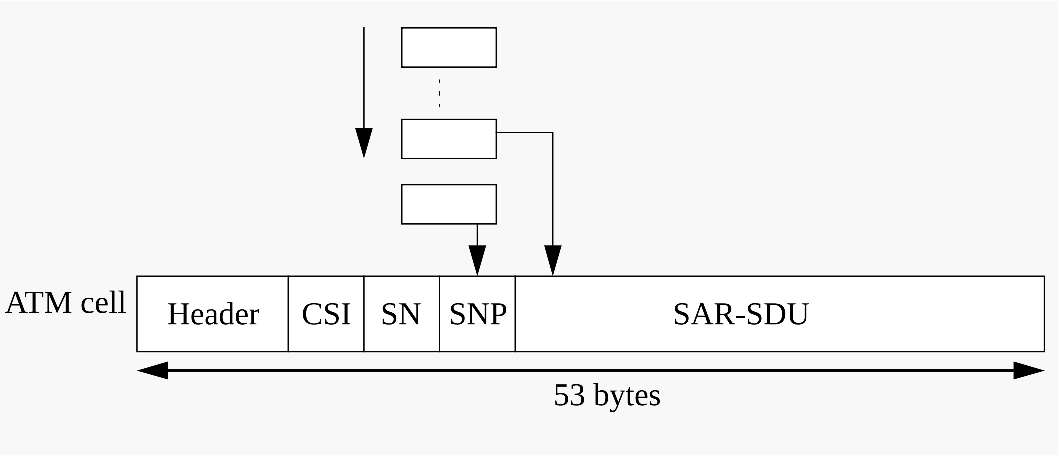


Figure 8 : An ATM cell according to the AAL 1 protocol, based on [5] and [9]. CSI (1 bit): CS indicator, SN (3 bits): Sequence number, SNP (4 bits): Sequence number protection, SDU: Service data unit.

- **AAL 2** corresponds to the service class B and was intended to transport VBR (variable bit rate) data streams in the same way as AAL 1, but is not yet defined!
- **AAL 3/4** corresponds to the service classes C and D, respectively, and was designed to carry VBR streams without explicit timing information. AAL 3 is connection-oriented, and AAL 4 is connection-less, although it is unclear what meaning this distinction actually has in ATM, and usually these two are lumped together [12].This protocol is meant for the transfer of SMDS (switched multimegabit data service) packages over an ATM network. Each SAR PDU is given a header which will preserve the order of the cells at reassembling, and also will be able to separate different broadcast sources.

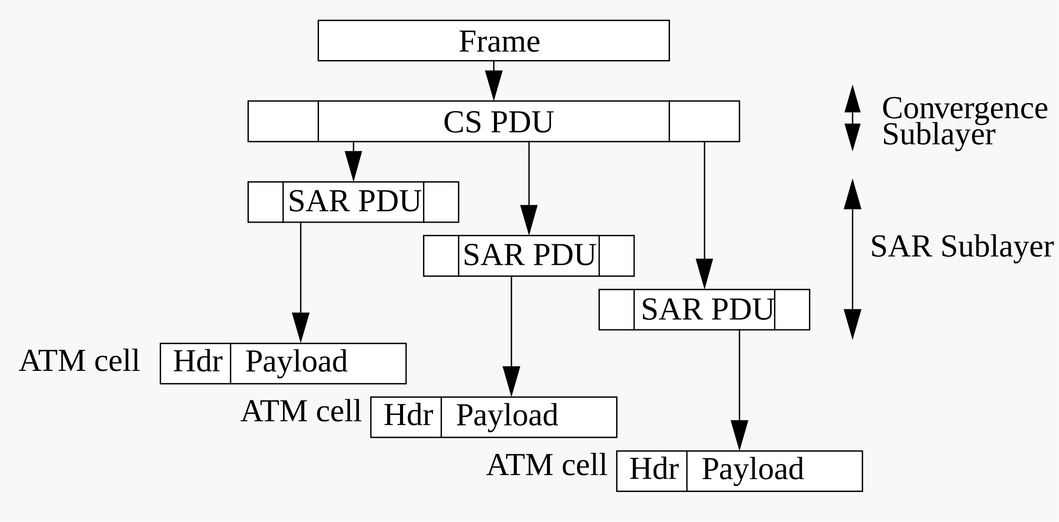


Figure 9 : *The ATM cell according to the AAL 3/4 protocol, from [9].*

- **AAL 5 or SEAL (Simple and Effective Adaptation Layer)** corresponds to the service class C (no timing, VBR, and connection-oriented), and was developed in response to a perception that AAL 3/4 was ineffective [12]. This protocol is used for non-SMDS data transfers. The CS layer adds padding bits to make the PDU to fit into n*48 bytes, and also a trailer with a crc-32 field in addition to the original frame length. SAR splits the frame into 48 byte blocks, and for all cells except the last one, one bit in the PT (payload type) field is set to 0. This protocol was introduced to provide a streamlined transport facility for higher-layer protocols that are connection-oriented, and has become (especially for ATM LAN applications) the most popular protocol.

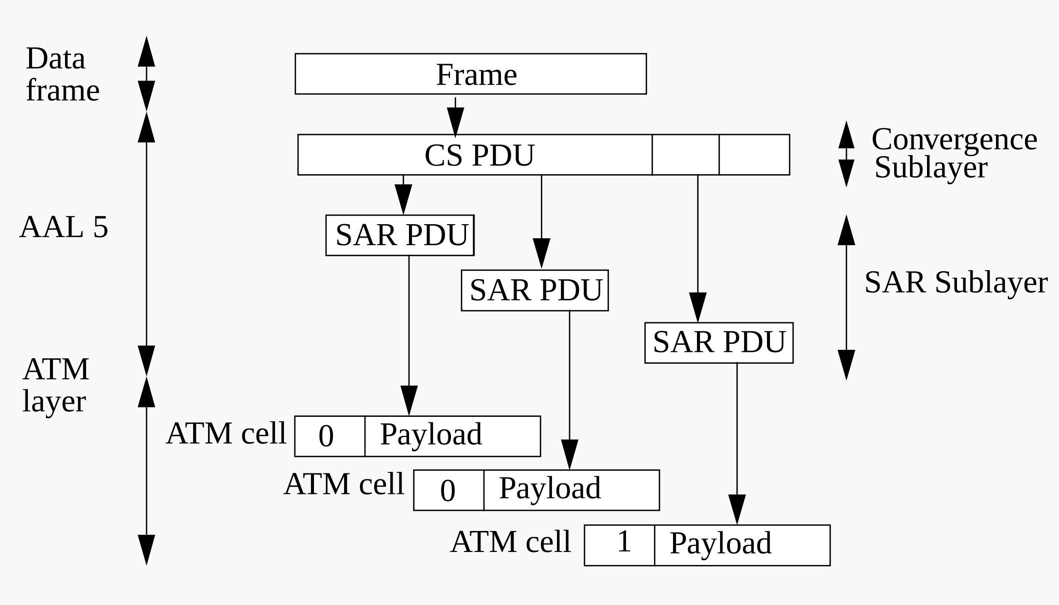


Figure 10 : *The ATM cell according to the AAL 5 protocol, from [9].*

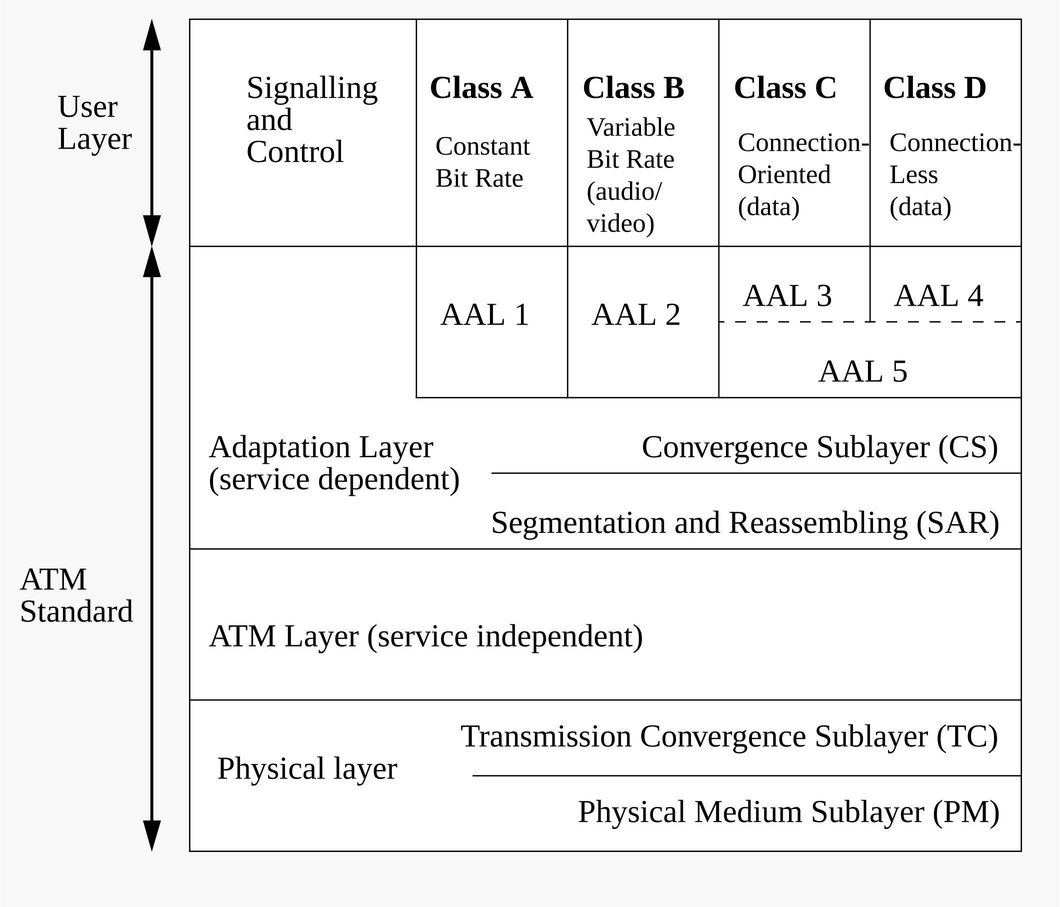

User Layer
Signalling and Control
Class A
Constant Bit Rate
Class B
Variable Bit Rate (audio/ video)
Class C
Connection-Oriented (data)
Class D
Connection-Less (data)
AAL 1
AAL 2
AAL 3
AAL 4
AAL 5
Adaptation Layer (service dependent)
Convergence Sublayer (CS)
Segmentation and Reassembling (SAR)
ATM Standard
ATM Layer (service independent)
Physical layer
Transmission Convergence Sublayer (TC)
Physical Medium Sublayer (PM)

Figure 11 : *Another version of the ATM reference model, based on [9].*

A revised version of the ATM reference model with the AAL service classes and service protocols put into place is shown i figure 11. Service class A represents the constant bit rate traffic property, and classes B, C, and D represent different aspects of the variable bit rate traffic property.

Controlling that the communication channels comply with the service classes is no function specified within the ATM protocol stack. This function is offered by the switches under Call Admission Control (CAC) and Conformance Monitoring (CM).

3.6 QoS and Traffic Management

ATM technology is intended to support a wide variety of services and applications, and a primary role of traffic management is to protect the network and the end-system from congestion. An additional role is to promote an efficient use of network resources. The control of ATM network traffic is fundamentally related to the ability of the network to provide appropriately differentiated Quality of Service (QoS) for network applications.

In the following procedures and parameters related to Traffic Management and Quality of Service (QoS) will be described according to The ATM Forum Technical Committee’s “Traffic Management Specification, Version 4.0, April 1996 [16].

3.6.1 ATM Service Categories

The ATM Layer consists of five categories of service which relate traffic characteristics and QoS requirements to network behavior, in a combination suitable for a given set of applications [17].

Service categories are distinguished as being either real-time or non-real-time. For real-time there are two categories, CBR (constant bit rate) and rt-VBR (real-time variable bit rate), distinguished by whether the traffic descriptor contains only the Peak Cell Rate (PCR) or both PCR and Sustainable Cell Rate (SCR) parameters (see subsection 3.6.3 for a description of the parameters). The three non-real-time service categories are nrt-VBR (non-real-time variable bit rate), UBR (unspecified bit rate), and ABR (available bit rate). All service categories apply to both VCCs and VPCs.

Constant Bit Rate (CBR)

The Constant Bit Rate service category is used for emulating circuit switching where the bit rate is constant. This is typically a connection that requests a static amount of bandwidth available during the total lifetime of the connection. This amount of bandwidth is characterized by a Peak Cell Rate (PCR) value.

Once the connection is established, the negotiated ATM layer QoS is assured to all cells conforming to the relevant conformance tests. The CBR service is intended to support real-time applications requiring tightly constrained delay variation (voice, video, circuit emulation), but is not restricted to these applications.

Variable Bit Rate (VBR)

The variable bit rate service category allows the users to send data with variable bit rate, and can be divided into two parts, one for real-time VBR, and one for non-real-time VBR.

The real-time VBR service category (rt-VBR) is intended for real-time applications that are time-sensitive (i.e., those applications that require tightly constrained delay and delay variation), as is the case for voice and video applications. Real-time VBR connections are characterized in terms of a Peak Cell Rate (PCR), Sustainable Cell Rate (SCR), and Maximum Burst Size (MBS). Real-time VBR service may support statistical multiplexing of real-time sources.

The non-real-time VBR service category (nrt-VBR) is intended for non-real-time applications which have bursty traffic characteristics, and which are characterized in terms of a PCR, SCR, and MBS. Non-real-time VBR service may also support statistical multiplexing of connections.

Available Bit Rate (ABR)

ABR is an ATM layer service category for which the limiting ATM layer transfer characteristics provided by the network may change after the connection has been established. The ABR service category is intended for sources having the ability to reduce or increase their information rate if the network requires them to do so. A flow control mechanism is specified which supports several types of feedback (in terms of Resource Management Cells, or RM-cells) to control the source rate in response to changing ATM layer transfer characteristics.

On the establishment of an ABR connection, the end-system specifies to the network both a maximum required bandwidth and a minimum usable bandwidth. These are designated as peak cell rate (PCR) and minimum cell rate (MCR), respectively.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) service category is a “best effort” service intended for non-critical applications, i.e., those that do not require tightly constrained delay and delay variation. Such applications will typically be traditional computer communications applications like file transfer and email. The UBR service does not specify traffic related service guarantees, and the service is indicated by use of the Best Effort Indicator in the ATM User Cell Rate Information Element.

,

Attribute	ATM Layer Service Category				
	CBR	rt-VBR	nrt-VBR	UBR	ABR
Traffic Parameters:					
PCR and CDVT	specified			specified[2]	specified[3]
SCR, MBS, CDVT	n/a	specified		n/a	
MCR[4]	n/a			n/a	specified
QoS Parameters:					
peak-to-peak CDV	specified		unspecified		
maxCTD	specified		unspecified		
CLR[4]	specified			unspecified	See note 1
Other Attributes:					
Feedback	unspecified				specified

Figure 12 : *ATM Service category Parameters and Attributes, based on [10], [11] and [16].*

Notes:

1. CLR is low for sources that adjust cell flow in response to control information. Whether a quantitative value for CLR is specified is network specific.
2. May not be subject to CAC (connection admission control) and UPC (usage parameter control) procedures.
3. Represents the maximum rate at which the ABR source may ever send. The actual rate is subject the control information.
4. These parameters are either explicitly or implicitly specified for PVCs (permanent VCs) or SVCs (switched VCs).
5. CDVT refers to the Cell Delay Variation Tolerance. CDVT is not signaled. In general, CDVT need not have a unique value for a connection. Different values may apply at each interface along the path of a connection.

The three non-real-time service categories nrt-VBR, UBR, and ABR differ as to the nature of the service guarantees provided by the network, and the mechanisms which are implemented in the end-systems and networks to realize them.

The nrt-VBR service category provides commitments for a cell loss ratio for those connections which remain within the traffic contract negotiated with the network at the time the connection is established The UBR service category offers no traffic related service commitments, and the ABR service category provides a low cell loss ratio for those connections whose end-station obey a specific reference behavior.

3.6.2 QoS Parameters

The ATM Layer Quality of Service (QoS) is measured by a set of parameters characterizing the performance of an ATM layer connection. Six QoS parameters are, according to [16], identified with correspondence to network performance objectives. Three of these may be negotiated between the end-systems and the networks [17]:

- *Peak-to-peak Cell Delay Variation* (peak-to-peak CDV): This is a QoS delay parameter associated with CBR and VBR services.
- *Maximum Cell Transfer Delay* (maxCTD): This is defined as the max elapsed time between a cell exit event at the measurement point 1, and the corresponding cell entry event at the measurement point 2 for a particular connection.
- *Cell Loss Ratio (CLR)*: The ratio of lost cells in relation to the total number of cells sent during a transmission.

The following parameters are not negotiated:

- *Cell Error Ratio* (CER): The ratio of errored cells in a transmission, in relation to the total cells sent in a transmission.
- *Cell Misinsertion Rate* (CMR): The ratio of cells received at an endpoint not originally transmitted by the source end, in relation to the total number of cells properly transmitted.
- *Severely Errored Cell Block Ratio* (SECBR)

3.6.3 Traffic Contract

A traffic contract specifies the negotiated characteristics of a VP/VC connection at an ATM UNI. The traffic contract at the Public UNI shall consist of a connection traffic descriptor and a set of QoS parameters for each direction of the connection.

The connection traffic descriptor specifies the traffic characteristics of the ATM connection. It includes the source traffic descriptor, the CDVT(cell delay variation tolerance), and the conformance definition. The source traffic descriptor is the set of traffic parameters which describes an inherent characteristic of the ATM source. The traffic parameter may be quantitative or qualitative, and includes

- *PeakCell Rate (PCR):* The maximum instantaneous rate for the transmission of user data (maximum cell rate).
- *Sustainable Cell Rate (SCR):* The average cell rate measured over a long time (continuous average cell rate).
- *Maximum Burst Size (MBS):* The burst tolerance (BT) is conveyed through this parameter, coded as a number of cells.

- *Minimum Cell Rate (MCR):* The minimum cell rate wanted by a user, or the rate at which the source is always allowed to send.

Traffic contract parameters and related algorithms:

Cell Delay Variation Tolerance (CDVT) for PCR and SCR. ATM layer functions may alter the traffic characteristics of connections by introducing Cell Delay Variation. When cells from two or more connections are multiplexed, cells of a given connection may be delayed whilst cells of another connection are being inserted at the output of the multiplexer.

Generic Cell Rate Algorithm (GCRA). The GCRA is used to define conformance with respect to the traffic contract. For each cell arrival, the GCRA determines whether the cell conforms to the traffic contract of the connection.

3.6.4 Functions and Procedures for Traffic Management

The traffic of an ATM connection is assumed not to comply with its agreement with the network, and it therefore has to be checked, a process called policing. This is done through the use of functions described below. Shaping is what is done to adapt the traffic to the agreement that is negotiated before it is sent out.

Functions referred to as congestion control functions are intended to react to network congestion in order to minimize its intensity, spread and duration. ATM networks can implement one or a combination of the following traffic and congestion functions in order to meet QoS objectives of connections.

Connection Admission Control

The Connection Admission Control (CAC) function is defined as the set of actions taken by the network at set-up of a connection or by Network Management during permanent virtual connection establishment in order to determine whether a connection can be progressed or should be rejected. The information in the traffic contract needs to be accessible to the CAC function.

Usage Parameter Control (Policing)

Usage Parameter Control (UPC) is defined as the set of actions taken by the network to monitor and control traffic. Its main purpose is to protect network resources from malicious as well as unintentional misbehavior which can affect the QoS of other already established connections. This is done by detecting violations of negotiated parameters and taking the appropriate actions. Actions of the UPC may include: cell passing, cell tagging, or cell discarding.

Connection monitoring at a UNI (private or public) is referred to as UPC. Connection monitoring at an NNI (private or public) is referred to as NPC. UPC is used as a more generic term unless otherwise specified.

Selective Cell Discarding

A congested network element may selectively discard cells which meet either or both of the following conditions:

1. cells which belong to a non-compliant ATM connection
2. cells which have CLP=1

This is to protect the CLP=0 flow as much as possible.

Traffic Shaping

Traffic shaping is a mechanism that alters the traffic characteristics of a stream of cells on a connection to achieve better network efficiency whilst meeting the QoS objectives. It is required that traffic shaping maintains the cell sequence integrity on a connection. Examples of traffic shaping are peak cell rate reduction, burst length limiting, reduction of CDV, and cell scheduling policy.

Explicit Forward Congestion Indication

A network element in an impending congested state or a congested state may set an Explicit Forward Congestion Indication (EFCI) in the cell header so that this indication may be examined by the destination end-system. An impending congested state is the state when a network element is operating around its engineered capacity level. The mechanism by which a network element determines whether it is in an impending-congested or a congested state is implementation specific.

Resource Management using Virtual Paths

Virtual paths are an important component of traffic control and resource management in ATM networks. With no relation to traffic control, VPCs can be used to:

- simplify CAC
- implement a form of priority control by segregating groups of virtual connections according to service category
- efficiently distribute messages for the operation of traffic control schemes
- aggregate user-to-user services such that the UPC can be applied to the traffic aggregate.

VPCs also play a key role in resource management. 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.

Frame Discard

If a network element needs to discard cells, it is in may cases more effective to discard at the frame level rather than at the cell level. The term “frame” means the AAL protocol data unit. The network detects the frame boundaries by examining the Service Data Unit (SDU) type in the payload type field of the ATM cell header. Frame discard may be used whenever it is possible to delineate frame boundaries by examining the SDU type in the payload type field of the ATM cell header.

ABR Flow Control

In the ABR service, the source adapts its rate to changing network conditions. Information about the state of the network like bandwidth availability, state of congestion, and impending congestion, in conveyed to the source through special control cells called Resource Management Cells (RM-cells).

3.7 Using ATM

The huge legacy of existing LAN applications needs to be readily migrated to the ATM environment before ATM fulfills its promise as a cost-effective technology for supporting future broadband multimedia services.

Various approaches have been tried out, one of them is to consider ATM as a link layer and modify the existing network layer protocols to this new technology, like IP over ATM, see subsection 3.7.2. Another approach proposed to support existing LAN applications in ATM networks is the provision of an ATM protocol to emulate existing LAN services, allowing network layer protocols to operate as if they are still connected to a conventional LAN. This approach is named LAN Emulation.

3.7.1 LAN Emulation

The LAN emulation specification defines how an ATM network can emulate a sufficient set of the medium access control (MAC) services of existing LAN technology, so that higher layer protocols can be used without modification.

Such a LAN emulation service can provide a huge cost benefit since it does not require the ATM users to change their network operating software. The drawback of the approach is that it prevents higher layer applications from accessing ATMs unique services.

LAN emulation service would be implemented as device drivers below the network layer in ATM-to-legacy LAN bridges and ATM end systems. In an ATM end system adapter, LAN emulation device drivers would interface with widely accepted driver specifications, such as Network Driver Interface Specifications (NDIS) and Open Datalink Interface (ODI) used by TCP/IP and IPX. The protocol layers for LAN emulation is illustrated in figure 13.

The LAN emulation service also needs to provide a capability similar to the “best-effort” service which existing LANs mainly supports. This capability is currently supported by the “available bit rate” (ABR) service.

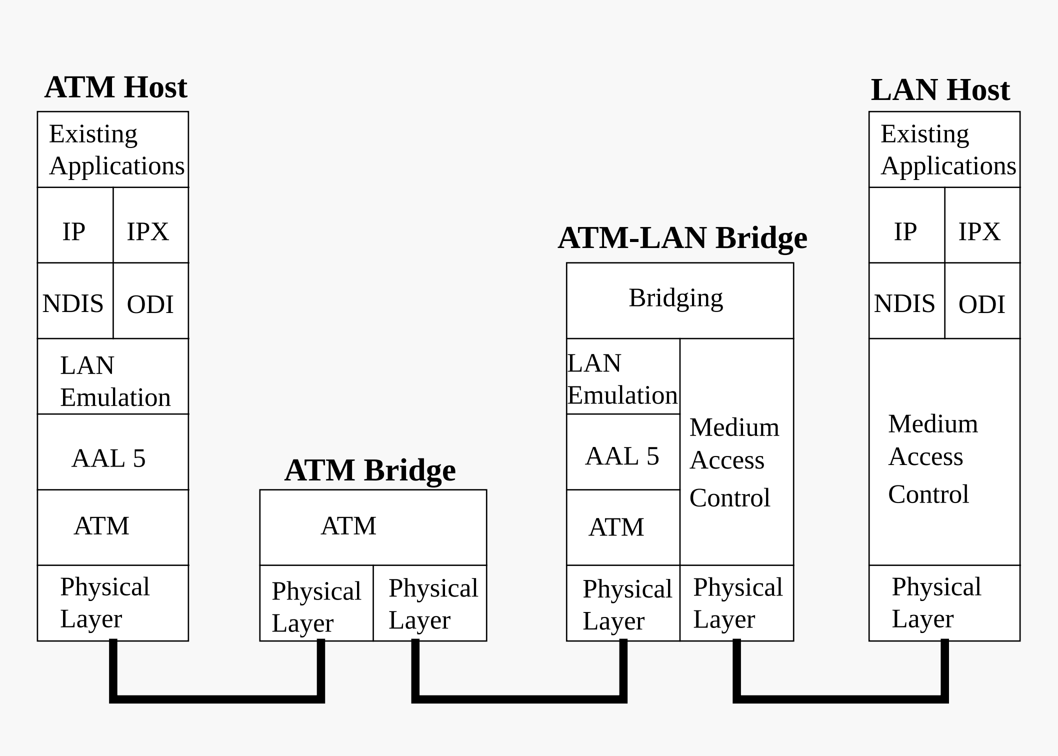


Figure 13 : *Protocol layers for LAN emulation, based on [10].*

- NDIS: Network Driver Interface
- ODI: Open Datalink Interface

LAN emulation uses a multicast server to emulate LAN technology (LAN has possibilities for multi-point to multi-point connections) where the connections to the server is point-to-point and from the server to all other nodes, the connection is point-to multi-point.

3.7.2 IP over ATM

When running IP over ATM, ATM is used as a new link layer protocol. Existing network layer protocols have to be modified to adapt to this new link layer technology. The figure below (14) shows a simplified OSI representation of an internetworking system. IP will here correspond to the network layer and part of the link layer, with the transport layer containing protocols such as TCP and UDP. In this environment the ATM layer is considered to be a form of physical layer, with ATM Adaptation Layers (AALs) providing the equivalent of Link Layer services. Two ATM Adaptation Layers - AAL3/4 and AAL5 - have been defined for packet protocols such as IP. The dashed arrows show the virtual peer-peer communication, and the solid line the actual communication path [15].

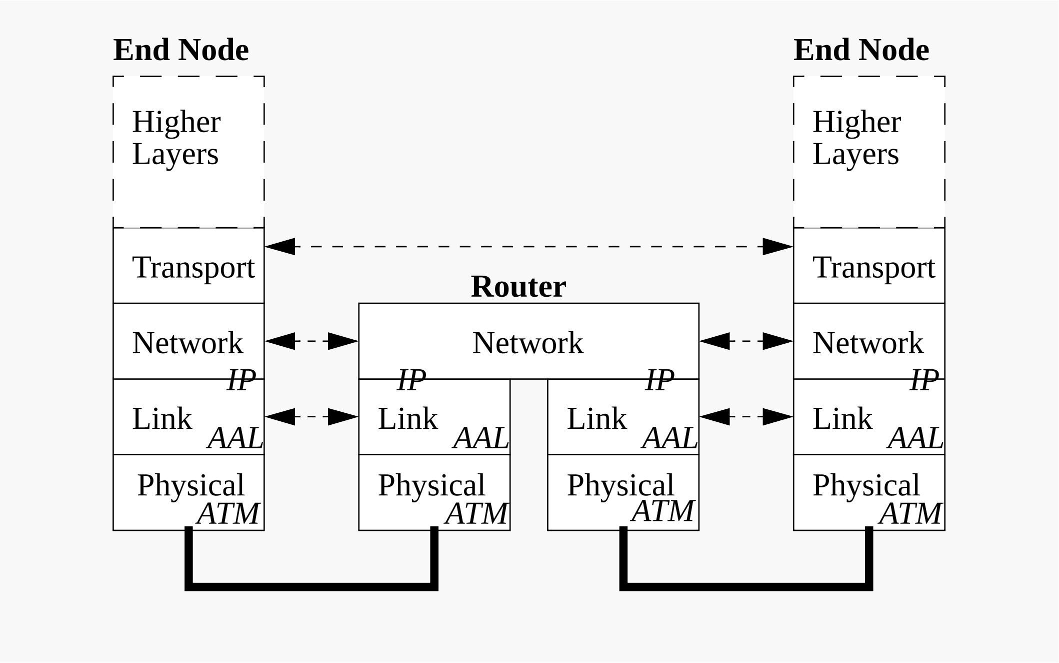


Figure 14 : *Protocol stack for IP over ATM, based on [10], [11] and [15].*

3.7.3 Raw ATM

Raw ATM applications is run directly on top of the ATM protocol stack. This is not very compatible with existing networks in that ATM differs quite a lot in its basics from existing network technology. The approach is not used very much, and few applications exist.

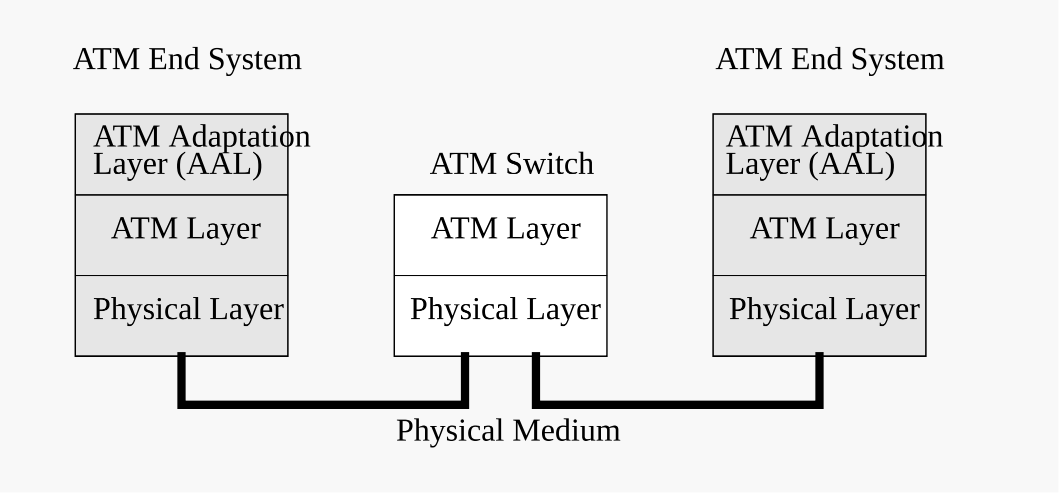


Figure 15 : *The ATM protocol Structure, from [10].*

3.8 ATM and Mobility

There are several problems concerning mobility when it comes to ATM [8].

ATM is connection oriented which basically does not comply with mobility. Connections are lightweight but signalling is potentially very slow.

ATM also makes assumptions about the cell-loss and mis-insertion rate, and it is not easy to meet these assumptions in a wireless environment.

ATM addresses have a number of hierarchical layers which are used to route a signalling request to the destination. Mobility implies that the name to address binding for ATM must be dynamic enough to support re-assignment of addresses.

The packet transmission overhead is also very likely to be higher in a wireless network than in a wired one.

3.9 ATM and Multimedia

Multimedia system designers should adopt an end-to-end approach to meet applications level QoS requirements. Many current network architectures address quality of service from a providers point of view and analyze network performance, failing to comprehensively address the quality needs of applications. A generalized QoS framework based on five design principles (integration, separation, asynchronous resource management and performance) is proposed in [6].

The underlying assumption that the technology capable of carrying a voice call is sufficient to carry multimedia traffic has been proved wrong - data traffic encounters congestion and video traffic suffers delay jitter and very poor real-time image quality due to the high levels of compression required. In order to generate more revenue from their considerable investment in infrastructure, telecommunications companies developed a cost-effective means for computer data and video streams to be mixed with the existing voice traffic and not interfere with each other.

ATM was developed as the core technology to provide this ability, and is a result of a compromise designed to handle voice, video, and data traffic. The capability of ATM to deliver guaranteed high-bandwidth with low latency and jitter makes it ideal for combining voice, video and data traffic in a single, scalable infrastructure for multimedia applications [13].

References

[1] William Stallings: Data and Computer Communications, Prentice Hall, 1997

[2] Fred Halsall: Data Communications, Computer Networks, and Open Systems, Addison-Wesley, 1992

[3] Allyn Romanow & Sally Floyd: Dynamics of TCP Traffic over ATM Networks

[4] Professor Jim Kurose at the Department of Computer Science, University of Massachusetts: Socket Programming Course (http:// www-ami.cs.umass.edu/ cs653/)

[5] Thomas Plagemann: Protocols for Multimedia Communications, course at UNIK, fall 1997 (http://www.unik.no/ pmc/)

[6] Campbell, Aurrecoechea & Hauw: A Review of QoS Architectures,

[7] ATM in detail, K-NET, updated 1995

[8] Håkan Mitts: Architectures for wireless ATM, 1996

[9] Lars Krogh: Tjenesteklasser i ATM, ATM Brukerforum 1/9-97

[10] Siu & Jain: A Brief Overview of ATM: Protocol Layers, LAN Emulation, and Traffic Management,

[11] Kessler: An Overview of ATM technology, Stacks, May 1995

[12] Williams: ATM - What Does it Mean?, NWS'93 Networkshop, December 1993.

[13] ATM and Multimedia, Multi Media Magazine, July 1996

[14] The ATM Forum, http://www.atmforum.com/

[15] G. J. Armitage & K. M. Adams: How Inefficient is IP over ATM anyway?, IEEE Network: 5/1994

[16] The ATM Forum Technical Committee: Traffic Management Specification, Version 4.0, April 1996

[17] ATM Forum White Papers, Livio Lambarelli: ATM Service categories: The Benefits to the User

4 ISPN and RSVP

Traditionally traffic on the Internet can be characterized as follows. A single best-effort service class, with transfer of pure data traffic in applications such as email, ftp, telnet and web. Such applications are often called *elastic*.

Tomorrow, and to some extent even today, this will no longer be true. Multicasting and real-time continuous multimedia traffic, consisting of text, graphics, images, video, audio will be the norm. New applications will then be either *rigid* or *adaptive.*

This is the main reason why there is a need for a new Internet model with new service classes such as guaranteed and predictive service, in addition to architecture and protocols to support this. The Integrated Service Packet Network (ISPN) is the IETF proposed way of realising this in a packet based network architecture like the Internet. However, it should be stated that not everybody is of the opinion that this is the way to go forward

In this chapter ISPN is first described in section 4.1, and in particular the service classes, reference model and traffic control are presented. Then, in section 4.2, the chapter focuses on another important aspect of the next generation Internet, reservation protocols. In particular Resource Reservation Protocol (RSVP), which has gained considerable interest, is presented.

4.1 Integrated Service Packet Network (ISPN)

Growing demands for multimedia real-time traffic on the Internet have led to the need for an extension of today's Internet model. The IntServ working group of the IETF has developed ISPN [1], which defines:

- An extended service model, including two new service classes, guaranteed and controlled load, in addition to best-effort
- A reference implementation model for network, router and host, to realize the extended service model

These models and corresponding concepts will be explained in this section.

However, there are critics, which believe that this is not the right direction, and that resource guarantees are unnecessary in the first place. The main arguments raised against are:

- Bandwidth will be infinite, with future fiber optics
- Simple priority is sufficient for real-time traffic preferences
- Applications can adapt to changing network conditions

Also, an alternative approach suggested is to establish a separate network for real-time traffic.

Still, there is a lot of activicy and interest in research communities, and among computer vendors for the ISPN approach.

4.1.1 Service classes in ISPN

The following service classes are defined:

Guaranteed service [10]

This service provides a deterministic upper bound for maximum packet delay, based on worst case asssumptions of token bucket traffic filter and weighted fair queuing (WFQ) in the router. The reservation parameters are delay and bandwidth. Guaranteed service is suitable for *rigid* applications, which can not tolerate any packet loss at all.

Controlled load service [13]

This service provides a better utilization of the network than guaranteed service, as shown in figure 1 below. However, it is more advanced, as the bound for packet delay should be as low as possible, but simultaneously with a behaviour as stable as possible. The behaviour of this service approximates that of a lightly loaded network, even as congestion occurs. Controlled load service is suitable for *adaptive* applications.

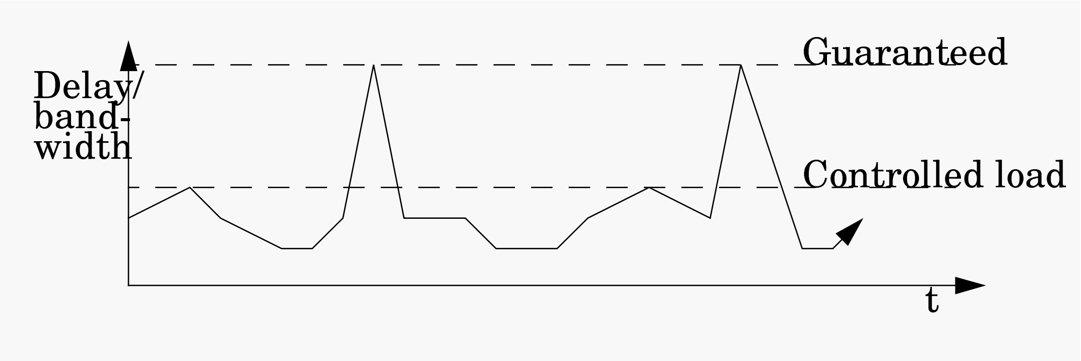


Figure 1 : *Difference between guaranteed and controlled load service*

Predictive service [6]

This service provides a statistical bound for packet delay. However, it has not been standardized by the IETF.

Best-effort service

This is the traditional Internet service, where all packets are treated equal. Best-effort service is suitable for *elastic* applications.

4.1.2 Service and reference model in ISPN

The extended service model for network architecture in ISPN is based on the existence of the following necessary components [15]:

- Flow specification
- Routing (also of multicast packets)
- Resource reservation
- Admission control
- Packet scheduling

A corresponding ISPN reference implementation model for a router is illustrated in figure 2. The model for a host is quite similar, with the addition of applications, and exclusion of a routing process [2].

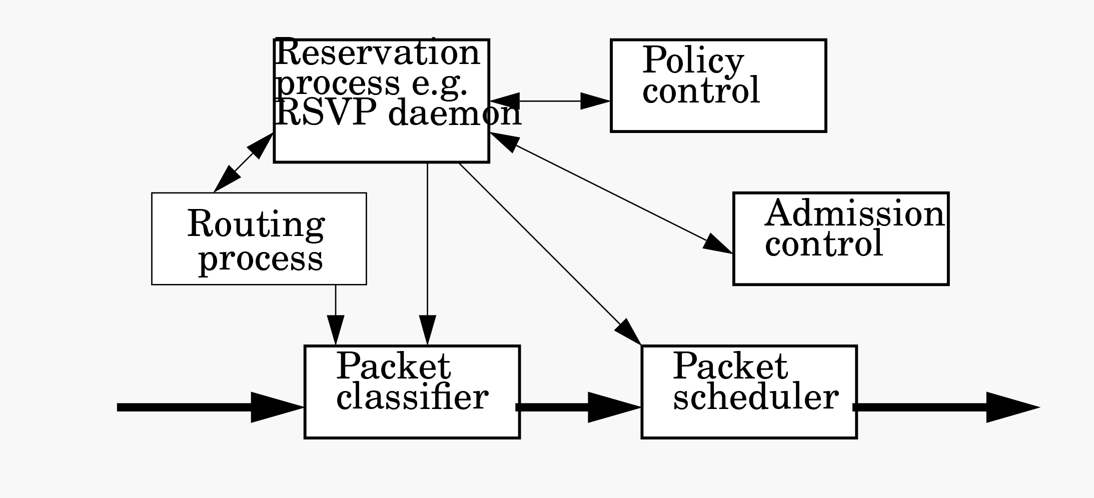


Figure 2 : *Elements of ISPN reference implementation model*

Notice that the Resource Reservation Protocol (RSVP), which is presented in section 4.2, only deals with resource reservation, and is independent of, and does not specify any of the other ISPN compenents. Also, none of the components are IP version dependent. For the use of RSVP with ISPN, see [12].

4.1.3 Traffic control in ISPN

Traffic control consists of packet scheduler, classifier and admission control [1]. Policy control is here defined to be part of packet scheduler (slightly confusing).

Figure 3 below illustrates one way of implementing hierarchical traffic control in ISPN.

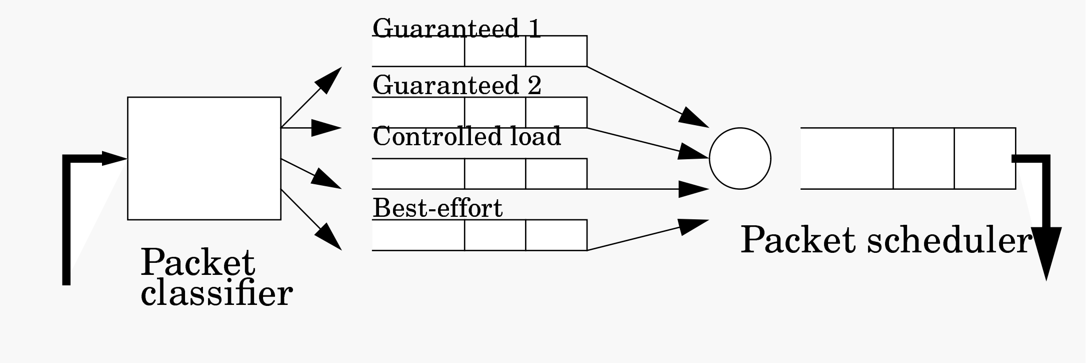


Figure 3 : *Hierarchical traffic control in ISPN*

Packet classification is based on the different service classes implemented by the router (host). WFQ is applied as a packet scheduling algorithm. Each guaranteed service flow is given an own queue, whereas the other flows are separated by priority. Among those, controlled load traffic is limited to ensure that also best-effort will slip through [8].

Admission control determines whether a new flow can be given the desired quality of service, or not. One way of implementing this is by applying the CSZ scheduler algorithm [4].

4.2 Reservation protocols

The task of any resource reservation protocol is to *establish* and *maintain* resource reservation over a path or a distribution tree in a network. As such, resource reservation protocols are signalling protocols, rather than routing protocols. Furthermore, another common misunderstanding is that reservation protocols in themselves improve quality of service. The accurate description is that they only provide *one* of the necessary mechanisms present.

Earlier reservation protocols include:

- ST (Stream Protocol - also named IPv5), which provides 1:1 duplex reservations [5]
- ST-II, which provides 1:n simplex reservations, is sender-oriented, and uses hard-states [11]

Currently, the Resource Reservation Protocol (RSVP) [15] is attracting the most interest. RSVP was and is being developed by the rsvp working group of the IETF, and is now an IETF proposed standard [2]. What most distinguishes this protocol from others are:

- *receiver-orientation*; actual reservations are initiated by receivers using Reverse Path Forwarding, and not senders, which allows heterogenous receivers
- *reservation types*; merging of reservation requests through filters, which makes routing more efficient
- *soft-state*; periodically refreshed “connection-less” conditions, which allows routing flexibility and adaptation, but with the danger of implosion

Furthermore, RSVP provides m:n simplex connections, and thus supports both multicast and unicast reservations. The protocol messages are either transported directly over IP, using protocol number 46, or encapsulated in UDP (user datagram protocol), as illustrated in figure 4 below.

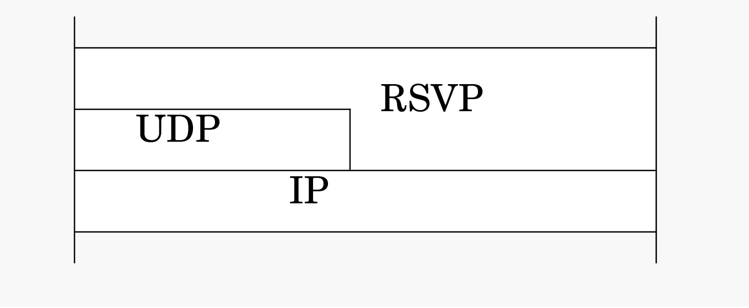


Figure 4 : *RSVP in the protocol stack*

4.2.1 RSVP states and messages

Figure 5 shows the different messages available in RSVP and the correrrsponding message flow, both upstream (<-) and downstream (->). Typically, senders will announce their traffic using the `Path` message, to whom interested receivers will respond with the `Resv` message, which contains the actual reservation request.

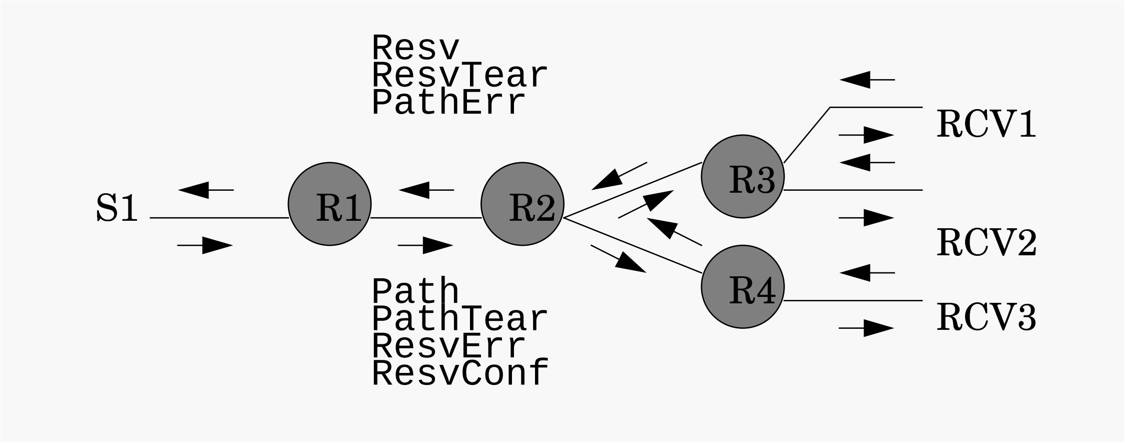


Figure 5 : *RSVP message flow, from [14]*

In each node along the way between sender and receiver, two types of soft states are kept, with following state attributes:

- *Path* (from sender), containing incoming link and outgoing links
- *Reservation* (from receiver), containing, for each outgoing link, sender information, resource description, and reservation type

The states must periodically (typically every 30 seconds) be refreshed by new `Path` and `Resv` messages, otherwise they will be deleted on timeout.

The message content for these two most important RSVP messages [14]:

- `Path`, including sender information (`Sender Template`), and traffic characteristics (`Sender Tspec` and optionally `Adspec`)
- `Resv`, including reservation specification, see next section for details

Additionally, the functionality of the other RSVP messages:

- `ResvTear`, `PathTear`: explicit deletion of soft states
- `ResvErr`, `PathErr`: error when establishing soft states
- `ResvConf`: confirmation of successful reservation

4.2.2 RSVP reservation

Reservations always take place on a per-flow basis, with each flow identified by e.g. the IPv6 flow label.

A detailed example of a reservation specification (`Resv` message) is given in figure 6.

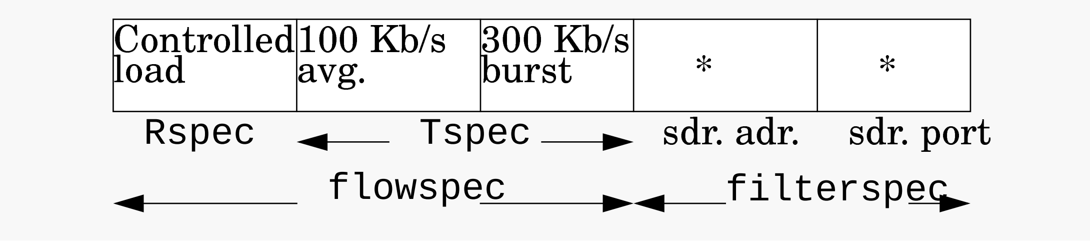


Figure 6 : *Example of* `Resv` *message, from [9]*

As can be seen, a reservation specification consists of two parts, a `flowspec` and a `filterspec`. The former specifies desired QoS, but the exact form and content of `Rspec` and `Tspec` are both opaque, and not defined in RSVP. Instead, they are specified by the IETF IntServ working group. The `filterspec` describes the *reservation style*:

- which senders the reservation should apply to
- how reservations from different senders should merge in state updating

If a `Path` message consists of an `Adspec`, which contains expanded traffic characteristics, such as service class, and which are updated in the intermediate routers, a correct reservation specification is more easily determined.

Such a reservation model is called OPWA - One Pass With Advertisement, and is the most common way of making reservations in RSVP today.

4.2.3 RSVP state updating

Three possible reservation styles are defined for merging reservations when updating *Reservation* soft states in nodes.

- *Fixed filter* (FF), where sender(s) is explicitely identified, and there is a separate reservation for each sender
- *Shared Explicit* (SE), where sender(s) is explicitely identified, but the reservation is shared
- *Wildcard filter* (WF), where senders are not identified, and the reservation is shared (see the reservation specification example in section 4.2.2)

Shared Explicit and Wildcard filter are suited for situations with multiple senders and receivers, but with only one active sender at a time, e.g. an audio conference. Fixed filter are more suited for the one sender, many receivers situations, e.g. a video-on-demand service.

An example of a *Reservation* state updating, using Fixed filer reservation style is given in figure 7

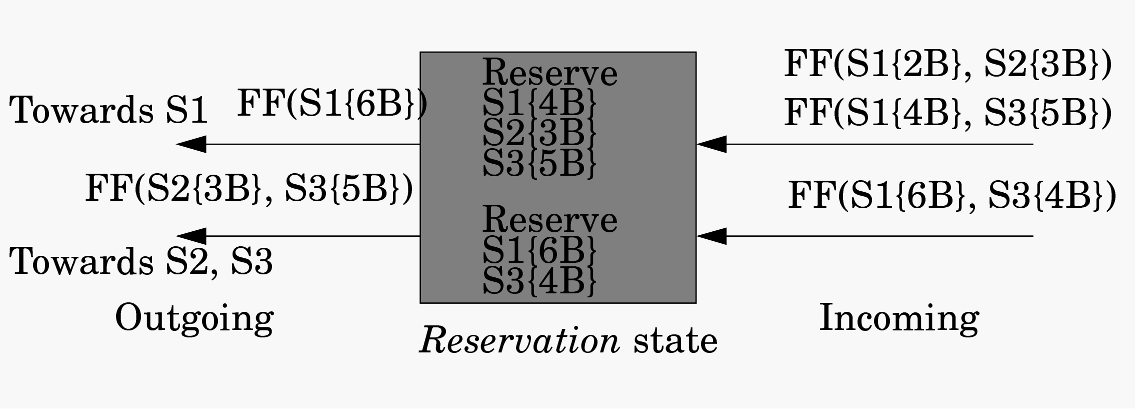


Figure 7 : *Reservation state updating*

In the example, incoming reservation requests are merged by taking the maximum of the requests received on that interface for that particular sender, and outgoing requests are given by the maximum of all reservations installed in that router for that particular sender.

4.2.4 RSVP problem areas

The use of RSVP is still very much in an experimental phase. One of the greatest concerns today is that RSVP is simply applied in more situations than it is meant for.

Originally, RSVP was developed for multimedia realtime applications of a certain duration, and with not many sessions, such as videoconferencing (1 Mbits/s per session). Nowadays, the protocol is also used to prioritize traffic characterized by numerous short-lived sessions, such as IP telephony and web browsing (http sessions). The result is a large number of reservations, big RSVP state tables, and ultimately reduced performance in the routers.

To rectify this, some guidelines on deployment have been published by the IETF [7]. This document also points out a number of unresolved issues affecting RSVP:

- *scalability*; involving router state processing and storage resource requirements for a large number of sessions
- *security*; dealing with spoofed reservation requests
- *policing*; addressing mechanisms for who can, or cannot, make reservations

Another fundamental problem is, for which kind of applications should it be possible to make reservations? All issues above are currently being subject to intense research.

4.2.5 Testing and experiments

Due to the unresolved issues above, it is recommended that RSVP is only deployed in local area networks, e.g. intranets, at the moment. More experience is needed before wide scale delpoyment is advisable. Norwegian Computing Center (NR) will experiment with RSVP over an IPv6 network as part of the IMiS Kernel project.

As for vendors supporting RSVP implementations in their products, the list now includes companies and institutions such as Cisco,Sun, IBM and ISI, and more are expected to follow. An RSVP application programming interface for hosts (RAPI) has also been developed [3].

References

[1] Braden, R. et al., *Integrated Services in the Internet Architecture: an Overview*, RFC 1633, 1994

[2] Braden, R. et al., *Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification*, RFC 2205, 1997

[3] Braden, R. & Hoffman, D., *RAPI -- An RSVP Application Programming Interface, Version 5*, Internet Draft, 1997 (work in progress)

[4] Clark, D. et al., *Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanisms*, Proc. SIGCOMM'92, Baltimore, 1992.

[5] Forgie, J., *ST - A Proposed Internet Stream Protocol*, Internet Experimental Notes - 119, 1979

[6] Jamin, S. et al., *An Admission Control Algorithm for Predictive Real-Time Service*, Proc. 3d International Workshop on Network and Operating System Support for Digital Audio and Video, 1992

[7] Mankin, A. et al., *Resource ReSerVation Protocol (RSVP) - Version 1 Applicability Statement - Some Guidelines on Deploiyment*, RFC 2208, 1997

[8] Parulkar, G., *Emerging Internetworking Architecture and Protocols*, lecture at UNIK, october 1997.

[9] Schwantag, U., *An Analysis of the Applicability of RSVP*, Diploma thesis, Uni. Karlsruhe (TH), 1997

[10] Shenker S. et al., *Specification of Guaranteed Quality of Service*, RFC 2212, 1997

[11] Topolcic, C., *Experimental Internet Stream Protocol: Version 2 (ST-II)*, RFC 1190, 1990

[12] Wroclawski, J., *The Use of RSVP with IETF Integrated Services*, RFC 2210, 1997

[13] Wroclawski, J., *Specification of the Controlled-Load Network Element Service*, RFC 2211, 1997

[14] White, P., *RSVP and Integrated Service in the Internet: A tutorial*, IEEE Communications Magazine, vol.35, no.5, 1997

[15] Zhang, L. et al., *RSVP: A New Resource ReSerVation Protocol*, IEEE Network Magazine, september 1993

5 Summary

In this note, a couple of emerging network protocols and architecture models have been presented: IPv6, ATM, ISPN and RSVP. The relationship between them is that ATM is mostly use as carrier in the core wide area network. IPv6 is run on top of link-layer protocols, such as ATM, and will eventually be deployed in every single computer connected to an Internet-based network. ISPN is a proposed architectural model of an extended Internet, which include RSVP as one possible protocol for the resource reservation component.

IPv6 is more efficiently designed and has better header composition than IPv4. And although the mechanisms for e.g. security and mobility are possible to achieve as IPv4 extensions, IPv6 provides a better solution and support of these features.

The relation between ATM and the two IP versions deserves some special attention. IPv4 over ATM is known as classical IP over ATM [3]. IPv6 is not developed to take advantage of the QoS and traffic management features in ATM particularly better than IPv4, and both protocols use ATM merely as a link-layer technology. One key difference, though, is the introduction of the generic IPv6 Neighbour Discovery protocol which assumes native multicasting on the link-layer level [1],[2]. The advantage is that no auxiliary address resolution protocol is needed at the link layer, but the drawback is that the multicast assumption requires a complicated convergence protocol.

The ISPN architecture model and RSVP are independent of the two IP versions, because neither impose demands on IP network layer mechanisms.

5.1 Future work

The knowledge from this study will be used in IMiS Kernel in the following ways:

- Establishment of national, experimental (IPv6) network infrastructure.
- Investigation of possible advantages in this new network infrastructure with regard to Quality of Service and mobility.
- Exploration of how (and if) new mechanisms provided by the network infrastructure can meet demands imposed on the network from multimedia applications.
- Investigation of how ATM, IPv6 and ISPN/RSVP can work together, and take advantage of the characteristic features of the respective protocols.

5.2 Web references

The most important web references on these subjects are:

IPv6:

- IETF IPng:
  `http://www.ietf.cnri.reston.va.us/html.charters/ipngwg-charter.htm`
- Ipsilon:
  `http://playground.sun.com/pub/ipng/html/ipng-main.html`

ATM:

- ATM Forum: `http://www.atmforum.com/`

ISPN:

- IETF IntServ: `http://www.ietf.cnri.reston.va.us/html.charters/int-serv-charter.html`

RSVP:

- IETF RSVP: `http://www.ietf.cnri.reston.va.us/html.charters/rsvp-charter.html`
- ISI: `http://www.isi.edu/div7/rsvp/rsvp.html`

References

[1] Armitage, G. et al., *IPv6 over Non-Broadcast Multiple Access (NBMA) networks*, Internet Draft, october 1997 (work in progress)

[2] Armitage, G. et al., *IPv6 over ATM Networks*, Internet Draft, October 1997 (work in progress)

[3] Laubach, M., *Classical IP and ARP over ATM*, RFC 1577, 1994