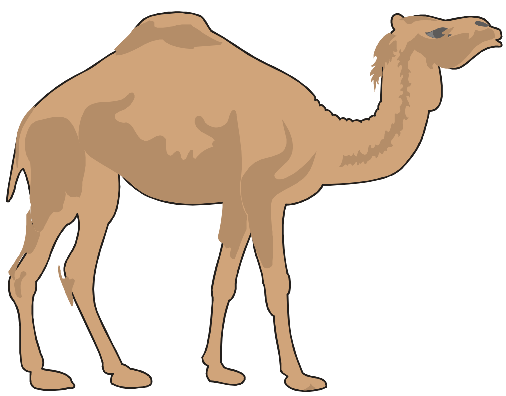
Aeronautical Telecommunication Network (ATN)

Comprehensive ATN Manual (CAMAL)

Part II
System Level Considerations



Editor's Draft (January 1999)

The preparation of this document has been on a "best efforts" basis and no warrantee is offered as to its correctness..

This PDF version has been prepared for the ATNP Working Groups by FANS Information Services Ltd - http://www.fans-is.com
Please check our Web Site regularly for information on updates to the SARPs and Guidance Material

9th January 1999

PART II

TABLE OF CONTENTS

1. System Level Requirements

1.1 Determination of requirements

1.1.1 System level requirements are provided in the standards and recommended practices (SARPs). However, the functional, safety, security, performance and interoperability requirements to support the intended operations of the aeronautical telecommunication network (ATN) may only be derived from an assessment of the operational environment. This includes:

a) Operational environment characterization. This involves the determination of operational objectives, such as the application of reduced separation minima, dynamic airborne re-route planning systems (DARPS) and so on;

b) Operational safety assessment. This identifies hazards and classifies them according to their severity. The hazards and their classifications will determine the extent to which failures, failure conditions, and their effects on air traffic services will be evaluated;

c) Operational security assessment. This assessment will identify security threats and determine the extent to which security measures are needed and allocate requirements appropriately;

d) Operational performance assessment. This determines the required performance parameters and allocates operational performance requirements to different parts of the system and operations;

e) Operational interoperability assessment. This evaluates what is necessary to ensure an acceptable level of interoperability between different systems; and

f) Other operational assessments. Other assessments may be performed to determine cost effectiveness and efficiency of the system.

1.1.2 Figure 1-1 provides the relationship between the ATN technical provisions and the associated operational and institutional requirements.

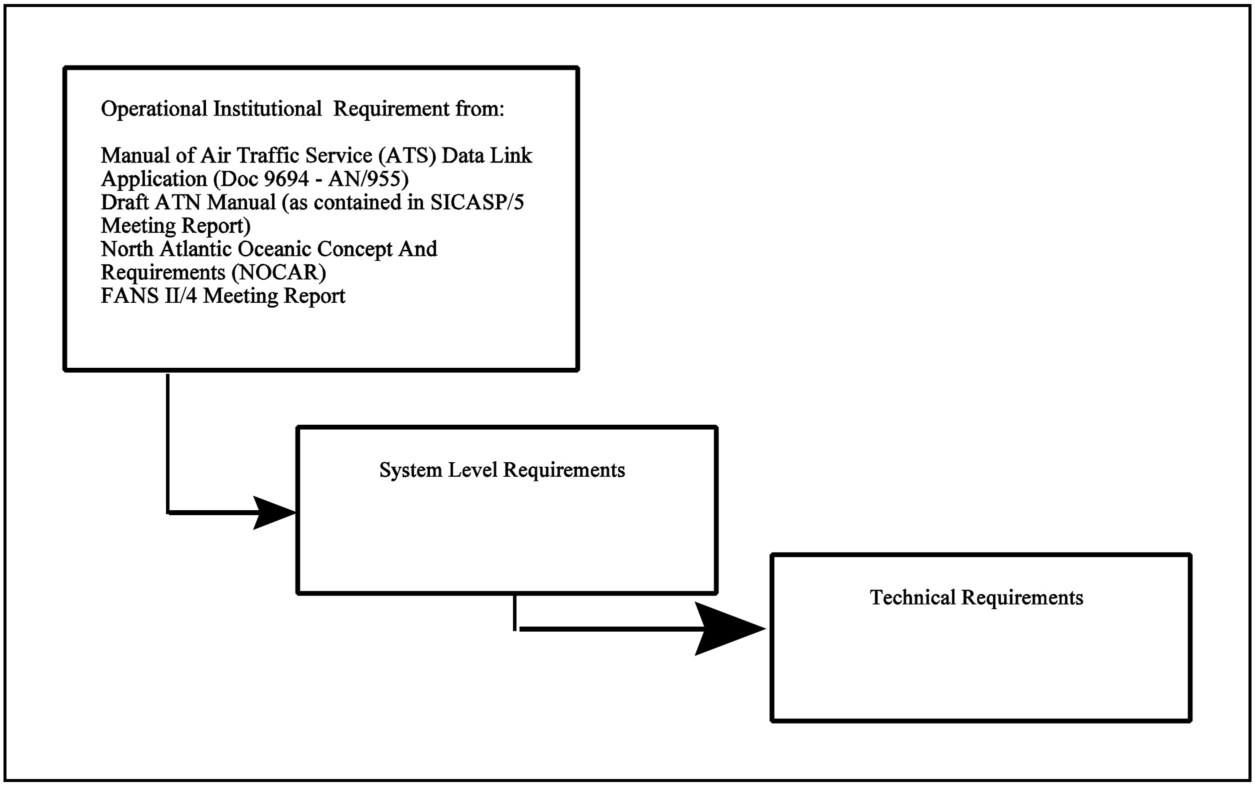


Figure 1-1. Traceability from requirements to SARPs

1.2 Communication Priorities

1.2.1 Fourteen application categories have been identified within the ATN requiring separate transmission priorities. These application categories have been derived from existing ICAO provisions and the ITU radio regulations.

1.2.2 In the ATN environment, Connection Oriented Transport Protocol (COTP) and Connectionless Network Protocol (CLNP) headers are transferred between communicating ATN end-systems; these protocols provide the sole mechanism at the internetworking level for conveyance of communication priority along the entire communication path. Table 1-1 shows the relationship between the CLNP priorities as used in the ATN SARPs and the priority levels defined with Annex 10 for Aeronautical Mobile Service (AMS) and Aeronautical Fixed Service (AFS) types of communications as well as in Part 51 of the ITU Radio Regulations.

1.2.3 The CLNP priority levels for [6] Network/Systems administration, [7] Aeronautical information service messages and [8] Flight regularity communications all represent communications relating to flight regularity.

Note.— While not used by any of the applications defined in the current ATN SARPs, connectionless Transport Protocol (CLTP) headers, while conveyed on an end-to-end *basis, do not explicitly convey priority, and thus rely on the underlying CLNP header for this purpose.*

Table 1-1. Relationship of communication priorities

ITU Radio Regulations, Part 51 [Priority]	ICAO Annex 10 Volume II, Chapter 5, Aeronautical Mobile Service [Priority]	ICAO Annex 10, Volume II, Chapter 4, Aeronautical Fixed Service [Priority]	ICAO ATN SARPs [CLNP Priority]
[1] Distress calls, distress messages and distress traffic	[a] Distress calls, distress messages and distress traffic	[1] Distress calls	[14] Network/Systems Management
as above	as above	as above	[13] Distress Communications
[2] Communications proceeded by the urgency signal	[b] Urgency messages, including messages proceeded by the medical transports signal	[2] Urgency messages	[12] Urgent Communications
[3] Communications relating to radio direction finding	[c] Communications relating to direction finding	Not Applicable	[11] High piority flight safety messages
[4] Flight safety messages	[d] Flight safety messages	[2] Flight safety messages	[10] Normal priority flight safety messages
[5] Meteorological messages	[e] Meteorological messages	[3] Meteorological messages	[9] Meteorological communications
[6] Flight regularity messages	[f] Flight regularity messages	[3] Flight regularity messages	[8] Flight regularity communications
as above	as above	[3] Aeronautical information services	[7] Aeronautical information service messages
as above	as above	Not Applicable	[6] Network/Systems administration
Not Applicable	Not Applicable	[3] Aeronautical administrative messages	[5] Aeronautical administrative messages
Not Applicable	Not Applicable	[*] Service message *priority as appropriate	[4] Unassigned
[7] Messages relating to the application of the United Nations Charter	Not Applicable	Not Applicable	[3] Urgent priority administrative and U.N. Charter communications

ITU Radio Regulations, Part 51 [Priority]	ICAO Annex 10 Volume II, Chapter 5, Aeronautical Mobile Service [Priority]	ICAO Annex 10, Volume II, Chapter 4, Aeronautical Fixed Service [Priority]	ICAO ATN SARPs [CLNP Priority]
[8] Government messages for which priority has been expressly requested	Not Applicable	Not Applicable	[2] High priority administrative and state/government communications
[9] Service communications relating to the working of the telecommunication service or to communications previously exchanged	Not Applicable	Not Applicable	Not Applicable
[10] Other aeronautical communications	Not Applicable	Not Applicable	[1] Normal priority administrative
as above	Not Applicable	Not Applicable	[0] Low priority administrative

————————

2. *Security Management*

Security of the ATN is necessary to ensure that the safety and performance of supported air traffic management services won't be affected by security threats. These threats may include denial of service, modification, replay, and masquerade. An important measure against these security threats is the physical security of the equipment and systems. This measure should be applied to the initial ATN installations. ICAO Annex 17 contains more information on physical security. Further guidance material are currently under development for features like message authentification services based on the use of digital signatures.

— — — — — — — —

3. *Systems Management*

3.1 Systems management of the ATN may be described as:

a) administrative management (e.g. cost management, service monitoring, and name and address management); and

b) Operational management (e.g. configuration control, performance monitoring, and fault management).

3.2 Much of administrative management is inherent in the operation and maintenance of a site which hosts an ATN end system (ES) or intermediate system (IS).

3.3 Operational management consists of means and procedures for managing ATN equipment and connections. Many of these tools and procedures can be local, especially for initial implementations.

3.4 The ATN is expected to grow from initial local/regional implementations to an ultimately global network. As the ATN grows, certain operational management tools may require international standardization to support exchange of management information between administrations. These standards and guidance material are currently under development.

— — — — — — — —

4. *Naming and Addressing*

4.1 General

4.1.1 The ATN naming and addressing scheme is based on the open systems interconnection (OSI) Reference Model (ISO 7498-3) which supports the principles of unique and unambiguous identification of information objects and global address standardisation.

4.1.2 The *OSI Basic Reference Model, Part 3* (ISO 7498-3) distinguishes the concepts of *name* and *address*. In brief, a *name* is an identifier which is expressed in some language and is used to identify an object (e.g. a system, a protocol entity, an application, etc.) while an *address* is used to locate an object. A name stays with an object as long as it exists, while the address of the object may change during its lifetime.

4.1.3 Names must be assigned to any information object which may need to be referred to during information processing. Addresses must be assigned to any information object to which data may be directed from another entity.

4.1.4 Names typically have meaning and are thus generally expressed in a mnemonic format. Correspondingly, the significance of addresses typically increases when descending in the communications stack. Addresses are generally expressed in a coded or numeric format. Typical examples of addresses are the network service access point (NSAP) address of a network service user, the address prefixes used by routing algorithms, or the port address of an interface device. In either case, in order to ensure unambiguous assignments, names and addresses must be *registered* by registration authorities within the context or environment in which they are to be used.

4.1.5 In order to manage large and complex networks, names and addresses should be assigned according to a hierarchical tree structure. The structure of such name/address trees should, in principle, represent the structure of the network operating environment. For example, as the ATN is an international network involving primarily two principal interest groups (providers and users of ATS), both the ATN internetwork (NSAP) address tree and the ATN application name tree split the overall naming and addressing space between these groups at a high level (see and Figures 4-1 and 4-6). At the same time, the responsibility for registration of addresses and names has effectively been divided between ICAO and IATA (representing ATS providers and users respectively) on a high level of the address stucture, with the provision of further delegation to subordinate authorities, if appropriate. Each authority is responsible for address allocation and registration within their sub-spaces and may further delegate responsibility to subordinate organisations or bodies. For example, the responsibility for NSAP address field allocation may be further delegated to the States for the ICAO's naming/addressing space and to airlines for the IATA's naming/addressing space.

4.1.6 Naming, addressing and registration concepts are closely related to directory services. A *directory* may be used to store name and address information and can provide lookup functions to retrieve address or other information on the associated object (e.g. a given application or service element). Directory information may be stored local to a system if the information is static and in small amount. However, in a dynamic operating environment like the one for which ATN is intended, applications cannot always know in advance the current addresses and names of all other communication partners. Consequently, a simple directory service for use between aircraft and ground entities, the *context management application (CMA)*, has been specified in ATN SARPs. The use and meaning of ATN addresses in the context of the CMA is presented later in this chapter.

4.2 Naming and Addressing Domains

4.2.1 Unambiguity of ATN names and ATN addresses is achieved through the use of naming/addressing domains with firmly allocated naming/addressing authorities.

4.2.2 A naming/addressing domain is the set of names/addresses that are assignable to objects of a particular type. Independent naming/addressing domains exist for objects of different types (e.g. an application process, a network entity or a subnetwork point of attachment). Each naming/addressing domain is administered by a naming/addressing authority (see section 4.3).

4.2.3 According to ISO 7498-3, naming/addressing domains may be hierarchically decomposed into subsets which are known as naming/addressing sub-domains. Each subset (sub-domain) is under the control of an individual naming/addressing authority and does not intersect with other subsets (sub-domains) administered by different naming/addressing authorities. The top of this hierarchical structure is the global OSI domain.

4.2.4 The ATN naming/addressing domains, i.e. the sets of all possible names/addresses of objects within the ATN, are subdomains of the global OSI naming/addressing domain. Several such ATN naming/addressing domains exist, as there are different types of ATN objects which have to be named or assigned addresses respectively. An ATN naming domain exists for ATN Application Processes and another ATN addressing domain exists, for example, for ATN network addresses.

4.2.5 The naming/addressing authority for the ATN naming/addressing domains is ICAO which controls and manages these domains through the ATN SARPs.

4.2.6 In order to facilitate the assignment and registration of ATN addresses (which is expected to comprise several thousands of objects), the ATN naming/addressing domains is divided into a set of hierarchical sub-domains. Each address sub-domain is a set of address formats and values which are administered by a single addressing authority. Each addressing authority is responsible for its own address sub-domain and may further partition it into several subordinate sub-domains and delegate authority for these sub-domains. This principle allows the establishment of sub-address spaces (i.e. the set of values within an addressing sub-domain) in a hierarchical fashion without the need to co-ordinate between sub-address spaces. This principle of hierachically structured ATN sub-domains within the global OSI naming/addressing domain is illustrated in Figure 4-1.

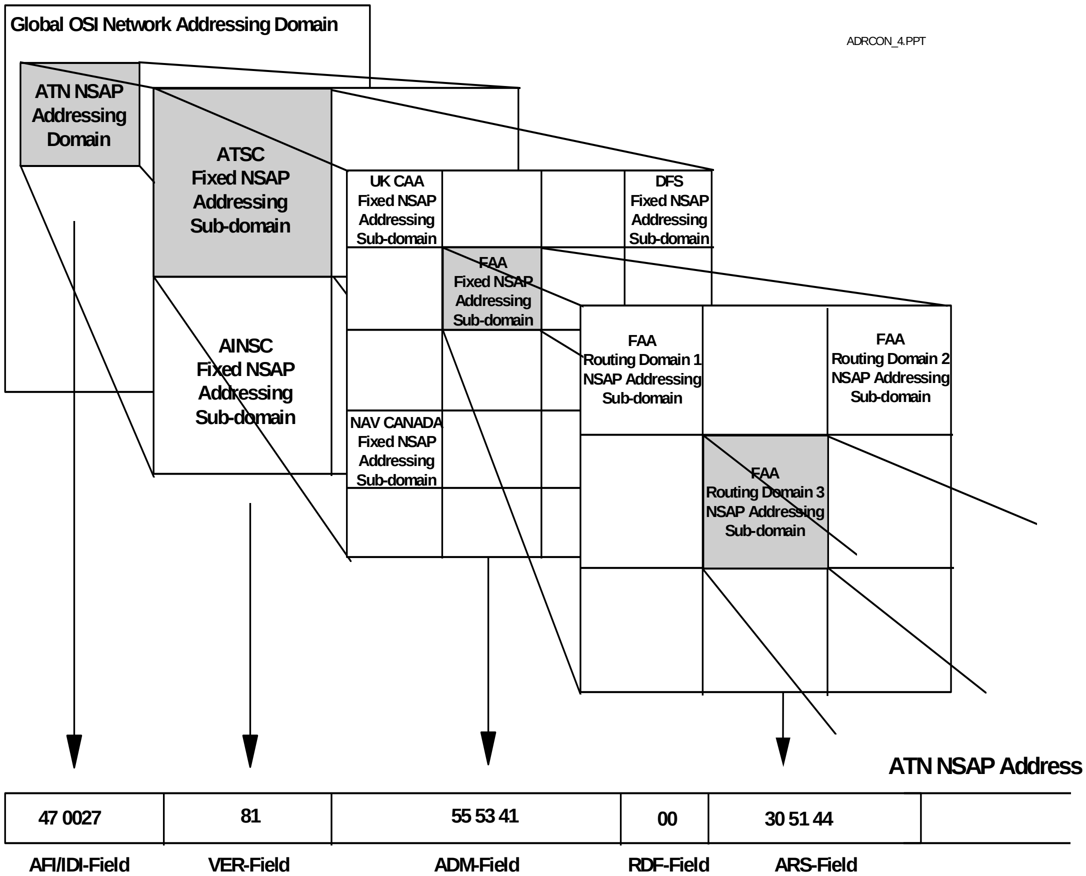


Figure 4-1. Hierarchical Decomposition of Addressing Domains Illustrated for ATN Network Addresses

4.3 Naming and Addressing Authorities

4.3.1 A naming/addressing authoritiy defines the rules including syntax (i.e. sizes and formats) and semantics (i.e. contents and interpretation) for specifying names/addresses within its naming/addressing domain and for the creation of further sub-domains. Furthermore, it allocates names/addresses within its domain according to specified rules, but does not perform the binding of the allocated names/addresses to the associated objects. This latter task is within the responsibility of the registration authority.

4.3.2 A naming/addressing authority may administer and allocate names/addresses itself, or, if it has partioned its naming/addressing domain into naming/addressing sub-domains, may delegate the responsibility for naming/addressing within each such sub-domain to a sub-domain naming/addressing authority.

4.4 ATN Elements Subject to Naming and Addressing

4.4.1 General

4.4.1.1 The following tables show the ATN elements which require the assignment of unambiguous names and addresses:

Table 4-1. ATN Elements Requiring Unambiguous Names

ATN Element	Generic Name
Network Layer Entities	Network Entity Title (NET)[1]
Routing Domains	Routing Domain Identifier (RDI)
Routing Domain Confederations	Routing Domain Identifier (RDI)
Administrative Domains	Administrative Domain Identifier (ADI)
Application Processes	Application Process Title (AP-Title)
Application Entities	Application Entity Title (AE-Title)
Application Context	Application Context Name
Presentation Context	Presentation Context Identifier
AMHS User	AMHS Originator/Recipient Name (O/R Name)
Security Type Objects	Security Registration Identifier
Managed Objects	Managed Object Name

Table 4-2. ATN Elements Requiring Unambiguous Addresses

ATN Element	Generic Address
Subnetwork Access Point	Subnetwork Point of Attachment (SNPA) Address
Network Layer Entities	Network Entity Title (NET)[1]
Network Service Users	Network Service Access Point (NSAP) Address
Transport Service Users	Transport Service Access Point (TSAP) Address
Session Service Users	Session Service Access Point (SSAP) Address
ATN Applications	Presentation Service Access Point (PSAP) Address

4.4.1.2 Whereas the SNPA addresses have to be unambiguous within the context of a given subnetwork, all other names and addresses listed in the Tables 4-1 and 4-2 have to be unambiguous throughout the whole ATN. As the ATN internetwork addressing plan defines NSAP addresses which are globally (i.e. within the OSI environment) unique, all addresses, except the SNPA addresses, listed in Table 4-2 are even globally unambiguous as they are derived from the NSAP address (see Figure 4-4).

4.4.1.3 Figure 4-2 illustrates the location of those ATN elements, which require unambiguous names or addresses. Those elements of the above tables not displayed in this figure either relate to an entity which is beyond the scope of an ATN End System (such as

[1] According to ISO/IEC 7498-3, network layer entities are both named and located by their NET.

Administrative Domains and Routing Domains), or which may be embedded in any layer of an ATN End System (such as Managed Objects or Security Type Objects).

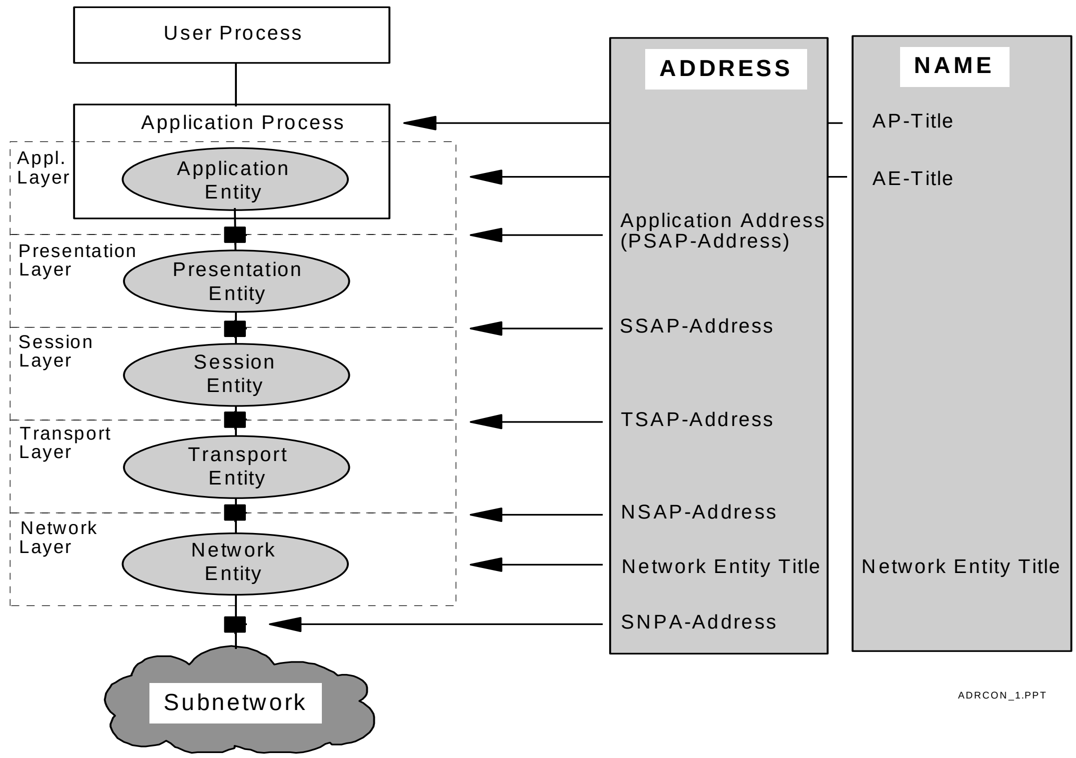


Figure 4-2. Addresses and Names of ATN Objects Contained in an ATN End System

As can be seen from Figure 4-2, ATN addresses and names/addresses relate to objects contained in different layers of an ATN End System's communication stack. There may be more than one object of a given type, e.g. application process or transport entity, within an ATN End System. In this case, the name/address of each such object has the same syntax, semantics and encoding, but differs in the assigned value. An example may be two NSAP addresses (differing in the N-SEL field value) within a given ATN End System, one of which identifies the transport entity providing the connection-oriented transport service and the other identifies the transport entity providing the connectionless mode transport service.

4.4.1.4 In addition to those names and addresses which must be unambiguous throughout the ATN (or OSI) environment , there are some ATN names and addresses that are used in a local context. For example, AE-invocations may have to handle one or more application associations. These can be identified by Application Association Identifiers which need to be unambiguous only within the scope of the co-operating AE-invocations. Another example of a name with local scope is an AE Invocation Identifier which is used locally to distinguish between various invocations of a given application entity running concurrently as part of an application process. These names/addresses do not have to be registered as they need not be unambiguous throughout the ATN due to their local scope.

4.4.2 Subnetwork Elements

In order to provide end-to-end data transfer, ATN systems will be interconnected via real subnetworks. The most likely subnetworks to be used during the initial deployment of ATN will be X.25 packet switched data network (PSDNs) for ground-ground, and VHF digital link (VDL), aeronautical mobile-satellite service (AMSS) and secondary surveillance radar (SSR) Mode S subnetworks for air-ground communications. This section briefly outlines the addressing elements within these subnetworks. It should be noted that the subnetworks listed in this section are only a subset of the network technologies which can be used to interconnect ATN systems.

a) **X.25 Network Addresses.** An X.25 network address identifies the subnetwork point of attachment (SNPA) of a data terminal equipment (DTE)/router on a given X.25 network. It has meaning only within the context of the X.25 network on which it is used subject to the provisions in *CCITT Recommendation X.25 - Interface Between DTE and data circuit-terminating equipment (DCE) for Terminals Operating In the Packet Mode And Connected to Public Data Network by Dedicated Circuit,* 1988.

b) **AMSS Network Addresses**. An AMSS network address identifies the SNPA of a DTE/router on a given AMSS subnetwork. An AMSS DTE may either be located on an aircraft or at a fixed site. The AMSS network address has meaning only within the context of the AMSS network in which it is used subject to the provisions in the *Aeronautical Mobile Satellite Service (AMSS) SARPs* (ICAO Annex 10, Volume III).

c) **VDL Network Addresses**. A VDL network address identifies the SNPA of a DTE/router on a given VDL subnetwork. An VDL DTE may either be located on an aircraft or at a fixed site. The VDL network address has meaning only within the context of the VDL network in which it is used subject to the provisions in the *VHF Digital Link (VDL) SARPs* (ICAO Annex 10, Volume III).

d) **Mode S Network Addresses**. A Mode S network address identifies the SNPA of a DTE/router on a given Mode S subnetwork. A Mode S DTE may either be located on an aircraft or at a fixed site. The Mode S network address has meaning only within the context of the Mode S network in which it is used subject to the provisions in the *Secondary Surveillance Radar (SSR) Mode S Subnetwork SARPs* (ICAO Annex 10, Volume III).

4.4.3 Internetwork Elements

The following addressing elements exist for ATN internetwork:

a) **Network Entity Title (NET)**. An ATN NET is a 20-octet string used to uniquely identify and locate a network layer entity of an ATN system (router or end system), and thus, in networking terms, is used to identify the system itself. Thanks to the global nature of the ATN internetwork addressing plan, a system's NET can be used to locate it anywhere within the ATN. The syntax of an ATN NET is equivalent to that of an ATN NSAP address. It differs from the NSAP addresses assigned to the same system only in the last octet, i.e. the network selector (N-SEL) field value (see section 4.5.2.1).

b) **NSAP Address**. An ATN NSAP address is a 20-octet string used to uniquely identify and locate a given NSAP (i.e. a network service user) within the context of the ATN.

c) **Administrative Domain Identifier**. Each ATN administrative domain can be identified by a unique domain address comprising of the AFI, IDI, VER and ADM fields of an ATN NSAP address (see section 4.5.2.2). An administrative domain identifier is the prefix of all ATN NSAP addresses and NETs within the same ATN administrative domain.

d) **Routing Domain Identifier**. Each ATN routing domain can be identified by a unique, unvarying 11-octet ATN routing domain identifier comprising of the AFI, IDI, VER, ADM, RDF and ARS fields of an ATN NSAP address. A routing domain identifier is the prefix of all ATN NSAP addresses and NETs within the same ATN routing domain.

4.4.4 Upper Layer and Application Elements

The following addressing elements exist for ATN upper layer and application elements:

a) **Transport Address**. An ATN transport address, or in OSI terms an *ATN TSAP address*, uniquely identifies and locates a given transport service user within the context of the ATN. An ATN TSAP address is comprised of a one- or two-octet TSAP selector (T-SEL) appended to the ATN system’s NSAP address. Consequently, the T-SEL identifies and locates a given transport service user within the context of the ATN system's NSAP address which, in turn identifies a particular network service user. Consequently, T-SEL values have only a local scope, i.e. within a given ATN End System, and do not need global registration.

b) **Session Address**. An ATN session address, or in OSI terms an *ATN SSAP address*, uniquely identifies and locates a given session service user within the context of the ATN. A SSAP address is comprised of a SSAP selector (S-SEL) appended to the TSAP address. Consequently, the S-SEL identifies and locates a given session service user within the context of the ATN system's TSAP address. S-SEL values have only a scope local to a given ATN system and do not need global registration.

c) **Application Address**. An ATN application address, or in OSI terms an *ATN PSAP address*, uniquely identifies and locates a given application within the context of the ATN. A PSAP address is comprised of a PSAP selector (P-SEL) appended to the ATN system’s SSAP address. Consequently, the P-SEL identifies and locates a given session service user within the context of the ATN system's SSAP address. For initial implementatons, the application address of an ATN application is a PSAP address with absent session and presentation selectors (S-SEL and P-SEL). Thus it has the form of a TSAP address (see section 4.5.3).

d) **Application Name**. An ATN application name, or in OSI terms an *ATN application entity title (AE-title),* uniquely identifies a given application within the context of the ATN. An AE-title consists of an *application process title (AP-title)* and an *AE-qualifier*. The AP-title is the name of the application process which contains the ATN application, and the AE-qualifier uniquely identifies this ATN application within the context of the application process. For initial implementation, the AP-title of an ATN application which is hosted by a ground system includes the ICAO Facility Designator, whereas the AP-title of an ATN application which is hosted by an aircraft system includes the ICAO 24-bit aircraft address.

AP-Titles and AE-Qualifiers may be assigned either an attribute-based name form or an object identifier name form (see section 4.5.4). When an AP-Title is allocated an attribute-based name form, all of the associated AE-Qualifiers must also be assigned an attribute-based name form. Correspondingly, when an AP-Title is allocated an object identifier name form, all of the associated AE-Qualifiers must also be assigned an object identifier name form.

The application name may be used as input to a directory service to determine the address, i.e. the PSAP address, of a given application. A simple form of such a directory service is provided by the ATN Context Management Application (CMA) as specified in Sub-Volume II of the ATN Technical Provision (Doc 9705-AN/956).

It may at times be necessary to distinguish between the various invocations of a given AE running concurrently as part of a given application process (AP). This is done through the use of AE Invocation Identifiers which must be unambiguous only within the scope of the {AP-invocation, AE} pair, and thus do not have to be registered. The use of invocation identifiers is not required for initial ATN implementation.

e) **Application Process Title**. Application Processes are each named in terms of a unique *application process title (AP-title)* which unambiguously identifies the application process throughout the OSI environment. Application processes are those elements in a given ATN end system which perform the information processing for particular user applications.

It may at times be necessary to make a distinction between the various invocations of a given AP running concurrently on an end system. This is done through the use of AP Invocation Identifiers which must be unambiguous only within the scope of the AP, and thus do not have to be registered. The use of invocation identifiers is not required for initial ATN implementation.

4.4.5 ATN Application Users

The following addressing elements exist for ATN application users:

a) **AMHS User Name**. An AMHS user name or in OSI-terms an *AMHS O/R name* is used to locate an AMHS user in the AMHS address space. An AMHS O/R name is composed of an *AMHS management domain identifier* and a set of attributes, which depend on the addressing scheme implemented by the AMHS management domain, and which uniquely identify the AMHS user within this management domain. Furthermore, an AMHS O/R name may optionally include the directory name of the AMHS user.

4.4.6 **Aircraft**

The following addressing elements exist for Aircraft

a) ICAO 24-bit Aircraft Address;

b) Registration Mark; and

c) Flight Number.

The *24-bit aircraft address* is used as a component (i.e. field value) in several of the ATN addresses and names, including the AE-title, the NSAP address as well as the SNPAs in VDL, AMSS, and SSR Mode S SNPAs.

4.4.7 **ATC Centres**

4.4.7.1 Currently, each Air Traffic Control Centre (ATCC) is assigned a unique network address through the *Aeronautical Fixed Telecommunication Network (AFTN) SARPs*, (ICAO Annex 10, Aeronautical Telecommunications, Volume II). There is no requirement from the ATN to address a particular ATCC, but rather to address ATN systems and applications within an ATCC.

4.4.7.2 In order to identify an ATN application within the context of a given ATC responsibility, the ICAO Facility Designator is used as part of the AE-title of ground-based ATN applications (see section 4.5.4.1).

4.5 **ATN Address and Name Definitions**

4.5.1 **Subnetwork Addressing**

4.5.1.1 ***General***

4.5.1.1.1 Subnetwork addresses are not ATN addresses in the strict sense, as their scope is limited to a given subnetwork. They are therefore not unique and unambiguous throughout the ATN. Subnetwork addressing is important to consider in the ATN context as ATN systems must identify the appropriate subnetwork point of attachment to communicate with other ATN systems. In general, only addresses (i.e. no names) are assigned to SNPAs.

4.5.1.1.2 Registration of SNPAs is generally a consideration local to a subnetwork, but the SNPA addresses assigned to specific systems or services should be made available to all interested parties attached to a given subnetwork.

4.5.1.1.3 This section presents addressing issues related to those subnetworks which are likely to be used for interconnecting various ATN organisations and routing domains in the time frame of the initial ATN.

4.5.1.2 ***X.25 Subnetworks***

4.5.1.2.1 Addressing of systems (typically referred to as Data Terminal Equipment (DTE) attached to an X.25 network is treated in CCITT Recommendations X.25 and X.121. Generally an X.25 network has a well-established local addressing plan according to the needs identified by the network operator. DTE addresses on a given network typically contain up to 10 binary coded decimal (BCD) digits. For calls placed to destinations outside of the network, a 4-digit BCD data network identification code (DNIC) defined by CCITT recommendation X.121 or other international agreements must be prepended to the DTE network address.

4.5.1.2.2 X.25 DTE network addresses do not need to be registered within the ATN-wide context as their use does not have ATN-global impact. Rather, organisations will exchange DTE network addresses as appropriate according to a prior agreement or service contract.

4.5.1.2.3 An ATN system connected to an X.25 network must have pre-configured knowledge of the DTE network addresses of the systems with which it will communicate using the X.25 network. Typically, this information will be loaded in the ATN system's routing table by systems management functions prior to putting the system into service.

4.5.1.3 ***VDL Subnetworks***

4.5.1.3.1 The addressing plan for the VDL subnetwork is described in the VDL SARPs in Annex 10. The scope and impact of the VDL addressing plan is limited to the VDL subnetwork. Systems not directly attached to the VDL subnetwork are not affected that addressing plan.

4.5.1.3.2 The two principal types of ATN systems which use the VDL subnetwork are aircraft routers and air-ground routers. The VDL address of an aircraft router is comprised of an 8 digit BCD-encoded representation of its ICAO 24-bit aircraft address plus an optional one or two digit subaddress. The VDL address of an air-ground router may simply be its DTE network address as assigned by the network operator to which it is attached.

4.5.1.3.3 A system not directly attached to a VDL subnetwork may be able to call a router attached to the VDL subnetwork by prepending the DNIC of the destination network to the VDL address of the called system.

4.5.1.3.4 The addresses of appropriate air-ground routers must be known by an aircraft router before a call is placed. An aircraft router must have the ability to determine which air-ground routers can be called via a given ground station. Ground stations providing the VDL service will broadcast information about reachable air-ground routers and will allow aircraft routers to call a *default* router without having to know its DTE network address. The specific operation of these VDL functions are specified in the VDL SARPs in Annex 10.

4.5.1.4 ***AMSS Subnetworks***

4.5.1.4.1 The addressing plan for AMSS is treated in the AMSS SARPs in Annex 10. The scope and impact of the AMSS addressing plan is limited to the AMSS subnetwork. Systems not directly attached to the AMSS network are not affected by that addressing plan.

4.5.1.4.2 The two principal types of ATN systems which use the AMSS subnetwork are aircraft routers and air-ground routers. The AMSS address of an aircraft router is generated using BCD-encoded digits as follows:

<AMSS aircraft address> ::	<DNIC> ‘5’ <AES> > <D>
<DNIC> ::	‘1111' (for AOR-E satellite) or ‘1112’ (for POR satellite) or ‘1113’ (for IOR satellite) or ‘1114’ (for AOR-W satellite)
<AES> ::	8-digit BCD-encoded ICAO 24-bit aircraft address
<D> ::	Optional subaddress digit

4.5.1.4.3 The digit ‘5’ following the DNIC is a discriminator indicating that the address refers to an aircraft system. An example AMSS address of an aircraft router in the satellite coverage area of the Atlantic Ocean Region East (AOR-E) satellite may be `1111.5.46721005`.

4.5.1.4.4 The AMSS address of an air-ground router is formatted using BCD-encoded digits as follows:

<AMSS ground address> ::	‘26’ <DNIC> <NTN>
<DNIC> ::	4-digit DNIC of the ground network as registered in CCITT recommendation X.121 or by international convention
<NTN> ::	Up to 9-digit network terminating number (DTE network address) of the air-ground router on the provider’s network.

4.5.1.4.5 The digits ‘26’ comprise a prefix indicating that the address is used to access an internetwork router within the AMSS addressing plan. As an example, a Société International de Télécommunication Aéronautique (SITA) air-ground router's AMSS address may be 26.1116.2331123.

4.5.1.4.6 As part of the routing initiation process over an AMSS subnetwork, aircraft routers are required to place the initial call to the air-ground router. Therefore, the addresses of appropriate air-ground routers must be known before a call is placed. An aircraft router must have the ability to determine which air-ground routers can be called via a given ground station. As the number of air-ground routers connected to the AMSS subnetwork is supposed to be small, this information can be pre-configured into the aircraft router by systems management. Therefore, limited address registration may be required within the scope of the AMSS.

4.5.1.5 ***SSR Mode S Subnetworks***

4.5.1.5.1 The addressing plan for the SSR Mode S Subnetwork is defined in Annex 10, Volume III. The scope and impact of the SSR Mode S subnetwork addressing plan is limited to the Mode S subnetwork. Systems not directly attached to the SSR Mode S subnetwork are not affected by that addressing plan.

4.5.1.5.2 The two principal types of ATN systems which use the Mode S subnetwork are aircraft routers and air-ground routers. The Mode S address of an aircraft router is generated from the ICAO 24-bit aircraft address using BCD-encoded digits as follows:

<Mode S aircraft address> ::	<ICAO 24-bit aircraft address> ‘00’
<ICAO 24-bit aircraft address> ::	Octal representation of the ICAO 24-bit aircraft address coded in BCD

4.5.1.5.3 The total length of the Mode S DTE address of an aircraft router is 10 digits. The subaddress formed by the last two digits of the aircraft SSR Mode S address identifies specific DTEs onboard an aircraft. The subaddress '00' is firmly assigned to the DTE of the aircraft ATN router per Sub-volume V of the ATN technical provisions (Doc 9705-AN/956). An example SSR Mode S DTE address of an aircraft router may be `46721005.00`

4.5.1.5.4 The SSR Mode S DTE address of an air-ground router is a 3-digit BCD-encoded value in the range of 0 through 255. Assignment of ground SSR Mode S DTE addresses is a local issue. However, all DTEs connected to Mode S ground data link processors having overlapping coverage must have unique addresses. This requires some form of bi-lateral or multilateral administrative coordination between neighbouring States when assigning ground Mode S subnetwork addresses.

4.5.1.6 ***Impact of Subnetwork Topology Changes and Outages***

4.5.1.6.1 From time to time, a subnetwork topology may change or an outage may occur which effectively results in changes to the subnetwork addresses. Such subnetwork-related address changes should be transparent to ATN users.

4.5.1.6.2 This is possible, if a change in the subnetwork address does not affect NETs or NSAP addresses (and consequently TSAP, SSAP and PSAP addresses). As illustrated in Table 4-3, the SYS field of the ATN NSAP address uniquely identifies a given end system or router within a routing area through a local identifier. It is a common approach to use the DTE address (e.g. the 48-bit Ethernet address) of the end system or router as the value of the SYS field. However, transparancy of ATN addresses from subnetwork topology changes is only ensured if a SYS field value is assigned which is independent from the end system's or router's subnetwork (DTE) address(es). In this case only the local intra-domain routing tables must be updated when the subnetwork topology or subnetwork addresses changes. These changes are limited to the local routing area and must not be propagated to other routing areas or routing domains.

4.5.2 Internetwork Addressing

4.5.2.1 *General*

4.5.2.1.1 The ATN internetwork addressing plan (i.e. ATN NSAP addressing plan) is defined in Sub-Volume V of the ATN technical provisions (Doc 9705-AN/956). It specifies the structure of ATN NSAP addresses and ATN NETs as well as the abstract syntax, semantic and encoding rules of the individual fields of these addresses. Furthermore, the above-mentioned document defines specific values for some of these address fields and consequently performs the role of a registration authority in part.

4.5.2.1.2 This hierarchical addressing plan reflects the expected (network and routing) topology of the ATN and accommodates the requirements of ATSC and AINSC service users and providers. Strict adherence to this hierarchical addressing plan is required for proper and efficient operation of the ATN internetwork.

4.5.2.2 *The ATN NSAP Address*

4.5.2.2.1 The ATN NSAP address format is illustrated in Figure 4-3. This address format starts with the Initial Domain Part (IDP) which comprises the Authority Format Identifier (AFI) and Initial Domain Identifier (IDI) fields and is followed by the Domain Specific Part (DSP).

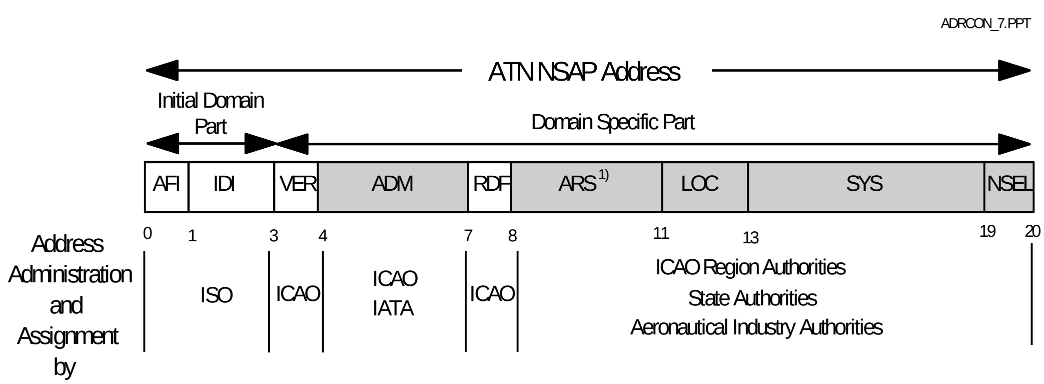


Figure 4-3. ATN NSAP Address Format

1) In mobile network addressing domains, the value of the ARS field is the ICAO 24-bit Aircraft Address and is consequently assigned and administered by ICAO.

4.5.2.2.2 The (decimal) IDP value 470027 forms the common, initial part of all ATN NSAP addresses and NETs, i.e. it is the common fixed address prefix of these addresses. This address prefix defines the ATN Network Addressing Domain as a sub-domain of the Global OSI Network Addressing Domain, as depicted in Figure 4-1.

4.5.2.2.3 The Domain Specific Part (DSP) of the ATN NSAP address format is structured into seven individual address fields. This allows the allocation of ATN NSAP addresses and NETs according to the hierarchical approach mentioned earlier.

4.5.2.2.4 Table 4-3 outlines the ATN NSAP addressing plan. This table describes the complete ATN NSAP address format, semantics and field contents from which NSAP addresses, NETs, NSAP address prefixes and RDIs are derived. Furthermore, Table 4-3 shows the addressing and registration authorities for each of the address fields.

Table 4-3. ATN NSAP Address Definition

Field Name	Size (Octets)	Value / Range	Semantic	Contents	Value Assignment	Addressing Authority	Registration Authority
AFI	1	47 (decimal)	ISO 6523 ICD IDI and binary DSP format	47	Fixed	ISO	ISO/IEC 8348
IDI	2	00 27 (decimal)	ATN NSAP Address	00 27	Fixed	ISO	British Standards Institute (BSI)
VER	1	01 (hex) 41 (hex) 81 (hex) c1 (hex)	Ground AINSC NSAP Address Mobile AINSC NSAP Address Ground ATSC NSAP Address Mobile ATSC NSAP Address	01 41 81 c1	Fixed Fixed Fixed Fixed	ICAO Doc 9705 - AN/956 Sub-volume V	ICAO (ICAO Doc 9705 - AN/956, Appendix 5, Chapter 5.4)
ADM	3	*00 00 00 - ff ff ff (hex)*	ATN Network Address (Sub-) Domain Authority	ISO Country Code, or ICAO Region Identifier, or IATA Airline or Aeronautical Stakeholder Designator	Fixed Fixed/Variable [2] Fixed	ICAO Doc 9705 - AN/956 Subvolume 5	ISO 3166 ICAO Doc 9705 - AN/956 Sub-volume V IATA Doc xxx
RDF	1	0	Unassigned	0	Fixed	ICAO Doc 9705 - AN/956 Sub-volume V	ICAO Doc 9705 - AN/956 Sub-volume V
ARS	3	*00 00 00 - ff ff ff (hex)*	Routing Domain (in Ground Network Addressing Domains) Aircraft or Routing Domain (in Mobile Netw. Addr. Domains)	Not defined (for Ground Netw. Addressing Domains) ICAO 24-bit Aircraft Address (for Mobile Netw. Addressing Domains)	Variable Fixed	ICAO Doc 9705 - AN/956 Sub-volume V	ATN Network Addressing (Sub-) Domain Authority defined in ADM field ICAO
LOC	2	*00 00 - ff ff (hex)*	Routing Area (in Ground Network Addressing Domains) Routing Domain or Routing Area (in Mobile Netw. Addr. Domains)	Not defined Not defined	Variable	ICAO Doc 9705 - AN/956 Sub-volume V	ATN Network Addressing (Sub-) Domain Authority which contains the parent Routing Domain
SYS	6	*00 00 00 00 00 00 - ff ff ff ff ff ff (hex)*	ATN System	Not defined	Variable	ICAO Doc 9705 - AN/956 Sub-volume V	ATN Network Addressing (Sub-) Domain Authority which contains the parent Routing Area

[2] When used to identify an ICAO Region, only the first octet of the ADM field contains the fixed ICAO Region Identifier, while the values of the remaining two octets are assigned by the identified ICAO Region.

N-SEL	1	*00 - ff* *(hex)*	Network Entity or Network Service User	fe (NE implementing optional non-use of IDRP) 00 (all other NEs) Remaining values not defined	Fixed Fixed Variable	ICAO Doc 9705 - AN/956 Sub-volume V	ICAO Doc 9705 - AN/956 Sub-volume V ICAO Doc 9705 - AN/956 Sub-volume V Locally

4.5.2.2.5 As shown in Table 4-3, four of the nine fields of an ATN NSAP address or NET have already fixed values allocated by the ATN technical provisions. The values of the remaining five fields, marked as v*ariable* in Table 4-3 and highlighted by grey boxes in Figure 4-3, may be allocated as follows:

ADM The ADM field is used to further break down the Ground and Mobile ATSC NSAP Addressing Domains and the Ground and Mobile AINSC Addressing Domains into a set of subordinate network addressing (sub-)domains to allow devolved administration of each resulting (sub-) domain by an ICAO Region, State, airline or aeronautical organisation. The value of the ADM field, combined with the values of the preceding fields, forms the NSAP address prefix of each such ATN NSAP addressing (sub-) domain and consequently of all NSAP addresses and NETs administered by a given ICAO Region, State, airline or aeronautical organisation.
Each State, airline or other organisation participating in the ATN is expected to be responsible for exactly one such addressing sub-domain and to perform the address allocation and establishment of subordinate registration authorities, if required, within its area of responsibility. Alternatively, States or ATS providers may opt to register (a subset of) their systems under the network address space associated with the relevant ICAO Region. This approach would relieve these States and organisations from being responsible for their own network addressing (sub-)domain (i.e. from operating their own registration facilities and procedures) and would support the efficient advertisement of routing information, as required by the ATN Routing Policies.
In the case of the ATSC addressing domains (i.e. for the ATN NSAP address prefixes *47 0027 81* and *47 0027 c1*) the ADM field either contains the three-character alphanumeric ISO country code, as defined in ISO 3166, of the State responsible for the relevant addressing sub-domain, or the one-octet ICAO Region Identifier (with the remaining two octets assigned within the responsibility of the identified ICAO Region) which is responsible for the relevant addressing sub-domain.
If the case of the AINSC addressing domains (i.e. for the ATN NSAP address prefixes *47 0027 01* and *47 0027 41*) IATA is the responsible registration authority for the ADM field values. After receiving applications from airlines and other aeronautical organizations, IATA will assign ADM field values according to its own procedures.

ARS In Ground Network Addressing Domains (i.e. for the ATN NSAP address prefixes *47 0027 01* and *47 0027 81*) the purpose of the ARS field is to distinguish routing domains operated by the same State, airline or organisation. In this case, the value of the ARS field, when combined with the values of the preceding fields, identifies a network addressing sub-domain that corresponds to an ATN routing domain. Each ICAO Region, State, airline or other aeronautical organisation identified by the value in the ADM field will be responsible for establishing one or more such network addressing sub-domains according to their local routing requirements and for the assignment of appropriate ARS field values to the corresponding routing domains. ARS field values should be assigned in a manner that supports efficient routing information exchange through appropriate address information reduction. This means, for example, that adjacent routing domains should be assigned the longest possible NSAP address prefix.

In Mobile Network Addressing Domains (i.e. for the ATN NSAP address prefixes *47 0027 41* and *47 0027 c1*) the purpose of the ARS field is to identify the aircraft on which the addressed ATN system is located. When the ATN systems onboard an aircraft form a single routing domain, then the ARS field also identifies the routing domain. In the case of an Mobile Network Addressing Domain the ARS field value is the aircraft's ICAO 24-bit aircraft address encoded as an hexadecimal value.

LOC In Ground Network Addressing Domains (i.e. for the ATN NSAP address prefixes *47 0027 01* and *47 0027 81*) the purpose of the LOC field is to distinguish routing areas within the same routing domain. In Mobile Network Addressing Domains (i.e. for the ATN NSAP address prefixes *47 0027 41* and *47 0027 c1*) the purpose of the LOC field is to distinguish routing areas within the same routing domain, if only one routing domain exists onboard the aircraft. When more than one RD is located on a single aircraft, the LOC field distinguishes each such RD and the routing areas contained within them.
The assignment of the LOC field value is under the responsibility of the organisation which constitutes the addressing authority for the routing domain in which the identified routing area is contained. LOC field values should be assigned in a manner that supports efficient routing information exchange through appropriate address information reduction. This means, for example, that adjacent routing areas should be assigned the longest possible NSAP address prefix.

SYS The SYS field is used to uniquely identify an ATN end or intermediate system within a given routing area. The assignment of the SYS field value is under the responsibility of the organisation which constitutes the addressing authority for the routing area in which the identified ATN system is contained. The SYS field should be assigned a meaningful value within the context of the given routing area. For example, if the ATN system is attached to an Institute of Electrical and Electronic Engineers (IEEE) 802 local area network, then a common approach is to use the LAN address of the system as the value of the SYS field.

N-SEL The N-SEL field is used to identify either a network layer entity (such as the IDRP protocol machine) or a network service user within the context of a given ATN system. The assignment of the N-SEL field value is a matter local to the administrator of the ATN system, except for the cases of the NE of an intermediate system. For these cases, Chapter 5.4 of the ATN Technical Provisions (Doc 9705-AN/956) has assigned appropriate N-SEL field values.

4.5.2.3 ***The Network Entity Title***

4.5.2.3.1 A NET is the name of a network layer entity in an ATN system. If an ATN system has exactly one network layer entity, the NET in fact "names" the entire system. Furthermore, as ATN NETs are derived from the ATN addressing plan, they may also be used to locate a given system, or as a source from which address prefixes of all systems within a given routing domain can be derived.

4.5.2.3.2 For internetwork addressing consistency within the ATN, the NET and all NSAPs in use on a given system should only differ by the value of the N-SEL field per Table 4-3.

4.5.2.4 ***Relationship To ATN Routing***

4.5.2.4.1 In order to support the ATN routing concept, the ATN NSAP addressing plan must be strictly followed, especially with regards to the registration and use of ADM and ARS values. As the NSAP addressing plan is based on the expected ATN topology, it has been defined hierarchically allowing routing information to be managed efficiently. Specifically, address prefixes comprising of simply an administrative domain identifier or routing domain address may be used to describe routes to all systems within a given domain. For example, the IDRP protocol may be used to indicate that a given router has routes to all systems in a given administration or airline rather than identifying every system individually.

4.5.2.4.2 During the initial ATN time frame, IDRP may not be supported over the mobile subnetworks by all aircraft routers. The N-SEL field of the ATN NSAP addressing plan is currently used to indicate the IDRP capability of the aircraft router. In the case of a non-IDRP equipped aircraft the routing initiation process will ensure that both the air-ground and aircraft routers will have enough information about each other and their corresponding communications capabilities. The air-ground router can derive the routing domain address of the aircraft from the received NET of the aircraft router and forward it to other domains requiring this information. On the other hand, the aircraft router must have some pre-configured knowledge of the reachability of destination systems via a given air-ground router as there may not be any means of dynamically advertising route information to all aircraft.

4.5.2.5 ***Impact of Topology Changes and Outages***

From time to time, the ATN internetwork topology may change or an outage may occur which effectively result in changes the internetwork topology. Because the ATN is expected to be used for air traffic management applications, operational availability must be very high and therefore the effects of ATN internetwork topology changes should be transparent or minimal to ATN users. There are two aspects to be considered: Planned or unforeseen changes.

4.5.2.5.1 **Planned Changes**

4.5.2.5.1.1 If a system is moved to another routing area or another routing domain or if routing areas or routing domains are reconfigured, new NSAP addresses or NETs must be assigned and all other operators affected must be informed well in advance. A period of time in which a system maintains two or more NSAP addresses for the same NSAP may also ease the transition. If this is the case, IDRP-equipped routers may broadcast the reachability of a given system by both its old and new addresses for a limited time, thus minimising the overall impact of the change.

4.5.2.5.1.2 Reconfiguration of the network topology inside a routing area or inside a routing domain, which is not partitioned into routing areas, should be made transparent to ATN users, i.e. the NSAP address should not be changed.

4.5.2.5.2 **Unforeseen Changes**

4.5.2.5.2.1 Unforeseen changes may occur due to failure of a given end system or router. If an end system fails, a standby or backup system must be available to avoid loss of communication. If a router fails, either a standby or backup router or a redundant path may guarantee operational availability of the system. In the latter case, the problem is rectified by routing procedures which re-route packets through alternative paths.

4.5.2.5.2.2 If a stand-by end system or router replaces the failed system, the replacement system should effectively adopt the NSAP address or NET of the failed system and the local routing tables should be updated to indicate the local topology change, thus ensuring the availability of ATN services. The effects of such failures are not propagated outside of the local domain.

4.5.3 **Transport, Upper Layer and Application Addressing**

4.5.3.1 According to ISO 7498-3, a TSAP, SSAP and PSAP address is composed of a globally unique NSAP address plus a local transport selector (T-SEL), session selector (S-SEL) and presentation selector respectively, as illustrated in Figure 4-4. This means that the ATN NSAP, TSAP and SSAP address of a given system can be derived from the address of an application, i.e. PSAP address, hosted by this system by cutting off the relevant selectors. In the same way the TSAP, SSAP and application addresses within a system can be constructed from the NSAP address using a priori knowledge of the local selector values.

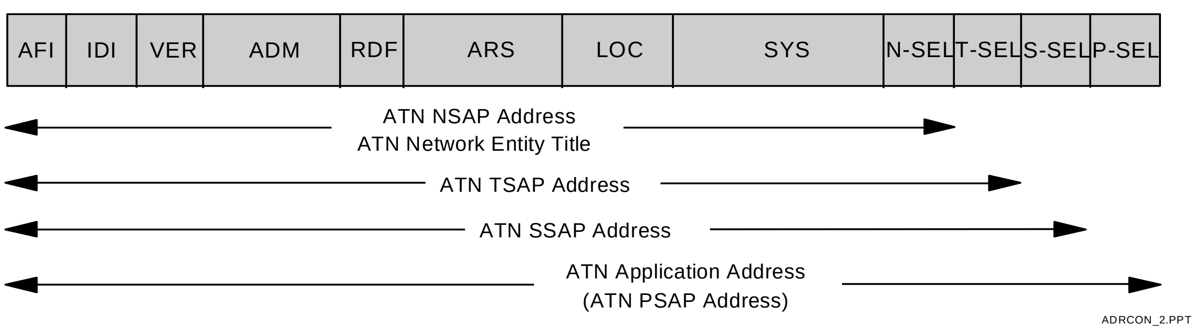


Figure 4-4. Relationship of Network Addresses and Upper Layer/Application Addresses within a given ATN End System

4.5.3.2 For initial implementations, the ATN address formats shown in Figure 4-4 apply to AMHS Servers, AMHS User Agents and AFTN-AHMS Gateways as specified in Sub-Volume III of the ATN Technical Provisions (Doc 9705-AN/956), whereas for datalink applications, AIDC applications and the AFTN/ATN Type A Gateway the session selector (S-SEL) and presentation selector (P-SEL) will be null. This means that the address of this latter group of ATN applications has exactly the same form as the TSAP address. As a consequence, the TSAP address is sufficient to unambiguously identify and locate ATN datalink applications, AIDC applications and AFTN/ATN Type A Gateways.

4.5.3.3 The format of the application address, i.e. PSAP address, of an ATN datalink application, an AIDC application and an AFTN/ATN Type A Gateway is illustrated in Figure 4-5.

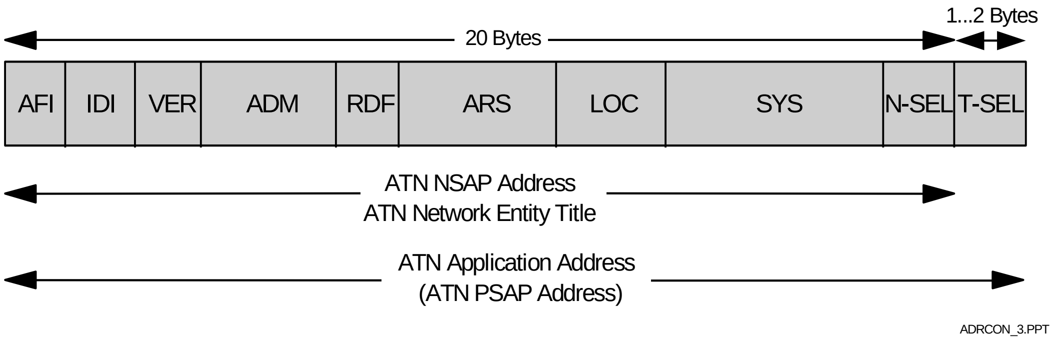


Figure 4-5. ATN Application Address Format for ATN Datalink Applications, AIDC Applications and AFTN/ATN Type A Gateways

4.5.4 Application Naming

4.5.4.1 *General*

4.5.4.1.1 Application names are generally referred to as *AP-titles* and must be globally unique within the ATN context. The abstract syntax of AP-titles (and also of AE-titles and AE-qualifiers) is defined in ISO/IEC 8650. This standard defines two syntactic forms of each type of a name: an object identifier (OID) form and a directory name form. Application names are defined in the form of OIDs in ATN technical provisions.

4.5.4.1.2 Following ISO naming principles (ISO 7498-3), consistency of all application names used in the ATN can be ensured by assigning them according to a well-defined ATN application naming tree. Figure 4-6 illustrates the ATN application naming tree in the object identifier form. This naming tree is under the ultimate authority of ISO.

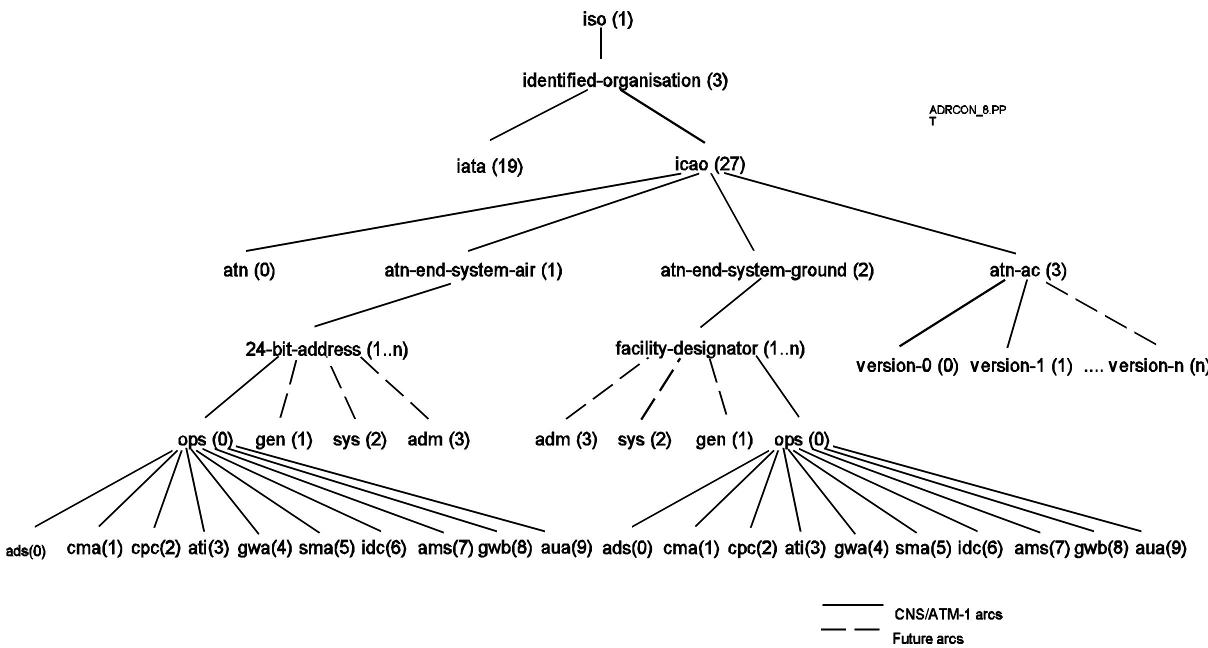


Figure 4-6. OID Form of the ATN Application Naming Tree

4.5.4.2 *Object Identifier Form of Application Names*

4.5.4.2.1 The object identifier form of an AP-title and AE-title respectively is the sequence of all object identifier components in the order of the assignment by the individual registration authorities. An object identifier component is an integer value, together with an (optional) component name.

4.5.4.2.2 ISO/IEC 8824 specifies the top of this hierarchical name space. It has the following three entries, i.e. object identifier components, in its register:

Component Name	Integer Value
ccitt	0
iso	1
joint-iso-ccitt	2

4.5.4.2.3 The ISO name space has been selected as the root of the ATN application naming tree. This name space is further subdivided by ISO/IEC 8824 into:

Component Name	**Integer Value**
standard	0
registration-authority	1
member-body	2
identified-organisation	3

4.5.4.2.4 ICAO has requested the allocation of an International Code Designator (ICD) and has obtained the ICD "0027" according to the dictates of ISO 6523. This corresponds to the object identifier (OID) "icao (27)", where "icao" represents the component name and "27" the integer value. This assignment allows ICAO to establish its own name space within the name space associated with the object identifier "identified-organisation (3)" and to assign sub-authorities as needed.

4.5.4.2.5 Sub-Volume IV of the ATN Technical Provisions (Doc 9705-AN/956) is currently the authority for this name space; it defines 4 entries, i.e. object identifier components, in this name space at the highest level:

Component Name	**Description**	**Integer Value**
atn	General ATN identifier	0
atn-end-system-air	ATN mobile end system	1
atn-end-system-ground	ATN ground end system	2
atn-ac	ATN application context name	3

4.5.4.2.6 Under the "atn-end-system-air (1) name space an object identifier component whose values correpond to the IACO 24-bit aircraft address is specified. Likewise, under the "atn-end-system-ground (2)" name space, an arc whose values correspond to the ICAO Facility Designator is specified.

4.5.4.2.7 According to ATN technical provisions, ATN AP-titles are allocated underneath either of these object identifiers. For the initial implementation, the object identifier component "ops (0)" has been assigned; other identifiers at this level (illustrated by dashed lines in Figure 4-6) are subject to future extension.

Examples

Referring to the ATN naming tree illustrated in Figure 4-6, the object identifier form of an AP-title of an application process hosted by a mobile ATN end system is:

{1 3 27 1 n 0} where n is the integer value of the ICAO 24-bit aircraft address of the aircraft carrying the ATN end system which hosts the AP.

The object identifier form of an AP-title of an application process hosted by a ground ATN end system is:

{1 3 27 2 n 0} where n is the integer value corresponding to the ICAO Facility Designator of the location of the ATN end system which hosts the AP.

4.5.4.2.8 Under the arc "iso (1) identified-organisation (3) icao (27) atn-ac (3)" ATN SARPs defines the name space of ATN application context names. There are currently two object identifier components allocated under this arc: "version-0 (0)" and "version-1 (1)". Additional components may be allocated by future amendments to ATN SARPs (illustrated by dashed lines in Figure 4-6).

Example

Referring to the ATN naming tree illustrated in Figure 4-6, the object identifier form of an application context name for ATN applications is:

{1 3 27 3}.

4.5.4.2.9 The object identifier form of an AE-title is constructed by appending the object identifier form of the AE-qualifier (in its integer value form) to the sequence of object identifier components that comprise the object identifier of the associated AP-title. In the ATN application naming tree of Figure 4-6 the object identifier values for the ATN AE-qualifiers are illustrated beneath the object identifier for the ATN AP-titles. Sub-Volume IV of Doc 9705 defines ten entries in the register for ATN AE-qualifiers. These are defined along the type of the ATN application service entities (ASEs):

Table 4-4. ATN AE-Qualifier Names and Values

Component Name	Description	Integer Value
ADS	AE-qualifier for ADS application	0
CMA	AE-qualifier for Context Management Application	1
CPC	AE-qualifier for Controller Pilot Data Link Communication	2
ATI	AE-qualifier for Automatic Terminal Information Services	3
GWA	AE-qualifier for Type A Gateway	4
SMA	AE-qualifier for Systems Management Application	5
IDC	AE-qualifier for ATS Inter-Facility Data Communications	6
AMS	AE-qualifier for ATS Message Server	7
GWB	AE-qualifier for AFTN-AMHS Gateway	8
AUA	AE-qualifier for ATS Message User Agent	9

4.5.4.2.10 Consequently, the complete sequence of object identifier components from the root of the ATN application naming tree to the last level of the hierarchy in Figure 4-6 provides the object identifier form of an ATN AE-title.

Example

The object identifier form of the AE-title of the CPDLC AE contained in an AP hosted by a mobile ATN end system is:

{1 3 27 1 n 0 2} where n is the integer value of the ICAO 24-bit aircraft address of the aircraft carrying the ATN end system which hosts the given AP and the last digit, i.e. 2, is the AE-qualifier.

4.5.4.2.11 In the future, it is likely that the ATN object identifier tree illustrated in Figure 4-6 will have further levels of structure including other information objects such, as security registration identifiers, managed objects, etc.

4.5.4.3 *Directory Name Form of Application Names*

4.5.4.3.1 **General**

4.5.4.3.1.1 Whereas the OID form of AP-titles, AE-titles and AE-qualifiers has some benefits in terms of efficiency when passing naming information in the protocol control information (PCI) field of ATN application protocols, the directory name form provides a much more user-friendly representation of application names.

4.5.4.3.1.2 Once established, such a naming scheme can be used as a directory scheme, when directory services will be provided to ATN users. A directory scheme is a set of rules and constraints concerning the Directory Information Tree (DIT) structure and its contents. These rules ensure that the contents are valid entries and contain valid information. They define, what the user can do with entries and their contents.

Note.— Even if no OSI Directory Service is intended to be used within the initial ATN time-frame, it is highly recommended to use the principles described in the OSI Directory standard.

4.5.4.3.1.3 The directory name form of an AP-title is the sequence of all relative distinguished names (RDNs) in the order of the assignment by the individual registration authorities. This ordered sequence of RDNs is referred to as Distinguished Name. A RDN consists of two elements: an attribute type and an attribute value. The attribute type is an Object Identifier characterising the name field and the attribute value is an International Alphabet No. 5 (IA5) string for the name itself.

4.5.4.3.1.4 The directory name form of an AE-qualifier is a relative distinguished name, which is unambiguous within the scope of the associated application process.

4.5.4.3.1.5 The directory name form of an AE-title is constructed by appending the relative distinguished name form of the AE-qualifier to the directory name of the associated AP-title.

4.5.4.3.1.6 Currently no AP-titles and AE-qualifier in the form of directory names or relative distinguished names are assigned to ATN APs and AEs.

4.5.4.3.1.7 Figure 4-7 shows a proposed ATN Application Naming Tree structure for ATN application processes and application entities following the DIT approach.

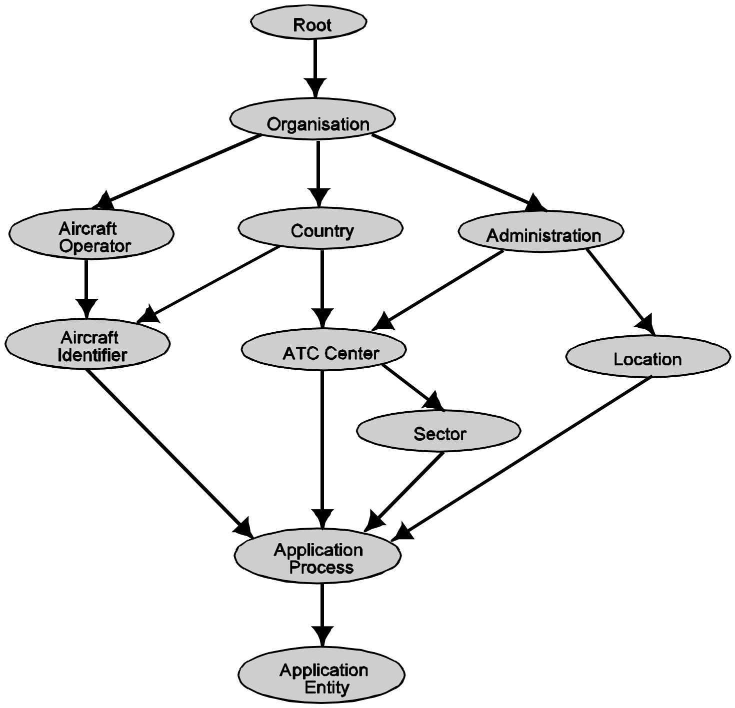


Figure 4-7. DIT Form of Proposed ATN Application Naming Tree

4.5.4.3.1.8 The ATN DIT of Figure 4-7 contains the following object classes:

a) Organisation (O): This object class is directly subordinate to the root. It is used to identify either ICAO or IATA as the top level international authority under which the object will be registered.

b) Administration (ADM): This object class may be used to identify either ATSC administrations (e.g. national CAAs, Eurocontrol etc.) or AINSC organisations (e.g. airlines).

c) Country (C): The country object class may be used instead of the administration object class to identify national CAAs. It shall contain the three letter ISO country code.

d) Aircraft Operator (AO): This object class shall be used to identify the aircraft operator (in the context of IATA).

e) Aircraft Identifier (AI): This object class shall be used for all aircraft applications or other names to identify objects on board.

f) ATC Centre (ATCC): This object class shall contain the ATCC name for all ATSC applications or other names to identify objects located in an ATCC.

g) Location (L): This object class shall identify the location of a ground located AINSC application.

h) Sector (SE): It may be useful to distinguish between different control sectors in an ATCC. This object class may be used to identify a control sector.

i) Application Process (AP) and Application Entity (AE): These object classes shall be used to identify the type of the ground or aircraft ATSC or AINSC application. The AE object class is always subordinate of the AP object class, while the AP object class may be subordinate to Sector, ATC Centre, Location or Aircraft Identifier.

Note.— Besides APs and AEs other object classes may be added to the proposed DIT of Figure 4-7 in the future, if other name types need to be standardised, e.g. end system or server names, user or user group names etc.

4.5.4.3.2 **Ground-Based ATM Applications**

The following are examples for ground based ATM application names:

Note.— AE types have not been identified yet. Therefore, only AP names are listed in the following examples.

a) Example for an Automatic Dependent Surveillance (ADS) application running in sector “SR 1” in the ATCC Munich:

O	=	ICAO
ADM	=	DFS
ATCC	=	Munich
SE	=	SR 1
AP	=	ADS

b) Same example as above, but using the ISO country code instead of an administration identifier:

O	=	ICAO
C	=	DE
ATCC	=	Munich
SE	=	SR 1
AP	=	ADS

4.5.4.3.3 **Aircraft ATM Applications**

Example for a Controller Pilot Communications (CPC) operated in a Lufthansa aircraft:

O	=	IATA
AO	=	LH
AI	=	46721005
AP	=	CPC

4.5.4.3.4 **Other Ground-Based Applications**

Example for a Flight Information Service (FIS) application operated by Lufthansa operational centre in Munich:

O	=	IATA
ADM	=	Lufthansa
L	=	Munich
AP	=	FIS

4.5.4.4 ***AE-Title***

4.5.4.4.1 Application entities (AEs) are each named in terms of a unique Application Entity Title (AE-title) which consists of an AP-Title and an AE-qualifier.

4.5.4.4.2 In initial implementations, the type of the application entity (AE) is the same as the type of the application service entity (ASE) of the ATN application. For example, an ADS AE will contain only an ADS ASE and an appropriate ACSE. Thus, on connection establishment the title of the peer application entity (AE-title) can be completly constructed as follows: The variable part of the AP-title is the peer end system identifier and is provided by the "Called/Calling Peer ID" value in the dialogue service. The peer AE-qualifier value is the type of the ATN application and is the same as the receiving application's AE-qualifier value.

4.5.4.5 ***Application Context Name***

An application context name is used to distinguish between different instances of an application context within the scope af a given AE type. It is exchanged during connection establishment. In initial implementations, the application context name is a simple construct since the ASE list can be inferred from the AE-title.

4.5.5 **ATN Name and Address Cross-Reference**

The following table provides an overview of the individual components of ATN names and addresses, and gives reference to the detailed specification of these addressing/naming components in terms of syntax, semantics, ecoding and value range. References are provided with respect to both the ATN technical provisions and relevant ISO/IEC standards.

Table 4-5. Overview of ATN Address and Name Specifications

	ATN System Providing								
	Automatic Dependent Surveillance	Controller Pilot Data Link Communications	Automatic Terminal Information Services	Context Management	ATS Inter-Facility Data Communications	Type A Gateway	ATS Message Server	ATS Message User Agent	AFTN-ATN Gateway
AE-Qualifier	ADS	CPC	ATI	CMA	IDC	GWA	AMS	GWB	AUA
AP-Title	Specified in ATN SARPs,Sub-volume IV,Section 3.2.2								
P-SEL	Null							Specified in ISO 11188-1, Section 7.2	
S-SEL	Null							Specified in ISO 11188-1, Section 9.3	
T-SEL	Specified in ATN SARPs, Sub-volume V, Chapter 5.4								
NSAP	Specified in ATN SARPs, Sub-volume V, Chapter 5.4								
SNPA	Specified in ICAO Annex 10 and relevant ISO/IEC Standards								

4.6 Name and Address Resolution

4.6.1 General

4.6.1.1 For distributed ATN air-ground applications, such as automatic dependent surveillance (ADS) and controller-pilot data link communications (CPDLC), name-to-address-resolvement is achieved through the Context Management Application (CMA) which is defined in Sub-Volume II of the Manual of Technical Provisions for the ATN (Doc 9705-AN/956). CMA is a critical function allowing systems onboard an aircraft or within a given ATC facility (or FIR) to identify their service capabilities (applications) and their corresponding addresses to each other. It should be noted however that CMA provides limited capabilities in a limited context.

4.6.1.2 In initial implementations, the mapping between ground application names and corresponding addresses may be resolved *a priori*, i.e. based on static information configured into the ground ATN systems. This assumption is not unreasonable, especially for applications such as AIDC which will likely have few address and name changes. However, the scalability of the ATN may be limited by requiring that all ATN applications individually maintain addressing information about all other applications with which they may need to communicate. In the longer term, ICAO may pursue the definition of a naming tree allowing the development of ATN directory services to support the potential growth of ATN.

4.6.2 Context Management as Basic Directory Service

4.6.2.1 This section introduces the use of the CMA as basic name-to-address resolver for ATSC applications distributed between aircraft and ground-based systems. Further and more detailed information about the context management application can be found in Part 3 of this Manual.

4.6.2.2 The CMA provides a basic directory service with the following capabilities:

a) The ground-based CM application may determine the ATSC application capabilities of a given aircraft and determine the addresses of relevant aircraft ATSC applications.

b) The aircraft CM applications may determine the ATSC application capabilities within the scope of the ground-based CM application (which may be for example a given FIR) and may determine the addresses of relevant ground ATSC applications.

c) The ground-based CM function may advertise the update of relevant ground based ATSC application addresses to the aircraft CM application.

d) The ground-based CM function may direct its aircraft peer CM to contact another ground-based CM application, perhaps in another FIR.

4.6.2.3 Once an aircraft has "logged on" using the CMA, the onboard systems are able to determine the application addresses of ATSC applications available from the logged-on ground CMA. The ground CMA may for example provide address information about all "accessible" ATSC applications within an ATCC. Correspondingly, the local control region's ATCC will know the aircraft's ATSC application capabilities and their respective ATN application addresses and names at completion of logon. The logon process can be described as follows:

a) Assuming one does not already exist, the aircraft's CMA establishes a transport connection with the CMA in the control region currently responsible for the aircraft. To do so, the aircraft is required to know which control region it is in and the corresponding address of the CMA application.

Note.— In the absence of generalised directory services, it may be worthwhile to establish default CMA application addresses within each ATN equipped control region. This would simply mean defining, at the ICAO level, fixed ARS, LOC, SYS, NSEL, TSEL for the ground CM applications. The RDI of a given control region can be derived from the name of the control region, presumably already known by the aircraft. The aircraft CMA would then append the predefined values of the above-listed fields to the RDI identifier to produce the required CMA address.

b) The aircraft CMA sends a *CMLogonRequest* message indicating the aircraft flight identification (its flight number), and an associative list of application names and addresses. The application names are in fact currently defined to simply be 3-character *Application IDs*. It is assumed that the ATCC can derive the full application name from the associated addressing information and flight identification. At this point, the ATCC will be able to associate the aircraft, identified in the flight plan by its flight identification, to the supported ATM applications and their corresponding addresses.

c) If the ground CMA is able to support the logon request, it sends a *CMLogonResponse* message indicating that the aircraft logon request has been accepted along with an associative list of applications and their associated application addresses similar to the aircraft's list. At this point, the aircraft will be able to associate the ATM applications supported by the ATCC with their corresponding applications addresses.

4.6.2.3.1 Following the logon procedure, peer application names and addresses can be distributed within the aircraft and ATCC domains by local means. At this point, ATM applications may now communicate between the aircraft and ATCC. If, for some reason, the ground application addresses change, the ATCC may send an updated associative name/address list to the aircraft. Additionally, to support transfer of control to the aircraft's next control region, the ATCC may send a *ContactRequest* message to the aircraft CMA indicating the next control centre's CMA address.

4.6.2.4 ***Resolution of ATN Application Address***

4.6.2.4.1 Following the establishment of the application context between an aircraft CMA and a ground-based CMA, the aircraft CMA provides pairs of information comprising:

a) an identifier for the type of ATSC application available onboard the aircraft; and

b) address fragment of the associated application.

4.6.2.4.2 The address fragment provided by the CMA is either a so called “Long TSAP” or a “Short TSAP”. The “Long TSAP” is the Domain Specific Part (DSP) of an ATN address (see section 7.5.2.1) plus the TSAP selector, and contains the values of the VER, ADM, RDF, ARS, LOC, SYS, N-SEL and T-SEL fields of the ATN TSAP address. It is illustrated in the upper address structure of Figure 4-7. The “Short TSAP” contains the values of the ARS, LOC, SYS, N-SEL and T-SEL fields of the ATN TSAP address and is also illustrated in Figure 4-7.

4.6.2.4.3 The full PSAP address of the associated aircraft application is generated by the ground CMA by adding the fixed 3-bytes Initial Domain Part (IDP) of the ATN PSAP address, i.e. 47 00 27, as prefix to the received “Long TSAP” and by inserting the ICAO 24-bit aircraft address between the received VER and RDF field values, as illustrated in the lower address structure of Figure 4-7.

Note.— To restore the full PSAP address of the aircraft application, the ICAO 24-bit aircraft address must be known to the ground CMA through a priori knowledge. This a priori knowledge may be, for example, information contained in the flight plan.

Note.— The “long TSAP” structure may be reduced by 1 byte, if the RDF field value is omitted. This field has the fixed value “00” which can be restored on the ground and inserted within the received TSAP fragments.

4.6.2.4.4 The full PSAP address of the associated aircraft application can be generated by the ground CMA from a received “Short TSAP” fragment only if a “Long TSAP” fragment has been received previously. In this case, the VER and ADM field values are restored from the last received “Long TSAP” fragment and added together with the fixed IDP (47 00 27 decimal) and the fixed ARS field value (ICAO 24-bit aircraft address) to the received “Short TSAP” fragment.

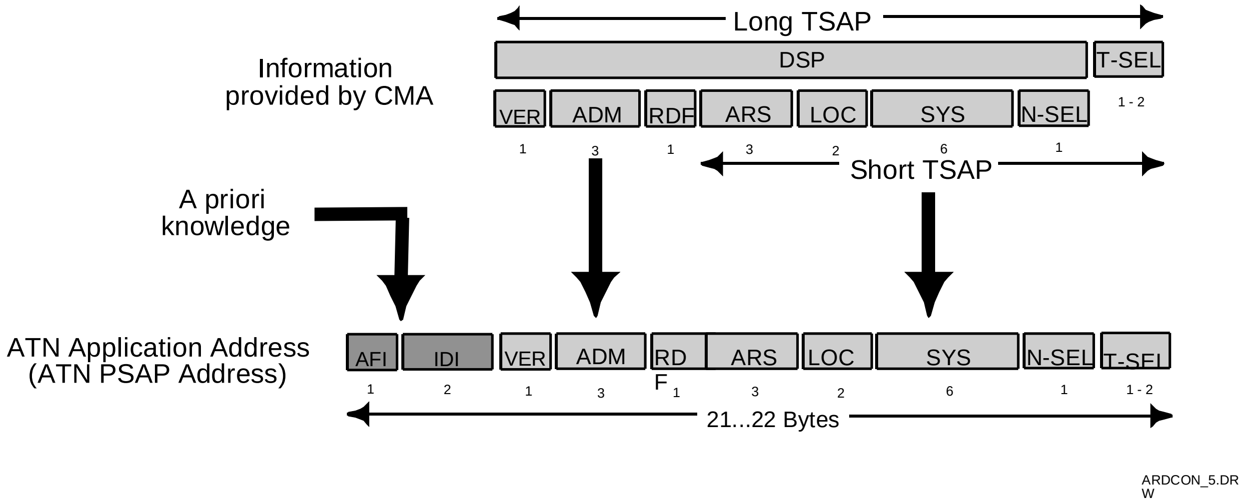


Figure 4-8. Generation of ATN Application Address From Received CM Information

4.6.2.5 ***Resolution of ATN AE-Title***

4.6.2.5.1 From the received aircraft application type identifier (see Table 4-4) the AE-qualifier of the associated application can be derived on the ground by a simple mapping procedure.

4.6.2.5.2 By adding the ICAO 24-bit aircraft address as prefix to the retrieved AE-qualifier, the full AP-title of the aircraft application can be generated on the ground.

4.6.2.5.3 Consequently, the ground CMA can completely resolve the addresses and names of the aircraft applications from the received CM information, following the procedures described above.

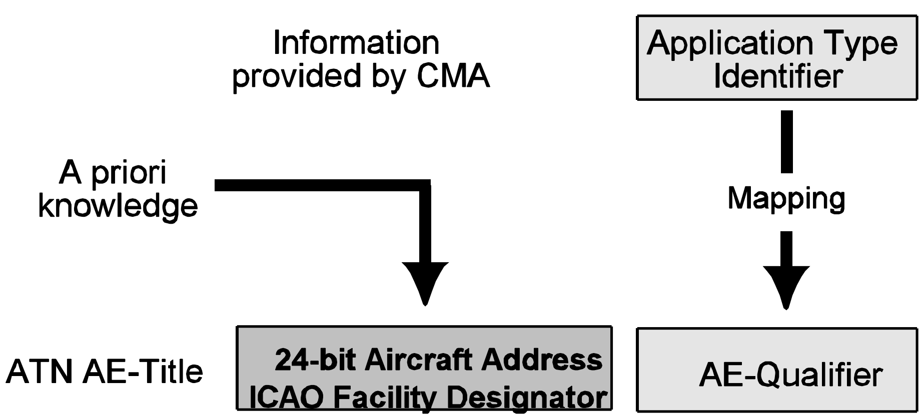


Figure 4-9. Generation of ATN AE-Title From Received CM Information

4.6.2.5.4 On request of the aircraft CMA or triggered by a change in its local information repository, the ground-based CMA transmits to the aircraft CMA information pairs comprising:

a) an identifier for the type of ATSC application available on the ground; and

b) address fragments of the associated application.

4.6.2.5.5 The name and address resolution can be performed onboard the aircraft in the same way as described above and illustrated in Figures 4-7 and 4-8.

4.6.2.5.6 The full AE-title of the ground applications is generated by concatenating the ICAO Facility Designator of the ground CMA to the AE-qualifier derived from the transmitted information concerning the application type.

4.6.2.5.7 The full PSAP address of the ground applications is restored from a priori knowledge about the PSAP IDP prefix (which is constant "47 00 27") and the received "long or short TSAP" fragments respectively, as described above. However it is currently undefined from which information the ARS field value of the PSAP address of the ground application is restored. It may be derived from the destination TSAP address used by the aircraft system when establishing the initial transport connection with the ground CMA server. However, such an approach would limit the scope of the address information provided by the ground CMA. As the ADS field value of the CMA is used to construct the PSAP address of the ground ATSC applications, these applications must be hosted by end systems which are located in the same routing domain as the ground CMA server.

4.6.3 Application Layer Directory

Each AE is associated with one or more PSAPs and hence the AE-title is associated with the corresponding PSAP addresses. The AE-title is mapped onto a PSAP address by means of an application layer directory function. This directory function provides a mapping from the AE-title into the presentation address required to access the referenced application entity.

4.7 ATN Name and Address Registration

Name/address registration is the mechanism through which a name/address assigned to an object is made available to interested parties. It is carried out by a naming/addressing registration authority (called registration authority in the following).

4.7.1 Registration Authority

4.7.1.1 A registration authority may be an organisation, a document, an automated facility, or any other body capable of name/address assignment that performs registration of one or more types of objects within its jurisdiction. The set of name/address values administered by a single registration authority consitutes the naming/addressing domain of this authority.

Note.— A registration authority is a specific instance of a naming/addressing authority (see section 7.3.3). A naming/addressing authority defines formats and/or values of names/addresses and assigns such values to entities.

Note.— According to this definition, the ATN SARPs constitute an international naming/addressing authority, as they define formats and values of ATN names and addresses (or components of those respectively) for objects such as ATN network layer entities or ATN application processes, at the international level.

4.7.1.2 The role of a name/address registration authority according to ISO/IEC 9834-1 is:

a) to assign and make available unambiguous names and addresses: and

b) to record definitions of the objects to which names and addresses are assigned.

4.7.2 General Procedures for Registration of ATN Objects

4.7.2.1 With regard to the initial assignment of names, addresses and definitions to objects and of subsequent additions to the register, each registration authority for ATN names/addresses should:

a) receive proposals for register entries from applicants[3];

b) process received proposals for register entries, i.e. effect any necessary rationalisation or coordination of these proposals, such as verification of responsibility of registration authority, verfication of the qualification of the applicant, verification of the compliance of the proposal with the relevant ATN provisions;

Note.— There is a need to specify the method used to determine whether a request for registration or deletion is accepted or refused

c) record names/addresses for each register entry that is accepted in accordance with the specified procedures;

Note.— The contents of a register entry should include at least
— the name/address assigned to the object
— the name of the organisation that proposed the entry
— the dates of submission and registration respectively
— the definition of the registered object.

[3] An applicant may be an ATS authority, a supra-national ATS organisation, an airline, an aircraft operator, an aeronautical communication service provider or any other aeronautical industry organisation.

d) convey the results of the registration, i.e. the decision taken on the proposal, to the appropriate applicant; and

e) promulgate the register entries within its sphere of responsibility according to specified procedures and in a specified form.

4.7.2.2 The procedures a) to e) should also apply with regard to deletions from the register, with item c) replaced by

c*) delete the relevant names/addresses from the register for each proposal that is accepted.

4.7.2.3 A user may request an allocation of names/addresses from a registration authority, leaving the choice of names to the registration authority. Alternatively, a user of a registration authority may request an allocation of particular names/addresses. The registration authority may grant that request if it chooses, provided the names/addresses have not previously been issued.

4.7.2.4 The use of a name/address can be terminated by a registration authority and then the name/address re-used at a later time. The precise rules and constraints related to the re-use of a name/address to ensure unambiguity are within the responsibility of the registration authority.

4.7.3 Internetwork Address Administration and Registration

4.7.3.1 *Administration*

ICAO is the ultimate administrative authority of the ATN internetwork addressing plan and administers this plan through Sub-volume V of the Manual of Technical Provisions for the ATN (Doc 9705 -AN/956). That document defines and administers the ATN NSAP address syntax (i.e. field boundaries, field sizes and field formats), the ATN NSAP address semantics (i.e. the field content and interpretation), and the ATN NSAP address encoding procedures (i.e. the representation of the abstract field syntax and semantics). The document also delegates authority for the definition of the semantic content and the encoding of particular fields (or portions of address fields) as well as the assignment of address values for these fields to other authorities, like ICAO Regions, States, and certain organisations.

4.7.3.2 *Registration*

Four of the nine address fields of an ATN NSAP address have been assigned fixed values in Sub-volume V of the above-mentiond document and, consequently, do not need further registration. The values of the remaining five fields should be registered as follows:

4.7.3.2.1 ADM-Field

4.7.3.2.1.1 The ADM field shall be assigned a value representing either the AINSC or ATSC organisation (depending on the value of the VER field) which is responsible for the identified ATN network addressing sub-domain.

4.7.3.2.1.2 In the case of an ATSC Network Addressing Domain, the ADM field may identify either a State or an ICAO Region. When used for identifying a State, the ADM field contains the State's three-character alphanumeric ISO country designator defined in ISO 3166. When used to identify an ICAO Region, the first octet of the ADM field contains the ICAO Region Identifier defined in Chapter 5.4 of Doc 9705-AN/956, while the value of the remaining two octets are assigned by the identified ICAO Region.

4.7.3.2.1.3 In the case of an AINSC Network Addressing Domain, the ADM field value should be an IATA 3-letter code for airlines (e.g. the "airline designator") and other aeronautical organizations (stakeholders). IATA has already set up a registration procedure based on the use of current alphanumeric "airline designators" with extensions for "other stakeholders" compatible with the IATA Passenger Services.

4.7.3.2.1.4 One (or more) registration document(s) should be established and maintained, where values for the ADM field of the ATN NSAP address will be registered and published. This could be similar to the ISO 6523 standard document, where International Code Designators (ICD) are listed for addressing authorities registered with ISO (e.g. the value "0027" for ICAO can be found there). The registration document for ADM values may for instance contain tables with the following layout:

ICAO member / ATSC Administration	***ISO Country Code (3 letter code)***	***ADM value (hexadecimal)***
...		
Finland	FIN	46 49 4E
France	FRA	46 52 41
Germany	DEU	44 45 55
...		

IATA member / AISC Administration	***IATA Airline Code (3 letter code)***	***ADM value (hexadecimal)***
...		
Air France	AFR	41 46 52
British Airways	BAE	42 41 45
Lufthansa	DLH	44 4C 48
South African Airlines	SAL	53 41 4C
United Airlines	UAL	55 41 4C
...		

4.7.3.2.2 **ARS-Field**

4.7.3.2.2.1 In Fixed Network Addressing Domains, ARS values are assigned, administered and registered by the authority designated in the ADM field. A guideline for registration procedures and an outline for a registration document may be established by ICAO and/or IATA as the parent registration authorities.

Note.— During the initial implementation of the ATN, i.e. until appropriate registration authorities have been established by States, registration of ARS field values under the address space of ICAO can be handled by the ATNP.

Note.— A common ICAO/IATA database comprising all registered NSAP address prefixes including the ARS value may be maintained and published through the appropriate ICAO and IATA channels. This database would identify all registered ATN routing domains and the organisations responsible for each one. This database may be the basis of generalised directory services for future ATN deployments.

Note.— In Mobile Network Addressing Domains, ARS values are defined a priori by the 24-bit ICAO Aircraft Identifier of the aircraft on which the addressed system is located.

4.7.3.2.3 **LOC-, SYS-, N-SEL-Fields**

Values for the LOC, SYS and N-SEL fields will be administered and registered either by the authority designated in the ADM field (i.e. an ICAO Region, State, or aeronautical industry organisation) or by appropriate subordinate authorities to which registration authority has been devolved.

4.7.4 **Transport Address Administration and Registration**

According to the hierarchical structure of ATN addresses, only the TSAP selector of the ATN address has to be administered and assigned in the process of defining and registering ATN transport addresses (ATN TSAP addresses).

Note.— To register a TSAP address the underlying NSAP address must previously have been registered.

4.7.4.1 ***Administration***

According to Chapter 5.4 of Doc 9705-AN/956, the TSAP selector of an ATN Transport address is administered on a local basis. This means that TSAP selector values are assigned by the organisation responsible for a given ATN End System within the constraints defined in the above-mentioned document.

4.7.4.2 ***Registration***

4.7.4.2.1 The value for the TSAP selector field will be registered locally by a State's authority, or airline's or other aeronautical registration authority. In general, there is little need for ATN-wide coordination and publication of registered TSAP selectors. However, in order to support ATN directory services in the long term, the registered TSAP addresses of

ATSC applications should be recorded and maintained in a possibly distributed ATN directory under the auspices of ICAO.

Note.— The recording and global publication of the TSAP addresses associated with ground CM applications is a requirement for ATN.

4.7.5 Application Name Administration and Registration

4.7.5.1 *General*

4.7.5.1.1 ATN AP-titles should be registered based on the registration procedures in ISO/IEC 9834-1 and ISO/IEC 9834-6. The latter defines rules applicable to the registration of APs and AEs by internationally recognized organisations. As ICAO has been assigned an ICD, these rules are applicable for the assignment of ATN AP-titles and ATN AE-titles by ICAO. Consequently, ICAO is the international registration authority for the ATSC application names and exercises this authority in the form of the Sub-volume IV of Doc 9705-AN/956. Likewise, IATA should act as the international registration authority for the naming of AINSC applications.

4.7.5.1.2 The registration responsibilities for application naming may be further delegated according to the administrative taxonomy of the ICAO and IATA organisations.

Note.— Registration of ATN application names, in particular the AE-qualifier, may, in the interim period be performed by the ATNP.

4.7.5.1.3 Both the *object identifier form* and *directory name form* described in ISO/IEC 9834-1 may be registered, especially when considering the potential use of OSI directory services for the ATN in the longer run.

Note.— According to ISO/IEC 9834-6, a registration authority shall assign both an object identifier form and a directory name form of an AP-title or AE-qualifier when registering an AP or AE respectively. To be compliant which ISO/IEC 9834-6, the ATN SARPs will have to be amended to include the definition of the directory names of ATN APs and AEs.

4.7.5.2 *AP Registration*

4.7.5.2.1 An AP is identified by an AP-title. The registration of an AP involves the assignment of an AP-title (in both an object identifier form and a directory name form) and the placement of these names (together with additional information, as appropriate) as the AP register entry for that AP.

4.7.5.2.2 In general, the assignment of the object identifier form of an AP-title involves the assignment of one (or more) object identifier components, which in combination with object identifier components assigned by superior registration authorities, form the object identifier for the AP-title. Likewise, the assignment of the directory name form of an AP-title involves the assignment of a relative distinguished name, which in combination with the set of relative distinguished names assigned by superior registration authorities, form the directory name for the AP-title.

Note.— Sub-volume IV of Doc 9705-AN/956 currently assigns only object identifiers to ATN AP-titles.

4.7.5.3 ***AE Registration***

4.7.5.3.1 An AE is identified by an AE-title. As an AE-title consists of an AP-title and an AE-qualifier, the registration of an AE involves the assignment of an AE-qualifier only, if the AP that contains the AE has been previously registered. The AE-title can then be generated by a combination of the AP-title and the AE-qualifier. The registration authority assigns for the AE-qualifer an object identifier component (by assigning an integer) and a relative distinguished name which are unambiguous within the scope of the associated AP and places these names together with the previously registered AP-title (and additional information, as appropriate) as the AE register entry for that AE.

4.7.5.3.2 Sub-volume IV of Doc 9705-AN/956 is currently the registration authority for ATN AE-qualifiers associated with ATSC air-ground applications.

Note.— Sub-volume IV assigns only object identifiers to ATN AE-titles.

4.7.5.3.3 For communication purposes, AE-invocations have to handle one or more application associations. These can be identified by Application Association Identifiers which need only be unambiguous within the scope of the co-operating AE-invocations, and thus do not have to be registered.

— — — — — — — —

5. *Data Definitions and Encoding*

5.1 General

5.1.1 The specification of an application necessarily includes a specification of the data structures that are manipulated by the program, including any messages that it will transmit or receive. When there is a requirement, as in ATN, to specify applications independently of the machines that will host them, and independently of the languages in which they will be written, there is a corresponding requirement to specify the data structures and messages in a machine and language independent manner. A syntax for doing this is termed an abstract syntax.

5.1.2 When one application is to transfer messages to another, there is, unless the two applications have been written in the same language and run on the same type of machine, a requirement to specify an encoding of the message that both applications will recognize. Such an encoding will be a common, or standard transfer encoding. Clearly, in order to specify a transfer encoding of a message, independently of any source machine or language, it is necessary to define the syntax of that message using a standard syntax notation. An abstract syntax notation is therefore a necessity for open application development and is a pre-requisite for a definition of any standard message transfer encoding.

5.2 ASN.1

5.2.1 Context

Abstract Syntax Notation number one (ASN.1) is a standard notation for representing data structures in an implementation-independent way. It was originally developed by CCITT to define the complex data structures employed in the X.400 protocols, and was subsequently adopted by ISO standards writers to define the protocol data units used in OSI application protocols. It is also used to define data structures in the integrated services digital network (ISDN) standards. Within the ATN, ASN. 1 has been used for the formal definition of application messages, and for the definition of the upper layer protocol data units used by the upper layer efficiency enhancements. The ASN.1 standards are ISO/IEC 8824-1 and ITU-T Rec. X.208.

5.2.2 Primitive Types

ASN.1 is based on several primitive data ***types*** and mechanisms for constructing, from these primitives, ***structured types*** to suit the application's requirements. ASN.1 also allows structured types to be defined recursively to construct further, increasingly complex structured types. Types are named and defined using ***Type Assignment*** statements, and ***Value Assignment*** statements allow values to be assigned to a specific instance of any primitive type or to a structured type of arbitrary complexity. The primitive types of ASN.1 are referred to with keywords which are always written in upper-case letters as follows:

a) INTEGER — the range of positive and negative whole numbers, including zero;

b) ENUMERATED — a set of positive whole numbers, not necessarily contiguous and having no numerical significance, each with an associated identifier;

c) REAL — the range of floating-point values expressed by the triplet {M, B, e} where M and e are any integers, B is 2 or 10 and the value is given by MxB*e;

d) BOOLEAN — self-explanatory, with the two values given by the keywords TRUE or FALSE;

e) BIT STRING — an ordered sequence of binary digits (bits) of arbitrary or zero length;

f) OCTET STRING — an ordered sequence of octets of arbitrary or zero length;

g) OBJECT IDENTIFIER — a sequence of positive integers corresponding to the nodes in a hierarchical tree structure which has been established to provide a naming and registration of all data objects which are to be universally known; and

h) NULL — used mainly in type assignment notation to indicate that the type may not, in fact, be present.

5.2.3 **Defined Types**

5.2.3.1 For any of the primitive types of ASN.1, simple types may be defined using type assignment statements to, in effect, rename a primitive type and optionally to define the domain of values which that type may take. Thus,

a) Airspeed ::= INTEGER defines a new type which has the characteristics of INTEGER; and

b) Airspeed ::= INTEGER (0..<1000)restricts the value of the type to below 1000.

When the domain of a variable is a set of discrete values, the ENUMERATED type would be used:

c) MachClass::= ENUMERATED {subsonic (0), transonic (1), supersonic (2) }.

Note.— that the name of a type always begins with a capital letter. A value assignment is used to define an instance of a type with a discrete value:

averageAirspeed Airspeed ::= 550

Note.— that the name of a value always begins with a small letter, and that neither value names or type names may contain spaces.

5.2.3.2 ASN.1 also includes simple types for commonly used data, ***Useful Types,*** such as UTCTime, and for various ***Character String Types*** such as PrintableString, GraphicString, IA5String etc.

5.2.4 **Structured Types**

5.2.4.1 The ASN.1 mechanisms for defining ***structured types*** are lists, repetition and alternatives.

5.2.4.2 The SEQUENCE and SET keywords are used to define ***structured types*** which consist of a set of other types, either simple or themselves structured. The difference between the two is that in the SET type, there is no significance to the order in which the sub-types are listed, whereas in the SEQUENCE type, values will always be assigned in the order in which the sub-types are defined. An example of a ***structured type*** defined by SEQUENCE might be:

```
Observations ::= SEQUENCE
{
location          IA5STRING (SIZE (6))
reportingOrNot    BOOLEAN
maxtemperature    INTEGER (0..120),
mintemperature    INTEGER (0..10),
windDirection     ENUMERATED { north (0), east (1), south (2), west (3) }
hourlyrainfalls   SET OF INTEGER (SIZE (24)) OPTIONAL
}
```

Note.— the formatting of this example. A lot of space is taken up, but without a clear presentation, ASN.1 specifications can be difficult to understand. Note also that the SET OF type has been used in a, hopefully, self-defining manner. The SEQUENCE OF keyword would be used instead of SET OF in the type assignment for 'hourlyrainfalls' if the pattern of rainfall within the 24 hour period were to be required.

5.2.4.3 In the SEQUENCE and SET types, the keyword OPTIONAL can be used to indicate that a constituent type may not be present.

5.2.4.4 The CHOICE keyword is used to define a type in terms of a collection of alternative types which are all distinct. For any single instance of the type, its' definition will be that of one of the alternative types. CHOICE is typically used to define a set of messages.

```
FlightServiceMessage ::= CHOICE
{
IFRFlightPlan [0],
FlightPlanAmendment [1],
VFRFlightPlan [2],
FlightNotification [3],
DepartureMessage [4]
}
```

The square brackets contain what is known as a ***Tag***. Clearly, when there is an alternative to be specified, the alternative chosen must be conveyed along with the actual data, whatever transfer encoding is used, i.e the message is tagged. There are several types of tag in ASN.1, which are used to distinguish the different types, including primitives and structured types. Most of these tags are not used in ATN ASN.1 however, because the transfer encoding used packed encoding rules (PER) is a canonical encoding (reduced to the simplest form without loss of information) in which the type of a data item is inferred from its position in the encoded data.

5.2.4.5 The foregoing section provides only the briefest introduction to ASN.1. Further study of a suitable text is recommended before attempting to read the ASN.1 message definitions in upper layer communications service (ULCS) and applications.

5.3 Standard Encoding Rules

5.3.1 Before an application transmits data to a peer on another machine, the data must be encoded in some form. The data on the local system will typically be encoded in some format which may not be acceptable to the peer application. Before being transmitted, the data will then have to be re-encoded using some mutually recognised encoding for the transfer. On receiving the data, the peer application reformats the data from this common transfer encoding into the format required for local use. Before the definition of the presentation layer, e.g. in the early version (1984) of X.400, the encoding rules had to be built into the application itself. Thus there was no possibility of choosing a more efficient encoding without changing the definition of the application. There now exist a number of standardised encoding rules which enable data structures expressed in ASN.1 to be encoded as a machine-independent octet stream which is well suited to data interchange.

5.3.2 The application need not be concerned with the encoding rules, it simply deals with information in its local syntax, which must be a realisation of the abstract syntax in which the application is defined; to date ASN.1 is the only such syntax used by OSI applications. ASN.1 compilers are available to generate an ASN.1 rendering of data structures defined in various local formats. These compilers also provide the very useful function of validating the syntactic correctness of the ASN. 1 strings input to them. A block of ASN.1 syntax describing a set of one or more data structures is referred to as a presentation data value (PDV). The association of a transfer syntax with a given PDV is termed a presentation context identifier (PCI), and one of the functions of the presentation layer is to negotiate the set of PCIs to be used during the connection.

5.3.3 Several sets of standard encoding rules have been defined or proposed, two of which are briefly described below. ATN protocols and applications, because of bandwidth limitations on air-ground connections, use only the more efficient PER transfer encoding.

5.3.3.1 Basic Encoding Rules (BER): BER is the original set of ASN.1 encoding rules, assumed by many existing OSI standards for their transfer syntax. The encoding is based on an octet-aligned TLV (type-length-value) approach. The Basic Encoding Rules provide a number of ways to encode ASN.1, giving the encoding entity a choice of methods of encoding lengths, and in some cases a choice of order. BER makes no attempt to change the encoding of long octet strings in order to reduce the size.

5.3.3.2 Packed Encoding Rules (PER): PER has been designed to minimise the bits transmitted. The encoding rules work on the basis that every bit that is not needed to transmit useful information is not sent. Thus for example, a Boolean is transmitted as a single bit rather than as an octet. Tags are generally not included and other ways of encoding this information are used instead. For example in a SEQUENCE with OPTIONAL and DEFAULT elements a single bit index is usually all that is needed to indicate the presence or absence of each element. There are four variants, namely:

a) Packed encoding of a single ASN.1 type (basic aligned);

b) Packed encoding of a single ASN.1 type (basic unaligned);

c) Packed encoding of a single ASN.1 type (relay-safe-canonical aligned); and

d) Packed encoding of a single ASN.1 type (relay-safe-canonical unaligned);

5.3.3.3 The last two of these are used when a PDV contains an Embedded PDV, that is - a PDV which was defined with different abstract syntax and/or transfer rules than those defined for the ‘outer’ PDV. This situation occurs when an application wishes to make use of some standard PDV, typically from a library. An encoding of a PDV is relay-safe only if the PDV contains no Embedded PDVs, or if standard Object Identifiers for the presentation context identifiers of such values are included with them. Happily, ATN currently does not make use of Embedded PDVs, so the only choice to be made was between the aligned and un-aligned encodings. The ALIGNED variety of PER inserts padding bits to align some elements to octet boundaries, whereas the UNALIGNED version does not. In the basic aligned and basic unaligned variants, the number of bits is minimised, but it is assumed that both encoder and decoder have precise foreknowledge of the abstract syntax being encoded, including all constraints. Thus, the flexibility of BER to handle unknown data types by skipping over them is lost. In some cases, but not in the ATN , the use of PER may result in a larger encoding and decoding processing overhead, compared with BER.

5.3.4 ASN.1/PER

5.3.4.1 The Packed Encoding Rules (PER) are defined in ISO/IEC 8825-2. PER makes use of features which appear in later versions of the ASN.1 syntax (constraint specification, EMBEDDED PDV, etc) to minimise the number of bits encoded for interchange. In each interchange, the receiver must have *a priori* knowledge of the types of data being sent for it to be possible to decode the data stream.

5.3.4.2 For the purpose of this document the term ASN.1/PER is used to indicate the packed encoding of a single ASN.1 type (basic unaligned), which has been registered as:

{joint-iso-ccitt asn1 (1) packed-encoding (3) basic (0) unaligned (1)}

5.3.4.3 The specification of PER requires that some fields are *bit aligned* (bit-fields) and other fields are *octet aligned* (octet-aligned-bit-fields). Note that the ALIGNED variants of PER uses a B`0' as alignment (padding) bits. A simplified review of the techniques involved in using Packed Encoding Rules follows.

5.3.4.4 An understanding of the following terms used in ASN.1/PER will be required. The PER standard - ISO/IEC 8825-2 - contains further tutorial material.

a) *Preamble* — is a bit-field with a bit corresponding to each OPTIONAL or DEFAULT item — if the entry is present the bit is set to `1' otherwise it is set to '0';

b) *Canonical order* — indicates that the elements are sorted as follows: Universal class tags first, followed by Application-wide, Context-specific and Private-use tags then within each class elements are sorted in ascending order of their tag number. A selection of types is shown below;

c) *Octet-aligned-bit-field* — a product of encoding that is a sequence of bits that begin on an octet boundary but need not finish on one;

d) *Bit-field* — a product of encoding that is a number of bits that may or may not begin on an octet boundary

e) *Field-list* — a set of bit-fields and octet-aligned-bit-fields. Each value is encoded to form either a octet-aligned-bit-field or a bit-field then the field is appended to the current field-list (being preceded by a length indicator is some cases);

f) Constrained — a number that has a known (or determinable) lower and upper bound. The use of bounded values assumes that the decoder has the same type definitions and can deduce the same values for the bounds as the encoder. This will most likely be specified through a profile if not explicit in the original defining standard;

g) *Unconstrained* — a number that has a unknown (or undeterminable) lower and upper bound; and

h) *Semi-constrained* — a number that has a known (or determinable) lower bound but an unknown (or undeterminable) upper bound. The use of the lower bound value assumes that the decoder has the same type definitions and can deduce the same value for the lower bound as the encoder. This will most likely be specified through a profile if not explicit in the original defining standard.

5.3.4.5 The encoding of a component of a data value consists of one of the following, where encoding b) applies where the contents are large:

a) three parts (any or all of which may be empty, bit-fields, or octet-aligned-bit-fields) which appear in the following order:

1) a preamble;

2) a length determinant;

3) contents;

b) an arbitrary number of parts as follows:

1) a preamble;

2) a length determinant for the first fragment of the contents (octet-aligned-bit-field);

3) the first fragment of the contents (octet-aligned-bit-field);

4) repeat ii) and iii) for all other fragments of the contents.

5.3.4.5.1 **Type Encoding**

ASN.1 PER does not use tags per se. It forms a canonical ordering of the alternatives and then uses a preamble as an indicator. The preamble uses a bit string to represent the presence (B`1') or omission (B`0') of DEFAULT or OPTIONAL items. A recipient of a PER-encoded data stream must know *a priori* the abstract syntax of the data being encoded.

5.3.4.5.2 **Length Determinant Encoding**

The length determinant is used, when required, to indicate the number of components in a SEQUENCE OF or the number of bits or octets in a data value. When a length determinant is present it can be encoded in a number of ways, but it will always be either constrained or semi-constrained with lower bound >= 0.

a) Constrained

The length determinant is treated as an Integer whose value corresponds to the offset from the lower bound, and may therefore be a bit-field or an octet-aligned-bit-field.

b) *Semi-constrained*

The length determinant is treated as an Integer whose value corresponds to the offset from the lower bound. The length is always octet-aligned. If the length is less than 128 it is encoded as B`0xxxxxxx', if the length is less than 16384 ($2^{+14}$) it is encoded as B`10xxxxxx xxxxxxxx' otherwise it is encoded using a length of lengths introducer octet followed by the length octets B`11yyyyyy xxxxxxxx ... xxxxxxxx'.

5.3.4.5.3 **Value Encoding**

Each type has its own methods of encoding.

Boolean

A Boolean type will occupy just one bit and immediately follows the current field-list. B`0' indicates FALSE and B`1' indicates TRUE.

Integer

An integer type has a number of options:

a) Constrained — A constrained integer type is specified as INTEGER (n..m). The lower bound (n) is subtracted from the value of the integer before encoding. A value in the range 0..255 uses a bit-field, a value equal to 256 uses 1 octet, a value in the range 257..65536 uses a 2 octet octet-aligned-bit-field and a value greater than 65536 uses indefinite length encoding and an octet-aligned-bit-field;

b) Semi-Constrained — A semi-constrained integer type is one whose values are constrained to exceed or equal some value "lb" , with no upper bound being specified. The lower bound (lb) is subtracted from the value of the integer before encoding, and indefinite length encoding is used; and

c) Unconstrained — Indefinite length encoding is used, and the value is encoded as a 2's-complement binary integer in an octet-aligned bit field with the minimum number of octets.

Bit String

If the bit string is constrained and contains up to (and including) 16 bits it is a bit-field. Larger bit strings are octet-aligned-bit-fields. If it is constrained there is no length, otherwise include a length.

OctetString

If the length is zero it is not encoded. If the length is fixed at 1 or 2 then it is not an octet-aligned-bit-field and has no length field. If it is a fixed length octet string then encode with no length octets. Otherwise for unconstrained octet strings the (unconstrained) length is present.

Null -No encoding

Object Identifier

It uses the BER encoding (octet-aligned-bit-field) preceded by a semi-constrained length (with a lower bound of 1).

IA5String

If the length is zero it is not encoded. If the length is fixed at 1 or 2 then it is a bit-field with no length. If it is a fixed length octet string then the (constrained or semi-constrained) length is present. Otherwise for unconstrained octet strings the (unconstrained) length is present.

Enumerated

Sort into ascending order, then index from 0. Then treat the index as an Integer.

Sequence

A preamble is used as an introducer when OPTIONAL or DEFAULT components are defined in the SEQUENCE. The presence or absence of each such component is indicated in the preamble bit-map by a `1' or `0' respectively. It is followed by the encodings for the individual elements.

Sequence Of

If the number of components is fixed there is no length field, otherwise a length field is present. It is followed by the encoding of each component in turn.

Set

The Set type has its elements sorted into a canonical order and is then encoded as if it had been declared a Sequence.

Choice

The Choices are assigned an index (the choice index) starting at 0 for the first and `n' for the last. The choice index is then encoded as an Integer with a range of 0..n.

PDV-type

A preamble is used as an introducer, with bits 8 and 7 set to B`1' the lower six bits are then used to select the Presentation Context Identifier. This is followed by a length and then the actual PDV.

— — — — — — — —

6. *Protocol Profiling*

6.1 Formal Specification Techniques

Text has long been recognized as being inexact and potentially ambiguous with regard to the specification of protocols and their profiling. In the ATN SARPs, the decision was reached to conform the formal description techniques used for profiling within the ISO community. These techniques are defined by OSI Conformance Testing Methodology and Framework: Implementation Conformance Statements (ISO 9646-7) and are referenced and used by Framework and taxonomy of International Standardized Profiles (TR-10000). Within the SARPs, ATN Protocol Requirements Lists (APRLs) and Managed Objects Requirement Templates (MORTS) are used to further specify or profile the standards as defined for use within the ATN.

6.2 Implementation Conformance Statements

6.2.1 Initial basis for APRLs and MORTS come from ISO 9646-7 which specifies the purpose and notational conventions for the writing of Implementation Conformance Statements (ICSs). ICSs consist of tables organized by individual features (questions, functions, protocol data units (PDUs), parameters, components, etc.) which define implementation conformance constraints on some reference specification. In the context of the SARPs, these specifications are for protocols, profiles and information objects (such as managed objects). Features designate rows in these tables to a sufficiently detailed level to allow conformance to the specification referenced to be verified or tested for conformance depending upon the purpose of the specific Internet Communication Service (ICS).

6.2.2 No generic format or proforma for an ICS is provided by the standards because of the wide variety of specifications for which conformance requirements are stated. Nevertheless 9646-7 and the SARPs state general rules, guidance and notational conventions needed to allow the ICSs (APRLs and MORTs) to be defined and interpreted unambiguously.

6.3 PICS and PICS Proformas

6.3.1 The development of ICSs grew out of the introduction into ISO standards of conventions to allow conformance testing of protocols. ISO 9646-2 states that in order to provide an effective basis for conformance testing of implementations ISO protocol standards must include Protocol Implementation Conformance Statement (PICS) Proforma. A PICS Proforma is considered a necessary pre-condition for the generation of an abstract test suite for a standard and in general PICS Proforma have been produced for all ISO protocol standards and are typically published as a normative part or annex to the protocol standard.

6.3.2 PICS Proformas are questionnaires or templates which cover all the known protocol features which apply to the process of static conformance testing for the standard. These templates contain one or more empty columns which indicate the support for and if appropriate the nature of support for the feature corresponding to that row. Once an implementor has filled in the support material for the support column(s), the PICS

Proforma becomes simply a PICS which is specific to the implementation the conformance statement is created for.

6.4 Profiles, ISPs and Requirements Lists

6.4.1 General

6.4.1.1 As various regional and application profiles were developed to further constrain the options within the ISO standards, it was recognized that text was no better a specification tool for profiling than it was for the definition of the standards themselves. As efforts within ISO came together to harmonize and standardize the various functional sets of profiles in progress, the definition of ICS became broadened to include more than PICS Proforma and PICS.

6.4.1.2 Initially the effort further constrained the PICS Proforma for a standard, but were still not specific to an implementation was attempted. The theory was that a Proforma could be used to define PICS and conformance testing for the profiles being specified.

6.4.1.3 PICS Proformas are concerned with static conformance requirements (i.e. what capabilities have to be or are allowed to be implemented in a conforming system). Profiles are more concerned with the use of implemented capabilities in order to meet requirements for interworking. A PICS Proforma only defines static conformance and does not reflect dynamic behavior, but the standard and profiles can. In an effort to allow conformance and constraints on dynamic behavior to be specified, Requirements Lists (RLs) were defined as another of the ICS types.

6.4.1.4 As International Standardized Profiles (ISPs) were developed, ISP Requirements Lists (IPRLs) were developed to allow the requirements for interoperability in accordance with these profiles to be specified. In particular notation is added to the RL notation to specify both status of features for both implementation and use (e.g. optional for implementation, prohibited for use etc.).

6.4.1.5 An RL expresses the constraints upon allowed answers in a corresponding PICS. Profile RLs are derived from the PICS Proforma of the base standard in question with its entries enabled, disabled, or pre-selected according to the profile's choices. Any special requirements that do not originate in the base standard should be documented in the profile RL.

6.4.1.6 It should be noted that ISO has prepared a copyright release with respect to all PICS Proforma stating that: “Users of this International Standard may freely reproduce this ICS Proforma so that it may be used for its intended purpose and may further publish the completed ICS.”

6.4.1.7 Many variations exist in ICS Proforma format and conventions. Almost all contain the four columns in the following sections. These columns are generically identical in meaning, but often use differing headings to be more specific to the features or items contained in each specific table. The various names for these headings are called out within the corresponding column section below. Other details which relate to the conventions (of the many options within ISO 9646-7) used in the SARPs are described within the sections specifically describing APRLs and MORTS.

Item

Usually the first column in an ICS Proforma, this entry contains a short mnemonic to indicate the feature for reference. This column is also referred to as index in some ICS Proforma.

Description (feature)

This column can have many names including Capability, Feature, Function, (N)PDU, Parameter, Dependency, Timer, etc. It is usually the second column in the ICS Proforma and specifies the row item in a longer and hopefully more common sense way than the item mnemonic. If the feature is a question the question is written out in this column.

Reference

This column references the feature back to the base standard (or other references, as appropriate). The entry should be as specific as possible and reference to the section number in the base standard. In some cases this column will contain references to specific sections in the SARPs, particularly for tables needed that are not based on ISO PICS Proforma tables.

ISO Status

This column indicates the ISO status of the feature in the base standard. Typically this uses a single character indicator for mandatory, optional, conditional, excluded, out of scope or not applicable.

6.5 ATN Profile Requirements Lists (APRLs)

6.5.1 General

6.5.1.1 Within the SARPs the conventions developed and used to specify IPRLs are used to define APRLs. Most of the component tables in APRLs are produced by copying selected tables from the relevant base standards PICS Proformas, removing the column(s) to be completed by the supplier and adding a new column giving the ATN requirements or support, both in terms of status and value ranges. Where appropriate ATN specific tables and features have been created to document what has been agreed to and is best documented in this form.

6.5.1.2 Both "ISO Status" and " ATN Support/Requirement" columns should contain whether the feature indicated for that row is mandatory (M), conditional (C), optional (O), excluded (X), out of scope (I) or not applicable (-).

6.5.1.3 SARPs material has traditionally been divided into Standards containing mandatory features indicated by statements containing the word "shall", and recommendations which contain the word “recommended”. This approach is not completely consistent with ISO ICS notation. While Mandatory (M) is considered to be synonymous with “shall” standard statement, the category Optional (O) contains both items that are recommended and options that are not precluded or recommended.

6.5.1.4 In order to maintain conformance to the ICS notation and provide information on the recommendations within the APRLs, tables of recommendations which are cross referenced to point to optional items elsewhere within the APRLs using the Item or Index value have been created. In order for users of the SARPs to take standards and recommendations into account, the appendix material should be read in conjunction with the APRLs, as there are both standards and recommendations which do not correspond to items in the APRLs.

6.5.2 **Footnotes**

6.5.2.1 Where explanations are needed they can be added at the bottom of the page, often referencing back to the item identifier in the table. Footnotes referencing status and support column items can be indicated by the status symbol immediately followed by an integer (e.g.C2). This notation is further extended for grouped items.

6.5.2.2 For groups of mutually exclusive or selectable options among a set, footnotes are created by placing after the “O” (for optional) a period followed by an integer. The following table shows an example of a group of three related options and means that the implementation shall support at least one of the group of options numbered 4.

Item	Feature	Reference	ISO Status	ATN Support
Item_1			O.1	
Item_2			O.1	
Item_3			C2	
Item_4			O.3	
Item_4			O.3	

Example wording below might be:

O.1: support for at least one of these options is required

C2: Item_2:M

O.3: support for exactly one of these options is required.

6.5.3 **Dynamic Requirements**

In the case where the static requirements differ from the dynamic requirements, ATN Support/Requirement columns can contain a two character notation that specifies the static (implemented) and dynamic (used) requirements. If static and dynamic requirements are identical, a single character should be used. The three simple cases shown below:

Item 1: optional to be implemented, optional to be used if implemented;

Item 2: mandatory to be implemented, optional to be used; and

Item 3: optional to be implemented, prohibited for use if implemented;
are expressed in tabular form as:

Item	Feature	Reference	ISO Status	ATN Support
Item 1			O	O
Item 2			O	MO
Item 3			O	OX

Note.— that this two character representation only applies to the ATN Support column where dynamic requirements can be expressed. Note also that in the example above, the profile made Item 2 mandatory for implementation, while the ISO Status reflected in the PICS Proforma had it only as an optional item.

6.5.4 Predicates

Within the SARPs a predicate is typically denoted using the item mnemonic associated with a feature in the same APRL. Predicates in general can grow in complexity from a simple YES/NO entry, to a relational expression involving a reference within the APRL which gives a value as an answer, or to a predicate expression (i.e. a Boolean expression involving multiple predicates). Whatever the nature of the predicate, it should resolve to a YES/NO or TRUE/FALSE value which can be used elsewhere in the APRL.

6.5.5 Conditional Requirements

Any conformance requirement in the base standard or APRL may be made conditional upon some predicate. If the base standard includes a conditional requirement, then the APRL must use the same predicate, but it may be possible to partially or fully evaluate it given the conditions that are known to apply in the APRL. If such a predicate is fully evaluated in the APRL, then the requirement becomes unconditional and should be specified as such in the ATN Support column.

6.5.6 Logical Negation

The logical negation symbol used in the SARPs is the circumflex symbol, “^”, due to its wide availability in character sets. This symbol can also be used within predicates.

6.5.7 Flagging Predicate References

An asterisk may be used to prefix the mnemonic reference in the item column for any feature that is referenced by a predicate or conditional expression elsewhere in the APRL.

6.5.8 **Conditional Expressions**

A “c” followed by an integer can be placed in the status column, providing a reference to a conditional status expression defined elsewhere in the APRL. These conditional status expressions are “if .. then .. else” expressions depending on the predicate following the IF. If a conditional requirement does not specify an “else” case, then the implied else case is optional. As an example, in the following table:

Item	Feature	References	ISO Status	ATN Support
P1			C1	C1
P2			C2	C2

footnotes C1 and C2 might be defined as:

C1: if P0 then M

C2: if P1 then (if (P4 AND ^P3) then M) else O

where c1 implies that for ^PO, P1 is optional. The use of AND and OR in predicate expressions should be consistent with boolean logic.

— — — — — — — —

7. AFTN/ATN Gateway Operating Concepts

7.1 Mission of the AFTN/ATN Gateways

7.1.1 Primary Mission of the Gateway

7.1.1.1 *AFTN/AMHS Gateway*

7.1.1.1.1 The primary mission of the AFTN/AMHS Gateway is to offer interoperability between the Aeronautical Fixed Telecommunications Network (AFTN), which provides the current aeronautical store-and-forward messaging service, and the ATS Message Handling System (AMHS), which provides the store-and-forward messaging service over the ATN Internet.

7.1.1.1.2 While the AFTN uses asynchronous character-oriented transmission technologies, the AMHS implements the ISO standards for Message Handling Systems, as specified in ISO/IEC 10021 and in CCITT/ITU-T X.400. Those two sets of documents are aligned in principle.

7.1.1.1.3 With the progressive development and implementation of the ATN, the AMHS will progressively replace the AFTN. However, both messaging systems, i.e. the AMHS and the AFTN, will co-exist during the transition period. During this period, it is essential that an interworking capability be offered by means of the AFTN/AMHS Gateway for two reasons:

a) for the proper end-to-end operation of aeronautical messaging services without discrimination of two sets of users; and

b) to avoid hindering the development of the AMHS in its first stage when the number of direct AMHS users is still limited and insufficient to justify a full migration to the AMHS.

7.1.1.1.4 The AFTN/AMHS Gateway will no longer be needed:

a) in the area of responsibility of an ATS Authority, when there is no longer any AFTN station, centre or connection (to other areas) in operation;

b) on a worldwide basis, when all AFTN stations and centres have been taken out of operations (an event not being expected to happen for a significant number of years).

7.1.1.2 *AFTN/ATN Type A Gateway*

7.1.1.2.1 The primary mission of the AFTN/ATN Type A Gateway is to offer a transmission facility over the ATN for AFTN, therefore allowing users at AFTN stations to communicate between themselves while making transparent use of the ATN.

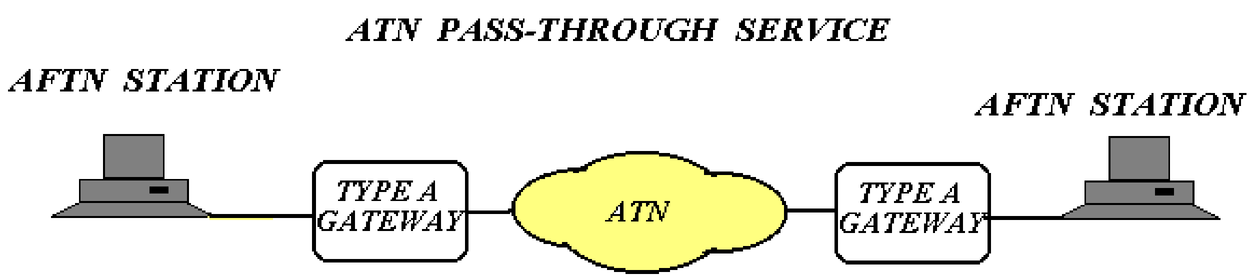
7.1.1.2.2 An AFTN/ATN Type A Gateway sends/receives IA-5 formatted messages. If it is connected to an AFTN centre which is capable of using only ITA-2 coding, a conversion to/from IA-5 is performed in the gateway.

7.1.1.2.3 This allows, for example, two AFTN Centres, each associated with an AFTN/ATN Type A Gateway, to use the global data communication infrastructure made available by the ATN for the exchange of AFTN messages.

7.1.1.2.4 The ATN pass-through service offers a point-to-point or point-to-multipoint transmission facility, and does not make provisions for message switching functionalities. The ATN pass-through service is therefore required to be used in conjunction with the AFTN message switching capability, i.e. it can't be considered as a replacement for AFTN.

7.1.1.2.5 The choice to implement the ATN pass-through service does not replace the requirement to implement the ATS message service at the earliest possible date.

7.1.1.2.6 Figure 7-1 shows the basic system concept of AFTN/ATN Gateway operations.



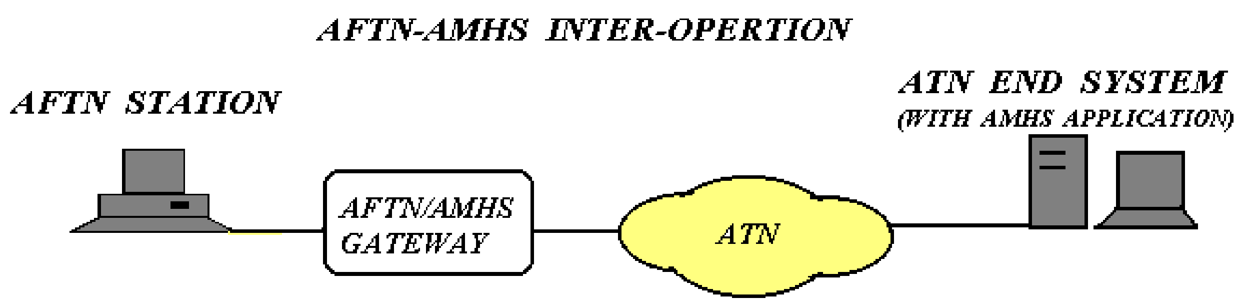


Figure 7-1. AFTN/ATN Gateway System Concept

7.1.2 Secondary mission of the AFTN/ATN Gateways

7.1.2.1 The secondary mission of an AFTN/ATN Gateway is to offer to an ATS Authority who only uses AFTN, the opportunity to interoperate with neighbouring ATS Authorities which have already started implementing the ATN. In this way the AFTN user can start learning about the implementation and the operation of ATN end systems and routers.

7.1.2.2 In such cases, the ATS Authority which implements the ATN is responsible for the implementation of the Gateway so that the Authority with AFTN will not have to change any local installations until sufficient experience has been gained with ATN end and intermediate systems.

7.1.3 Summary of the Gateway Functional Concept

7.1.3.1 Each type of AFTN/ATN Gateways implements:

a) an AFTN Component which handles the AFTN procedure;

b) an ATN Component which incorporates an ATS Message Protocol Stack depending on the type of AFTN/ATN gateway; and

Note.— Since the ATN Component of an AFTN/AMHS Gateway is a message transfer agent (MTA), this may serve, if required, as the basis for a co-located ATS Message Server for direct AMHS users. However this is not addressed in the present document which is limited to gateway considerations.

c) a Message Transfer and Control Unit which implements a set of general and mapping procedures defining the interworking between the AFTN Component and the ATN Component.

7.1.3.2 The ATS Message Protocol Stack for the AFTN/AMHS gateway consists of the protocols defined in ISO 10021 and in the CCITT/ITU-T X.400 Recommendations, while the ATS Message Protocol Stack for the AFTN/ATN type A gateway uses the Upper Layer Architecture as defined in the ATN SARPs.

7.1.3.3 Additionally the specification of the AFTN/AMHS gateway in the SARPs defines the notion of a control position, which is for the handling of exceptional situations reported.

7.2 Operational Environment and System Architecture

7.2.1 Gateway hardware

7.2.1.1 An AFTN/ATN Gateway may be implemented using a variety of hardware platforms such as:

a) personal computer-type platforms, based on single microprocessor systems and running an operating system (e.g. Unix) for multitasking/multithreading. Although such platforms have a limited capability for system duplication and fault resilience, it is possible to introduce with them a limited amount of duplication, in particular in the area of mass storage, where disk mirroring technology can be used to provide a guarantee against loss of information. Duplication of such systems may also be obtained by co-location of such systems on a local area network (LAN), in conjunction with switching mechanisms for hot stand-by;

b) workstations or servers based on multi-microprocessors or on reduced instruction set computer (RISC) processors, generally running under a Unix-type operating system. Other operating systems, usually denominated as "proprietary", may also be used in conjunction with this type of hardware platform, depending on the hardware manufacturer; and

c) fault-tolerant computer systems, running either under a Unix-type or a "proprietary" operating system. Such systems inherently have the capability to react upon a hardware fault, without the operating application being functionally affected. Such hardware platforms are, for example, those that are currently used to support certain AFTN Centre implementations.

Memory and storage capacities are dependent on the traffic to be conveyed by the gateway and on the expected level of performance.

7.2.1.2 The classification above also highlights the possibility to co-locate AFTN/ATN Gateways with AFTN centres, either physically by use of a single computer system to support both functions, or logically by use of LAN-based systems. Due to capacity and performance reasons, configurations of type b) or c) above are more appropriate for the co-location of an AFTN/ATN Gateway with an AFTN centre. In such cases, certain functions in the Gateway specification do not require to be implemented provided that the overall behaviour of the system is identical to that of two separate systems.

7.2.1.3 The AFTN/ATN Gateway hardware also needs to include communication interfaces, as described in section 7.2.5 under the title "Connectivity".

7.2.2 Gateway software

The AFTN/ATN Gateway software includes the communication application software providing the functions specified for the gateway, and an underlying operating system. The communication application software depends partly on the type of gateway and is therefore described in the two following sections.

7.2.2.1 *AFTN/AMHS Gateway software*

7.2.2.1.1 Although the decomposition of the AFTN/AMHS Gateway into the components specified in the SARPs is a functional one, and does not need to be implemented as described, it may be a practical way to divide an implementation into the following:

a) the ATN Component is functionally equivalent to an MHS MTA, for which portable “off-the-shelf” software is available. However, further integration (with other elements of the ATN) work may be required:

b) the AFTN component is functionally close to an AFTN station, provided that an application process interface (API) is available to make possible the use of that AFTN station software by other application; and

c) the MTCU (Message Transfer and Control Unit) software is specific to the AFTN/AMHS Gateway and will require software development by the implementors. However, since this piece of software is conceptually a MHS Access Unit (AU), it is possible that building bricks from previous AU developments, for gateways between MHS and other telegraphic environments (e.g. military telegraphic procedures or telex) may be used by suppliers to rapidly develop AFTN/AMHS Gateways.

7.2.2.1.2 Additional software parts may be designed by gateway implementors, as local implementation decisions, in the following areas:

a) the management and administration functions of the gateway are by definition local matters. For the proper management of the gateway, adequate management software using either text- or graphics-oriented operator interfaces (see 9.5.3 of this chapter) is required to monitor and configure items such as:

1) size of message queues;

2) link availability to the adjacent AFTN Centre;

3) status of associations and of links with adjacent ATS Message Servers and AFTN/AMHS Gateways;

4) off-line statistics and reports on gateway, link and subnetwork usage;

5) address conversion tables; and

6) and the usual parameters to be configured as part of the MTA (ATN Component), and of an ATN ES.

Note.— The above list under is not exhaustive, it rather gives examples of information to be managed in gateway operations.

b) for the automation of certain operator actions to be taken at the Gateway control position, depending on the agreed procedures.

7.2.2.2 ***AFTN/ATN Type A Gateway software***

7.2.2.2.1 Although the decomposition of the AFTN/ATN Type A Gateway into components specified in the SARPs is a functional one, and does not need to be implemented as described, it may be a practical way to divide an implementation into the following:

a) the ATN Component incorporates an implementation of the ATN Upper Layer Architecture, as specified in the SARPs (common to several ATN applications). Portable “off-the-shelf” software for this component could be available soon;

b) the AFTN Component is functionally close to an AFTN station, provided that an API is available to make possible the use of that AFTN station software by other application; and

c) the MTCU software is specific to the AFTN/ATN Type A Gateway and will require software development by the implementors.

Integration work will be required to aggregate, into a single software implementation, the different parts mentioned above. The ease of integration will depend on the API availability for each module.

7.2.2.2.2 Additional software parts may be designed by gateway implementors, as local implementation decisions, for:

a) the management and administration functions of the gateway which are by definition local matters. For the proper management of the gateway, adequate management software using either text- or graphics-oriented operator interfaces (see 9.5.3 of this chapter) is required to monitor and configure items such as:

1) size of message queues;

2) link availability to the adjacent AFTN Centre;

3) status of associations and of links with peer AFTN/ATN Type A Gateways;

4) off-line statistics and reports on gateway, link and subnetwork usage;

5) address conversion tables; and

6) the usual upper and lower layers parameters to be configured as part of an ATN ES.

Note.— The above list is exhaustive; it rather gives examples of information to be managed in gateway operations.

7.2.3 Gateway Operator and Operator Procedures

7.2.3.1 The role of the AFTN/ATN Gateway Operator is to act in the following areas:

a) communication application; and

b) computer system.

7.2.3.2 Operator procedures need to be defined for each of these areas. While certain procedures related to the application operation may have a certain degree of commonality among AFTN/ATN Gateway Operators, e.g. on a regional basis, computer system operations are essentially local and depend on the hardware and software configuration of the Gateway.

7.2.3.3 Computer system operation procedures can become more complex as more complex hardware platforms (such as LANs) are chosen. Due to the local and implementation-dependent nature of such operations, this subject is not further addressed in this document.

7.2.3.4 Potential error situations exist for which operation procedures are required. Specific Operator Procedures should be made:

a) at the level of an AMHS Management Domain, which is likely to be equivalent to the level of ATS Authorities; or

b) at the level of several Management Domains co-ordinating their actions (e.g. on a regional basis).

7.2.4 Performance Criteria

7.2.4.1 Performance criteria are defined as "the specification of the performance of an AFTN/ATN Gateway." They imply the preliminary definition of an average message size (see 7.3.3).

7.2.4.2 Considering that the AFTN/ATN Gateway aims at conveying messages to/from the AFTN, the average values used for AFTN message size may be used for this purpose. Exceptions to this principle relate to larger messages originated in the AMHS which would be split into several messages at an AFTN/AMHS Gateway.

Note.— The procedure for splitting messages with an excessive length in the AFTN is specified in Part III of this manual, and its implementation is not mandatory.

7.2.4.3 Possible performance criteria for an AFTN/ATN Gateway are:

a) message conveyance capability (peak, expressed in messages per second);

b) message conveyance capability (average, expressed in messages per hour);

c) maximum message transit time in the gateway (expressed in seconds/milliseconds, from input queue entry time to output queue entry time);

d) message short-term storage capability (expressed in number of messages);

e) long-term storage capability (expressed in number of messages);

f) maximum size of address conversion/mapping tables (expressed in number of entries);

g) maximum number of simultaneous ATN transport connections and application associations:

   1) to peer AFTN/ATN Type A Gateways for an AFTN/ATN Type A Gateway,

   2) to ATS Message Servers and/or to peer AFTN/AMHS Gateways for an AFTN/AMHS Gateway;

h) maximum time to establish a transport connection and an application association (expressed in seconds/milliseconds); and

i) system availability and other usual computer system performance criteria.

Note.— The above list is not exhaustive.

7.2.5 Connectivity

7.2.5.1 An AFTN/ATN Gateway requires connectivity with both the AFTN and the ATN. Connectivity with an AFTN Centre may be achieved by:

a) an AFTN asynchronous circuit operating in compliance with the AFTN procedures specified in Annex 10, Volume II, for the exchange of ITA-2 messages. In such a case the AFTN Component of the Gateway is required to perform ITA-2 to IA-5 message conversion;

b) an AFTN asynchronous circuit operating in compliance with the AFTN procedures specified in Annex 10, Volume II, for the exchange of IA-5 messages;

c) a code and byte independent circuit or network; or

d) any type of local physical or logical interface if the AFTN/ATN Gateway is co-located with an AFTN Centre.

7.2.5.2 Connectivity with the ATN may be achieved by means of an interface to any ground ATN subnetwork, for example with an X.25 wide-area network for long distance exchanges, or with an ISO/IEC 8802-2 compliant local-area network for local exchanges.

7.2.6 Security

7.2.6.1 The security procedures to be implemented at an AFTN/ATN Gateway are divided into three categories:

a) security procedures relevant to the ATN;

b) security procedures relevant to the AFTN; and

c) security procedures dedicated to the AFTN/ATN Gateway.

7.2.6.2 Security procedures belonging to item a) above are or will be described in appropriate ATN-related documents, to be established by appropriate bodies at a national, regional or international level.

7.2.6.3 Security procedures belonging to item b) above, if existing, are by definition already in place and need to be extended to the AFTN/ATN Gateway.

7.2.6.4 Security procedures dedicated to item c) above should be established on the basis of a preliminary risk analysis. In doing so, the following points may be taken into account:

a) the physical security procedures for an AFTN/ATN Gateway do not differ fundamentally from the equivalent procedures related to an AFTN Centre;

b) operator actions should be protected by appropriate means (e.g. password, keycard control, etc.) against intended or non-intended inappropriate actions. These considerations affect Gateway configuration, operation and maintenance.

7.3 Gateway Planning

7.3.1 Acquisition procedures

7.3.1.1 Acquisition procedures for an AFTN/ATN Gateway do not differ, from a formal, administrative and commercial viewpoint, from the procedures used for the provisioning of other aeronautical CNS systems such as an AFTN Centre.

7.3.1.2 The technical specification for an acquisition procedure should include at least:

a) the requirement for conformance with Gateway SARPs, specifying whether an AFTN/AMHS Gateway, an AFTN/ATN Type A Gateway or both (co-located or separate) are requested;

b) performance requirements, on the basis of the criteria expressed in 7.2.4.3 complemented as appropriate;

c) additional hardware and software requirements, if any, including for example :

1) the type of requested hardware platform;

2) the type of requested Operating System (OS);

3) the modularity requested in the software; or

4) the additional software pieces, the format expected for their delivery, etc.

7.3.1.3 The potential suppliers for AFTN/ATN Gateways include:

a) companies from the aeronautical communications industry;

b) companies from the communications industry with a product range including software implementations of ISO standards; and

c) software houses with an integration capability.

7.3.2 Conformance Test Criteria and Procedures

7.3.2.1 When establishing the hardware and software conformance test criteria and procedures to be used in the process of acquisition of an AFTN/ATN Gateway, the following points may be taken into account:

a) Credit may be given to the certification, if any, granted to the system components by National or International Standard Institutes and Certification bodies;

b) Information about test methods and procedures included in the ATSMHS SARPs validation report; and

c) it is recommended that pre-operational trials be performed with adjacent systems, ATS Message Servers and/or peer AFTN/ATN Gateways on an ICAO regional basis.

7.3.3 Assessing Performance Requirements

7.3.3.1 Determination of average message size

7.3.3.1.1 Considering that the AFTN/ATN Gateway aims at conveying messages to/from the AFTN, the average values used for AFTN message size may be used for this purpose. Exceptions to this principle relate to messages originated in the AMHS which could be split into several messages at an AFTN/AMHS Gateway, due to message length.

Note.— The procedure for splitting messages with an excessive length in the AFTN is specified in Part III, Chapter 6 of this document, and its implementation is not mandatory in the SARPs.

7.3.3.1.2 Therefore, either of the following values may be taken as a reasonable average message length:

a) the average length of AFTN messages relayed by the AFTN Centre to which the AFTN/ATN Gateway is connected; or

b) if such a statistical value is not available, an average length of 300 characters may be considered.

7.3.3.2 ***Performance assessment***

7.3.3.2.1 When assessing the gateway performance requirements, the following should be taken into account:

a) any existing traffic statistics for the AFTN Centre to which the Gateway is connected may be taken as a basis for the assessment of the conveyance capability and from these statistical values, gateway performance requirements may be derived as follows:

1) by analysing the part of the AFTN Centre traffic which may go through the Gateway;

2) by extrapolating this data in view of:

— the additional application or inter-personal message exchanges possibilities provided by the ATN implementation; and

— the natural traffic growth observed and planned for AFTN traffic.

b) for transit delays, connection establishment times, the store-and-forward nature of the AMHS and of the AFTN should be taken into account, as well as the performance improvement made possible by the ATN.

7.3.3.2.2 Performance requirements should be, if possible, harmonised between different States or organisations on a regional basis, since the level of performance of an isolated system in a store-and-forward environment is not always significant in relation with the over-all end-to-end performance level.

7.4 Environment

7.4.1 Both the AFTN and the ATN are expected to operate 24 hours a day, 365 days a year. Hence there is a requirement for the same level of operation by an AFTN/ATN Gateway. The need for inter-relation with both the ATN and the AFTN operations and support staff should be taken into consideration when setting up the support organisation for the AFTN/ATN Gateway. Furthermore, similar to AFTN operation, general computer system knowlefdge and ability of the operators to communicate verbally with operators in neighbouring countries (if necessary) would be very helpful.

7.4.2 The support environment may include:

a) a first level of support and maintenance, performed by properly trained operators;

b) a second level of support, provided either by skilled technical staff of the managing authority or by the supplier itself. The decision to have the level-two support performed by internal resources or by the supplier may depend on:

1) the resources and skills available within the managing authority;

2) the authority's policy concerning support;

3) the supplier's ability to deliver the requested level of service for on-site intervention when required; and

c) A third level of supplier support and maintenance.

7.4.3 Physical access to an AFTN/ATN Gateway should be governed by appropriate physical security procedures, in a manner consistent with the general policy of the managing authority for the security of AFTN Centre(s).

7.5 User and/or Operator Definition

7.5.1 Operator Profile

7.5.1.1 The AFTN/ATN Gateway Operator Profile includes the need for the following skills:

a) computer system operation (in relation with the selected hardware platform and Operating System for the AFTN/ATN Gateway);

b) knowledge of ISO communication protocols (the skill level requirement depends on the selected support organisation);

c) knowledge of AFTN procedure;

d) knowledge of ATN, AMHS and AFTN organisation, topology and operational procedures in the considered area;

e) ability to exchange technical information for fault correction with:

1) internal level-two support, and/or

2) level two or three supplier support or maintenance teams. The considered suppliers may include the gateway supplier and/or the communication facilities supplier.

7.5.1.2 Depending on the available resources within the managing authority, and on its organisational policy, these skills may either be concentrated in specific individuals dedicated to the gateway operation or shared between several people in an operating team. For example the Gateway may be operated in conjunction with an AFTN Centre, or with other categories of ATN End Systems and/or Intermediate Systems.

7.5.2 **User Profile**

7.5.2.1 The users of an AFTN/ATN Gateway are either;

a) direct AMHS users exchanging messages with users at AFTN Stations; or

b) users at AFTN Stations exchanging messages with other AFTN users, over the ATN Internet via two AFTN/ATN Gateways, or with direct AMHS users.

7.5.3 **Human Machine Interface (HMI)**

7.5.3.1 The HMI at an AFTN/ATN Gateway is used for the performance of the following functions:

a) on-line monitoring and supervision (system and application faults, alarms, etc.);

b) gateway fault diagnosis and correction;

c) input of operator commands;

d) gateway configuration;

e) display of statistics;

f) security control procedures; and

g) other functions.

7.5.3.2 The use of graphical user interfaces (GUI), including window-type screens is recommended to ease and accelerate the gateway operation under normal operating circumstances. On-line help procedures may also be included to assist the operator in tasks such as system configuration.

7.5.3.3 The use of text-oriented interfaces should be limited, when possible, to support operations which are performed by staff with higher skills, in particular with respect to computer system operation.

7.5.4 Support Personnel/Procedure Profile

7.5.4.1 The AFTN/ATN Gateway Support Personnel Profile includes the need for:

a) skills in computer system support (in relation to the selected hardware platform and Operating System for the AFTN/ATN Gateway);

b) good knowledge of the ATN Communication Services, including the ISO lower layer protocols for ATN End Systems, the ATN naming and routing principles, etc.;

c) good knowledge of the ATS Message Handling Services (ATS Message Service and/or ATN Pass-Through Service), of the associated upper layer architecture and of the related organisational and addressing considerations;

d) good knowledge of the AFTN; and

e) ability to exchange technical information of any nature with the suppliers' support team.

7.5.4.2 Depending on the type of hardware selected for the Gateway, on the level of development of the ATN in the considered authority, and of the skills and resources available within the authority, various types of organisations may be set up to provide such a support (e.g. certain individuals dedicated to computer system support, other to communications functions, etc.).

7.5.4.3 Depending on the implementation architecture, and particularly in case of co-located systems, this HMI may be added to an existing system supervision position.

7.6 Operational Modes

7.6.1 Activation

7.6.1.1 Activation is the first phase in the operational lifecycle of an AFTN/ATN Gateway. It may occur after completion of a pre-determined set of tasks, including the following:

a) installation of the gateway in its operational site;

b) system configuration, including:

   1) computer system configuration;

   2) gateway software configuration;

   3) configuration of physical interfaces (AFTN interface and ATN subnetwork interface),

   4) configuration of communication parameters at each layer, as appropriate,

5) configuration of address conversion tables and routing tables,

c) preparation of the updated configurations for the existing systems managed by the same authority to be connected to the Gateway (e.g. amended routing tables in the connected AFTN Centre);

d) elaboration of operator and support procedures; and

e) co-ordination with other authorities who operate existing systems that are to be connected to the Gateway (if any).

Note.— The list above does not represent a sequential order of the tasks to be performed.

7.6.1.2 On the basis of the list above, a complete installation and activation procedure needs to be developed and promulgated by the managing authority to describe the tasks to be performed for putting the AFTN/ATN Gateway into operational service.

7.6.1.3 The result of the activation is the start-up of the Gateway's operational service.

7.6.2 Integration of new systems

7.6.2.1 When new Gateways or ATS Message Services are installed in the general area/region of a given Gateway, the impact of this expansion needs to be taken into account.

7.6.2.2 The physical configuration of the communication interfaces in existing AFTN/ATN Gateways does not necessarily need to be modified in such circumstances.

7.6.2.3 Prior to the integration of an additional system, the following tasks need to be co-ordinated and planned:

a) preparation of the updated configurations (e.g. address conversion tables and routing tables) for the existing AFTN/ATN Gateway;

b) update of operator and support procedures, if needed; and

c) co-ordination with the authorities managing existing and forthcoming systems.

The result of such an integration phase is the expansion of the AMHS and/or of the ATN Pass-Through Service in a co-ordinated and harmonised manner.

7.6.2.4 The integration of new systems can occur repeatedly in the gateway lifecycle.

7.6.3 Operations

7.6.3.1 Gateway operations include day-to-day operation of the Gateway itself, encompassing hardware platform operations and communication software operation. The main tasks are expected to be:

a) system supervision and fault processing, including:

   1) detection by means of alarms and monitoring,

   2) correction procedure or activation of support procedure,

   3) return to normal operating conditions.

b) processing of erroneous messages by means of appropriate operator actions;

c) communication facilities supervision and fault processing;

d) load monitoring and off-line statistics production and analysis; and

e) hardware platform operations (back-up procedures, etc.).

7.6.4 **Support**

7.6.4.1 Fault processing and maintenance

7.6.4.1.1 Support is activated in case of faults which could not be solved by normal, pre-determined, correction procedures executed by the Gateway operator. The support mode is therefore activated upon his/her request.

7.6.4.1.2 Support for fault processing involves procedures, which may activate different levels of support as described in 7.4.2.

7.6.4.1.3 Upon correction of the fault which caused the transition to the support mode, the system is returned to the normal operations mode.

7.6.4.2 ***Training***

7.6.4.2.1 Training is a background task which is required at two levels in relation with an AFTN/ATN Gateway:

a) the support staff itself needs to be trained to reach the skill level described in 7.5.4, aimed at providing an internal level-two support, if the organisation has been set up as such. It is expected that such training may be obtained either from the gateway supplier or from peer authorities as the result of bilateral agreements; and

b) gateway operators need to be trained for gateway operation, with the objective of developing the skills listed in 7.5.1. This training may be obtained either from the internal level-two support or from the gateway supplier.

Such training needs to be provided to ensure that operators, and support staff have acquired an adequate level of skill prior to normal operations.

7.6.5 De-commissioning

7.6.5.1 Deactivation is a particular operational mode, where all existing systems in the vicinity of an AFTN/ATN Gateway need to be reconfigured due to its withdrawal from service.

7.6.5.2 Prior to the withdrawal of an AFTN/ATN Gateway, the following tasks need to be planned and co-ordinated:

a) preparation of the updated configurations for the existing systems communicating directly (or indirectly) with the Gateway, including:

   1) updating configuration of communication parameters at each layer, as appropriate; and

   2) updating configuration of address conversion tables and routing tables.

b) updating of operator and support procedures, if needed; and

c) co-ordination with neighbouring authorities.

The deactivation mode occurs only once, at the end of the gateway lifecycle.

7.6.5.3 The result of the deactivation is the move to a wholly-ATN environment, where the managing authority no longer operates any AFTN station, centre or circuit.

— — — — — — — —

8. *CIDIN/ATN Gateway Operating Concepts*

8.1 General

8.1.1 The primary mission of the CIDIN/ATN Gateway is to offer interoperability between the Common ICAO Data Interchange Network (CIDIN), which provides a currently used, improved aeronautical messaging service, and the ATS Message Handling System (AMHS) of the ATN.

8.1.2 It is expected that with progressive development and implementation of the ATN, the AMHS will gradually replace the CIDIN, since the ATN provides homogeneous communications infrastructure for a number of application services. However, CIDIN will still be operating for a number of years, and both messaging services, the AMHS and the CIDIN, will therefore co-exist during a certain period of time.

8.1.3 Operating concepts for such a gateway are currently under development.

— — — — — — — —

9. *Support for ACARS-based air traffic services*

9.1 General

9.1.1 Since the 1970s, commercial airlines have exchanged company operations data over various air ground subnetworks through international network service providers (commonly called aircraft communications addressing and reporting system (ACARS)). A limited number of States have made use of ACARS for some air traffic services (e.g. pre-departure clearance, digital airport terminal information service, oceanic & route clearances, and position reporting). There is no expectation that the use of ACARS for these air traffic services will transition to and/or be accommodated by States implementing CNS/ATM systems, specifically, the ACARS based air traffic services will either be phased out or handled separately from ATN based applications. The continucation of these other ACARS-based air traffic services, after the availability of ATN, should be discouraged.

9.2 FANS 1/A Accommodation

9.2.1 General

9.2.1.1 This section provides guidelines to States that implement ATN to support air traffic services and also elect to accommodate FANS-1/A aircraft.

9.2.1.2 The FANS-1/A accommodation solution comprises two parts: operational accommodation and technical accommodation.

9.2.1.3 As the CNS/ATM system is intended to be a global seamless system, only one technical accommodation solution should be defined for both aircraft and ATS providers.

9.2.1.4 The FANS-1/A accommodation strategy assumes that:

a) the global implementation strategy taken by States is based on the implementation of ATN;

b) there is some mixture of both FANS-1/A aircraft and ATN aircraft in common airspace; and

c) the main objective is migration to ATN rather than supporting competing technologies over an extended period of time.

9.2.2 Background

9.2.2.1 FANS-1/A provides a data communication capability (controller-pilot communication) for the provision of air traffic services in oceanic and remote airspace.

9.2.2.2 Unlike FANS-1/A, the ATN is standardized by ICAO and, therefore, is internationally recognized as the aeronautical telecommunication network serving the needs of the aviation industry.

9.2.3 Considerations for FANS-1/A operational accommodation solutions

9.2.3.1 It is expected that the FANS-1/A operational accommodation solutions will be mainly considered by regional planning and implementation groups.

9.2.3.2 The FANS 1/A operational accommodation solutions should be defined in cases where data communications is a required function for the intended operations. The operational accommodation solutions are necessary to determine the acceptability of the technical accommodation solution for FANS-1/A aircraft.

9.2.3.3 The operational safety, performance, security, and interoperability requirements need to be defined by the State or region for specific operational objectives (e.g., reduce separations, increased capacity, user-preferred trajectories) within an airspace to evaluate the FANS-1/A, ATN, and mixed fleet operations.

9.2.3.4 The operational accommodation solutions should take into account:

a) FANS-1/A and ATN aircraft operating in a common ATN airspace;

b) FANS-1/A aircraft operating on the same flight in both ATN and FANS-1/A airspace; and

c) different levels of operational requirements in different kinds of ATN airspace.

9.2.4 FANS 1/A technical accommodation solution

9.2.4.1 The FANS-1/A technical accommodation solution should be evaluated according to operational requirements and in the context of the chosen operational accommodation solution. The evaluation should consider both the applications and the communication services.

9.2.4.2 Consideration should be given to avoid having two applications for the same operational purpose interfacing the pilot or controller in different ways. 'Operationally significant differences' can not be tolerated by either the pilot or the controller.

9.2.4.3 Communication services provide integrity measures to minimize the probability of failure conditions, such as "undetected corruption of data," and " messages received out of sequence."

9.2.4.4 The FANS-1/A technical accommodation solution needs to provide adequate protection based on the concept that the end-system that hosts the operational applications provides the integrity. The communication infrastructure should not compromise integrity by manipulating data to/from the operational applications, i.e. it should provide a pass-through service only.

9.2.4.5 FANS-1/A uses different methods from the ATN for providing the integrity measures. While both provide integrity measures in the end-system hosting the application, the means are not interoperable. Therefore, FANS-1/A technical accommodation solution should include the provisions to meet operational requirements for integrity of the messages between the controller and the pilot.

9.2.4.6 The decision on FANS1/A technical solution should consider the cost and technical feasibility of implementing integrity measures and development of assurance methods necessary to show compliance with operational requirements.

9.2.4.7 The FANS-1/A technical accommodation solution should consider the costs and feasibility associated with the certification and regulatory criteria for each option.

9.2.5 Other considerations

9.2.5.1 Further guidance is needed for managing technological changes to CNS/ATM systems to support an evolving technology in operational service. ATS providers, airspace users, and other stakeholders will need to be involved in this effort. As part of this effort, the aviation community will need to agree on a timeline that defines operational capabilities and possible migration path(s).

9.3 Other ACARS-Based Air Traffic Services

9.3.1 General

9.3.1.1 This section provides guidelines to States that implement ATN based applications, and continue to be ACARS-based air traffic services other than those supported by FANS 1/A.

9.3.1.2 There is no expectation that the use of ACARS for these non-FANS 1/A air traffic services will transition to and/or be accommodated by States implementing CNS/ATN systems, specifically, the non-FANS 1/A ACARS based air traffic services will either be phased out or handled separately from ATN based applications.

9.3.1.3 It is recognized that there is some mixture of both non-ATN aircraft and ATN aircraft in common airspace, and that non-ATN aircraft may or may not have other ACARS-based air traffic services.

9.3.1.4 The continuation of these other ACARS-based air traffic services, after the availability of ATN, should be discouraged as only the ATN is standardized by ICAO and hence recognized as the appropriate means of providing a communication service for the aviation industry.

9.3.2 Considerations for other ACARS-based air traffic services

9.3.2.1 The temporary operational use of other ACARS-based air traffic services is the responsibility of the States and/or regional planning and implementation groups.

9.3.2.2 The operational safety, performance, security, and interoperability requirements need to be defined by the State or region for specific operational objectives.

9.3.2.3 The operational use of other ACARS-based air traffic services should take into account:

a) non-ATN and ATN aircraft operating in a common ATN airspace;

b) non-ATN aircraft operating on the same flight in both ATN and non-ATN airspace; and

c) different levels of operational requirements in different kinds of ATN airspace.

9.3.3 Consideration on technical issues on continued support for other ACARS-based air traffic services

9.3.3.1 The technical implication of the use of other ACARS-based air traffic services should be evaluated to the acceptance criteria as defined by the operational requirements for intended operational objectives. The evaluation should consider the applications and the communication services.

9.3.3.2 Consideration should be given to avoid having two applications for the same operational purpose interfacing the pilot or controller in different ways. "Operationally significant differences" can not be tolerated for either the pilot or the controller.

9.3.3.3 Communication services should meet specific communication performance requirements, including requirements on integrity in order to satisfy operational requirements on ATS data link applications. As is not expected that ACARS can meet the operational communication performance requirements (see paragraph 9.3.2.2), the use of ACARS for air traffic services should be operationally constrained.

9.3.3.4 The continued use of other ACARS-based air traffic services should consider the feasibility associated with the certification and regulatory criteria for each option.

— — — — — — — —