The ATM Forum

Technical Committee

ATM Forum Addressing: Reference Guide

AF-RA-0106.000

February, 1999

The ATM Forum
Worldwide Headquarters
2570 West El Camino Real, Suite 304
Mountain View, CA 94040-1313
Tel:+1-650-949-6700
Fax: +1-650-949-6705

Acknowledgments

The Routing and Addressing working group was chaired by Ethan Mickey Spiegel. Bob Epley and Katie Taaffe edited the *ATM Forum Addressing: Reference Guide* specification. The minutes at related working group meetings were recorded by Tim Dwight.

The following people made significant technical contributions to the *ATM Forum Addressing: Reference Guide* specification:

Francois Audet
David Cypher
Tim Dwight
John Elwell
Bob Epley
Joel Halpern
Juha Heinanen
Heinrich Hummel
Demos Kostas
Gerhard Maegerl
Shawn McAllister
Tom Shaver
Ethan Mickey Spiegel
Katie Taaffe
David Wells
Greg Wetzel

Table of Contents

Table Of Figures

Table Of Tables

1 Introduction and Scope

[Informational]

This document has been prepared by the ATM Forum to assist equipment manufacturers, and designers and implementers of ATM networks. The document provides a consolidated view of the addressing related aspects of the various ATM Forum specifications.

A companion document entitled the *ATM Forum Addressing: User Guide* [1] provides recommendations on addressing of private ATM networks and several detailed examples of call setup across interconnected private and ATM Service Provider (ASP) networks.[1] This document includes a more comprehensive list of interworking scenarios.

In the event of a conflict, the information in the normative sections of this document takes precedence over addressing information in other ATM Forum Specifications. Following is a list of the normative sections of this document.

1. Section 3 - Categorization of Addresses by Structure (with the exception of section 3.2.1, Description of E.164 Numbers)
2. Annex A - Individual and Group AFI Values
3. Annex B - Organizational Scope
4. Annex C - Interworking With Public and Private N-ISDN

2 Key Concepts

[Informational]

2.1 Addresses

An address indicates the location of an interface. In some cases the term 'address' has been used to describe an identifier[2]. For example Ethernet identifiers have been called Media Access Control (MAC) addresses. However, in ATM Forum Specifications, the term address is used to mean locator. To ensure a manageable routing system, an address should have significance within the network topology (not necessarily geography), that is, it should be a *locator* that indicates *where* in the network topology the interface can be found.[3]

Note that porting of addresses from one ATM Service Provider to another, or from one network to another, or even from one part of a network to another, defeats their ability to function as locators. There may be exceptions, but every exception causes the routing system to have to deal with routes that cannot be aggregated and so increase the routing table size throughout the ATM network.

Addresses are assigned to interfaces through which traffic enters or exits the routing domain, to enable the establishment of switched connections.

2.2 Address Prefix

A prefix of an address is a contiguous portion of the address, starting with the most significant bit. An address prefix is an abstraction of the block of addresses that the prefix represents. An address prefix does

[1] An ATM Service Provider network is defined as any ATM network that provides transit services for other ATM networks belonging to different administrative entities.

[2] In this context, an identifier is simply a unique label. Unlike a locator, its value does not reflect the topology of the network in which the associated device is deployed.

[3] Group addresses, which are discussed in Section 3.3, are an exception.

not identify an interface but may be associated with one or more interfaces. Address prefixes occur in a variety of circumstances:

- call routing tables, in which the prefix stands for any address beginning with that prefix that is not more specifically mentioned
- call screening, in which an address prefix is used as a pattern against which addresses may, or may not, match and then be screened (e.g., calling party and calling party prefix validation at a public User Network Interface [UNI])

In Private Network-Network Interface (PNNI), a prefix of an ATM End System Address is the first p bits of that address. The value of p may vary from 0 to 152. A prefix with zero length summarizes all ATM End System Addresses. PNNI routing will direct calls for which there is no more specific match to systems which advertise such a zero length prefix (i.e. the default route). Prefixes with lengths greater than zero and less than 152 are used to summarize some portion of the addressing domain. Shorter prefixes summarize greater portions than do longer prefixes (i.e., longer prefixes are more specific).

2.3 Multiplicity of Addresses

It is entirely possible to associate multiple addresses or address prefixes with a given interface. This association may actually locate the interface, in the case of an address, or a route toward a destination/location, in the case of a prefix.

When a single address or address prefix appears at multiple interfaces in the global ATM network, it usually designates a route toward the destination(s) summarized by the address or prefix. If a full 20 octet address appears multiple times, then in one instance it is used as an address to identify the interface and in all the others it is used as a route toward that interface.

3 Categorization of Addresses by Structure

[Normative (with the exception of sub-section 3.2.1)]

Addresses may be categorized by their structure or by ownership. This section describes the possible ATM address structures.

NOTE 1: The use of various address formats is allowed by ATM Forum specifications, which means that the protocols defined therein provide the means by which an ATM Service Provider may construct a network that uses any or all of these formats. This does NOT imply that an ATM Service Provider is required to support all of them or that a customer is required to use all of them.

In no case should any ATM Forum specification be interpreted as requiring an ATM Service Provider to use or to support or to accommodate any particular address type or address plan. That is a matter strictly between the service provider and the (potential) customer.

NOTE 2: ATM Forum specifications support the use of E.164 numbers as addresses for ATM end systems in two ways:

- The address may be exactly the digits of the E.164 numbers, or
- The address may be coded as described in Annex A of ISO 8348 [2], using the preferred binary encoding of the ISO NSAP format, with the E.164 number contained within the resulting structure.

This document uses the term “native E.164”, and the abbreviation “E.164N”, to refer to the former. It uses the terms “embedded E.164”, abbreviated “E.164e” or “E.164 AESA”, abbreviated “E.164A”, to refer to the latter.

The encodings involving encapsulation of the E.164 number within an AESA are discussed in sections 3.1, 3.1.1.3, and 3.2.3. The “Native” encoding of E.164 addresses is discussed in section 3.2.

An ATM address may be either a native E.164 number up to 15 digits in length, or a 20-octet ATM End System Address (AESA).[4]

3.1 AESA Format

An ATM End System Address (AESA) is derived from the International Organization for Standardization (ISO) definition of Network Service Access Point (NSAP) addresses which are defined in Annex A of ISO/IEC 8348 [2] (which is also available as ITU-T X.213 [3]). This derivation defines a distinguished subclass of NSAP and includes:

- The use of NSAP as a sub-network point of attachment on an ATM network
- The abstract syntax and coding rules [1]
- The Address Authority and its delegations [2]

In addition, the ATM Forum defines an AESA to be 20 octets in length.

Note [1]: The semantics are limited to the use as a sub-network point of attachment.

Note [2] : The registration information may include some higher-order part of the Higher Order-Domain Specific Part (e.g. the Domain Specific Part Format Indicator (DFI) and Organization Identifier (org) fields in a US DCC AESA). Note that the local AFI (0x49) has no Address Registration Authority.

An ATM End System Address identifies the location of one or more ATM interfaces. The structure of the low-order part (ESI and SEL) of the Domain Specific Part (DSP) is as specified in ISO 10589 [3], with the following modifications:

- The “ID” field defined in ISO 10589, is known as the “End System Identifier” (ESI) in ATM Forum specifications.
- ISO 10589 allows the “ID” field to vary in length, from one to eight octets. In ATM Forum specifications, the corresponding field (ESI) must be six octets long.

Initial Domain Identifier (IDI) formats are specified in this section. The structure of the AESA address with the IDI in each of these formats is illustrated in Figure 3-1, Figure 3-2, Figure 3-3, and Figure 3-4.

In ATM networks there are two types of AESA: individual and group. An ATM individual address identifies the location of a single ATM interface, whereas an ATM group address is associated with one or more ATM interfaces. The definition and guidelines for usage of the group address can be found in Section 3.3 of this document. One use of group addresses is in the definition of the Anycast service.

The hierarchy of the AESA structure has implications on the PNNI routing hierarchy (see the ATM Forum PNNI Specification, Version 1.0 [5]).

Useful tutorial material and supporting technical information on the use of Open Systems Interconnection (OSI) NSAP addresses can be found in RFC 1629 [6].

[4] The signalling protocols differentiate address formats based on other fields in the encompassing information elements (IEs). In the case of the Calling or Called Party Number, the “Type of Number” and “Addressing/Numbering Plan Identification” fields are used. In the case of the Calling or Called Party Subaddress, the “Type of Subaddress” field is used.

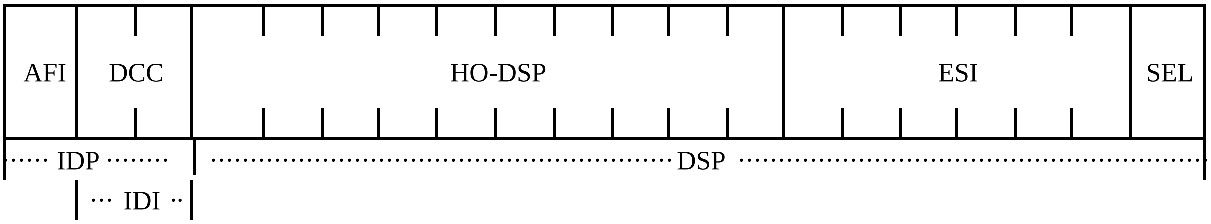


Figure 3-1: DCC AESA Format

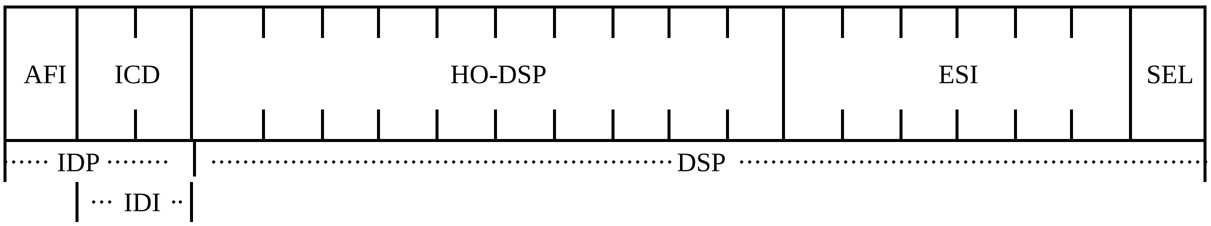


Figure 3-2: ICD AESA Format

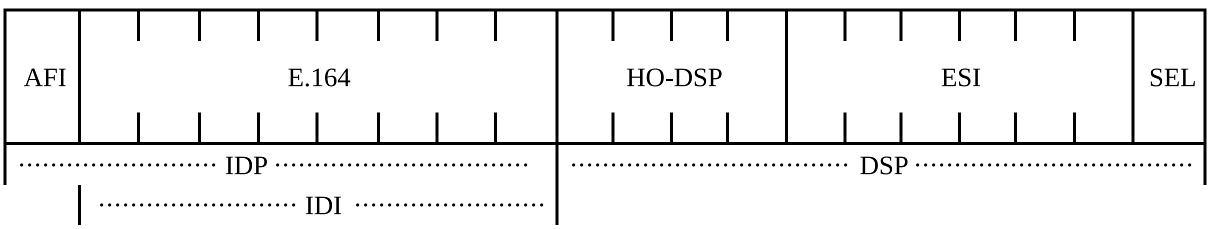


Figure 3-3: E.164 AESA Format

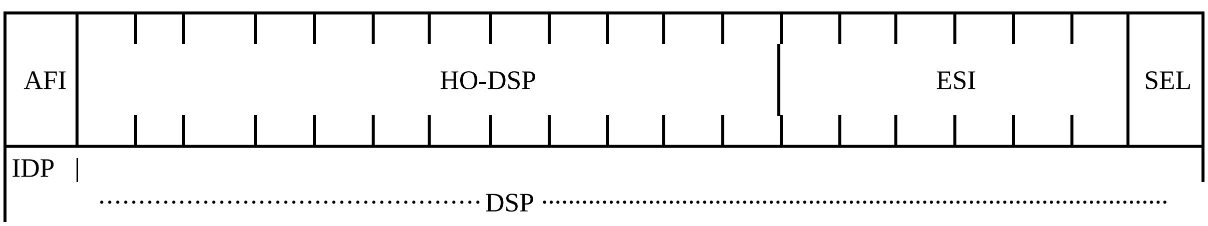


Figure 3-4: Local AESA Format

In addition to the structure, abstract semantics, abstract syntax, and coding specified in this Specification, endpoints and networks may, by mutual agreement, support other forms of AESA. However, the AESA will always be 20 octets.

ATM Forum specifications UNI 3.1 [7], UNI Signalling 4.0 [8], ILMI 4.0 [9], and PNNI 1.0 [5] discuss the use of ICD, DCC, and E.164 AESAs, and Voice and Telephony over ATM (af-vtoa-0083.001)[5] [10] discusses the Local AESA as well. The ATM Forum protocols can carry any AESA with binary coded DSP. However, the use and assignment of AESAs other than ICD, DCC, E.164, and Local may not be allowed due to regulatory or other restrictions.

Each of the address fields in the formats above are specified below.

5 Note that the use of Local addresses was incorrect in af-vtoa-0083.000 and is updated in Annex C of this document. af-vtoa-0083.001 references this document as the correction.

3.1.1 Initial Domain Part (IDP)

The Initial Domain Part (IDP) uniquely specifies an administration authority which has the responsibility for allocating and assigning values of the Domain Specific Part (DSP). The IDP consists of two fields, the Authority and Format Identifier (AFI) and Initial Domain Identifier (IDI).

According to ISO/IEC 8348, the purpose of the AFI is to specify: the format of the IDI; the network addressing authority responsible for allocating values of the IDI; whether or not leading zero digits in the IDI are significant; and the abstract syntax of the DSP. The length of this field is 1 octet.

The IDI specifies: the network addressing domain from which the values of the DSP are allocated; and the network addressing authority responsible for allocating values of the DSP from that domain. Thus, the combination of the AFI and IDI, which form the Initial Domain Part (IDP) of the ATM address, uniquely specify an Administrative Authority (AA) which has responsibility for allocating and assigning values of the DSP.

The following codes are specified for individual addresses (not group addresses) for the types of AESAs discussed in ATM Forum specifications. Use of other AFIs is not precluded.

AFI		Format
Hexadecimal	Bits	
0x39	0 0 1 1 1 0 0 1	DCC ATM Format
0x47	0 1 0 0 0 1 1 1	ICD ATM Format
0x45	0 1 0 0 0 1 0 1	E.164 ATM Format
0x49	0 1 0 0 1 0 0 1	Local ATM Format

Additional AFIs are defined for group addresses in Annex A.

AFIs 53, 55, 57, and 59 (ICD, DCC, E.164, and Local AFIs that indicate that the IDI starts with a zero) and AFIs (43 and 57) indicating an E.163 IDI (superseded by E.164) should not be used to create AESAs.

3.1.1.1 Data Country Code (DCC) Format

The IDI element of a DCC format AESA is a Data Country Code that specifies the country in which an address is registered. The codes are given in ISO 3166 [11]. The length of this field is two octets. The digits of the Data Country Code are encoded in Binary Code Decimal (BCD) syntax. The codes are 3 digits long and will be left justified and padded on the right with the hexadecimal value ‘F’ to fill the two octets. For example, the three digit DCC 007 is encoded as 0x007F.

IDP length: 5 digits

AFI value: 0x39

3.1.1.2 International Code Designator (ICD) Format

The IDI element of an ICD format AESA is a 4 digit (two octet) ICD. This ICD identifies an authority responsible for allocating and assigning values of the DSP.

The digits of the International Code Designator are encoded in Binary Coded Decimal (BCD) syntax. For more details on NSAP coding of ICD addresses see Annex A of ISO/IEC 8348 [2] (which is also available as ITU-T X.213 [3]).

IDP length: 6 digits

AFI value: 0x47

3.1.1.3 E.164 AESA Format

The IDI element of an E.164 AESA specifies an Integrated Services Digital Network (ISDN) number. These numbers include telephone numbers. The international format of these numbers will be used. These numbers can be up to 15 digits long. The length of this field is eight octets. The digits of the E.164 number are encoded in Binary Coded Decimal (BCD) syntax. The E.164 address is padded with as many leading semi-octets 0000 as needed to obtain the maximum length of 15 digits. A single semi octet 1111 is then added at the end to obtain an integral number of octets.

The full ISDN number identifies an authority responsible for allocating and assigning values of the DSP. The authority is some entity within the organization which subscribes to the ATM network interface.

IDP length: Up to 17 digits

AFI value: 0x45

3.1.1.4 Local IDI Format

The IDI is null.

IDP length: 2 digits.

AFI value: 0x49

ISO/IEC 8348 specifies AFI values for a “Local IDI”. The purpose of such an AFI is to accommodate the coexistence of OSI and non-OSI network addressing schemes, particularly in the context of transition from non-OSI to OSI protocols. In case of the Local IDI format, the IDI is null, i.e., the total length of the IDP is 2 digits (corresponds to one octet according to the preferred binary encoding).

3.1.2 Domain Specific Part (DSP)

The Domain Specific Part is subdivided into the High Order DSP (HO-DSP) and low order part which consists of the End System Identifier (ESI) and Selector (SEL).

3.1.2.1 HO-DSP

The coding of this field is specified by the authority or the coding scheme identified by the IDP. The authority determines how identifiers will be assigned and interpreted within that domain. The authority can create further sub-domains. That is, the authority may define some number of sub-fields of the HO-DSP and use these to identify a lower authority which in turn defines the balance of the HO-DSP. Sub-fields of the HO-DSP to the left are always more significant than fields to the right. The contents of this field not only describe the hierarchy of addressing authority, but should also convey topological significance. That is, the HO-DSP field of the AESA should be constructed in such a way as to facilitate hierarchical routing and efficient use of resources. This Specification makes no restriction on the number of subfields within the HO-DSP. The total length of the HO-DSP is fixed at 10 octets for the DCC and ICD formats, at 4 octets for E.164 AESA and at 12 octets for the Local AFI format.

3.1.2.2 End System Identifier (ESI)

The end system identifier identifies an end system. This identifier must be unique within a particular value of the IDP + HO-DSP. In addition, to ensure the ability of an end system to autoconfigure its address, this end system identifier can be a globally unique identifier specified by an IEEE MAC address. The length of this field is 6 octets.

3.1.2.3 Selector

The selector is not used for ATM routing, but may be used by end systems. The length of this field is 1 octet.

3.2 E.164 Numbering

E.164 numbering is defined by ITU-T Recommendation E.164, which specifies the use of numbers in establishing ISDN/telephony calls. ITU-T recommendation E.191 defines how E.164 numbers will be used within the context of Broadband ISDN.

This document refers to addresses formatted in accordance with Recommendation E.164 as “native” E.164 addresses. This differentiates them from addresses formed by encapsulating the E.164 number within an NSAP structure.

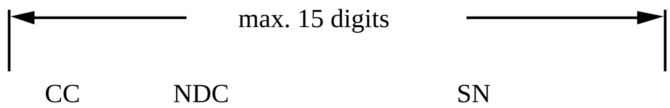
In ATM Forum specifications, the only type of E.164 number that is recognized is the international format. This differs from ITU-T Recommendations Q.2931 [12] and Q.2764 [13] which, for native E.164 addresses, allow other ‘type of number’ formats (see Section 3.2.2).

3.2.1 Description of E.164 Numbers

[Informational]

This section describes E.164 numbers as defined in ITU-T recommendation E.164 [14].

The structure of an international number according to E.164 is shown below in Figure 3-5.



CC Country Code
NDC National Destination Code, which can be of the type
- trunk code or often referred to as area code
- service access code
- destination network code

SN Subscriber Number

Figure 3-5: Number Structure According to E.164

The ITU recommendation defines the following number structure:

- The maximum length of an international number is 15 digits.
- By means of a country code, the ITU allocates numbering resources to a country (nation) or a geographical region, to a network or to a global service (e.g., International Freephone).
- National numbers generally consist of a national destination code followed by a subscriber number.

Each country has defined its own specific national numbering plan.

E.164 numbers are administered by the ITU, by the National Numbering Authority and by their delegates.

3.2.2 Restriction of the Use of E.164 to Address Semantics

An E.164 number can be either an address associated with a public UNI or a service request identifier that invokes a service (usually an address translation, e.g., 800, 500, or special billing, e.g., 800, 900). The use of E.164 numbers in ATM Forum specifications is limited to their use as addresses. This does not restrict the use, in some networks, of E.164 numbers as service request identifiers; it simply does not require such support.

No current ATM Forum Specifications define call states and exchange protocols (e.g., TCAP in SS7) that would allow a switch to exchange such service requests with a Network or Service Control Point. Therefore, services such as 800 or 900 are not supported by ATM Forum signalling protocols.

The information contained in the number fields of the Called or Calling party number information element of a call set-up message is expected to be only an address, not dialing plan information. As specified, the information in these fields is encoded as an international number. Dialing plan digits are not accommodated by the current capabilities of the ATM Forum specifications.

[Note: Dialing plan digits are typically escape sequences allowing a user at a telephone instrument to indicate what type of address information or service selection is intended by the user. In North America, for example, dialing 1 as the first digit indicates what follows is a 10 digit North American Numbering Plan number; dialing 011 as the first 3 digits indicates what follows is an international number. These conventions are not encoded in ATM Forum call setup messages. Service selection escapes, such as beginning a dialing sequence with a “*” or “#” in some networks, are also not accommodated.]

3.2.3 Terminology and Notation of E.164 Addresses

An E.164 AESA that has the DSP set to all zeros is called an Embedded E.164 AESA.

In this document, the following symbolic notation is used to describe the different types of E.164 addresses.

- An embedded E.164 AESA is denoted as **E.164e**.
- An E.164 AESA that has a non-zero DSP is denoted as **E.164A.**
- A native E.164 number is denoted as **E.164N.**

3.3 Group Addresses

An ATM Group Address is acts in the role of a service identifier rather than an address. An ATM group represents a collection of ATM end systems. An ATM group has one or more members, and an ATM end system can be a member of zero or more ATM groups at any time. An ATM end system may join or leave a group at any time by registering a group address using the ILMI client address registration and deregistration procedures (see the ATM Forum ILMI Specification, Version 4.0 [9]). The membership of an ATM end system in a group may have an address scope associated with it that determines how widely advertised or known that address is (see Section 7.5 for further details).

The only ATM Forum -defined service using group addresses is the Anycast Service. The use of the Anycast Service, as defined in UNI Signalling 4.0 and PNNI 1.0 allows multiple systems to register as a server for some service (e.g., a printer server, file server). When an end system wishes to connect to any single server for a particular service, it uses a point-to-point call setup message with the group address as the Called Party Number. The PNNI network will route the call to the "nearest" server advertising that address (i.e., of wide enough scope). *Nearest* is implementation specific in this context – this is not defined or constrained in the PNNI 1.0 specification.

Anycast procedures are only specified to support the ATM group address in the Called party number information element.

3.3.1 Format of ATM Group Addresses

There are two classes of ATM End System Addresses: individual and group addresses. These are distinguished by their AFI values. There is a fixed relationship between the AFIs of individual addresses and AFIs of group addresses. Table A-1 in Annex A defines this relationship.

Group address space is implicitly allocated when an organization obtains a block of individual addresses from a registration authority. This space is derived from the allocated individual address space using the above relationship (for example, by replacing AFI 0x47 with 0xC5).

The AFIs defined in Section 3.1 are extended to support the following new group AFIs:

AFI		Format
Hexadecimal	Bits	
0xBD	1 0 1 1 1 1 0 1	DCC ATM Format
0xC5	1 1 0 0 0 1 0 1	ICD ATM Format
0xC3	1 1 0 0 0 0 1 1	E.164 ATM Format
0xC7	1 1 0 0 0 1 1 1	Local AFI Format

3.3.2 ATM Forum Well-known Group Addresses

A well-known group address is used to identify the group of devices that provide a well-known ATM service, e.g., LAN Emulation Configuration Server (LECS) service. To support well-known group addresses for services defined in ATM Forum specifications, the ATM Forum uses ICD AESA Initial Domain Part "C50079" (derived from its IDP of 470079). For example

C5.0079.00000000000000000000.00A03E000001.00

is the well-known group address for the LECS, and

C5.0079.00000000000000000000.00A03E000002.00

is the well-known group address used by ATM Name System (ANS).

ATM Forum well-known addresses will be assigned for use in specifications of the ATM Forum's technical committees. To request an ATM Forum well-known group address, a contribution shall be submitted to the technical committee stating the need. The well-known addresses that have been assigned by the ATM Forum can be found in the ATM Forum Well-Known Addresses and Assigned Codes document on the public ATM Forum web site (see public_assigned_codes.pdf [or .txt] at http://www.atmforum.com/atmforum/specs) [15].

4 Categorization of Addresses by Ownership[6]

[Informational]

ATM address prefixes can be obtained by organizations without regard to the topologies and address prefixes of the ATM Service Provider networks to which the organizations are connected. In terms of routing, each of these prefixes is a highest level prefix, i.e., there is no topological information before the field(s) identifying the organization. At this highest level, the ATM address space is flat. If a large percentage of ATM customers get their own top level prefixes, routing tables of backbone ATM switches will become unmanageably large. Therefore, we introduce a further categorization of ATM addresses. The class of registered addresses can be split into two categories based on ownership of the associated prefix. This document uses the terms ATM Service Provider (ASP) addresses and Customer Owned (CO) addresses to differentiate addresses in this manner.

To ensure scalability of the interconnected global ATM network, the ATM Forum recommends that ASPs minimize the propagation of Customer Owned addresses. Whether or not an ASP supports Customer Owned addresses within its own network is a matter of local policy. Advertisement of customer owned addresses between ASPs, however, has the potential to both increase the size and decrease the stability of routing tables, globally.[7]

4.1 ATM Service Provider Addresses

An ATM **Service Provider address** is an address from a block of addresses allocated to the service provider by the appropriate national or world registration authority. The registration authority and the ATM Service Provider are identified in the leftmost part of the address.

In some cases, the ASP may sub-allocate part of its address space to its customers. This is particularly useful when the customer wishes to attach an ATM switch to the ASP's UNI, and thereby provide connectivity to multiple ATM end systems. The octets allocated from the ASP's address space (typically the low-order portion of the HO-DSP) can be used by the customer to construct an address plan for the devices reachable through a given UNI.

When sub-allocation of address space is used, verification of Calling Party number by the ASP can only be performed on the subset of the HO-DSP over which the service provider has retained assignment authority.

4.1.1 Example Service Provider Addresses

Figure 4-1 shows an example of an ATM Service Provider ICD AESA. In this example the ASP has allocated (y + 7) octets to its customer.

[6] In general, ATM addresses are not truly "owned" by those who obtain them from registration authorities. The registration authority may retain actual ownership of the addresses and retain the right to reclaim them.

[7] This assumes that the number of ASPs is small, relative to the number of ASP customers; that ASPs structure their addresses such that aggregation is possible; and that ASP networks are relatively stable.

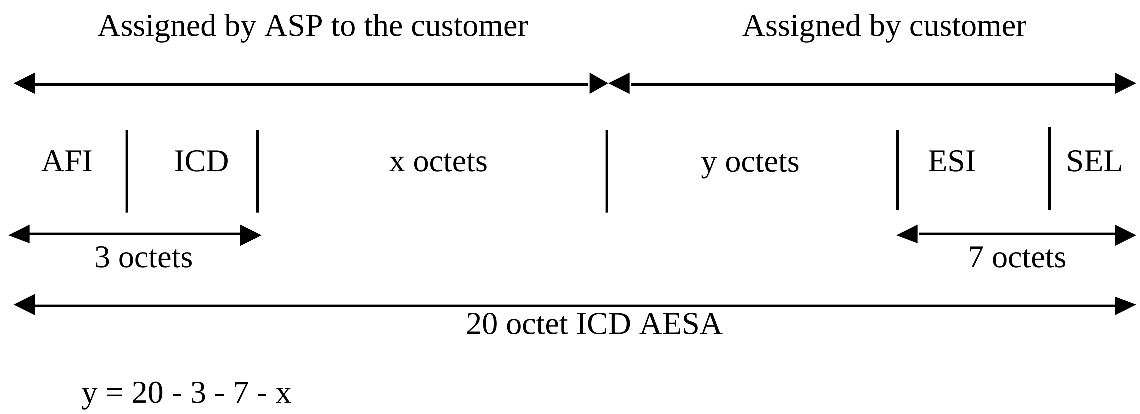


Figure 4-1: Example ASP ICD AESA

Figure 4-2 shows an example of a ATM Service Provider E.164 AESA.

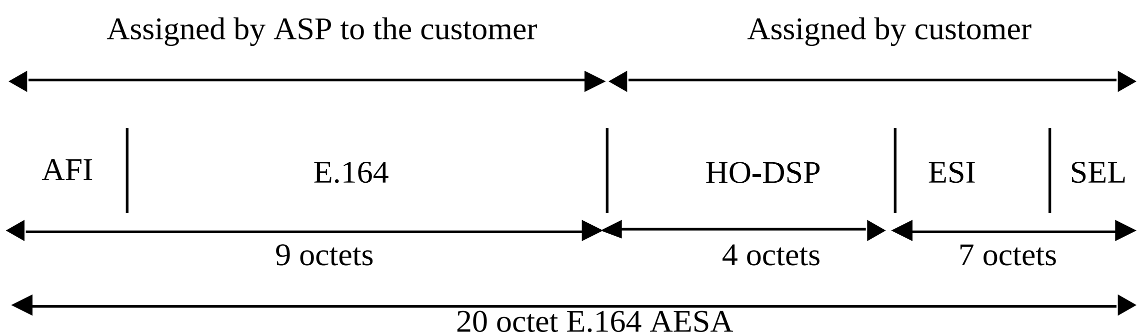


Figure 4-2: Example ASP E.164A (E.164 AESA with non-zero DSP)

4.2 Customer Owned ATM Addresses

A **Customer Owned ATM address** is an address from a block of addresses allocated directly to the private networking customer by the national or world registration authority.

4.2.1 Example Customer Owned Address

Figure 4-3 shows an example of a Customer Owned DCC AESA. After the DCC is a national code allocated by the ISO National Member Body to the customer who has applied for a DCC. The rest of the DSP may be allocated by the customer subject to rules and regulations of the ISO.

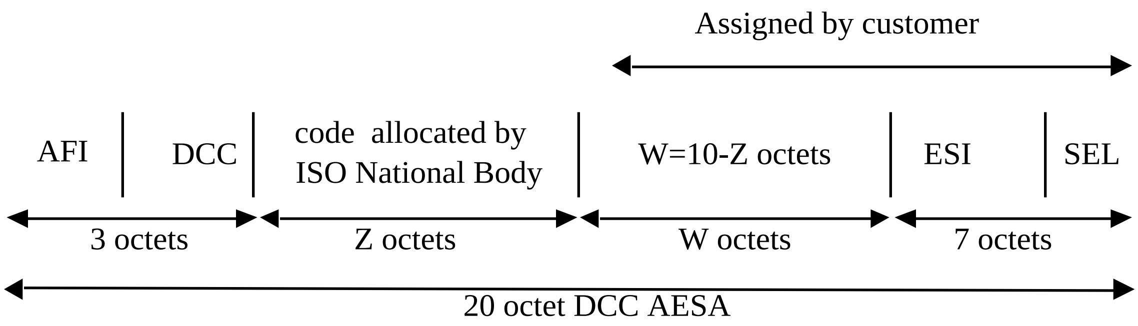


Figure 4-3: Example of a DCC Customer Owned AESA

5 Where to get Addresses

[Informational]

This section gives a guide to users and developers of ATM networks who may wish to obtain various types of ATM addresses. Section 5.1 describes the options available to ATM Service Providers wishing to obtain ATM addresses, and Section 5.2 describes where private networks may obtain ATM addresses.

5.1 ATM Service Providers

The availability and applicability of address options will vary from country to country and may be subject to regulatory rules and conditions.

5.1.1 ICD AESAs

The International Code Designator uniquely identifies a coding identification scheme. The Issuing Organization (IO), responsible for the coding scheme identified by the ICD, provides an Administrative Authority that is responsible for the allocation of identifiers within this coding scheme to organizations. For more details on ICD structure and administration see ISO 6523 [16].

An ATM Service Provider 'already possessed of an ICD, for the purposes specified in ISO 6523, may use that ICD for the *additional* purpose of allocating network addresses' [Quote from ISO/IEC 8348 Annex B]. All applications for an ICD must be submitted through a **Sponsoring Authority**, usually the National Standards body of the applicant (e.g., the American National Standards Institute [ANSI] for the US, the British Standards Institution [BSI] for the UK) to the ISO Registration Authority in accordance with the criteria established in ISO 6523.

Although a number of ICDs have been allocated to various organizations, including ASPs, it is becoming increasingly difficult to obtain an ICD for the purpose of ATM addressing. There are a number of reasons for this, including the shortage of ICD codes and the purpose for which the ICD scheme was originally intended. It was originally intended for **coding** identification, not **organization** identification. Therefore, the British Standards Institution in the UK has introduced a scheme based on the ICD format which is intended to satisfy the needs of organizations requiring ATM addresses. This scheme is known as IOTA - Identifiers for Organizations for Telecommunications Addressing.

5.1.1.1 The IOTA Scheme

The IOTA scheme uses the ICD 0124. A fixed length 6 digit IOTA identifier (called an "Organization ID") is allocated to the organization. This can be used to construct an ATM address with the following structure.

AFI	ICD	Organization ID	Organizationally Assigned	End System ID	SEL
47	01 24				

Applications for an IOTA identifier must be made to:

IOTA
BSI-DISC
389 Chiswick High Road
LONDON W4 4AL
UK

Tel: +44 181 996 9000

or an application form may be found at http://www.bsi.org.uk/disc/iota.html [17].

5.1.2 DCC AESAs

The Data Country Code is a 3 digit code that specifies the country in which an address is registered. The codes are given in ISO 3166.

The ISO National Member Body for that country (or, where no Member Body exists, another appropriate organization) allocates and assigns the Administrative Authority.

The ATM Service Provider shall apply to the ISO National Administrative Authority (Registration Authority) for ISO DCC addresses. For example, ANSI is the Registration Authority for the US, the Federation of the Electronics Industry (FEI) for the UK, and Deutsche Industrie-Normen (DIN) for Germany.

A useful list of national DCC Authorities and contact information is maintained by FEI. This information may be found at http://www.fei.org.uk/fei/dcc-nsap.htm [18].

5.1.3 E.164

E.164 numbers are administered by the ITU, the National Numbering Authority and their delegates. E.164 numbers generally identify interfaces to ATM Service Provider networks. ITU-T Recommendation E.191 [19] recommends that E.164 numbers be assigned for the purpose of addressing for broadband networks.

The ATM Service Provider who chooses to use E.164 Addresses, will apply for an E.164 address allocation from the National Numbering Authority (e.g., Oftel for the UK) or the ITU-T.

An E.164 number can be encoded in any of the following ways:

- native E.164 (**E.164N**),
- embedded E.164 AESA (**E.164e**), or
- E.164 AESA (**E.164A**).

The encoding(s) allowed at a UNI may be subject to negotiation between the customer and the ASP.

Where the E.164 has been encoded as **E.164A**, the private customer connected to the ATM Service Provider network may assign the values of the DSP.

5.1.4 Other ASP Addresses

An ASP may have the opportunity to apply to another ASP for a block of addresses. This would usually take the form of a smaller ASP applying to a larger ASP. This scenario may be subject to the commercial agreements between the ASPs involved and should not be assumed to be standard practice. This scenario may also be subject to regulatory constraints.

5.1.5 Local AFI

AESAs with AFIs 49 and C7, which represent the local AFI, should **NOT** be used for addressing within ATM Service Provider networks.

5.1.6 Other AESAs

ATM Forum specifications UNI 3.1, UNI Signalling 4.0, ILMI 4.0, and PNNI 1.0 discuss the use of ICD, DCC, and E.164 AESAs. The ATM Forum protocols can carry any AESA with binary coded DSP. However, the implications of using AESAs other than ICD, DCC, and E.164 are not understood.

5.2 Private Networks

Private ATM networks have three main methods of obtaining addresses.

1. They can apply to their ATM Service Provider for addresses.
2. They can apply to a Registration Authority for a globally unique registered address space.
3. They can create their own addresses that are not registered with any National or International Registration Authority as being used for ATM networking. These addresses shall be referred to as 'un-registered' addresses as they have not been registered with a Registration Authority for the specific use of ATM addressing. This is not a recommended practice.

5.2.1 ATM Service Provider Addresses

Usually, a user with terminal equipment will apply for, or automatically receive, an ATM address or address prefix from the user's ATM Service Provider when the user connects to the ATM Service Provider network and subscribes to switched service (i.e., the ability to establish SVCs).

Private networks may also have the opportunity to apply to their ATM Service Provider for an address prefix when they connect to the ATM Service Provider network.

Where the ATM Service Provider is using the AESA format it may assign values to the octets between the ending of the ASP assigned prefix and the end of the 20 octet AESA. The exact number of octets available for use by the private network varies and may be subject to negotiation between the ATM Service Provider and the private network.

5.2.2 Registered Addresses

There is no central ATM address registration authority, but private ATM customers can obtain Customer Owned ATM addresses from the sources identified in the following sections.

5.2.2.1 ICD AESAs

Private schemes within a single organization are not normally eligible for registration for an ICD. A private network 'already possessed of an ICD, for the purposes specified in ISO 6523, may use that ICD for the *additional* purpose of allocating network addresses' [Quote from ISO/IEC 8348 Annex B].

The British Standards Institution in the UK has introduced a scheme based on the ICD format which is intended to satisfy the needs of organizations requiring ATM addresses. This is known as the IOTA scheme - Identifiers for Organizations for Telecommunications Addressing.

5.2.2.1.1 The IOTA Scheme

The IOTA scheme uses the ICD 0124. A fixed length 6 digit IOTA identifier (called an "Organization ID") is allocated to the organization. This can be used to construct an ATM address with the following structure.

<table>
<tr><td>AFI</td><td colspan="2">ICD</td><td colspan="3">Organization ID</td><td colspan="7">Organizationally Assigned</td><td colspan="6">End System ID</td><td>SEL</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

47	01	24																	

Applications for an IOTA identifier must be made to:

IOTA
BSI-DISC
389 Chiswick High Road
LONDON W4 4AL
UK

Tel: +44 181 996 9000

or an application form may be found at http://www.bsi.org.uk/disc/iota.html [17].

5.2.2.2 DCC AESAs

The Data Country Code is a 3 digit code that specifies the country in which an address is registered. The codes are given in ISO 3166.

The ISO National Member Body for that country (or, where no Member Body exists, another appropriate organization) allocates and assigns the Administrative Authority.

The private network shall apply to the ISO National Administrative Authority (Registration Authority) for ISO DCC addresses. For example, ANSI is the Registration Authority for the US, FEI for the UK, and DIN for Germany.

A useful list of national DCC Authorities and contact information is maintained by FEI. This information may be found at http://www.fei.org.uk/fei/dcc-nsap.htm [18].

5.2.3 Unregistered ATM Addresses

Private networks may create their own addressing scheme using unregistered addresses. In so doing, they bypass the administrative chore of obtaining a block of registered addresses, but they also lose the protections associated with registered addresses.

If a network wishes to use unregistered addresses, it is recommended that they be formed using the local AFI (49), which is defined explicitly for this purpose.

Unregistered ATM Prefixes can also be formed through the use of other address formats which are not registered to the network in which they are deployed. While this may work (for a time), it presents a number of serious issues and is strongly discouraged.

5.2.3.1 Local AFI

AESAs can be created using the local AFI 49/C7. This AESA format is created purely by the private customer with no reference to an external registration authority and should only be used within the context of an isolated private network. Such numbers are **not globally unique** and can be duplicated by other private networks.

6 ATM Addressing Tools

[Informational]

This section describes ATM Forum-defined mechanisms that help support ATM addressing.

6.1 ATM Name System

ATM Forum specification “ATM Name System Specification Version 1.0” (af-saa-0069.000, [20]) defines a protocol, the ATM Name System (ANS), that can be used to translate ATM system names to ATM

Addresses. The ATM Name System is based on the Internet's Domain Name System protocol and derives its name structure similarly. The specification provides the details of the information kept for each ATM end system, how the end system contacts the ATM Name System server, and the form of the queries and replies. ATM names use the same names as in the Domain Name System, but new resource records are defined to contain the ATM addresses associated with those names. ANS supports both types of ATM addresses: ATM End System Addresses (AESAs) and native E.164 numbers.

Network administrators who maintain a large ATM enterprise network may wish to consider the use of the ATM name system to reduce the amount of work (and inaccuracies) involved in manually typing in 20 octet AESAs. In some cases, the AESA may not be portable among ASPs (portability of addresses has negative consequences for the global ATM network routing system). However, names are almost always portable. For this reason, ATM end-system names should be the item exchanged among users, not AESAs.

The ATM Name System is not widely deployed. While it is based on the DNS, the new resource record types containing the ATM Addresses are not recognized by most DNS server software, nor is there easily available client software that performs a query for that information.

6.2 ILMI Address Registration

The ILMI protocol includes mechanisms for address assignment at the UNI. The switch uses the ILMI address registration protocol to provide one or more 13 octet prefixes to the end system. It is expected that just one AESA prefix will normally be supplied to the end system; typically the same 13 octet prefix will be used even if there are multiple ATM addresses on the same UNI. The end system constructs an AESA by appending its End System Identifier (ESI) and a Selector to the prefix provided by the switch. The resulting 20 octet address is then returned to the switch. . The end system may register multiple addresses using different network prefixes or different ESIs. The switch uses the addresses, usually after validating the prefix(es) of the returned address(es), to identify the UNI for purposes of call delivery. For the purposes of address registration, the value of the Selector field is irrelevant, i.e., one address is a duplicate of another if they have the same 13 octet prefix and ESI values, even if they have different Selector values.

The ILMI address registration protocol may also be used to inform end systems of native E.164 numbers assigned to the Public UNI by the ATM Service Provider. For native E.164 numbers, the switch supplies the whole ATM address to the end system. In effect, the network prefix is the native E.164 number and can only be validly combined with a null user part. In this situation, the use of multiple network prefixes at a single UNI occurs whenever multiple native E.164 numbers are used at that UNI.

The most recent version of ILMI is defined in the ATM Forum ILMI 4.0 specification [9].

7 Routing

[Informational]

Routing in this document is used to mean either:

1. The procedures whereby a (source or intermediate) node, using the call set-up destination address (called party number), determines where the call set-up should be forwarded next. In PNNI networks this process determines not only the next node, but all nodes from the source to the destination; or

2. The PNNI routing information distribution protocol which allows a node to advertise the prefixes to which it has direct reachability. This process also advertises the status (and the resource allocation) of all directly attached links. This information is distributed to all nodes in the network.

PNNI routing information distribution allows each node to construct a routing table that is used to determine the path from a source node to the egress node serving a given destination (as defined by an AESA prefix). Prefixes of varying lengths, depending on how much is necessary to distinguish an appropriate route, are kept in the routing table. The route from the source to the destination is based on the called party number's 19 octet prefix in conjunction with the routing table.

7.1 Address Aggregation

Address summarization/aggregation is one mechanism that is used to allow networks to scale. If all the addresses assigned in a locality of the network share a common prefix, then that prefix can be used in other parts of the network instead of enumerating each local address. Note that in this context the term *locality* refers to network topology, not necessarily geography.

An address aggregate is a set of addresses that are derived from a common prefix **and** a common locality within the network (e.g., the interfaces on a switch or cluster of switches). Address aggregates are used by routing protocols as an abbreviation for the associated set of destination interfaces. If addresses which share a common prefix **do not** have a common locality, the result of their aggregation is normally not useful for routing.

Thus one goal of address plan design is to consistently assign addresses in a locality of the network topology such that they share a common address prefix. If an address or a smaller aggregate (longer prefix) is assigned outside the locality of the larger aggregate, then it is called an *exception* and requires a separate entry in the routing table to identify it throughout the network. The benefit of aggregation is therefore inversely proportional to the number of exceptions which need to be provided. Guidelines are proposed in Section 9 to control the potential explosion of non-aggregatable address prefixes.

A primary concern is to reduce the *number of non-aggregatable address prefixes*. While the support of multiple address formats may reduce the extent to which addresses may be aggregated, the use of multiple formats is not itself the concern. The concern is the extent to which the network's address structure reflects the network topology and so facilitates address aggregation. See Section 3 of the PNNI 1.0 specification for related information.

7.2 Longest Prefix Matching

Routing within the AESA address space is based on matching the called party number against the entries (prefixes) in the routing table. There may be several entries that begin with the same few octets. For example, all US DCC AESAs begin with the same 4 octets; all US DCC AESA prefixes within the same organization begin with the same 7 octets (where the 8th octet might be used to distinguish one site from another). Thus each entry in the routing table has a prefix and its length (in bits) associated with a source route (if using PNNI) or an out-bound trunk (possibly more than one, with a metric allowing selection of the "best").

The 19 octet prefix of the called party address might match, to some number of bits in length, many of the prefixes in the routing table. The longest match is the prefix in the routing table that matches the 19 octet prefix of the called party to the largest number of bits. The source route or out-bound trunk of the longest match typically determines where the call should be routed.

7.3 Address Prefix Aggregation

Longest prefix matching allows for *address aggregation*. Because an ASP prefix is usually structured geographically in its high order parts (by country, region within country, etc.), routing tables for nodes in New York do not need to know all the address prefixes of nodes in California. They need to know only that those nodes can be reached by traversing one or more of the trunks directly attached. Thus all the 13 octet prefixes (104 bits) of UNIs and nodes in California can be represented as a single, shorter, prefix (say 72 bits long, for example). This means that routing tables can be quite small and that scaling properties are good. Note that the aggregation of addresses typically is not automatic, but done by administration during the network planning phase.

When customer *networks* are attached, however, there are problems. Such customers may use customer-owned addresses, as described in Section 4.2. These addresses are not necessarily distributed across the ASP network in any fashion that might allow address prefix aggregation (i.e., the customer's high order address might be structured by organization within the enterprise, e.g., finance, engineering, sales). The numbering plan must align with network topology to allow aggregation to occur, and we have no guarantee that a particular customer has numbered its network to align with an ASP's topology. Aggregation, therefore, may not be possible.

In practice, customers with locations in many parts of the country (or the world) will likely have numbering plans that use geography, at least roughly, in their structure. ASPs may be able to aggregate to some degree using these addresses. However, each point at which the customer attaches to the ASP network typically results in one or more exception routes. The ASP's routing table size grows linearly with the number of attachments using customer owned addressing. Such growth inhibits scaling to a global network.

7.4 Distribution of Addressing Information

Address prefixes may be distributed using a routing protocol, e.g., PNNI, that allows a node to pass to each of its neighbors information about what it has directly connected to it and what it has learned from its other neighbors. This is called "flooding". In a connected network, all nodes are reachable, via some concatenation of neighbors, from all others. This information from one node is passed, hop by hop, to all the others. Aggregation occurs along the way, so not all information is passed. As information is aggregated, detail is lost, but reachability is not.

Networks without a dynamic routing protocol (e.g., BISUP networks) must manually (or through some network management system) provision the routing tables in each switch with the appropriate address prefixes.

7.5 Address Scope

The scope of an address determines how widely advertised or known that address is. The scope identifies the inclusive routing hierarchy in which the address is known. Calls made to the address by an ATM end system within this routing range may reach the destination and calls made to the address by an ATM end system outside the routing range will not reach the destination.

The address scope is learned when an address is registered (e.g. via ILMI) or provisioned. The ATM Forum ILMI 4.0 specification supports client registration of address scope.

The term *address scope* as used for group addresses, replaces the term *membership scope* used in ATM Forum UNI Signalling 4.0.

Within a network, the scoping model for enumeration of scope levels is defined by the network routing system. This scoping model should be structured according to the network's routing hierarchy. For example, in ATM Forum PNNI, the scope levels are enumerated using the PNNI routing level.

To allow flexibility in re-structuring a network's routing levels while not affecting the user's scope control, the address scope uses an indirect mapping from the user's scoping model to a network's routing scope. This mapping is network specific and shall be configurable.

The ATM Forum has defined one scoping model that can be used across routing domain boundaries (e.g. at a UNI). This is called the *organizational scope* model. This scoping model is defined in Annex B - Organizational Scope.

7.5.1 Group Address Scope

Group addresses are defined in Section 3.3.

Since advertisement of a group address is the mechanism for announcing group membership, the scope of a group address determines the region of the network in which the membership is to be known. If multiple separate registrations of a group address are known by one entity advertising that group address, the group address should be advertised with the widest scope among the multiple registrations.

By default, the scope of a group address should be constrained to a limited portion of the network. In ATM Forum specifications (e.g. ILMI 4.0 and UNI Signalling 4.0), the default organizational scope for a group address is always 'local'.

7.5.2 Individual Address Scope

Individual addresses can also have a scope associated with them. ILMI 4.0 supports the registration of individual address scope. PNNI 1.0 supports advertisement of individual addresses within a limited scope.

The default organizational scope for an individual address is always 'global'.

8 Signalling

[Informational]

This section describes a number of information elements that are used within various signalling protocols for the carriage or manipulation of routing and addressing information. This section covers the following protocol specifications:

1. UNI Signalling 4.0 [8] (and the Addressing Addendum [21])
2. PNNI 1.0 [5]
3. BICI 2.0 [22] (and the addendum, BICI 2.1 [23])

UNI and PNNI signalling are based on Q.2931 [12], while BICI (BISDN [Broadband ISDN] Inter Carrier Interface) signalling is based on BISUP (Broadband ISUP [ISDN User Part]). ITU-T's BISUP is defined in Q.2764 [13] and related ITU-T specifications.

8.1 Called Party Number

The Called Party Number (CdPN) is used to carry the address that is used for routing within or across ATM networks.

Note: Although not explicitly defined, the following is also true for the Calling Party Number, which is used to identify the origin of a call.

8.1.1 UNI

On a UNI, the CdPN contains either an E.164N or an AESA.

When an AESA is carried in the CdPN, the Type of Number is coded as "Unknown", and the Addressing/Numbering Plan Identification is coded as "ATM End System Address".

Note: Q2931 (1995) uses the Numbering Plan Identification (NPI) "NSAP Addressing" rather than "ATM End System Address".

When an E.164N is carried in the CdPN, the Type of Number is coded as "International number", and the Addressing/Numbering Plan Identification is coded as "Recommendation E.164".

8.1.1.1 Public UNI

On a Public UNI, the CdPN in a SETUP or ADD PARTY message contains either an E.164N or an AESA.

The types of addresses supported on a given Public UNI are determined by agreement with the ATM Service Provider.

8.1.1.2 Private UNI

On a private UNI, the CdPN in a SETUP or ADD PARTY message contains an AESA.

8.1.2 BICI

On a BICI interface, the CdPN in an Initial Address Message (IAM – the BISUP equivalent of a SETUP or ADD PARTY message) contains an E.164N. This E.164N may contain a 'null' value (i.e., no address digits). Such a 'null' value may indicate that the Transit Network Selection (see Section 8.4) or the AESA for Called Party (see Section 8.3) value should be used for routing.

8.1.3 PNNI

On a PNNI interface, the CdPN in a SETUP or ADD PARTY message contains an AESA.

8.2 Called Party Subaddress

The subaddress, carried in the Called Party Subaddress (CdPSA)/Calling Party Subaddress (CgPSA) provides additional information to identify the user/application. Furthermore, it may also be used for tunnelling private addresses through intermediate networks. In the UNI 3.1 and UNI Signalling 4.0 specifications, the use of the Called Party Subaddress to carry an AESA was only allowed if the Called Party Number was in E.164N format. However, this restriction is relaxed in the Addressing Addendum to UNI Signalling 4.0 [21], which allows the use of the CdPSA to carry an AESA even if an AESA appears in the CdPN. The addressing addendum also allows the CdPSA at the private UNI to contain an AESA, which was previously not supported.

Note: Although the following sections do not mention the Calling Party Subaddress (CgPSA), the statements about the CdPSA are also true for the CgPSA.

8.2.1 UNI

UNI Signalling 4.0 allows a SETUP message to convey up to two Called party subaddress information elements - one containing an AESA, and the other containing any other type than AESA (NSAP or user-specified). The ‘Type of sub-address’ is coded as “ATM endsystem address” for an AESA, as “NSAP (Rec. X.213 | ISO/IEC 8348)” for an NSAP, and as “user-specified” for a user-specified address.

Note: ITU-T Recommendation Q.2931 describes the same Type of sub-address codepoint as “User specified ATM endsystem address” rather than “ATM endsystem address”.

Q.2931 supports only one instance of a CdPSA (and one instance of a CgPSA) in a message.

8.2.1.1 Public UNI

The carriage of the CdPSA is a subscription option at the public UNI, i.e., the private network must negotiate with its ASP to provide this service (carriage of CdPSA).

The CdPSA may contain an AESA, an NSAP, or a user-specified address.

8.2.1.2 Private UNI

The CdPSA may contain an AESA, an NSAP or a user-specified address.

8.2.2 BICI

The CdPSA may contain an AESA, an NSAP, or a user-specified address.

BICI does not discuss a second Called Party Subaddress. ITU-T BISUP supports only one CdPSA (and one CgPSA) parameter.

8.2.3 PNNI

The CdPSA may contain an AESA, an NSAP, or a user-specified address.

PNNI supports the passing of two Called Party Subaddresses.

8.3 AESA For Called Party Number

The AESA for Called Party (AESA4CdP) parameter is only present at the BICI (or ITU-T BISUP) interface. It is not defined for the UNI or PNNI. It was added to BICI (and ITU-T BISUP) because BISUP does not support AESAs in the Called Party Number parameter.

This parameter is used by an ATM Service Provider that is running BICI/BISUP within or between networks, for the transparent transport of any of the following AESAs:

- DCC AESA
- ICD AESA
- E.164 AESA (E.164A)

Q.2726.1 (an ITU-T BISUP recommendation) [24] defines this parameter.

When interworking a Q.2931-based interface (e.g., UNI, PNNI) with BISUP, and an E.164 AESA is received in the Called party number information element of a SETUP or ADD PARTY message, a switch does the following when constructing the outgoing Initial Address Message (IAM):

· Place this E.164 AESA in the AESA4CdP parameter.

· Extract the E.164 portion of the E.164 AESA and place it in the Called Party Number parameter.

When interworking a Q.2931-based interface with BICI, networks may optionally also support DCC and ICD AESAs received in Called party number information elements. In this case, the AESA is placed in the AESA4CdP parameter, and a valid E.164 address is placed in the Called Party Number parameter. This E.164 number may be obtained via network-specific means, or a "null" (zero length) E.164 address may be coded in the Called Party Number parameter.

If a null E.164 address is received in the Called Party Number parameter of the incoming IAM, the receiving network may progress the message by routing on the Transit Network Selection (TNS) parameter, if present. If no TNS is present in the incoming IAM, and the CdPN parameter contains a null E.164 address, the receiving network may base its route selection on the AESA for Called Party parameter, or may clear the call.

When exiting a BISUP network, the contents of the AESA4CdP parameter is placed in the Called party number information element of the outgoing SETUP or ADD PARTY message.

Note that the AESA for Calling Party parameter is defined and works similarly to the AESA for Called Party parameter.

8.4 Transit Network Selection

The Transit Network Selection information element/parameter is defined in standards for the UNI, PNNI and BISUP interfaces. However, the procedures on how to use transit network selection are subject to national regulations.

Currently, carriers in the U.S. (e.g., Interexchange Carriers) are identified by 3-digit carrier identification codes (XXX codes). Starting in 1995, these codes are allowed to be expanded to 4-digit codes (XXXX). Therefore, the possibility of both 3- and 4-digit carrier identification codes must be taken into account. These carrier identification codes are carried in the TNS.

TNS overrides normal Called Party Number based routing. If the TNS is present in the SETUP message, it will be used for routing purposes. The call shall be routed to the carrier indicated in the TNS. The mandatory Called Party Number may contain no address digits or a valid set of address digits. The TNS parameter is not normally passed to the selected carrier network.

Note: For more information on routing within BICI domains, refer to Addendum to B-IC1 2.0 (BICI 2.1).

8.4.1 PNNI

PNNI 1.0 supports advertisement of reachability from a PNNI node to a transit network, but does not support identification of a PNNI node as a specific transit network. PNNI supports TNS only as a means of selecting an exit point from the PNNI domain.

If the TNS information element is present in the SETUP or ADD PARTY message, the call is routed based on the specified Transit Network Selection. Optionally the called party address may also be considered to select one of several paths to the specified transit network.

8.5 Summary

The following table gives a summary of the type of signalling protocol information elements used in ATM networks and the address types that may appear in each element.

Table 8-1: Signalling Summary

			AESA	E.164N	E.164A	E.164e	non-AESA	Carrier code
CdPN	UNI	Public	√	√	√	√	-	-
		Private	√	-	√	√	-	-
	BICI		-	√	-	-	-	-
	PNNI		√	-	√	√	-	-
CdPSA	UNI	Public	√	-	√	√	√	-
		Private	√	-	√	√	√	-
	BICI		√	-	√	√	√	-
	PNNI		√	-	√	√	√	-
AESA4CdP	BICI		√	-	√	√	-	-
TNS	UNI	Public	-	-	-	-	-	√
		Private	-	-	-	-	-	√
	BICI		-	-	-	-	-	√
	PNNI		-	-	-	-	-	√
Additional CdPSA	UNI[8]	Public	√	-	√	√	√	-
		Private	√	-	√	√	√	-
	PNNI		√	-	√	√	√	-

Key: √ = information element/parameter can be populated with the value indicated
- = information element/parameter cannot be populated with the value indicated
Note: carriage of a Customer Owned AESA is subject to agreement by the ASP.

[8] If two CdPSAs are carried in a UNI SETUP message, one must be an AESA and the other a non-AESA.

9 Basic Rules of Address Interworking

[Informational]

This section provides some basic rules for interworking.

The following Annex and Appendixes provide more examples of interworking:

- Annex C describes interworking with Narrowband ISDN,
- Appendix I gives more detailed examples of address interworking, and
- Appendix II provides a detailed explanation of interworking between networks that are using various formats of E.164.

9.1 Between ASP and Private Networks

In addition to assignment of address information to customers and its use in routing, customers may also request call set-up to destination addresses that have not been assigned to them (for example, other customers of the same ATM Service Provider or customers of another ATM Service Provider).

All aspects of call setup may be subject to restriction by an ASP with the concurrence of the calling and called parties. For example, call requests to destinations on the same ASP as the originating customer, but to addresses other than those assigned to that customer may be blocked or not. Some customers may request that other customers not be allowed to call them. Customers should investigate the status of reachable parties during subscription.

At the interface between the private network and an ASP, as a minimum, ATM Service Provider addresses must be supported in the CdPN and, as an optional extra, the ASP may support Customer Owned addresses.

An ATM Service Provider that offers SVC services to its subscribers will typically also offer addressing services in conjunction with it. This addressing service *may* include the assignment of addresses from an address space administered by the service provider (i.e., the ATM Service Provider offers the use of its own ASP addresses). In addition the ASP *may* also include the capability for the subscriber to use Customer Owned addresses. Such addresses may be used for call setup by a service provider. They may be used directly (i.e., by loading them into the ASP switch routing tables) or indirectly (i.e., by translation from a CO address to an ASP address at ingress).

When the ASP only accepts calls using ASP addresses, calls to private networks using customer-owned addresses may still be supported by using address translation at the originating endpoint or at the private side of the Public UNI. In this case, the customer-owned addresses are carried across the ASP network as subaddresses.

AESAs based on the local AFI are not used for routing by ATM Service Provider networks.

9.1.1 E.164 Support and Delivery

To handle proper delivery of E.164 addresses across Public UNIs, each Public UNI must be configured to send one of the following sets of E.164 address types in the CdPN and CgPN:

1) only E.164N addresses, or

2) only E.164A and E.164e addresses, or

3) E.164N, E.164A, and E.164e.

A call originated on a Private UNI destined for an end system which only has a native E.164 address (i.e., a system directly attached to a public network supporting the native E.164 format) will code the CdPN as an embedded E.164 (i.e., an E.164 AESA format, with the DSP field set to zero).

9.2 Between ASP and ASP Networks

It is expected that the wider public network will route ATM calls using ASP addresses. This should reduce the number of entries in top level world route tables.

9.3 Between Private Networks

A private network may accept and route on any of the recognized AESAs. Not all private networks will accept all AESA formats. The AESA formats supported at an interface between two private networks should be agreed upon by the two private organizations. Call screening of the addresses specified in the setup or add party indication may also be used within between private networks.

9.4 E.164 Interworking

E.164-based addresses may be encoded as E.164N, E.164e, E.164A, or combinations of these three types (e.g., E.164N CdPN with E.164A CdPSA). As described in Section 8, different interfaces may support different combinations of E.164N and/or AESA (including E.164e and E.164A) formats in the Called and Calling party number information elements. The encoding type of E.164-based addresses may need to be converted as a call is progressed across different interfaces supporting different address formats.

The basic rules for conversion of E.164-based addresses are as follows:

- E.164N and E.164e encodings of the same E.164 address indicate the same location. These two encodings can be interchanged as a call is progressed. An E.164A based on the same E.164 address indicates a different location, usually located in the private network behind the Public UNI indicated by the E.164 address.
- E.164N may be converted to E.164e by using the AFI 0x45, placing the E.164 address in the IDI (encoded and padded as described in Section 3.1.1.3) and adding a DSP of all zeros.
- E.164e may be converted to E.164N by extracting the E.164 address from the IDI. In some cases the E.164e may be carried in addition to the converted E.164N form (see Section 8.3 for one example).
- E.164A may be converted to E.164N by extracting the E.164 address from the IDI, but the E.164A *must* be carried in addition to the converted E.164N (e.g. in the CdPSA, CgPSA, AESA4CdP, or AESA4CgP, depending on the network interface) so that the information in the DSP is not lost.

Tables with detailed E.164 interworking scenarios are included in Appendix II.

10 Acronyms

AA – Administrative Authority
AESA – ATM End System Address
AESA4CdP – AESA for Called Party
AESA4CgP – AESA for Calling Party
AFI – Authority and Format Identifier
ANS – ATM Name System
ANSI – American National Standards Institute
ASP – ATM Service Provider
ATM – Asynchronous Transfer Mode
BCD – Binary Coded Decimal
BISUP – Broadband ISDN User Part
BSI – British Standards Institution
B-TE – Broadband Terminal Equipment
CdPN – Called Party Number
CdPSA – Called Party Subaddress
CgPN – Calling Party Number
CgPSA – Calling Party Subaddress
CO – Customer Owned
DCC – Data Country Code
DFI – Domain Specific Part Format Indicator
DIN – Deutsche Industrie-Normen
DSP – Domain Specific Part
E.164A – E.164 AESA
E.164e – E.164 embedded
E.164N – Native E.164
ESI – End System Identifier
FEI – Federation of the Electronics Industry
HO-DSP – Higher Order Domain Specific Part
ICD – International Code Designator
IDI – Initial Domain Identifier
IDP – Initial Domain Part
IE – Information Element
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
IISP – Interim Interswitch Signalling Protocol
ILMI – Integrated Local Management Interface
IO – Issuing Organization
IOTA - Identifiers for Organizations for Telecommunications Addressing
ISDN – Integrated Services Digital Network
ISO – International Organization for Standardization
ISUP – ISDN User Part
IWF – Interworking Function
ITU-T – International Telecommunications Union – Telecommunication Standardization Sector
LAN – Local Area Network
LECS – LAN Emulation Configuration Server
MAC – Media Access Control
N-ISDN – Narrowband ISDN
NSAP – Network Service Access Point

OSI – Open Systems Interconnection
PNNI – Private Network-Network Interface
PNP – Private Numbering Plan
PSTN – Public Switched Telephone Network
SEL – Selector
SS7 – Signalling System Number 7
TCAP – Transaction Capabilities Application Part
TNS – Transit Network Selection
UNI – User Network Interface

11 References

1. ATM Forum, "ATM Forum Addressing: User Guide," af-ra-0105.000.
2. ISO/IEC, "Information technology – Open Systems Interconnection – Network Service Definition," ISO/IEC 8348:1996(E), 1996-09-15.
3. ITU-T, "Information technology - Open Systems Interconnection - Network Service Definition," X.213 (1995 E), November 21, 1995.
4. ISO, "Information technology – Telecommunications and information exchange between systems – Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)," ISO 10589, 1992.
5. ATM Forum, "Private Network-Network Interface Specification version 1.0 (PNNI 1.0)," af-pnni-0055.000, March 1996.
6. R. Colella, R. Callon , E. Gardner, Y. Rekhter "Guidelines for OSI NSAP Allocation in the Internet," RFC 1629, May, 1994.
7. ATM Forum, "ATM User-Network Interface (UNI) Specification Version 3.1," af-sig-0010.002, September, 1994.
8. ATM Forum, "ATM User-Network Interface (UNI) Signalling Specification Version 4.0," af-sig-0061.000, July 1996.
9. ATM Forum, "Integrated Local Management Interface (ILMI) Specification," Version 4.0, af-ilmi-0065.000, July 1996.
10. ATM Forum, "Voice and Telephony Over ATM to the Desktop Specification," af-vtoa-0083.001, 1998.
11. ISO, "Codes for the representation of names of countries," ISO 3166:1993(E/F), 1993-12-15.
12. ITU-T, "Broadband Integrated Services Digital Network (B-ISDN) - Digital Subscriber Signalling System No. 2 (DSS 2) - User-Network Interface (UNI) Layer 3 Specification for Basic Call/Connection Control," Recommendation Q.2931, February 7, 1995.
13. ITU-T, "Broadband Integrated Services Digital Network (B-ISDN) - Signalling System No. 7 B-ISDN User Part (B-ISUP) - Basic Call Procedures," Recommendation Q.2764, February 7, 1995.
14. ITU/CCITT, "Numbering Plan for the ISDN Era," Recommendation E.164, August 23, 1991.
15. ATM Forum, "ATM Forum Well-Known Addresses and Assigned Codes," http://www.atmforum.com/atmforum/specs/public_assigned_codes.pdf).
16. ISO, "Data interchange – Structure for the identification of organizations," ISO 6523-1984(E), 1984-02-01.
17. British Standards Institution, IOTA application form, http://www.bsi.org.uk/disc/iota.html.
18. FEI, List of DCC Authorities, http://www.fei.org.uk/fei/dcc-nsap.htm.
19. ITU-T, "B-ISDN numbering and addressing," Recommendation E.191, 10/96.
20. ATM Forum, "ATM Name System Specification Version 1.0," af-saa-0069.000, November 1996.
21. ATM Forum, "Addressing Addendum for UNI Signalling 4.0," af-ra-0107.000.
22. ATM Forum, "BISDN Inter Carrier Interface (B-ICI) Specification, version 2.0 (Integrated)," af-bici-0013.003, December 1995.
23. ATM Forum, "Addendum to BISDN Inter Carrier Interface (B-ICI) Specification, v2.0 (B-ICI Specification v2.1)," af-bici-0068.000, November 1996.
24. ITU-T, "Broadband ISDN – B-ISDN application protocols of the network - B-ISDN user part – ATM end system address," Recommendation Q.2726.1, July 9, 1996.
25. ISO/IEC 11571, "Information technology - Telecommunications and information exchange between systems - Numbering and sub-addressing in private integrated services networks," ISO/IEC 11571:1994, 1994.

Annex A - Individual and Group AFI Values

[Normative]

Table A-1: Relationship of AFI Individual and Group Values

Individual	Group	Individual	Group	Individual	Group
0xFF					
10	A0	40	BE	70	DC
11	A1	41	BF	71	DD
12	A2	42	C0	72	DE
13	A3	43	C1	73	DF
14	A4	44	C2	74	E0
15	A5	45	C3	75	E1
16	A6	46	C4	76	E2
17	A7	47	C5	77	E3
18	A8	48	C6	78	E4
19	A9	49	C7	79	E5
20	AA	50	C8	80	E6
21	AB	51	C9	81	E7
22	AC	52	CA	82	E8
23	AD	53	CB	83	E9
24	AE	54	CC	84	EA
25	AF	55	CD	85	EB
26	B0	56	CE	86	EC
27	B1	57	CF	87	ED
28	B2	58	D0	88	EE
29	B3	59	D1	89	EF
30	B4	60	D2	90	F0
31	B5	61	D3	91	F1
32	B6	62	D4	92	F2
33	B7	63	D5	93	F3
34	B8	64	D6	94	F4
35	B9	65	D7	95	F5
36	BA	66	D8	96	F6
37	BB	67	D9	97	F7
38	BC	68	DA	98	F8
39	BD	69	DB	99	F9

Annex A - Organizational Scope

[Normative]

The ATM Forum has defined one scoping model for enumeration of scope levels that can be used across routing domain boundaries (e.g., at a UNI). This is called the *organizational scope* model. The organizational scope model is used at the ATM Forum UNI in ILMI 4.0 and UNI Signalling 4.0. This scoping model is used in two different contexts: to identify the scope of an address (see Section 7.5), and to identify the maximum scope of a connection (see Section 7.2 and Annex 6 of UNI Signalling 4.0).

To allow flexibility in re-structuring a network's routing levels while not affecting the user's scope control, ATM Forum specifications use an indirect mapping from the user's scoping model (e.g. organizational scope) to a network's routing scope. This mapping is network specific and shall be configurable. The PNNI 1.0 specification defines the default mapping from the *organizational scope* to the routing level of PNNI's routing protocol.

The design of the organizational scope control considers how it may be used in the real world. Most applications would like to control the reachability according to a human organization's hierarchy such as intra-network, intra-site, intra-organization, intra-community, and global. This model is adopted to design the organizational scope model for ATM networks.

To allow finer granularity between the identified organizational hierarchy and to allow growth, fifteen levels of scope hierarchy are defined as follows:

1 local network
2 localPlusOne
3 localPlusTwo
4 siteMinusOne
5 intraSite
6 intraSitePlusOne
7 organizationMinusOne
8 intraOrganization
9 organizationPlusOne
10 communityMinusOne
11 intraCommunity
12 communityPlusOne
13 regional
14 interRegional
15 global

The following defines the semantic of the identified organizational scope levels -

1. Local Network - this shall map to the concept of a physical network. Using Ethernet as an example, a single Ethernet segment and multiple Ethernet segments extended by repeaters or bridges may be treated as a local network. Therefore, the network operator shall configure the mapping of organizational scope “local network” to map to the routing levels which provides the semantics as defined above. For example, the mapping may be to a bottom level peer group, or a peer group of higher level in PNNI’s routing hierarchy to simulate extended physical networks.

2. The levels 2-4 may be mapped to ATM sub-networks which do not use inter-building or wide-area links.

3. Intra-Site - this scope identifies the inclusive routing hierarchy which are not geographically separated. This is to allow the network operator to confine the traffic within a local location, therefore to avoid using wide-area links or inter-building links.

4. The levels 6-7 can be used to identify ATM networks that may use inter-building links or wide-area links.

5. Intra-Organization - this scope identifies ATM networks which represent the inclusive routing hierarchy of an autonomous organization. An autonomous organization is defined to be an

organization who has administrative authority of the network. The ATM networks identified by this organizational scope therefore may use inter-building and wide-area links.

6. The levels 9-10 can be used to identify union of more than one organizations.

7. The levels 11-14 can be used to identify ATM networks which represent a collection of autonomous organizations that are organized by a provider or organizational partnership.

8. Global - this scope represents all autonomous organizations which form a connected ATM network.

In ATM Forum specifications (e.g. ILMI 4.0 and UNI Signalling 4.0), the default organizational scope for a group address is always ‘local’. The default organizational scope for an individual address is always ‘global’.

Annex A - Interworking With Public and Private N-ISDN

[Normative]

This section supersedes Section 6 af-vtoa-0083.000.

This section applies to UNI and PNNI.

To interwork an ATM address with a public or private N-ISDN, there needs to be a way to map between one address to the other. Many means are available, e.g.: a database look-up mechanism such as the ATM Name System Specification (af-saa-0069.000) can be used, the same address formats can be used in both cases, or an algorithmic mapping between the two addressing plans can be defined.

11.1 Interworking with Public N-ISDN

A public N-ISDN address consists of an E.164 number (E.164N).

If E.164N address structure is used on the ATM network side of the interworking function (IWF), the mapping between the ATM address and the N-ISDN E.164 address is trivial for all addressing information elements (Called party, Calling party or Connected number information elements).

If an AESA format is used on the ATM Network side of the IWF, the following will apply.

For outgoing calls from an ATM Network through an IWF to a public N-ISDN, an E.164e may be used (embedded E.164 AESA - see Section 3.2.3).

In order to be able to be reached directly from the global public Narrowband ISDN (N-ISDN) and Public Switched Telephone Network (PSTN) through an interworking function (IWF), a B-TE (Broadband Terminal Equipment) must have an E.164 number assigned to it in the public N-ISDN/PSTN. This does not imply that an E.164e or E.164A has to be used within the ATM network. However, if the B-TE uses that E.164e or E.164A in the ATM network in the AESA, the IWF can easily map the numbering information between N-ISDN and ATM network by doing a simple format translation. One way to accomplish a simple format translation is to use an E.164e for the Called party number information element in a call from the IWF to the ATM network.

Note - On the ATM network side of the IWF, an E.164 number (within the E.164e or E.164A) is always a full international E.164 number. On the N-ISDN side, it may be a subscriber or national number, or even a partial number. The IWF has to perform the conversion.

If the ATM network supporting the B-TE cannot establish a call based on E.164 addresses, the IWF will have to maintain a database to map between the non-E.164 ATM addresses used within the ATM network and the corresponding E.164 numbers, or it will have to have a mechanism to algorithmically map between the ATM address and the E.164 number. Such mechanisms are outside the scope of this specification.

11.2 Interworking with Private N-ISDN

Private N-ISDNs typically allow for the use of E.164 numbers, in which case Section 11.1 applies. This section applies to interworking with private N-ISDN Private Numbering Plan (PNP) addresses as defined in ISO/IEC 11571 [25].

In order to be able to be reached directly from a private N-ISDN through an interworking function (IWF), a B-TE must have a PNP number assigned to it in the private N-ISDN. This does not imply that the Local AESA format (see Section 3.1.1.4) has to be used within the ATM network. However, if the B-TE encodes that PNP number in the ATM network using the Local AESA format, the IWF can easily map the numbering information between N-ISDN and ATM network provided that an algorithmic mapping between the numbers is defined. Similarly, for outgoing calls from an ATM network through an IWF to a private N-ISDN, a PNP number in the ATM network in the Local AESA format could be algorithmically mapped to a PNP number in N-ISDN.

Note - On the ATM network side of the IWF, a PNP number is always a number at the highest level, i.e., the full PNP number. On the N-ISDN side, it may be at a lower level. The IWF has to perform the conversion.

If the private ATM network supporting the B-TE cannot establish a call based on a PNP number encoded in the Local AESA format, the IWF will have to maintain a database to map between the non-PNP ATM addresses used within the private ATM network and the corresponding PNP numbers, or it will have to have a mechanism to algorithmically map between the ATM address and the PNP number. Such a mechanism is outside the scope of this specification.

11.3 Suggested Encoding of the PNP Digits in the Local AESA Format

This section suggests an encoding mechanism for PNP numbers in the Local AESA format allowing for a simple algorithmic mapping. This suggested format may not be feasible if the Local AESA format is also used for other addressing plans within a private ATM network.

Use of the Local format for these non-standard addresses ensures that they cannot be confused with standard OSI or ITU-T network addresses.

To support PNP addresses within an ATM network as “Local” AESAs, the specification of a preferred encoding of a Local address (and correspondingly, its mapping to PNP addresses) is extremely useful. The PNP address should be coded at the highest level of the private network numbering plan. This is parallel to the encapsulation of E.164 addresses into AESA as per UNI Signalling 4.0 (though the IDI is structured differently from E.164 AESAs), in that the international form of an E.164 address is always used when constructing an E.164 AESA.

In order to perform a direct format translation between an AESA-encoded PNP format (AFI=0x49 [Local]) in an ATM network and a PNP numbering plan in a N-ISDN, the following preferred encoding is suggested:

- The PNP digits should be encoded as binary coded decimal in octets 2 to octet 9 (thus 16 digits) of the AESA structure, left-justified and padded by trailing “1111” semi-octets. The maximum length of an ISO/IEC 11571 number is 15 digits.
- The remaining octets (10 to 20) should be set to zero.

Appendix I- Address Interworking Examples

[Informational]

The following tables illustrate various addressing scenarios. Note that this is not an exhaustive listing of scenarios.

11.4 Key and Terminology

Here is the key to the terminology used in the tables:

S_o Originating Switch

S_i Intermediate Switch

S_t Terminating Switch

NNI Any Service Provider switch to Service Provider switch interface. As needed, network boundaries are identified in the scenarios.

Q.2931-based

This is used to distinguish protocols such as PNNI and IISP from BISUP/BICI. Note that a Q.2931-based protocol is used for NNIs between two Q.2931-based networks as well as for NNIs between a BISUP network and a Q.2931-based network.

IEs (and Parameters)

This shows the positional key for the information elements (IEs) or parameters at each interface. For example, in Table I-1, at the Originating UNI, the Called party number is always shown as the top entry, and the Called party subaddress is shown as the bottom entry.

Note: *A '-' means that the IE or parameter is defined but not present. A space indicates that the IE/parameter is not defined.*

E.164N/e A Native E.164 or embedded E.164 address. It is assumed that whether a UNI wishes to receive native E.164 addresses or embedded E.164 addresses is a configurable option.

X A bold X in a Switch column indicates that that switch must perform address translation.

S A bold S in a Switch column indicates that that switch must split an E.164 AESA, forming a copy of itself and a native E.164 address.

R A bold R in a Switch column indicates that that switch must restore (undo) an address translation or split.

[sub] This notation is used for subaddresses. The brackets indicate that the subaddress might or might not be present, and its presence or absence does not affect the rest of the scenario. The notation indicates one of the following:

1) no subaddress is present,

2) an AESA style subaddress is present,

3) a non-AESA (NSAP or user-defined) style subaddress is present, or

4) both an AESA style subaddress and a non-AESA style subaddress are present.

[TNS] This notation is used to indicate that the Transit Network Selection (TNS) parameter may be present, and if so, is transparently transported.

TSP Terminating Service Provider

CO Customer Owned

11.5 Scenarios – All Q.2931 Networks

The following table illustrates those scenarios in which all NNIs use Q.2931-based protocols (e.g., PNNI, IISP).

Table I-1: Q.2931-based Networks

Call Path:	**Orig UNI**	**S_o**	**Q.2931-based NNI**	**S_i**	**Q.2931-based NNI**	**S_t**	**Term UNI**
IEs:	CdPN CdPSA TNS		CdPN CdPSA TNS		CdPN CdPSA TNS		CdPN CdPSA TNS
AESA	TSP AESA [sub] -		TSP AESA [sub] -		TSP AESA [sub] -		TSP AESA [sub] -
AESA with TNS	TSP AESA [sub] Carrier code		TSP AESA [sub] Carrier Code		TSP AESA [sub] -		TSP AESA [sub] -
E.164N	TSP E.164N [sub] -		TSP E.164e [sub] -		TSP E.164e [sub] -		TSP E.164N/e [sub] -
E.164N with TNS	TSP E.164N [sub] Carrier code		TSP E.164e [sub] Carrier code		TSP E.164e [sub] -		TSP E.164N/e [sub] -

TNS is not passed to the selected network (the network identified by the Carrier code in the TNS). In the TNS scenarios shown, $\mathbf{S_i}$ doesn't pass TNS to $\mathbf{S_t}$ because $\mathbf{S_t}$ is the entry to the selected network.

11.6 Scenarios - All BISUP Networks

The following table illustrates those scenarios in which all NNIs use BISUP.

Table I-2: BISUP Networks

Call Path:	**Orig UNI**	**S_o**	**BISUP NNI**	**S_i**	**BISUP NNI**	**S_t**	**Term UNI**
IEs and Parameters :	CdPN CdPSA TNS		CdPN AESA4CdP CdPSA TNS		CdPN AESA4CdP CdPSA TNS		CdPN CdPSA TNS
E.164N	TSP E.164N [sub] -		TSP E.164N - [sub] -		TSP E.164N - [sub] -		TSP E.164N/e [sub] -
E.164N with TNS	TSP E.164N [sub] Carrier code		TSP E.164N - [sub] Carrier code		TSP E.164N - [sub] -		TSP E.164N/e [sub] -
E.164A	TSP E.164A [sub] -	**S**	TSP E.164N TSP E.164A [sub] -		TSP E.164N TSP E.164A [sub] -	**R**	TSP E.164A [sub] -

E.164A with TNS	TSP E.164A [sub] Carrier code	**S**	TSP E.164N TSP E.164A [sub] Carrier code		TSP E.164N TSP E.164A [sub] -	**R**	TSP E.164A [sub] -
E.164e	TSP E.164e [sub] -	**S**	TSP E.164N TSP E.164e [sub] -		TSP E.164N TSP E.164e [sub] -	**R**	TSP E.164N/e [sub] -
E.164e with TNS	TSP E.164e [sub] Carrier code	**S**	TSP E.164N TSP E.164e [sub] Carrier code		TSP E.164N TSP E.164e [sub] -	**R**	TSP E.164N/e [sub] -
TSP AESA	TSP AESA [sub] -	**X**	TSP E.164N TSP AESA [sub] -		TSP E.164N TSP AESA [sub] -	**R**	TSP AESA [sub] -
TSP AESA with TNS	TSP AESA [sub] Carrier code	**X**	TSP E.164N TSP AESA [sub] Carrier code		TSP E.164N TSP AESA [sub] -	**R**	TSP AESA [sub] -
CO AESA with TNS	CO AESA [sub] Carrier code		'null' CO AESA [sub] Carrier code		'null' CO AESA [sub] -		CO AESA [sub] -

Note the following:

1) Except for the CO AESA with TNS scenario, these scenarios require that every terminating UNI (or at least every terminating network) have a TSP E.164 address.

2) Embedded E.164 addresses (E.164e's) are treated just like E.164A's; intermediate switches are not expected to treat an AESA differently because its DSP is all zeros.

3) In the TSP AESA scenarios, the originating network must be able to translate between the terminating network's AESA address and a corresponding E.164 address. The mechanism by which such a translation may be accomplished is not standardized.

5) TNS is not passed to the selected network (the network identified by the Carrier code in the TNS). In the TNS scenarios shown, $\mathbf{S_i}$ doesn't pass TNS to $\mathbf{S_t}$ because $\mathbf{S_t}$ is the entry to the selected network.

6) The TNS scenarios are not exhaustive but illustrate the two main uses that have been discussed for TNS:

a) Selection of an interexchange carrier.

b) A means for routing a connection attempt when the network is unable to route on the number in the Called party number IE, and in particular, when this number is a Customer Owned AESA. Notice that this requires the selected carrier to be able to somehow deliver the call (perhaps by routing on the AESA4CdP parameter). This requires an agreement between this carrier and the customer owning the CO AESA. Without such an agreement, such a connection attempt will fail.

11.7 Scenarios - Mixed Q.2931-based and BISUP Networks

The following table shows scenarios which include both Q.2931-based and BISUP networks.

Table I-3: Mixed Q.2931-based Network and BISUP Network Scenarios

OrigUNI	S_o	Q.2931-based NNI	S_i	BISUP NNI	S_i	Q.2931-based NNI	S_i	BISUP NNI	S_t	Term UNI
CdPN CdPSA		CdPN CdPSA		CdPN AESA4CdP CdPSA		CdPN CdPSA		CdPN AESA4CdP CdPSA		CdPN CdPSA
TSP AESA [sub]		TSP AESA [sub]	**X**	E.164N TSP AESA [sub]	**R**	TSP AESA [sub]	**X**	E.164N TSP AESA [sub]	**R**	TSP AESA [sub]
TSP E.164N [sub]		TSP E.164e [sub]	**S**	TSP E.164N TSP E.164e [sub]	**R**	TSP E.164e [sub]	**S**	TSP E.164N TSP E.164e [sub]	**R**	TSP E.164N/e [sub]
TSP E.164A [sub]		TSP E.164A [sub]	**S**	TSP E.164N TSP E.164A [sub]	**R**	TSP E.164A [sub]	**S**	TSP E.164N TSP E.164A [sub]	**R**	TSP E.164A [sub]
TSP E.164e [sub]		TSP E.164e [sub]	**S**	TSP E.164N TSP E.164e [sub]	**R**	TSP E.164e [sub]	**S**	TSP E.164N TSP E.164e [sub]	**R**	TSP E.164N/e [sub]

The Q.2931-based NNI to BISUP interworking and BISUP to Q.2931-based NNI interworking are the only thing noteworthy here. Existing procedures for the AESA4CdP parameter have been defined assuming end-to-end BISUP networks, and thus define interworking only with the UNI. This UNI interworking needs to be extended to occur at any Q.2931-based interface. This is shown in the above scenarios: the AESA4CdP parameter is populated on an outgoing BISUP interface when an AESA is received as the CdPN on a Q.2931-based NNI, and the Called Party Number is restored when exiting a BISUP switch over a Q.2931-based NNI.

To simplify the table, TNS is not shown. If present, it functions as shown in Tables I-1 and I-2, i.e., it is passed until the link to the selected network is reached, at which point it is dropped.

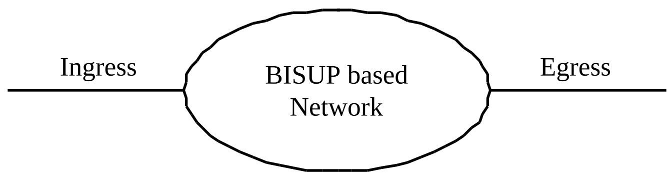
Appendix I- E.164 Interworking Across BISUP Networks

[Informational]

When considering interworking between networks with different addressing schemes, it is important to ensure that the E.164 based addressing schemes still stay intact and can interwork when network boundaries are crossed.

This section describes the mechanisms to do that across BISUP based networks.

Scenario



The ingress and the egress can be either a UNI or an NNI.

All networks use E.164 addresses which may be represented as

native E.164 (E.164N)
or
embedded E.164 (E.164e)
or
AESA format E.164 (E.164A).

Note: For the purpose of this Annex it does not make a difference whether E.164A or E.164e is used; hence the term E.164A/e is used.

11.8 Actions at a BISUP based Network

According to existing specifications (UNI Signalling 4.0, BICI 2.1, Q.2764, Q.2726.1) support of E.164 addresses in the CdPN and CgPN is as follows (see also Sections 8.1 and 8.3):

At a BICI ingress, either

1) E.164N only, or
2) E.164N plus E.164A/e (in the AESA for Called Party parameter)

is received.

At a BICI egress, either

1) E.164N only, or
2) E.164N plus E.164A/e (in the AESA for Called Party parameter)

is sent.

Note: According to BICI 2.1, the E.164N may be a "dummy", i.e. with no digits in case 2. This depends on mutual agreement by the network operators

At the (public) UNI (UNI Signalling 4.0, Section 3.2), either

1) E.164N only, or
2) E.164A/e only, or
3) E.164N or E.164A/e

must be supported.

The UNI has to be configured to be of type 1, 2 or 3 as a subscription option (this relates to delivery of the SETUP message).

For the case of a type 1 UNI at the ingress and a type 1 UNI at the egress, the mechanisms and procedures are defined in ITU-Recs. Q.2931 and Q.2764.

For the case of an E.164A/e UNI at the ingress and an E.164A/e UNI at the egress, the mechanisms and procedures are defined in ITU-Rec. Q.2726.1.

If the network receives an E.164N, and an E.164e is expected at an egress UNI, the E.164 number in the Called Party Number parameter (derived as described in Table II-2) is used to map to the Called party number IE at the UNI, and the Called party number is delivered as an E.164e. See also Section 9 for E.164 support and delivery.

In the following tables, a type 1 interface is indicated in the tables with 'E.164N' as the Egress type, and a type 2 interface is indicated with 'E.164A/e' as the Egress type. Both the E.164N and E.164A/e rows must be consulted to determine the possible actions at a type 3 interface.[9]

Note: The same mechanisms will apply to Calling Party Number and Connected Party Number.

Table II-1: E.164 Interworking Scenarios

Ingress Interface Type	Received Addressing Information	Egress Interface Type	Action by BISUP	Transmitted Addressing Information
UNI	SETUP with E.164N in Called party number IE	UNI E.164N	As specified in Q.2764	SETUP with E.164N in Called party number IE
UNI	SETUP with E.164N in Called party number IE	UNI/PNNI E.164A/e	Act on address as specified in Table II-2 (NOTE 6,7)	SETUP with E.164e in Called party number IE
UNI/PNNI	SETUP with E.164e in Called party number IE	UNI E.164N	Act on address as specified in Table II-2, (NOTE 8)	SETUP with E.164N in Called party number IE
UNI/PNNI	SETUP with E.164A in Called party number IE	UNI E.164N	Call cleared (NOTE 8)	-
UNI/PNNI	SETUP with E.164A/e in Called party number IE	UNI/PNNI E.164A/e	Act on address as specified in Q.2726.1 (see Table II-2)	SETUP with E.164A/e in Called party number IE
UNI/PNNI	SETUP with E.164A/e in Called party number IE	BICI E.164N	Act on address as specified in Q.2726.1 (see Table II-2)	IAM with E.164N in Called Party Number parameter and E.164A/e in AESA for Called Party parameter
UNI	SETUP with E.164N in Called party number IE	BICI E.164N	Act on address as specified in Q.2764 (BISUP)	IAM with E.164N in Called Party Number parameter
BICI	IAM with E.164N in Called Party Number parameter	UNI/PNNI E.164e	Act on address as specified in Q.2726.1 (see Table II-2)	SETUP with E.164e in Called party number IE

[9] Given a choice, the more permissive action should be taken (e.g., a call should not be unnecessarily cleared).

BICI	IAM with E.164N in Called Party Number parameter and E.164A/e in AESA for Called Party parameter	UNI/PNNI E.164A/e	Act on address as specified in Q.2726.1 (see Table II-2)	SETUP with E.164A/e in Called party number IE
BICI	IAM with E.164N in Called Party Number parameter	UNI E.164N	Act on address as specified in Q.2764 (BISUP)	SETUP with E.164N in Called party number IE
BICI	IAM with E.164N in Called Party Number parameter and E.164e in AESA for Called Party parameter	UNI E.164N	Act on address as specified in Table II-2, (NOTE 8)	SETUP with E.164N in Called party number IE
BICI	IAM with E.164N in Called Party Number parameter and E.164A in AESA for Called Party parameter	UNI E.164N	Clear call (NOTE 8)	-
BICI	IAM with E.164N in Called Party Number parameter	BICI E.164N	As described in Recs. Q.2764 and Q.2726.1	IAM with E.164N in Called Party Number parameter
BICI	IAM with E.164N in Called Party Number parameter and E.164A/e in AESA for Called Party parameter	BICI E.164N	As described in Recs. Q.2764 and Q.2726.1	E.164N in Called Party Number parameter and E.164A/e in AESA for Called Party parameter

The format of the AESA for Called Party parameter field is shown in Figure II-1 (taken from Figure 1/Q.2726.1).

The parameter name code allocated to the AESA for Called Party parameter is 0101 1000.

	8	7	6	5	4	3	2	1
1	1 ext	Coding standard		Reserved				
2	Further contents as in Q.2931 Called party number IE starting with octet 5							

Figure II-1: AESA for Called Party Parameter Field

Table II-2: Details for Some Table II-1 Scenarios

Ingress	**BISUP Network**	**Egress**
Called party number E.164A/e - Number digits (NOTE 1) - Numbering plan (NOTE 2) - Type of number (NOTE 3)	**Called Party Number** - Address signals (NOTE 4) - Numbering plan (NOTE 5) - Nature of address indicator **AESA for Called Party** Contents as shown in Figure 1	**Called party number E.164A/e** Contents starting with octet 5 as in AESA for Called Party starting with octet 2.
Called party number E.164e - Number digits (NOTE 1) - Numbering plan (NOTE 2) - Type of number (NOTE 3)	**Called Party Number** - Address signals (NOTE 4) - Numbering plan (NOTE 5) - Nature of address indicator **AESA for Called Party** Contents as shown in Figure 1	**Called party number E.164N** As received in Called Party Number - Address signals (NOTE 4) - Numbering plan (NOTE 5) - Nature of address indicator NOTE 8
Called party number E.164N	**Called Party Number** - Address signals as received - Numbering plan (NOTE 5) - Nature of address indicator **AESA for Called Party** not present	**Called party number E.164e** Contents as shown in Figure 1 (NOTE 6, 7) - Number digits (NOTE 1) - Numbering plan (NOTE 2) - Type of number (NOTE 3) .

NOTE 1: The address is coded as described in X.213 | ISO/IEC 8348 using E.164 format.

NOTE 2: The numbering plan is coded as ATM Endsystem Address. Notice that Q.2931 (1995) uses the more general term "NSAP addressing" for this codepoint (0010).

NOTE 3: The type of number is coded as unknown when NSAP addressing is used.

NOTE 4: The address signal is coded using E.164 address digits from the initial domain identifier field of the AESA in the Called party number IE.

NOTE 5: Numbering plan is coded as E.164.

NOTE 6: The DSP field in the E.164 AESA derived from a native E.164 number will be set to zero.

NOTE 7: The E.164A/e always contains the full international address, starting with the country code (cf. ISO/IEC 8348, A.5.2.1.2.5).

If the calling user had used a native E.164, the country code and or city code may have been stripped off when BISUP networks had been traversed. These will have to be added when the E.164A/e is inserted in the SETUP message.

NOTE 8:

If the network receives an AESA for Called party number and the terminating UNI does not support AESA (only E.164N is supported as the Called party number), the following procedures apply:

- If the AESA is an E.164e (i.e., the DSP is all zeros), the E.164 address may be extracted from the E.164e and encoded as an E.164N, and then placed in the Called party number information element.
- Otherwise, the call or party must be rejected.