INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

I.364
(02/99)

SERIES I: INTEGRATED SERVICES DIGITAL NETWORK

Overall network aspects and functions – Protocol layer requirements

---

Support of the broadband connectionless data bearer service by the B-ISDN

ITU-T Recommendation I.364

(Previously CCITT Recommendation)

ITU-T I-SERIES RECOMMENDATIONS

INTEGRATED SERVICES DIGITAL NETWORK

GENERAL STRUCTURE	
Terminology	I.110–I.119
Description of ISDNs	I.120–I.129
General modelling methods	I.130–I.139
Telecommunication network and service attributes	I.140–I.149
General description of asynchronous transfer mode	I.150–I.199
SERVICE CAPABILITIES	
Scope	I.200–I.209
General aspects of services in ISDN	I.210–I.219
Common aspects of services in the ISDN	I.220–I.229
Bearer services supported by an ISDN	I.230–I.239
Teleservices supported by an ISDN	I.240–I.249
Supplementary services in ISDN	I.250–I.299
OVERALL NETWORK ASPECTS AND FUNCTIONS	
Network functional principles	I.310–I.319
Reference models	I.320–I.329
Numbering, addressing and routing	I.330–I.339
Connection types	I.340–I.349
Performance objectives	I.350–I.359
Protocol layer requirements	**I.360–I.369**
General network requirements and functions	I.370–I.399
ISDN USER-NETWORK INTERFACES	
Application of I-series Recommendations to ISDN user-network interfaces	I.420–I.429
Layer 1 Recommendations	I.430–I.439
Layer 2 Recommendations	I.440–I.449
Layer 3 Recommendations	I.450–I.459
Multiplexing, rate adaption and support of existing interfaces	I.460–I.469
Aspects of ISDN affecting terminal requirements	I.470–I.499
INTERNETWORK INTERFACES	I.500–I.599
MAINTENANCE PRINCIPLES	I.600–I.699
B-ISDN EQUIPMENT ASPECTS	
ATM equipment	I.730–I.739
Transport functions	I.740–I.749
Management of ATM equipment	I.750–I.799

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION I.364

SUPPORT OF THE BROADBAND CONNECTIONLESS DATA BEARER SERVICE BY THE B-ISDN

Summary

This Recommendation describes the support of the Broadband Connectionless Data Bearer Service (BCDBS) by the B-ISDN. It describes the framework for network support of BCDBS and the protocols used at the user interface and network interface.

This Recommendation relates to the direct provision of the BCDBS as defined in Recommendation I.211 using connectionless service functions. However, aspects of this Recommendation can be applied also to the indirect provision of the BCDBS.

Source

ITU-T Recommendation I.364 was revised by ITU-T Study Group 13 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 15th of February 1999.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration, ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Recommendation I.364

SUPPORT OF THE BROADBAND CONNECTIONLESS DATA BEARER SERVICE BY THE B-ISDN

(revised in 1999)

1 Scope

This Recommendation describes the support of the Broadband Connectionless Data Bearer Service (BCDBS) by the B-ISDN in accordance with:

- Recommendation I.113 which defines "connectionless service" (vocabulary).
- Recommendation F.812 which provides the service description of the "Broadband Connectionless Data Bearer Service". Recommendation F.812 generally describes the service to include:
  - source address validation;
  - addresses based on E.164 numbering;
  - point-to-point information transfer;
  - multicast information transfer;
  - address screening supplementary service for point-to-point and multicast information transfer;
  - network capabilities for charging;
  - interworking to other connectionless and connection-oriented data services;
  - quality of service parameters.
- Recommendation I.211 which describes connectionless data service aspects. Recommendation I.211 identifies two configurations, Type (i) and (ii) to support connectionless data service. In Type (i), a Connectionless Service Function (CLSF) is installed outside the B-ISDN. In Type (ii), a CLSF is installed within the B-ISDN, which handles routing of data to be transferred based on connectionless techniques.
- Recommendation I.327 which describes "higher layer capabilities" for the support of services (e.g. connectionless service) and gives functional architectural models for the cases mentioned above.
- Recommendation I.363.3 which specifies AAL type 3/4.

This Recommendation relates to Type (ii) (direct) provision of the BCDBS, using B-ISDN connectionless service functions. However, aspects of this Recommendation can be applied to some Type (i) provision of BCDBS. This Recommendation describes the framework for network support of the BCDBS and the protocols used to support it.

2 Framework for the provision of the Broadband Connectionless Data Bearer Service by the B-ISDN

2.1 Definition of the Broadband Connectionless Data Bearer Service by the B-ISDN

This definition is provided by Recommendation F.812 in conjunction with this Recommendation.

2.1.1 Group addressing

Group addressing is a mechanism used for multicast communication (see clause 2/F.812).

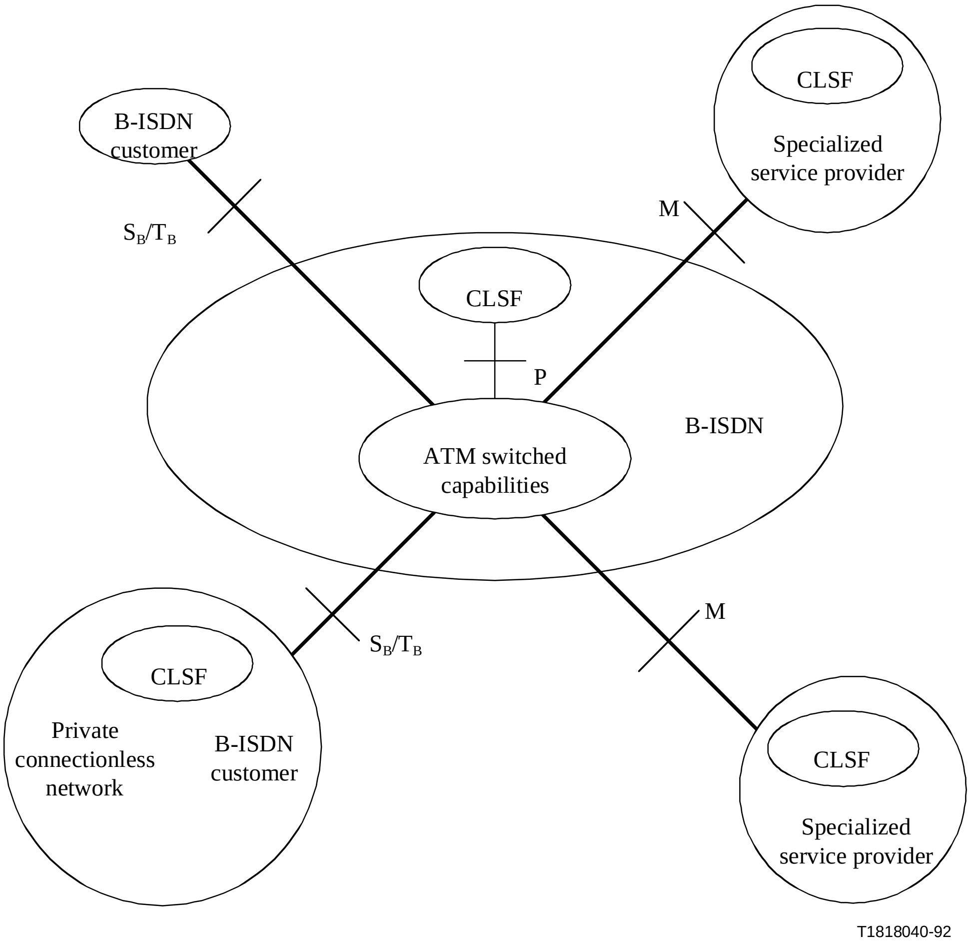
Multicast information transfer allows a user to send a CLNAP-PDU to the network which delivers the same CLNAP-PDU to several intended recipients. The network shall deliver one and only one copy of a group addressed CLNAP-PDU (GAP) across each of the CLAIs associated with the individual addresses represented by the group address (i.e. each CLAI associated with multiple destination addresses will receive a single copy from the network). The GAP shall not be copied back to the originating CLAI. Any recipient of a GAP may make use of the destination group address carried by that GAP to multicast to the recipients of the GAP (but excluding himself). Non-members of a group address may send GAPs to that group.

As a result of address screening, some of the copies of the GAP may not be delivered; all other copies should be delivered.

The service provider is responsible for assigning group addresses and ensuring that each GA (Group Address) identifies uniquely only one set of individual addresses. GAs can be distinguished from individual addresses by the address type.

2.2 Functional architecture

The provision of the BCDBS by the B-ISDN is realized by means of ATM switched capabilities and Connectionless Service Functions (CLSF). The ATM switched capabilities support the transport of connectionless data units in B-ISDN between specific functional groups CLSF able to handle the connectionless protocol and to realize the adaptation of the connectionless data units into ATM cells to be transferred in a connection-oriented environment. The CLSF functional groups may be located outside B-ISDN, in a Private Connectionless Network or in a Specialized Service Provider, or inside B-ISDN. The relevant reference configuration for the provision of the BCDBS by the B-ISDN is depicted in Figure 1.



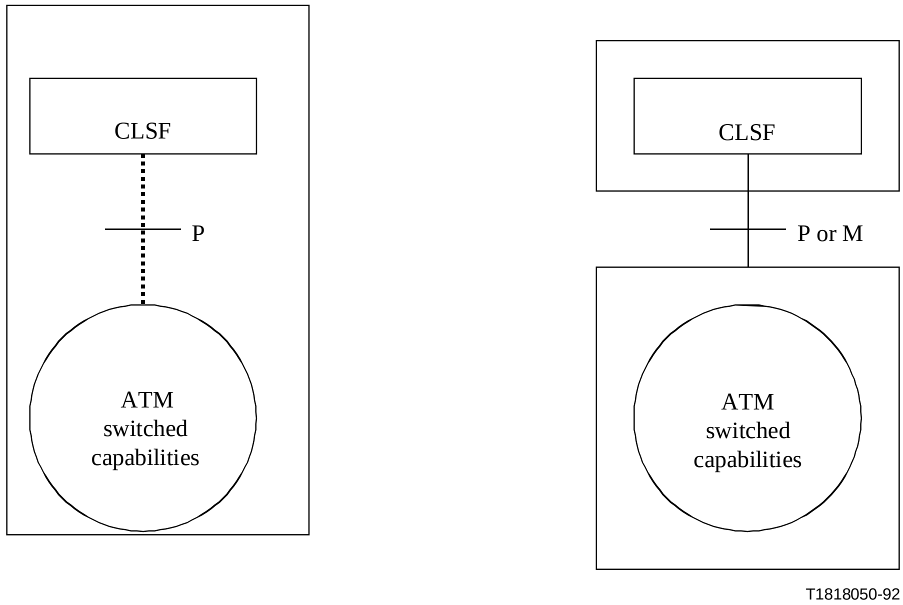
CLSF Connectionless Service Function
M, P, S, T Reference point

Figure 1/I.364 – Reference configuration for the provision of the CL data service in B-ISDN

The ATM switched capabilities are performed by the ATM nodes (ATM switch/cross-connect) which realize the ATM transport network. The CLSF functional group terminates the B-ISDN connectionless protocols and performs functions for the adaptation of the connectionless protocol including preservation of PDU sequence integrity to the intrinsically connection-oriented ATM layer protocol. The connectionless functions are those related to the layer directly above the AAL denoted Connectionless Layer (CLL) and performed by the Connectionless Network Access Protocol (CLNAP), Connectionless Network Interface Protocol (CLNIP) and related Routing and Relaying (CLLR&R) functions, respectively. The adaptation functions encompass the mapping of the connectionless protocols to the connection-oriented ATM layer protocol and the functions performed by the ATM Adaptation Layer 3/4 (AAL 3/4).

The CLL protocols include functions such as routing, addressing and QoS selection. In order to perform the routing of CL data units, the CLSF have to interact with the Control/Management Planes of the underlying ATM network. The interactions between the CLSF and the Control/Management Planes require further study.

The CLSF functional group can be considered to be implemented in the same equipment together with the ATM switched capabilities as depicted in Figure 2 (option A). In this case there is no need to define the interface at the P Reference Point. The CLSF functional group and ATM switched capabilities can be implemented also in separate equipments (Figure 2, option B). In this case, interfaces shall be defined at the M or P Reference Points (refer to Recommendations I.324 and I.327) depending on whether the CLSF is located outside or inside the B-ISDN.

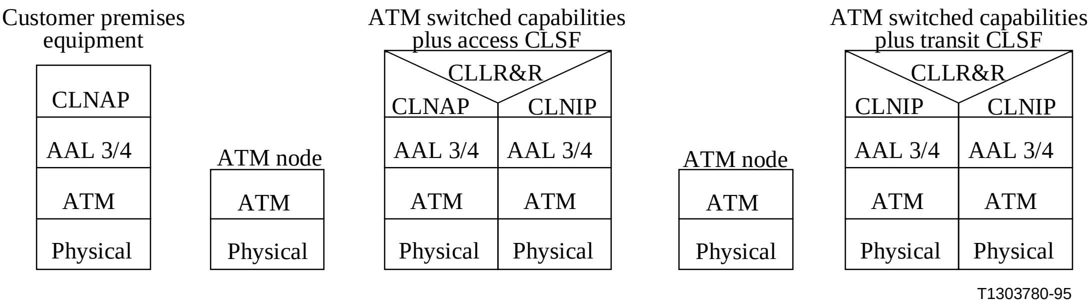


Option A
CLSF and ATM switched capabilities implemented in the same equipment

Option B
CLSF and ATM switched capabilities implemented in different equipment

Figure 2/I.364 – Implementation of CLSF and ATM switched capabilities

The general protocol structure for the provision of the BCDBS by the B-ISDN is shown in Figure 3.



NOTE – In the scope of this Recommendation, a null (empty) SSCS for AAL 3/4 is used.

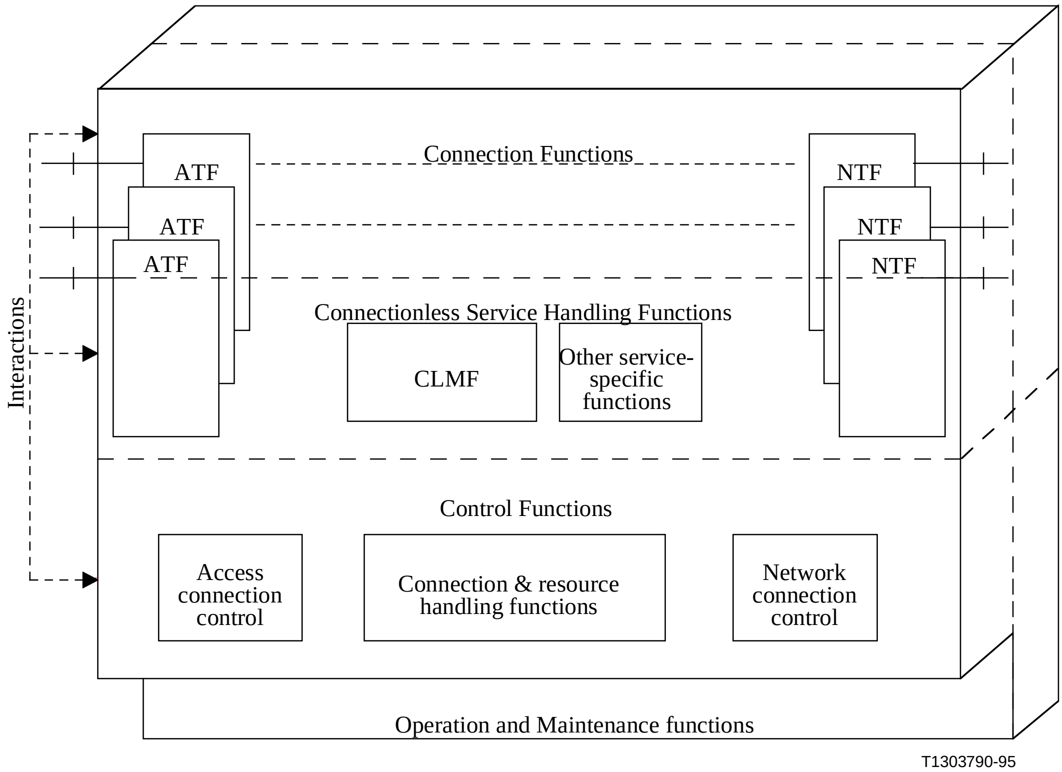
Figure 3/I.364 – General protocol structure for provision of BCDBS by the B-ISDN

2.3 Connectionless server functional description

A Connectionless Server (CLS) is a network element which includes the CLSF. It interfaces ATM nodes or other CLSs at the P/M Reference Points and B-ISDN customer equipment at S_B/T_B Reference Points. The CLS may perform among others the following functions (see also Figure 4):

– Connection Functions (CF) which include all port-related functions for the termination of ATM connections;

– Connectionless Service Handling Functions (CLHF) which include all the service-specific functions required for the support of the BCDBS by the B-ISDN. In general they are related to network integrity issues (e.g. address validation/screening, access class enforcement) and to relaying issues (e.g. routing, group address handling);
– Control Functions (CTF) are related to connection/resource handling and service processing; the information necessary to effect control over the communication resources in the server can be exchanged with other network elements through signalling or management protocols.
– Operation and Maintenance (OAM) functions.



NOTE – Transit CLSs do not contain access termination functions and access connection control functions.

Figure 4/I.364 – Connectionless server functional model

The Access Termination Functions (ATF) blocks contain the functions required to receive/transmit information from/to a B-ISDN user possibly through one or more ATM nodes. The block performs protocol functions corresponding to physical, ATM, AAL type 3/4 protocols and CLNAP.

The Network Termination Functions (NTF) blocks include the functions required to receive/transmit information from/to a CLS possibly through one or more ATM nodes. The block performs protocol functions corresponding to physical, ATM, AAL type 3/4 protocols and CLNIP.

Both ATF and NTF blocks include functions for terminating ATM connections and some CL services specific functions. The description of the functional architecture of the ATF and NTF blocks relevant to the specification of the Connectionless Access Interface (CLAI) and Connectionless Network Interface (CLNI), respectively, is given in 2.4.

The CLHF are located partly in the ATF/NTF blocks and partly in the Connectionless Mapping Functions (CLMF).

The CLMF block performs routing, protocol conversion between access and network terminations and group address handling functions. The CLMF block is composed of the following functional blocks: Group Address Handling Functions (GAHF), Protocol Conversion Functions (PCF) and Routing.

The GAHF block handles both group-addressed CLNAP-PDUs and group-addressed CLNIP-PDUs whose resolution is requested by this CLS. This functional block performs group-addressed data unit handling, resolving the group address into its associated individual addresses. The resolved individual addresses may identify end users served either by this CLS or by a remote CLS.

The PCF block performs protocol conversion between the Access Termination (ATF) and the Network Termination Functions (NTF). In particular, it provides all the relevant information necessary to properly create a CLNIP-PDU from a CLNAP-PDU or to recover a CLNAP-PDU from the received CLNIP-PDU.

The block denoted as Routing, on the basis of the destination address of the PDU to be forwarded across a User Network Interface (UNI) or Network Node Interface (NNI), selects the proper outgoing physical link and Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) to reach that destination.

The Control Functions (CTF) include the following functional blocks: access connection control, network connection control, connection/resource handling functions. These blocks perform functions related to internal resource allocation (e.g. associated with CL message multiplexing, QoS preservation), connection establishment/release, etc. In particular, if the BCDBS is provided on the basis of switched ATM connections between the terminal equipment and the CLS or between CLSs, the access and network connection control functions provide the ability to support user access and network signalling systems, respectively. The access and network connection control functions are, instead, related to the management plane if the BCDBS is provided on the basis of permanent or semi-permanent ATM connections between the terminal equipment and the CLS or between CLSs.

The functions described above do not imply any particular implementation.

2.4 Interfaces

In the following subclauses, the access and network interfaces for the support of the BCDBS by the B-ISDN are described for the user plane. The description of the functionalities of the control and management planes for these interfaces is for further study (see also 2.9).

2.4.1 Connectionless Access Interface (CLAI)

The Connectionless Access Interface supports user access to the BCDBS on an ATM network. User access to the ATM network is provided at the S_B/T_B Reference Points. A CLAI supports a set of AAL connections (over which the CLNAP runs) related to a single ATM connection on a given UNI. The CLAI is identified by one or a set of E.164 numbers allocated to the given UNI.

Direct service provision is performed through the use of CLSs.

User equipment may have direct access to the CLS at the S_B/T_B Reference Points. The protocol stack includes the UNI physical and ATM layers both in the user equipment on one side of the CLAI and in the CL Server on the other side. Policing functions, as foreseen for ATM user access, are performed on the server side of the CLAI.

Indirect user access to the server through one or more ATM nodes is also possible. In this case, the interface between the user equipment and the adjacent ATM node is defined at the S_B/T_B Reference Points, while that between the server and the adjacent ATM node(s) is defined at the P/M Reference Points.

At the S_B/T_B Reference Points, the physical and ATM layers of the CLAI protocol stack are terminated in the user equipment and the ATM node(s). They are based on the ATM UNI. UPC functions as foreseen for ATM user access are performed by the ATM network elements at the network side of the UNI.

At the P Reference Point, the physical and ATM layers of the CLAI stack are terminated in the server and the ATM node(s) and are based on the ATM NNI.

At the M Reference Point, the ATM access termination functions are for further study.

The functions performed by the CL specific protocols (AAL type 3/4 and CLNAP) are the same both in the direct and indirect access cases. The CLAI protocol stack for the "direct" and "indirect" access is shown in Figure 5. The CLNAP protocol functions and elements are defined in clause 3.

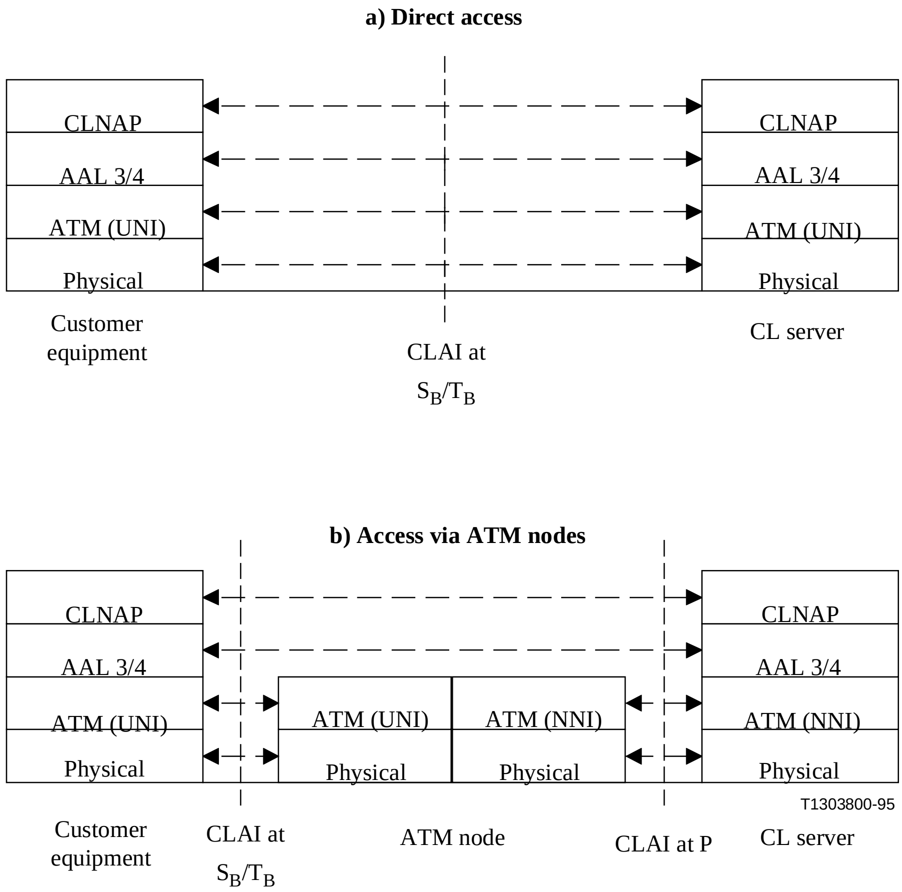


Figure 5/I.364 – Protocol stack at the U-plane for CLAI

2.4.1.1 Access Termination Functions (ATF)

The ATF functional block performs all termination functions associated with the CLAI protocol stack and some service support functions. Figure 6 gives a functional decomposition of the ATF block.

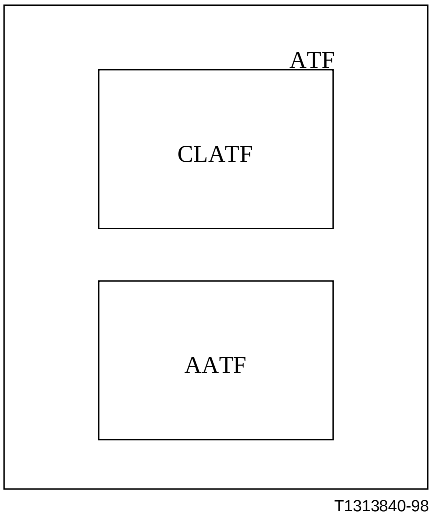


Figure 6/I.364 – ATF functional decomposition

The description given in the following does not imply any particular implementation.

2.4.1.1.1 ATM Access Termination Functions (AATF)

The AATF perform the protocol functions of the physical and ATM layers of the B-ISDN protocol reference model.

Moreover, the AATF perform the functions needed for the request of connection establishment and release to support communication between the server and the users served by it.

Traffic monitoring and control functions based on UPC and/or NPC may also be performed by the AATF, according to the specification of Recommendation I.371.

2.4.1.1.2 CL Access Termination Functions (CLATF)

This subclause only describes the CL access termination functions performed in the CLS.

The CLATF of the CLS perform the protocol functions of the AAL type 3/4 (SAR and CPCS sublayer) and the CLNAP.

Other functions performed include:

– *Source address validation*

  The source address of each CLNAP-PDU is checked by the CLNAP entity at the server side of the CLAI.

– *Local traffic filtering*

  The destination address of each CLNAP-PDU is checked by the CLNAP entity at the server side of the CLAI to screen out communications internal to the Customer Premises Equipment (CPE) except for loopback testing (see also 2.9).

– *Destination address screening*

  If the address screening supplementary service is provided in addition to the basic BCDBS, destination address screening is performed by the CLNAP entity at the server side of the CLAI on both individual and group addresses, in accordance with the service specifications.

– *Source address screening*

If the address screening supplementary service is provided, source address screening is performed by the CLNAP entity of the server before delivering a CLNAP-PDU at the destination CLAI.

– *Access class enforcement*

If the network offers access classes, the CLNAP entity on the server side of the CLAI performs access class enforcement (see 2.8.1).

– *Control of the maximum number of concurrent PDUs*

PDUs in excess of this value are discarded in the user-to-network direction and stored up to a pre-subscribed limit in the network-to-user direction (Note).

NOTE – When the number of the concurrent PDUs exceeds the maximum number of MIDs allowed in the AAL 3/4 entity, the AAL 3/4 entity discards the PDUs exceeding the limit.

2.4.2 Connectionless Network Interface (CLNI)

The Connectionless Network Interface supports the BCDBS provision, allowing for transparent transfer of connectionless service data units between CL servers using the ATM switched capabilities of the B-ISDN.

The CLNI protocol stack is terminated in CL servers and is based on the ATM Network Node Interface (NNI) protocol. A CLNI supports a set of AAL connections (over which the CLNIP runs) related to a single ATM connection between adjacent CLS.

Servers may be interconnected directly. Indirect interconnection through one or more ATM nodes is also possible. In both cases, the AAL type 3/4 protocol and the CLNIP of the CLNI protocol stack are terminated in CL servers.

The physical and ATM layers are terminated in adjacent servers or between servers and adjacent ATM node(s). They are in both cases based on the ATM Network Node Interface (NNI) when servers are attached at the P Reference Point.

At the M Reference Point, the ATM network termination functions are for further study.

The protocol stack for the CLNI is shown in Figure 7.

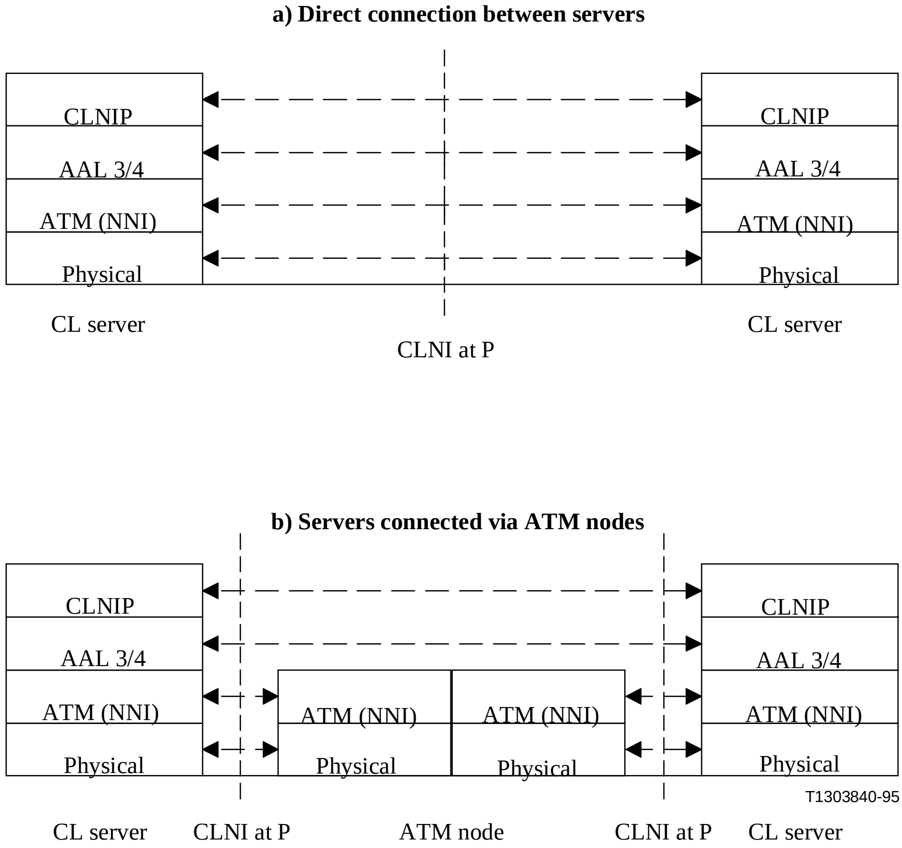


Figure 7/I.364 – Protocol stack at the U-plane for CLNI

The protocol stack for the CLNI includes, in the user plane, the physical, ATM, AAL type 3/4 and CLNIP.

This protocol stack for the user plane applies both when the connected network elements belong to the same network operator/service provider and when the network elements belong to different operators/service providers.

The CLNIP protocol functions and elements are defined in clause 4.

2.4.2.1 Network Termination Functions (NTF)

The NTF functional block performs all termination functions associated with the CLNI protocol stack. Figure 8 gives a functional decomposition of the NTF block.

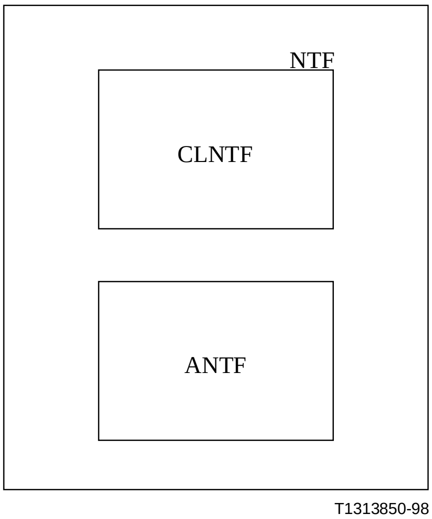


Figure 8/I.364 – NTF functional decomposition

The description given in the following does not imply any particular implementation.

2.4.2.1.1 ATM Network Termination Functions (ANTF)

The ANTF perform the protocol processing of the physical and ATM layers of the B-ISDN protocol reference model.

Moreover, the ANTF perform the functions needed for the request of connection establishment and release to support communication between servers.

Traffic monitoring and control functions based on NPC are also performed by the ANTF, according to the specification of Recommendation I.371.

2.4.2.1.2 CL Network Termination Functions (CLNTF)

The CLNTF perform the protocol processing of the AAL type 3/4 (SAR and CPCS sub-layers) and the CLNIP.

2.5 Connections

The BCDBS will be supported by point-to-point ATM connections provisioned on permanent, semi-permanent, or switched (Note 1) basis. The CLL and AAL type 3/4 functions will be implemented in the CL server(s).

NOTE 1 – The control of switched connections is for further study.

Connectionless communications take place at the CLL. For simultaneous transmission of multiple CLNAP/CLNIP-PDUs, each of them is associated with one AAL type 3/4 connection. Multiple AAL type 3/4 connections each associated with one MID value can be mapped on a single ATM connection.

At the CLAI, the maximum number of concurrent PDUs is agreed at subscription time.

At the CLNI, the maximum number of concurrent PDUs is either a service provider option or is fixed by bilateral agreement between service providers. In order to keep the transit delay low, this number should be set as high as possible.

For a given pair of source and individually addressed destination, at the CL layer the PDU sequence integrity shall be preserved (Note 2).

NOTE 2 – Missequencing occurs at a given receiving interface when the order of reception of two PDUs issued from the same source interface is different from the sending order. A PDU is considered as received when the EOM (End of Message) cell/SAR segment of the PDU has been received. Similarly, a PDU is considered as having been sent when its EOM (End of Message) has been sent.

2.6 Protocols

The protocols for the support of BCDBS by the B-ISDN at the UNI and NNI are described in clauses 4 and 5.

2.7 Numbering and addressing

The number structure of Recommendation E.164 shall be supported. One or more E.164 numbers are assigned to the individual interface at the T_B Reference Point. The same number is used in the CLL protocol address fields to identify the CLL entity.

NOTE – The need for identification of the entities at the interfaces located at P or M Reference Points is for further study.

2.7.1 Individual Address (IA)

An individual address represents the address of a particular interface at the T_B Reference Point. More than one number may be assigned to a T_B Reference Point (and could be used as an address in a PDU). An IA can be used either as a source or a destination address.

2.7.2 Group Address (GA)

A group address is used as a destination address where a number of recipients is intended, each recipient being accessed through the use of the "unique" group identity. Each GA identifies uniquely a set of individual addresses.

The intended recipients of a GA may be served by more than one network.

A GA shall only be used as a destination address.

A particular interface at the T_B Reference Point can be identified by more than one Group Address (GA). An interface at the T_B Reference Point is identified by a group address if one or more of the individual addresses assigned to the interface at the T_B Reference Point is identified by the group address.

2.7.3 Nested Group Address (NGA)

A Nested Group Address (NGA) is related to a GA and identifies a subset of individual addresses belonging to that GA. The NGA represents a set of individual addresses of members of a GA that are located inside a given network; this network can be different from the network where the GAP originated and from the network resolving the GA. (The resolution function provides, for a given GA or NGA, the list of addresses of all the members and/or NGAs in the case of a GA using NGAs.) The type of address used for an NGA is the same as the one defined for a GA.

An NGA is globally unique. A given NGA associated with a GA cannot be reused for another GA in order to allow independent evolution of the two GAs. An NGA shall not be used in a CLNAP-PDU.

2.8 Traffic aspects

2.8.1 Access class enforcement

In the direction from the user to the network, access class enforcement applies between the CPE and the CLS to which it is connected. An access class is defined as a subscription condition based on the maximum allowed sustained information rate (Note 1) across the CLAI. An access class mechanism is defined as a set of functions limiting the information rate (Note 1) across the CLAI at the T_B Reference Point to enforce the access class and it is based on the following three parameters:

NOTE 1 – In this subclause, the term "information rate" identifies the bit rate available to the CLL user at the CLAI excluding the overhead.

– Maximum Information Rate (MIR) – The maximum instantaneous value of the information rate during transmission. As the MIR is defined under the assumption of maximum length Service Data Unit (SDU) and maximum header extension in the Protocol Data Unit (PDU), it is possible to directly deduce the required bandwidth (peak cell rate) of the underlying ATM connection by the following formula.

  ATM peak cell rate = MIR * (maximum number of user data octets + length of CLNAP header in octets + length of CPCS header and trailer in octets) / (maximum number of user data octets * SAR-PDU payload length in octets * bits/octet), i.e.:

  ATM peak cell rate = MIR * (9188 + 44 + 8) / (9188 * 44 * 8) cell/sec.

– Sustained Information Rate (SIR) – The long-term average of the information rate for bursty traffic.

– PDUs Per Time Unit (PPTU) – It is the long-term average PDU rate for bursty traffic.

NOTE 2 – The PPTU parameter can be set to a value such that no enforcement results from it.

The user sending only messages shorter than the length L defined by the formula L = SIR / (8 * PPTU) is not able to utilize the SIR declared at subscription time.

For the BCDBS, AAL type 3/4 can operate in two different modes: message mode and streaming mode. In the case of message mode operation, the BAsize field is equal to the length of the CPCS-PDU payload and the user credit will be correctly decremented for access class enforcement. In the case of streaming mode, the AAL type 3/4 specifies that the BAsize is equal to or greater than the CPCS-PDU length, which is derived from the maximum length indication given in the CPCS-UNITDATA-invoke primitive. The parameter in this primitive represents the maximum length of the CPCS-SDU, i.e. the CLNAP-PDU.

NOTE 3 – If the access class enforcement is based on the BAsize value and if the maximum length is, for example, 9188 octets, too much credit could be consumed with regard to the actual length of the CLNAP-SDU. This could lead to the network's discarding of CPCS-PDUs carrying CLNAP-PDUs which could have been accepted otherwise.

In order to control the parameters related to an access class, the following algorithms are defined.

2.8.1.1 Maximum Information Rate (MIR)

Due to the direct relationship between the MIR and the ATM peak cell rate, it is sufficient to rely on the UPC at the ingress to the ATM network, to check this parameter.

NOTE – The UPC enforces the ATM peak cell rate regardless of the PDU structure and therefore the impact of violation of the MIR may lead to a high degradation of the QoS.

2.8.1.2 Sustained Information Rate (SIR) and PDUs Per Time Unit (PPTU)

For each user the access class enforcement is to be applied to, the following set of variables shall be maintained by the ingress CLS:

C It represents the current number of octets that is acceptable to the network.

P It represents the current number of BOM or SSM SAR-PDUs that is acceptable to the network.

Dt It represents the time period after which the C variable is incremented.

dt It represents the time period after which the P variable is incremented.

DC It represents the number of octets by which C is incremented every Dt period of time.

DP It represents the number of CLNAP-PDUs by which P is incremented every dt period of time.

CMAX It represents the maximum value that the variable C may reach.

PMAX It represents the maximum value that the variable P may reach.

The following algorithm shall be applied:

every Dt: C = C + DC up to CMAX

every dt: P = P + DP up to PMAX

Whenever a BOM or SSM SAR-PDU arrives in the ingress CLS

if ((C ≥ BAsize – 20 (see Note 1)) and (P ≥ 1))

then {CPCS-PDU is transmitted

and C = C – BAsize + 20

and P = P – 1}.

else {CPCS-PDU is discarded}

NOTE 1 – It has been assumed that the header extension field length is zero since no standard use has been defined for the header extension field.

NOTE 2 – SIR = 8 * DC/Dt, where SIR corresponds to the user information, i.e. the CLL-SDU.

2.9 Operations and maintenance

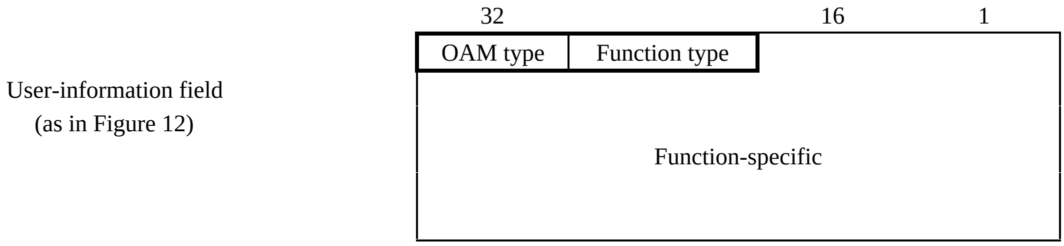
2.9.1 Identification of OAM information flow

The CLL protocols provide the means by which an OAM-related information flow can be identified. The OAM information flow is transported in specific CLNAP/CLNIP-PDUs (called CL-OAM-PDU).

The CL-OAM-PDU is identified by a HLPI value at the CLAI (see Table 3) and by a PI value at the CLNI (see 5.4.3).

2.9.1.1 General structure of the CL-OAM-PDU

The OAM-specific information field is carried in the user-information field of the CLNAP-PDU. The structure is defined as follows (see Figure 9):



NOTE – For CL-OAM-PDUs, the same application rules apply as defined in 6.1.

Figure 9/I.364 – General structure of the CL-OAM-PDU and its location in the CLNAP-PDU

2.9.1.1.1 OAM type

This 1-octet field identifies the OAM functions.

Table 1/I.364 – Coding of the OAM type field

OAM type	Coding
fault management	01H

2.9.1.1.2 Function type

This 1-octet field identifies the function types of the different OAM functions:

Table 2/I.364 – Coding of the function type and its relation to OAM types

OAM type	Coding	Function type	Coding
fault management	01H	loopback	08H

2.9.1.1.3 Function-specific fields

This variable length field can range from 0 to 9186 octets and is used to carry the function-specific information indicated by the OAM type (see 2.9.1.1.1) and the function type (see 2.9.1.1.2). Its structure and coding vary according to OAM type and function type.

2.9.1.2 Addressing of OAM entities

The OAM entity located in the CPE is identified by the corresponding HLPI value (see Table 3) and the address associated with the CLL entity located in the CPE.

Addressing of CLSs is for further study.

2.9.2 OAM-supported functions

The following functions are identified:

- loopback;
- others are for further study.

2.9.2.1 Loopback

Loopback has been identified as an OAM function to test the communication integrity, i.e. the receiver's capability to receive, process and return a CL-OAM-PDU to the sender. The loopback function is initiated by:

1) the CPE to the CLSF at the CLAI;

2) the CLSF to the CPE at the CLAI;

3) a CLSF to an adjacent CLSF.

In order to perform loopback, the originating CLS or CPE needs to know whether the equipment under test supports the loopback facility.

2.9.2.1.1 Initiation by the CPE

The CPE has the capability to check the integrity of the communication between itself and the connection functions and connectionless service handling functions of the CLSF at the CLAI. The CPE sends a CL-OAM-PDU to the CLSF. The CLSF processes and returns (loops back) the CL-OAM-PDU to the CPE.

2.9.2.1.2 Initiation by the network (CLSF to CPE)

The CLSF at the CLAI has the capability to check the integrity of the communication between itself and the CPE. The CLSF sends a CL-OAM-PDU to the CPE. The CPE processes and returns (loops back) the CL-OAM-PDU to the CLSF.

2.9.2.1.3 Initiation by the network (CLSF to adjacent CLSF)

The CLSF has the capability to check the integrity of the communication between itself and the connection functions and connectionless service handling functions of the adjacent CLSF. The originating CLSF sends a CL-OAM-PDU to the adjacent CLSF. The receiving CLSF processes and returns (loops back) the CL-OAM-PDU to the originating CLSF.

2.9.3 OAM mechanisms

2.9.3.1 Loopback mechanism

2.9.3.1.1 Specific fields for loopback

The functions specific field for loopback operation consists of two subfields as shown in Figure 10.

MSB	LSB
Correlation Tag	Loopback indication
7 bits	1 bit

MSB Most significant bit

LSB Least significant bit

Figure 10/I.364 – Structure of function-specific subfields for the loopback operation

2.9.3.1.1.1 Loopback indication

This subfield is a 1-bit indicator. The initial value is set to "0" by the originating entity. To indicate that the PDU has been looped back, the value is set to "1" by the loopback entity.

2.9.3.1.1.2 Correlation Tag

This subfield is set by the originating entity. The value is in the range of "0" to "127" inclusive. The value shall not be modified by the loopback entity.

2.9.3.1.2 Setting the SA and DA at the CLAI

For the exchange of CL-OAM PDUs across a CLAI, the DA and SA fields of the CL-OAM PDU are populated with the address of the corresponding CPE. The value of the DA and SA fields shall not be modified.

2.9.3.1.3 Setting the SA and DA at the CLNI

For the exchange of CL-OAM PDUs across a CLNI, the DA and SA fields of the CL-OAM PDU are populated with any valid E.164 number chosen by the network operator/service provider. Bilateral agreement is required to identify the E.164 numbers to be used for loopback between two adjacent CLSs belonging to different operator/service provider.

NOTE – For security reason the E.164 number utilized for loopback should be screened at the network entrance and the number should therefore be restricted.

2.9.4 Operations

For further study.

2.10 Network charging capabilities

For further study.

2.11 Interworking with non-B-ISDN connectionless data protocols

For further study.

2.12 Interworking with connection-oriented data services

For further study.

3 Layer service and functions provided by the Connectionless Layer

The Connectionless Layer Service (CLL Service) and the functions of the CLL are provided by appropriate interactions of CLNAP, CLNIP and CLLR&R entities. They are accessed by a CLL user via an interface to a CLNAP entity.

3.1 Layer service provided by the Connectionless Layer

The CLL provides for the transparent transfer of variable size CLL Service Data Units from a source to one or more destination CLL user(s) in a manner such that lost or corrupted data units are not retransmitted. This transfer is performed using a connectionless technique, including embedding of destination and source CLL user addresses in each corresponding CLL Protocol Data Unit.

The information exchanged between a CLNAP entity and a CLL user entity across a CLL SAP uses the following primitives:

1) CLL-UNITDATA request (source-address, destination-address, data, QOS);

2) CLL-UNITDATA indication (source-address, destination-address, data, QOS).

The information exchanged between a CLNAP entity and the associated management entity uses the following primitives:

1) MCL-UNITDATA request (source-address, destination-address, data);

2) MCL-UNITDATA indication (source-address, destination-address, data).

3.1.1 Description of primitives

3.1.1.1 CLL-UNITDATA request

This primitive is issued by the CLL user to request the transfer of a CLL-SDU to its peer CLL user entity if an individual destination address is used, or peer entities if a group destination address is used. This CLL-SDU is not retransmitted in the event of loss or corruption.

3.1.1.2 CLL-UNITDATA indication

This primitive is issued to a CLL user to indicate the arrival of a CLL-SDU. In the absence of errors, the contents of the CLL-SDU are complete and unchanged relative to the data parameter in the associated CLL-UNITDATA request.

3.1.1.3 MCL-UNITDATA request

This primitive is issued by the management entity to request the transfer of a CL-OAM data to a peer management entity. This CL-OAM data is always transmitted in a manner such that lost or corrupted data units are not retransmitted.

NOTE – The use of GA in this primitive is not foreseen.

3.1.1.4 MCL-UNITDATA indication

This primitive is issued to the management entity to indicate the arrival of CL-OAM data. In the absence of errors, the CL-OAM data is complete and unchanged relative to the data parameter in the associated MCL-UNITDATA request.

3.1.2 Definition of parameters

3.1.2.1 source-address

The source-address parameter identifies the individual source CLL user/OAM entity.

3.1.2.2 destination-address

The destination-address parameter identifies either an individual CLL destination user/OAM entity or a group of CLL destination users.

3.1.2.3 QOS (Quality of Service)

The QOS parameter specifies the quality of service requested for the CLL-SDU transfer.

3.1.2.4 data

The data parameter is the CLL-SDU/CL-OAM data to be transferred.

3.2 Connectionless Layer functions for user data transport

The functions provided by the Connectionless Layer may include:

3.2.1 Preservation of CLL-SDUs

This function provides for the delineation and transfer of CLL-SDUs.

3.2.2 Addressing

This function provides the ability to a CLL user entity to select, on a per CLL-SDU basis, to which destination CLL user entity or entities the CLL-SDU is to be delivered and provides the ability to indicate to the destination CLL user(s) the source of the CLL-SDU.

3.2.3 Transit operator selection

This function provides the ability to a CLL user entity to explicitly select, either on a permanent or a per CLL-SDU basis, the source CLL user's preferred transit operator(s). The mechanism for selection of the transit operator on a CLL-SDU basis is for further study. The provision of this function by the network is for further study.

NOTE – The word "carrier" may alternatively be used instead of "transit operator" in some regulatory environments.

3.2.4 QOS selection

The QOS function provides selection of the quality of service desired for the CLL-SDU transfer. Actions taken by the network based on the QOS selected are for further study. A network may choose to support only one QOS class.

3.3 Connectionless Layer functions for CL-OAM data transport

For further study.

4 Protocol for the support of the Broadband Connectionless Data Bearer Service by the B-ISDN at the UNI

The clause describes a protocol for supporting a connectionless data service across the B-ISDN UNI. The protocol provides a layer service similar to the MAC sub-layer service described in the ISO/IEC IS 10039, with enhanced capabilities.

The protocol elements defined at the CLL and CPCS sub-layers of the AAL type 3/4 protocol correspond to the elements defined for the IM-PDU defined in ISO/IEC 8802-6. This alignment is considered highly desirable in order to facilitate ease of interworking between the two protocols for supporting connectionless service.

4.1 Protocol stack

The subclause provides a description of the protocol stack for supporting BCDBS (Figure 11) at the UNI. The CLNAP uses the AAL type 3/4 unassured service and includes the necessary functionality to provide the CLL Service. The CLL provides its layer service to the CLL user(s) as illustrated.

CLL User Protocol
CLNAP
AAL type 3/4
ATM
Physical

Figure 11/I.364 – Protocol stack for supporting the Broadband Connectionless Data Bearer Service

4.2 Layer service expected from the AAL

The CLL expects the AAL to provide for the transparent and sequence-preserving transfer of CLNAP-PDUs between two CLNAP entities when accessing a point-to-point AAL connection (refer to Recommendation I.363.3 for the definition of AAL connections). This transfer is provided in a manner such that lost or corrupted data units are not retransmitted (Unassured Operation).

NOTE 1 – The use of multicast AAL connections is for further study.

The information transfer between the CLNAP entity and the AAL entity can be performed in message mode or streaming mode. The use of streaming mode by CLNAP entities is for further study.

The information exchange between the AAL entities and the CLNAP entities across the AAL-SAP uses the following primitives:

1) AAL-UNITDATA request [Interface Data, More (Note 2), Maximum Length (Note 2)];
2) AAL-UNITDATA indication [Interface Data, More (Note 2), Maximum Length (Note 2), Reception Status (Note 3)];
3) AAL-U-Abort request (Note 2);
4) AAL-U-Abort indication (Note 2);
5) AAL-P-Abort indication (Note 2).

NOTE 2 – This primitive/parameter is used in streaming mode only.

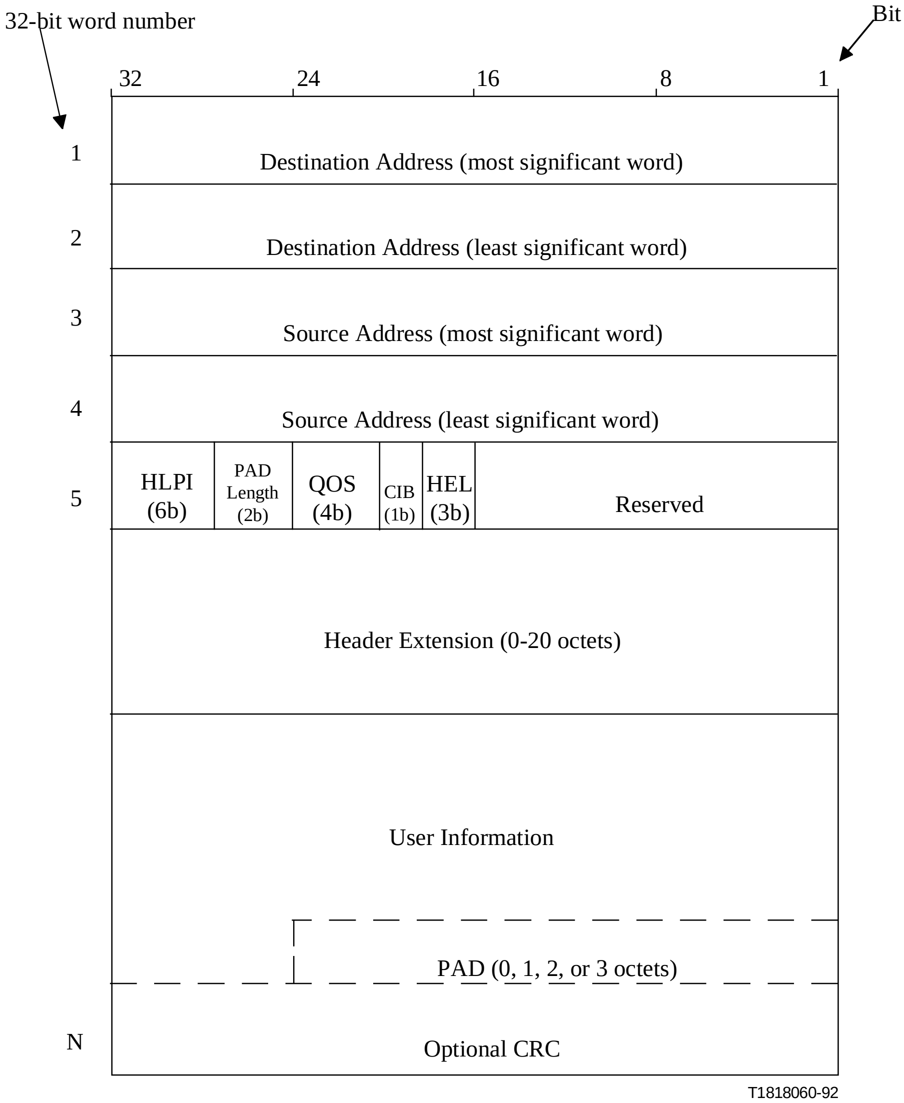
NOTE 3 – The CLNAP entities do not make use of the Corrupted Data Delivery option which may be supported by the AAL type 3/4 protocol, i.e. the optional Reception Status parameter in the AAL-UNITDATA indication primitive is not used.

A detailed description of the primitives and parameters is provided in Recommendation I.363.3.

4.3 CLNAP protocol data unit structure and encoding

The detailed structure of the CLNAP-PDU is illustrated in Figure 12.

It contains the following fields:



(nb) Length of field (n) in bits

NOTE – The order of transmission is from left to right and from top to bottom.

Figure 12/I.364 – Structure of the CLNAP-PDU

4.3.1 Destination Address

This 8-octet field contains a 4 bit "address-type" subfield, followed by the 60-bit "address" subfield. The "address-type" subfield indicates whether the "address" subfield contains a publicly administered 60-bit individual address or a publicly administered 60-bit group address. The "address" subfield identifies to which CLNAP-entity(ies) the CLNAP-PDU is destined. The encoding of this "address-type" subfield is described in Annex A. This "address" subfield is structured according to Recommendation E.164. The encoding of the 60-bit "address" subfield is described in Annex A.

4.3.2 Source Address

This 8-octet field contains a 4 bit "address-type" subfield, followed by the 60-bit "address" subfield. The "address-type" subfield indicates that the "address" subfield contains a publicly administered 60-bit individual address. The "address" subfield identifies the CLNAP-entity that sourced the CLNAP-PDU. The encoding of this "address-type" subfield is described in Annex A. This "address" subfield is structured according to Recommendation E.164. The encoding of the 60-bit "address" subfield is described in Annex A.

4.3.3 Higher Layer Protocol Identifier (HLPI)

This 6-bit field is used to identify the CLL user entity or the CL-OAM entity to which the CLL-SDU is to be passed at the destination node.

The means by which the originating CLL user entity indicates the destination CLL user entity is out of the scope of this Recommendation. See Table 3.

Table 3/I.364 – Coding table of the HLPI field

HLPI range	Protocol entity
1	Reserved for logical Link Control (Notes 1 and 2)
2	Reserved for MAN applications (Notes 1 and 2)
43	Reserved for identification of CL-OAM-PDU
44-47	Reserved for indication of encapsulation inside the network. Additional network use for this range is for further study. These values shall never be set by a CLL user entity. Any CLNAP-PDU having the HLPI set to any of these values shall be discarded by the network.
48-63	Reserved for end-to-end user application. This range of values is not subject to standardization (Notes 1 and 2)
Other values	Reserved for future standardization
NOTE 1 – This value shall be transparently transported by the network. NOTE 2 – The network shall not discard CLNAP-PDUs on the basis of this value.	

The mapping of higher layer protocols to/from CLNAP is not within the scope of this Recommendation.

4.3.4 PAD Length

This 2-bit field indicates the length of the PAD field (0-3 octets). The number of PAD octets is such that the total length of the User-Information field and the PAD field together is an integral multiple of four octets.

4.3.5 Quality of Service (QOS)

This 4-bit field is used to indicate the quality of service requested for the CLNAP-PDU. The semantics of this field are for further study. The default value of this field is "0".

NOTE – A network which supports only one QOS class shall ignore this field.

4.3.6 CRC Indication Bit (CIB)

This 1-bit field indicates the presence (if CIB = 1) or absence (if CIB = 0) of a 32-bit CRC field.

4.3.7 Header Extension Length (HEL)

This 3-bit field can take on any value from 0 to 5 and indicates the number of 32-bit words in the header extension field.

4.3.8 Reserved

This 16-bit field is reserved for future use. Its default value is "0".

4.3.9 Header Extension

This variable-length field can range from 0 to 20 octets, its length is indicated by the value of the Header Extension Length field (see 4.5.7). Its use is for further study.

In cases where the Header Extension Length (HEL) is not equal to zero, all unused octets in the header extension are set to zero. The information carried in the header extension is structured into information entities. An information entity (element) consists (in this order) of element length, element type, and element payload.

– *Element length*: This is a one octet field and contains the combined lengths of the element length, element type, and element payload in octets.

– *Element type*: This is also a one octet field and contains a binary encoded value which indicates the type of information found in the element payload field.

– *Element payload*: This is a variable length field and contains the information indicated by the element type field.

4.3.10 User Information

This field is of variable length up to 9188 octets and is used to carry the CLL-SDU. Different values of maximum length are for further study.

4.3.11 PAD

This field is 0, 1, 2 or 3 octets in length and coded as all zeros. Within each CLNAP-PDU the length of this field is chosen such that the length of the resulting CLNAP-PDU is aligned on a 32-bit boundary.

4.3.12 CRC

This optional 32-bit field may be present or absent as indicated by the CIB field. The field contains the result of a standard CRC32 calculation performed over the CLNAP-PDU with the "Reserved" field always treated as if it were coded as all zeros.

The CRC is calculated using the following generator polynomial:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

The support of this CRC field by the network is for further study.

4.4 Procedures

For further study.

5 Protocol for the support of the Broadband Connectionless Data Bearer Service by the B-ISDN at the NNI

5.1 Scope

The CLNIP supports the BCDBS as specified in Recommendation F.812 between Connectionless Servers inside a network operator's domain and between two network operators' domains.

NOTE – It is assumed that this protocol applies to all cases. Additional functionalities may be needed for the support of this service within a network operator domain.

The CLNIP provides two modes of operation: encapsulation and non-encapsulation. For the conditions for the selection of the mode of operation and the mechanism to be applied in either mode, see clause 6.

The CLNIP shall be applied at the CLNI, as shown in Figure 13.

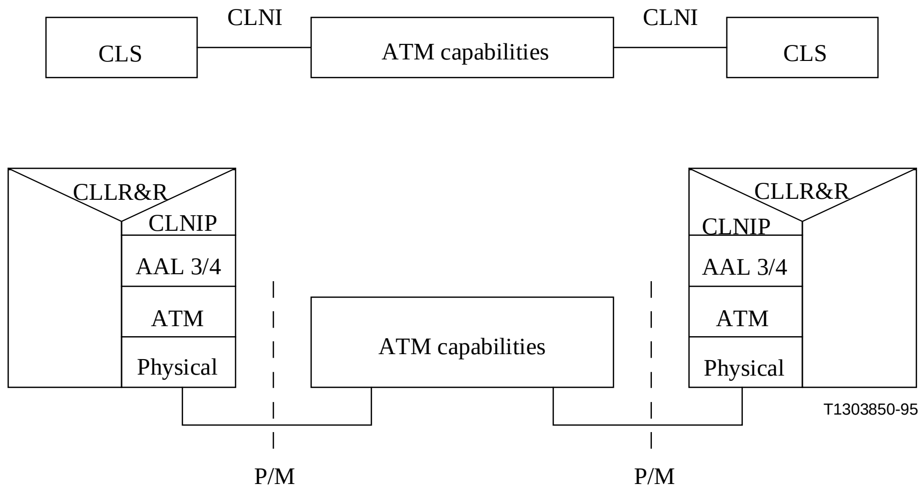


Figure 13/I.364 – Network and protocol architecture

5.2 Protocol stack

The protocol stack for supporting the transfer of connectionless data between CLSs is depicted in Figure 14. The CLNIP uses the AAL type 3/4 unassured service and includes the necessary functionality to provide the CLL service. For structure and encoding of AAL type 3/4 (SAR and CPCS sub-layers) see Recommendation I.363.3.

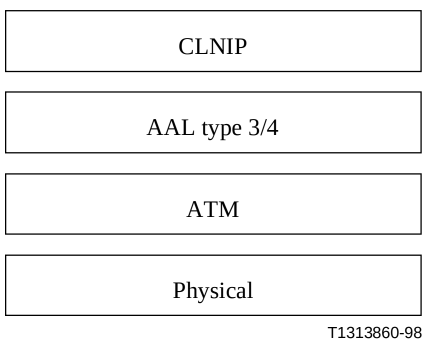


Figure 14/I.364 – Protocol stack for CLNIP

5.3 Layer service expected from the AAL

The CLL expects the AAL to provide for the transparent and sequence-preserving transfer of CLNIP-PDUs between two CLNIP entities when accessing a point-to-point AAL connection (refer to Recommendation I.363.3 for the definition of AAL connections). This transfer is provided in a manner such that lost or corrupted data units are not retransmitted (Unassured Operation).

NOTE 1 – The use of multicast AAL connections is for further study.

The information transfer between the CLNIP entity and the AAL entity can be performed in a message mode or streaming mode.

The information exchanged between the AAL entities and the CLNIP entities across the AAL-SAP uses the following primitives:

1) AAL-UNITDATA request [Interface Data, More (Note 2), Maximum Length (Note 2)];
2) AAL-UNITDATA indication [Interface Data, More (Note 2), Maximum Length (Note 2), Reception Status (Note 3)];
3) AAL-U-Abort request (Note 2);
4) AAL-U-Abort indication (Note 2);
5) AAL-P-Abort indication (Note 2).

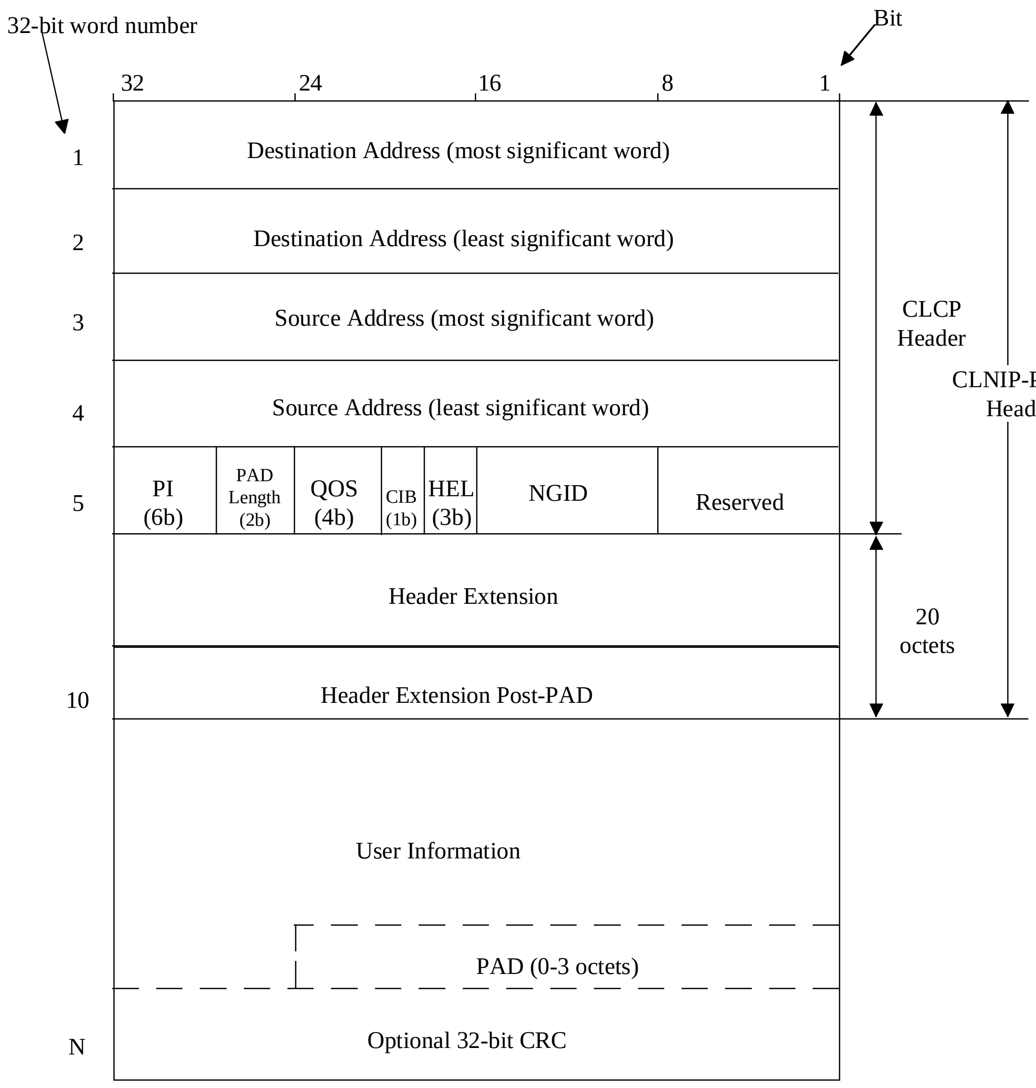
NOTE 2 – This primitive/parameter is used in streaming mode only. In the streaming mode, the maximum length parameter is derived from the incoming CLL-PDU.

NOTE 3 – The CLNIP does not make use of the Corrupted Data delivery option which may be supported by the AAL type 3/4 protocol, i.e. the optional Reception Status parameter in the AAL-UNITDATA indication primitive is not used.

A detailed description of the primitives and parameters is provided in Recommendation I.363.3.

5.4 CLNIP Protocol Data Unit structure and encoding

The detailed structure of the CLNIP-PDU is illustrated in Figure 15.



(nb) Length of field (n) in bits
CLCP Header Connectionless Convergence Protocol Header

NOTE 1 – The Header Extension Post-PAD is only present when encapsulation applies. In this case the Header Extension and the Header Extension Post-PAD sum to 20 octets.

NOTE 2 – The order of transmission is from left to right and from top to bottom.

Figure 15/I.364 – Structure of the CLNIP-PDU

The CLNIP-PDU contains the following fields.

5.4.1 Destination Address (DA)

This 8-octet field contains a 4-bit "address-type" subfield, followed by the 60-bit address subfield. The "address-type" subfield indicates whether the address subfield contains a publicly administered 60-bit individual address or a publicly administered 60-bit group address. Encoding of the "address-type" subfield is described in Annex A.

The information included in the "address-subfield" identifies to which CLNIP entity(ies) the CLNIP-PDU is destined. The structure of the "address" subfield is modelled according to Recommendation E.164. Encoding of the "address" subfield is described in Annex A.

5.4.2 Source Address (SA)

This 8-octet field contains a 4-bit "address-type" subfield, followed by the 60-bit address subfield. The "address-type" subfield indicates that the address subfield contains a publicly administered 60-bit individual address. Encoding of the "address-type" subfield is described in Annex A.

The "address" subfield identifies the CLNAP entity that originated the CLL user data packet included in the CLNIP-PDU. The structure of the "address" subfield is modelled according to Recommendation E.164. Encoding of the "address" subfield is described in Annex A.

5.4.3 Protocol Identifier (PI)

If encapsulation is performed, this 6-bit field takes one of the values [44-47] and is used to indicate that the CLNIP-PDU is an encapsulating one. If the encapsulating CLNIP-PDU carries CLL user data, the value 44 shall be used. The values [45-47] are reserved (Note).

NOTE – In the future these values may also be used to identify encapsulated user data transfer associated with additional functions.

The following PI code points for the identification of CL-OAM-PDU are defined:

– '45' for encapsulating CLNI;

– '43' for non-encapsulating CLNI.

If encapsulation is not performed, the field has the same coding and meaning as in the CLNAP-PDU sent by the originating CLNAP entity.

At CLNI between CL service providers, the sender is responsible for the encoding of the PI field of PDUs carrying user data with a value that is appropriate for the network directly across the interface. On the basis of bilateral operator's agreement, the PI values outside the range [44-47] may be used by the sending CLS. Currently identified values are 50 and 51.

5.4.4 PAD length

This 2-bit field indicates the length of the PAD field (0-3 octets). The number of PAD octets is such that the total length of the "User-Information" field and the PAD field together is an integral multiple of 4 octets. This field is always coded to "0" when encapsulation is performed.

5.4.5 Quality of Service (QOS)

This 4-bit field is used to indicate the quality of service requested for the CLNIP-PDU. In case of non-encapsulation, this field has the same coding and meaning as in the CLNAP-PDU sent by the originating service user. In case encapsulation is performed, this field shall be coded to "0".

5.4.6 CRC Indication Bit (CIB)

This 1-bit field indicates the presence (CIB = 1) or absence (CIB = 0) of a 32-bit CRC. In case encapsulation is performed, this field shall always be coded to "0" as it is not necessary to use the CRC for the encapsulating PDU.

5.4.7 Header Extension Length (HEL)

This 3-bit field indicates the number of 32-bit words in the Header Extension field.

In the case of encapsulation, this field shall be set to "3".

In the case of non-encapsulation, this field can take any of the values in the range [0, 5].

5.4.8 NGID

This field, denoted as NGAA Identifier (NGID), is used by the enhanced group address resolution functions as described in 7.3.3.

This field carries the identification (NGID) of the last network which did a partial resolution on the destination GA of the encapsulated CLNAP-PDU. The default value of the NGID field is "0".

5.4.9 Reserved

This 8-bit field is reserved for future use. The default value of the reserved field is "0".

5.4.10 Header Extension

In the case of encapsulation, the length of this field shall be 12 octets.

In the case of non-encapsulation, the length of this field is in the range [0, 20] octets and it is indicated by the value of the Header Extension Length field.

The content of this field is not constrained by this Recommendation.

5.4.11 HE Post-PAD

In the case of encapsulation, this field has a length of eight octets. The first octet contains the protocol version number. It shall be set to "1" for this version of this Recommendation. The content of the remaining seven octets is not constrained by this Recommendation.

This HE Post-PAD is always absent if encapsulation is not performed.

5.4.12 User Information

This field is of variable length in the range [20, 9236] octets in encapsulating PDUs and in the range [0, 9188] in non-encapsulating PDUs.

In the case of encapsulation, this field carries the encapsulated CLNAP-PDU + alignment header (Note) (4 octets long) and shall be an integer multiple of 4 octets.

In the case of non-encapsulation, the field carries the source SDU.

NOTE – The content of the alignment header shall not be checked.

5.5 Error conditions

5.5.1 In the case of encapsulation

This subclause applies to CLNIP-PDUs which are identified as encapsulating PDUs only.

Various errors may occur in receiving CLNIP-PDUs. Whenever one of the following conditions is encountered at the receiver, the respective CLNIP-PDU shall be discarded:

- invalid address format;
- CLNIP Source Address different to CLNAP-PDU Source Address;
- CLNIP Destination Address different to CLNAP-PDU Destination Address in the case that the latter is an individual address;
- PAD length different from 0;
- Quality Of Service field other than 0;
- CLNIP CRC Indicator Bit equal to 1;
- value of HEL field not equal to "3";

– PI field content different from the allowed range (see 5.4.3).

5.5.2 In the case of non-encapsulation

This subclause applies to CLNIP-PDUs which are identified as non-encapsulating by means of the PI field.

Various error conditions may occur in receiving CLNIP-PDUs. Whenever one of the following conditions is encountered at the receiver, the respective CLNIP-PDU shall be discarded:

– invalid address format;

– PAD length such that the total length of user-information and PAD fields is not a integral multiple of 4 octets;

– value of HEL field not in the range of 0 to 5 inclusive.

6 Mapping between CLNAP and CLNIP

A CLS may include one or more of the following general types of functions.

For a given CLNAP/CLNIP-PDU, each CLS involved performs one of these types of functions.

a) *Originating functions*

See Figure 16.

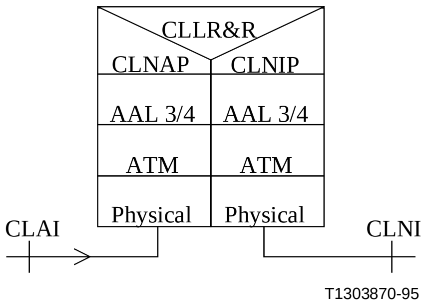


Figure 16/I.364

Originating functions get CLNAP-PDUs from customer equipment via a CLAI and forward corresponding CLNIP-PDUs (either encapsulating or non-encapsulating ones) to another CLS via a CLNI.

b) *Terminating functions*

See Figure 17.

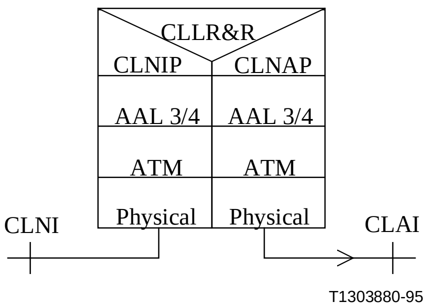


Figure 17/I.364

Terminating functions get (encapsulating and/or non-encapsulating) CLNIP-PDUs from another CLS via a CLNI and forward corresponding CLNAP-PDUs to customer equipment via a CLAI.

c) *Transit functions*

See Figure 18.

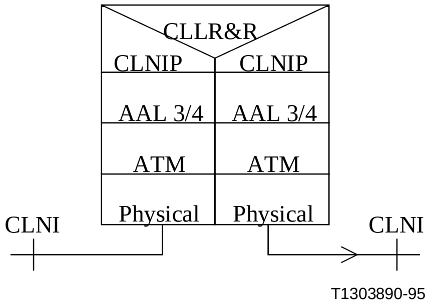


Figure 18/I.364

Transit functions get encapsulating and/or non-encapsulating CLNIP-PDUs from another CLS via a CLNI and forward corresponding CLNIP-PDUs to another CLS via another CLNI. If the next CLS belongs to another operator's domain, non-encapsulating CLNIP-PDUs are encapsulated before they are forwarded.

d) *Access-only functions*

See Figure 19.

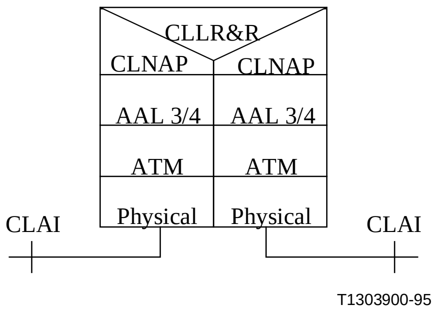


Figure 19/I.364

Access-only functions get CLNAP-PDUs from customer equipment via a CLAI and forward them to other customer equipment via another CLAI.

Additional definitions:

– Access functions: Common name for originating, terminating and access-only functions;
– Originating CLAI: CLAI over which incoming CLNAP-PDUs are received;
– Terminating CLAI: CLAI over which outgoing CLNAP-PDUs are transmitted;
– Originating CLNI: CLNI over which incoming CLNIP-PDUs are received;
– Terminating CLNI: CLNI over which outgoing CLNIP-PDUs are transmitted.

6.1 Application rules for encapsulation and non-encapsulation

The following application rules apply:

i) At a CLNI between CL service providers, encapsulation is always used for both group and individually addressed PDUs.

ii) At a CLNI within a single CL service provider's domain, encapsulation and/or non-encapsulation may be used by the CL service provider.

Depending on the mechanism (encapsulation, non-encapsulation) used within the CL service provider's domain to which a CLS belongs, one or both mechanisms must be supported:

a) *Originating functions*

If encapsulation is used within the CL service provider's domain, the originating functions encapsulate every CLNAP-PDU.

In case of a CLNI within a CL service provider's domain, the non-encapsulation mechanism may alternatively be used by the originating functions.

b) *Terminating functions*

If encapsulation is used within the CL service provider's domain, the terminating functions have to decapsulate every CLNIP-PDU.

Terminating functions in a CL service provider's domain where the non-encapsulation mechanism is used have to differentiate between encapsulating and non-encapsulating CLNIP-PDUs and to appropriately handle them.

c) *Transit functions*

If encapsulation is used within the CL service provider's domain, the transit functions forward CLNIP-PDUs without being actively involved in the encapsulation mechanism.

If the originating CLNI is an intra-domain CLNI and the terminating CLNI is an inter-domain CLNI, the transit functions have to differentiate between encapsulating and non-encapsulating CLNIP-PDUs: non-encapsulating CLNIP-PDUs must be mapped to encapsulating CLNIP-PDUs before they are forwarded.

d) *Access-only functions*

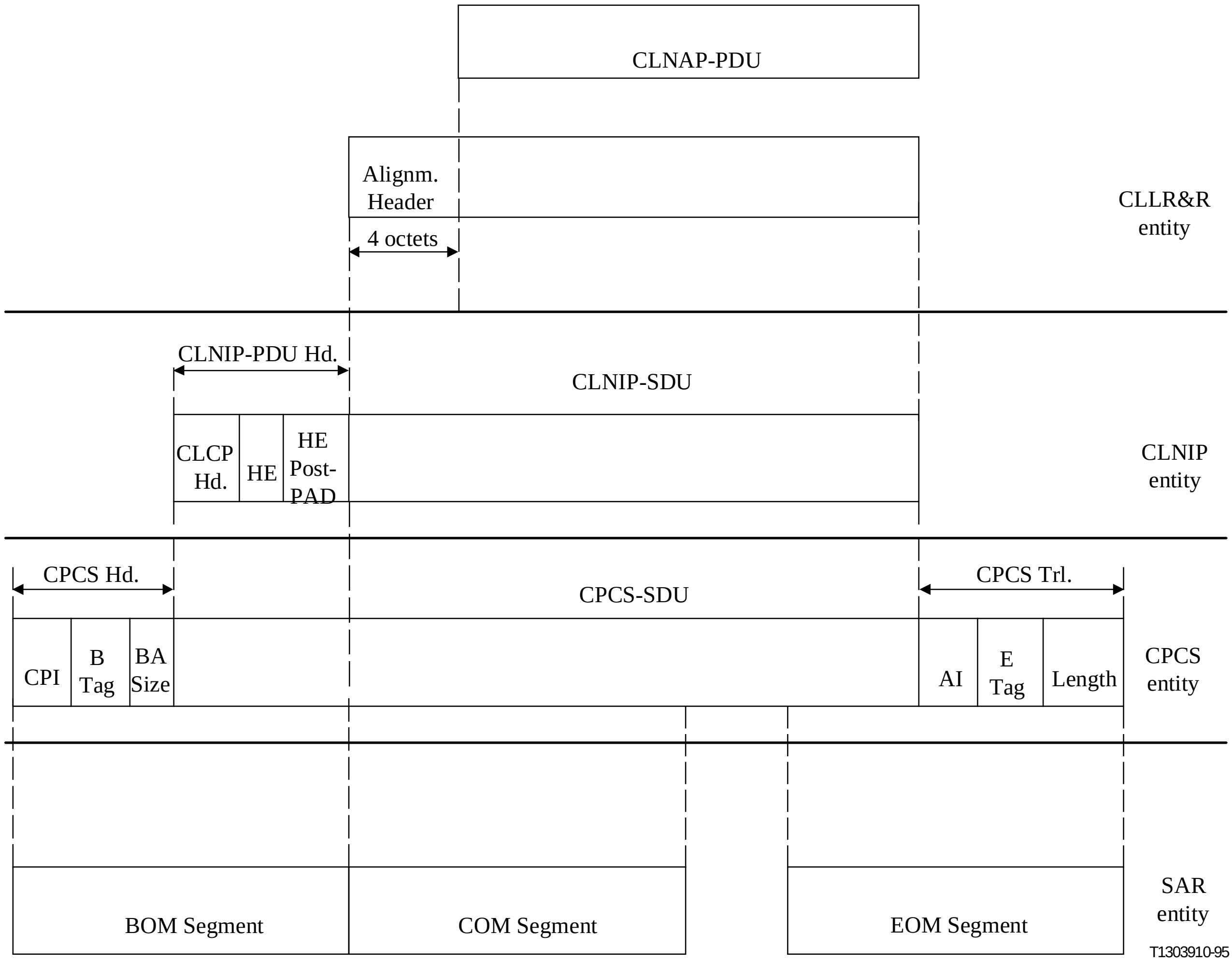
Access-only functions forward CLNAP-PDUs without applying either mechanism.

6.2 Encapsulation/decapsulation and non-encapsulation mechanisms

When encapsulation is performed, the CLSF adds a CLNIP-PDU header plus a 4-octet Alignment Header to the beginning of the CLNAP-PDU or the non-encapsulated CLNIP-PDU. The values of the fields of the CLNIP-PDU header are either derived by the CLSF or fixed due to protocol specifications.

The decapsulation mechanism strips the header plus the Alignment Header from the CLNIP-PDU in order to recover the CLNAP-PDU. See Figure 20.

In the case of non-encapsulation inside the CL service provider's domain, the CLNAP-PDU is regarded as a CLNIP-PDU and transparently transmitted within the network except for the Reserved field. Therefore, no special mechanism is required.



CLCP Header Connectionless Convergence Protocol Header

Figure 20/I.364 – Encapsulation of a CLNAP-PDU within a CLNIP-PDU

6.2.1 Derivation of the encapsulating CLNIP-PDU fields

The encapsulating CLNIP-PDU fields are derived from the CLNAP-PDU fields content, from the information (network configuration, management, subscription contract, etc.) available in the CLSF and the protocol specification. How the information available in the CLSF affects the derivation of the CLNIP-PDU fields contents (e.g. for group addressing) is for further study.

Destination Address

The content of this field may be different from the Destination Address received in the CLNAP-PDU (e.g. due to address resolution).

Source Address

This field is copied from the source address of the CLNAP-PDU.

Protocol Identifier

This field shall be set according to 5.4.3.

Header Extension

The derivation of the content of this field is for further study.

Header-Extension Post-PAD

It is generated according to 5.4.11.

Data

This field is derived by concatenating the content of the CLNAP-PDU and the Alignment Header.

Quality of Service (QOS)

It is set to "0".

6.2.2 Derivation of the non-encapsulating CLNIP-PDU fields

All the fields, except for the Reserved field, of the non-encapsulating CLNIP-PDU are kept equal to the corresponding fields of the CLNAP-PDU.

7 Group Addressed PDU handling

Group Address handling comprises administrative aspects and the transport of the Group Addressed PDUs. The data necessary to resolve a GA can be centralized in a network or distributed among networks. When receiving a Group Addressed PDU across a CLAI, the originating network needs to route the packet to the resolution function which is identified by the destination GA.

7.1 Definitions

For the definition of GA and NGA, see 2.7.

7.1.1 Group Address Agent (GAA)

The administrative aspects of a GA shall be undertaken by one and only one GAA. The GAA is responsible for assigning, deleting, amending group addresses and for inclusion, addition and deletion of individual addresses to the group according to the instructions of the user/client.

From the numbering point of view, the GAA assigns to a group a globally unique group address which belongs to the GAA's domain.

The GAA performs a complete or partial address resolution function. In the case of a partial resolution by the GAA (e.g. use of NGA), the complete resolution is accomplished with the support of other networks.

7.1.2 Nested Group Address Agent (NGAA)

The Nested Group Address (NGA) concept is applicable to encapsulating networks; its applicability within non-encapsulating networks requires further study.

The administrative aspects of an NGA shall be undertaken by one and only one NGAA. The NGAA is responsible for assigning, deleting, amending nested group addresses and for inclusion, addition and deletion of individual addresses associated with the NGA in cooperation with the GAA which is responsible for the group. The NGAA enables a stepwise and distributed GA resolution. It ensures the delivery of a group addressed CLNAP-PDU (GAP, see 2.1.1) to all members of the GA belonging to this NGAA.

From the numbering point of view, the NGA belongs to the address domain of the network to which the NGAA belongs and is globally unique. An NGA is of the type group address.

NOTE – No requirement for a special address type has yet been identified.

7.1.3 Architectural configurations for Group Addressing

The architectural configurations for transport of Group Addressed PDUs may include GAAs only or GAAs and NGAAs on a group address basis depending on agreements between service providers. In the following, the two approaches (GAAs only and GAAs plus NGAAs) are described as respectively "centralized database approach" and "centralized database approach in conjunction with NGAA".

It has to be noted that both approaches may have to be supported simultaneously by the network.

NOTE – The specific procedures described in 7.2 and 7.3 are not applicable for non-encapsulated CLNIP-PDUs.

7.2 Centralized database approach

In this approach, all the functions related to group address resolution for a specific GA are performed by the appointed GAA.

A typical centralized scheme is shown in Figure 21.

7.2.1 Transport mechanism

This subclause describes the transport mechanism by means of the example shown in Figure 21.

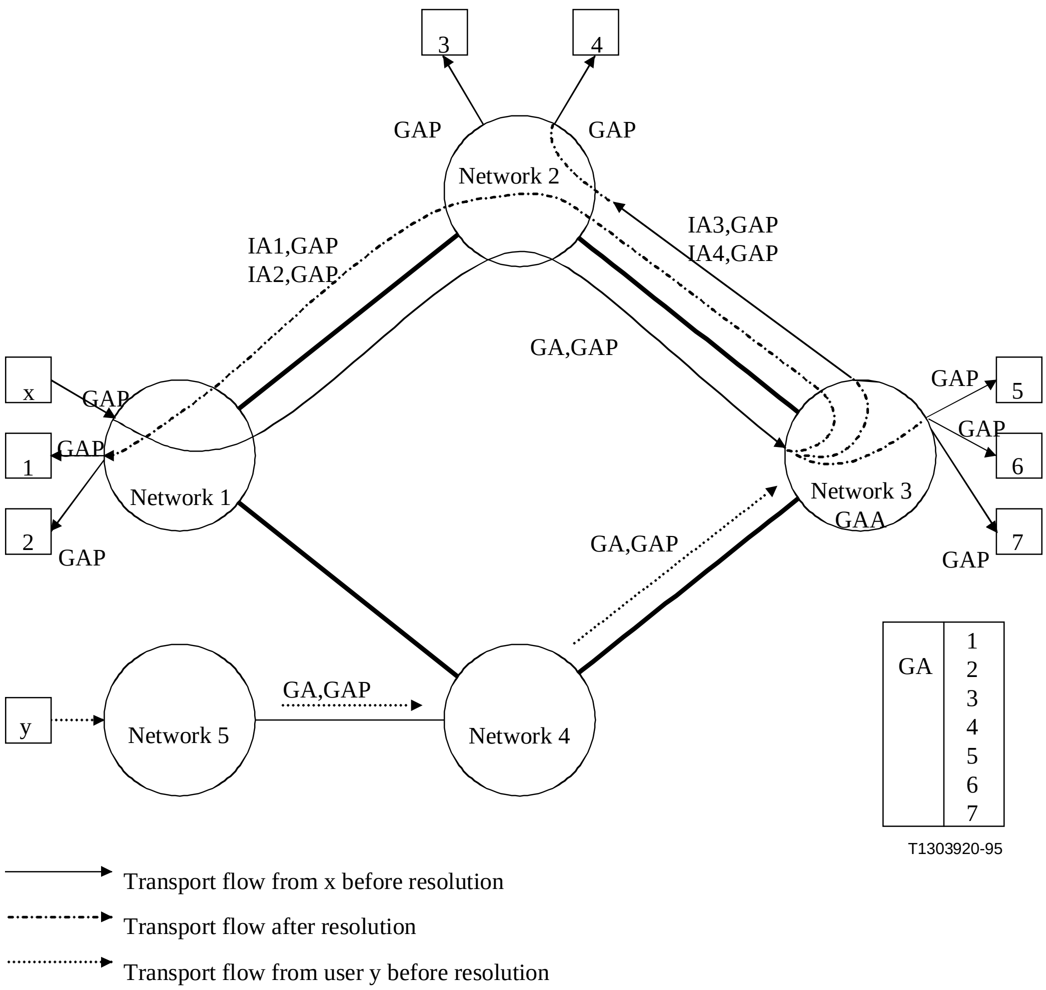


Figure 21/I.364 – Centralized database approach – An example

The GA identifies members 1 to 7; network 3 contains the GAA for the GA.

The transport operates as follows:

User x connected to network 1 originates a CLNAP-PDU with DA = GA. This PDU (GAP) is routed to network 3 which contains the GAA for the GA. Network 3 resolves the GA into the individual addresses of all the members (i.e. 1 to 7). Network 3 delivers the GAP directly to its own members (5, 6, 7) and sends to each of the other members a CLNIP-PDU carrying the individual destination address of the member (e.g. member 4 notation IA4, GAP).

No PDU is sent back to the originator x.

A GAP from user y connected to network 5 (network 5 does not serve any member of the group) is routed normally using the DA. A PDU, with GA as destination address, will be sent via network 4 to network 3 where resolution will take place. The transport mechanism after resolution works in the same way as above.

7.2.2 Adding a new member to the group

This subclause describes the addition of a new member to the group by means of the example shown in Figure 22.

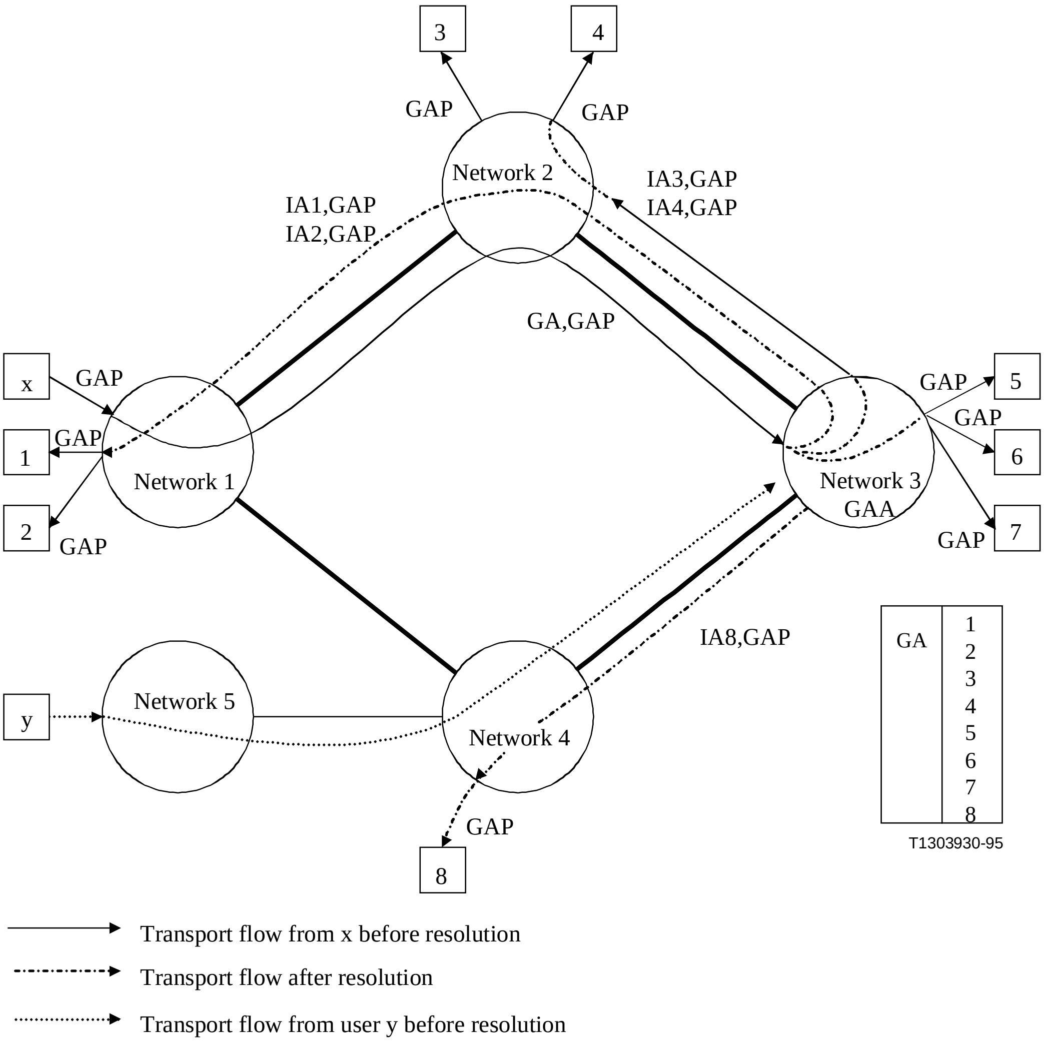


Figure 22/I.364 – Centralized database approach – An example of the addition of a new member

Member 8 on network 4 is added to the GA. The GA database in network 3 is updated. The transport then operates as follows: in addition to what is described in 7.2.1, network 3 sends an encapsulated PDU (notation IA8, GAP) to network 4 which will send the GAP to member 8.

7.3 Centralized database in conjunction with NGAAs

7.3.1 Centralized database in conjunction with one level of NGAAs

In this approach some of the functions related to group address resolution of a specific GA are devolved to NGAAs, which may be located in the same domain as the appointed GAA or in different domains than the appointed GAA. This approach avoids sending multiple copies of a group addressed PDU to another network. This approach may still require sending multiple copies of the group addressed PDU across other networks.

Each network serving one or more members of the GA may have the NGAA functionality.

7.3.1.1 Definition

The GAA has to arrange with some of the networks which serve members of the group to share the resolution task between the GAA and these networks which will operate as NGAAs. Each NGAA is identified by a NGA.

Once resolution has taken place, it is sufficient for the GAA to send a PDU addressed with NGA (notation NGA, GAP) as a destination address to each NGAA associated with the GA. Each of the NGAAs receiving a PDU with a destination address NGA which belongs to its network will complete GA resolution for its own network. A network which receives an encapsulated PDU with an NGA as the DA will route this PDU towards the network identified by the NGA.

Upon creation or extension of the GA, the GAA decides whether or not to distribute the resolution function. Criteria to create NGAAs are service provider dependent (e.g. topology of the group across different networks, number of members per network) and are outside the scope of this Recommendation.

7.3.1.2 Transport mechanism

This subclause describes the transport mechanism by means of the example shown in Figure 23.

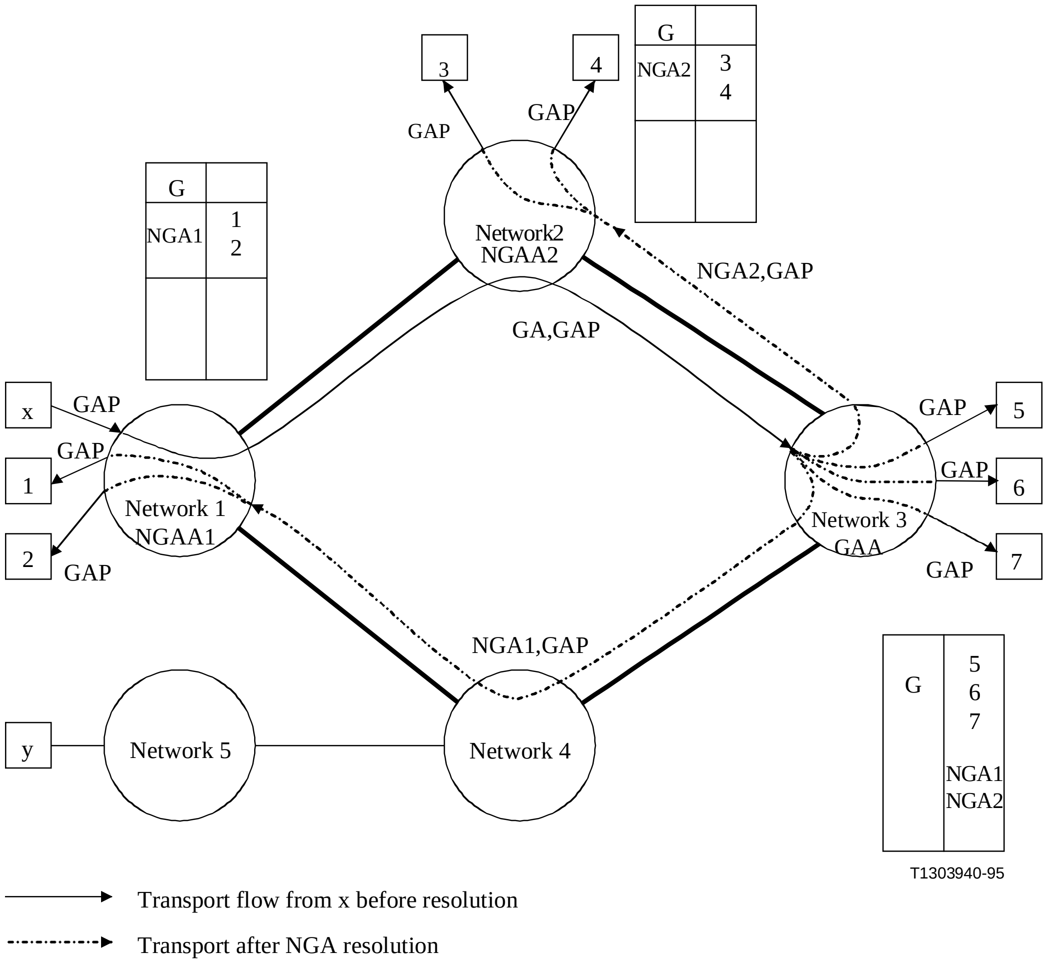


Figure 23/I.364 – Centralized database approach with one level of NGAAs – An example

From the point of view of the GAA, the GA identifies members 5, 6, 7 and NGA1, 2.

The transport operates as follows:

User x connected to network 1 originates a CLNAP-PDU with DA = GA.

The GAP is passed encapsulated (notation GA, GAP) to network 3 as described in 7.2.1.

Group address resolution takes place in network 3:

– GAPs are copied to local members 5, 6, 7 in network 3;

– only one PDU carrying a nested group address NGA2 as a DA is passed between the GAA and network 2 which is a nominated NGAA, this is for all members of NGA2;

– resolution of the NGA2 takes place at network 2, resulting in the PDU being copied to each individual member of the NGA, in the case shown members 3 and 4.

The same description applies for NGA1 and network 1.

7.3.1.3 Adding a new member to the group

This subclause describes the addition of a new member to the group by means of the example shown in Figure 24.

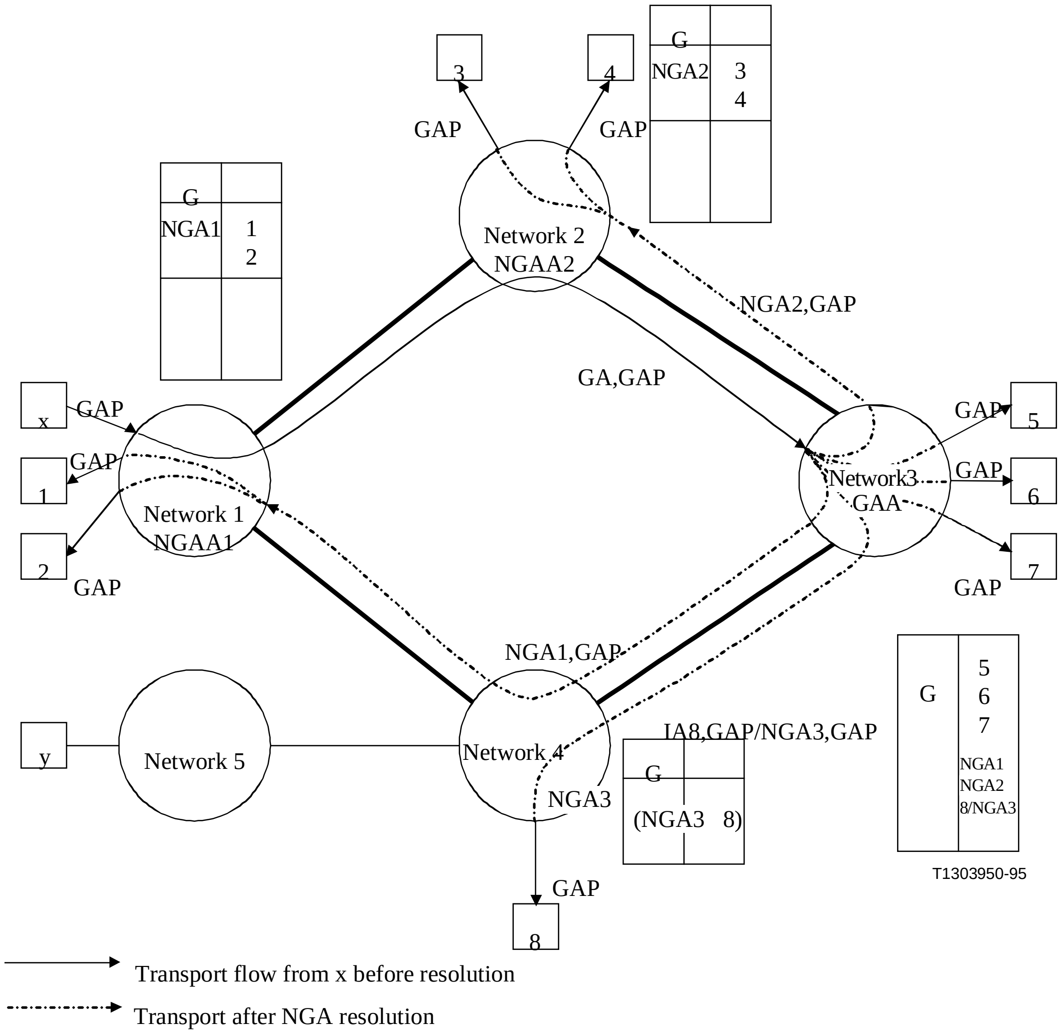


Figure 24/I.364 – Centralized database approach with one level of NGAAs – An example of the addition of a new member

With respect to Figure 23, member 8 on network 4 is added to the GA. On the basis of the arrangements of the GAA, this results in either:

a) the creation of NGA3 with the single entry of member 8; or

b) the addition of member 8 to the database in network 3 without the creation of an NGA.

The transport then operates as follows: in addition to what is described in 7.3.1.2, the network 3 sends an encapsulated PDU (notation NGA3, GAP) in case a) above, or an encapsulated PDU (notation IA8, GAP) in case b) above, to network 4 which will send the GAP to member 8.

7.3.2 Centralized database approach in conjunction with multiple levels of NGAAs

In this approach some of the functions related to group address resolution of a specific GA are devolved to multiple levels of NGAAs, which may be located in the same domain as the appointed GAA or in different domains. This approach can avoid sending multiple copies of a group addressed PDU across other networks.

Each network having one or more members of the GA may have the NGAA functionality.

7.3.2.1 Definition

The GAA has to arrange with other networks to share the resolution task between the GAA and these networks which will operate as different level NGAAs. Each NGAA is identified by an NGA.

Once resolution has taken place, it is sufficient for the GAA to send a PDU addressed with NGA (notation NGA, GAP) as the destination address to the subset of NGAAs at the first level that will themselves multicast to other NGAAs of the next level associated with the GA. Each of the NGAAs receiving a PDU with its destination address NGA will complete the GA resolution for its members.

7.3.2.2 Transport mechanism

For further study.

7.3.3 Partial resolution before the GAA

In this approach partial group address resolution may take place in any of the NGAAs crossed before the GAP arrives at the GAA.

7.3.3.1 Definition

A number of networks may participate in the group address resolution process. The GAA resolves either the complete or only part of the group address. In case of partial resolution by the GAA, the complete resolution is accomplished with the support of NGAAs.

The elements participating in the group address resolution process for a given group are interconnected in a tree-like structure. This structure is also known as a spanning tree. It has to be noted that this tree is fairly static and restructuring will be initiated from the root.

The GAA has to arrange with other networks to share the resolution task between the GAA and these networks which will operate as partial resolution NGAAs. This resolution task is named "enhanced group address resolution".

A special case is the source resolution. It allows an originating network (and only the originating network) which is an NGAA for the GA of a GAP to perform the partial resolution function for its NGA.

7.3.3.2 Transport mechanism

7.3.3.2.1 Required configuration information

For a given GA, a certain service provider (a) is the GAA for this particular group. Another service provider (b) may participate in the group address resolution process as NGAA. This service provider (b) creates a Nested Group Address (NGA) associated with this particular GA. A number of NGAA associated with this particular GA can be created, yielding a multiple level address resolution tree.

In the enhanced group address resolution functionality, each of these NGAAs is identified by a NGAA Identifier (NGID). Those NGIDs are only unique within a GA. The value of the NGID is always non-zero.

A new NGID value is allocated by the GAA each time a NGA for this particular GA is created (even through several levels of the hierarchy). Each NGID is unique for a given GA, but its significance is limited to this GA.

7.3.3.2.2 Example

For a more comprehensive example and description of the algorithm, see Appendix III.

This subclause describes the transport mechanism by means of the example shown in Figure 25.

From the point of view of the GAA, the GA identifies members 12, 13 and NGA 1, 2, 3 and 4.

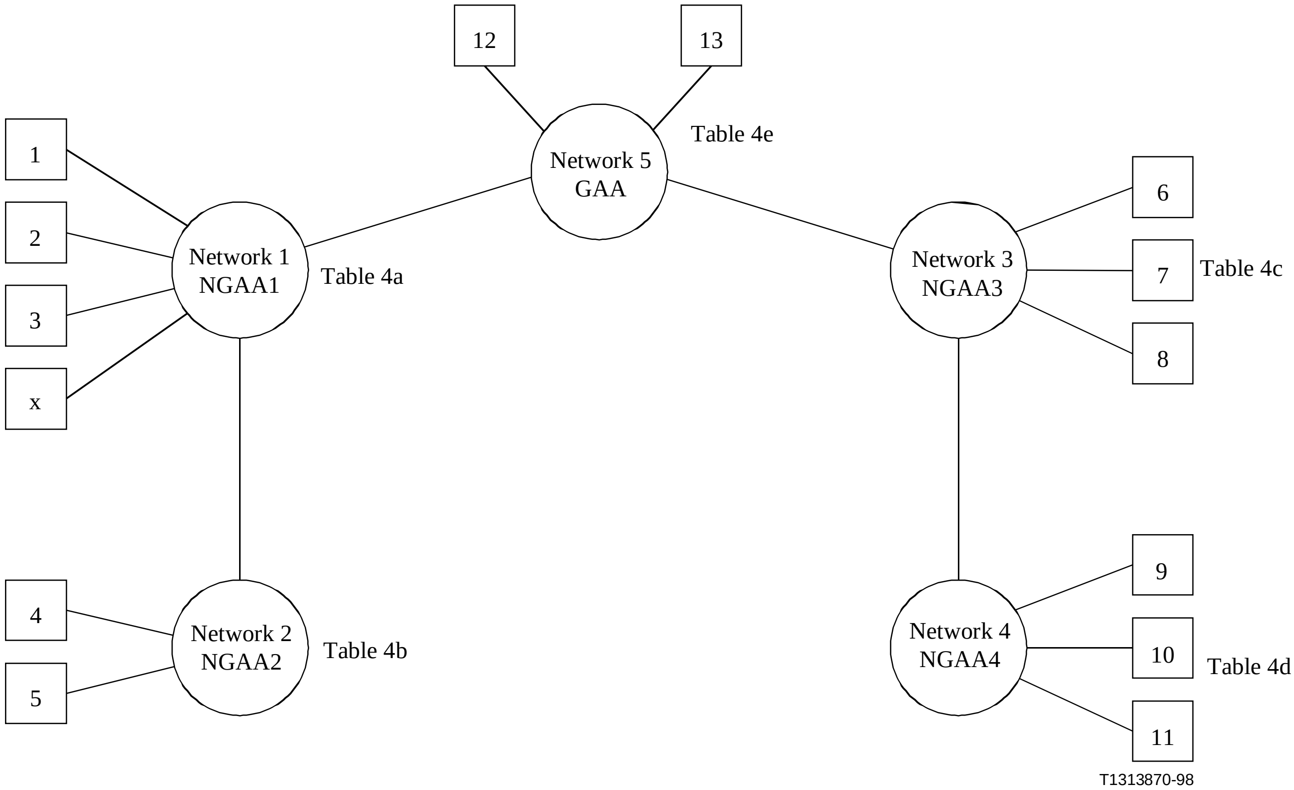


Figure 25/I.364 – Partial resolution before the GAA – An example

Table 4/I.364 – Reachability information for partial resolution

Table 4a

NGAA1 (G)	NGID1	GAA
		1, 2, 3, NGAA2

Table 4b

NGAA2 (G)	NGID2	NGAA1
		4, 5

Table 4c

NGAA3 (G)	NGID3	GAA
		6, 7, 8, NGAA4

Table 4d

NGAA4 (G)	NGID4	NGAA3
		9, 10, 11

Table 4e

GAA (G)	NGID5	12, 13
	NGAA1	1, 2, 3, NGAA2
	NGAA2	4, 5
	NGAA3	6, 7, 8, NGAA4
	NGAA4	9, 10, 11

The transport operates as follows:

User x connected to network 1 originates a CLNAP-PDU with DA = GA.

Group address resolution takes place in network 1:

– GAPs are copied to the local members 1, 2 and 3 in network 1;

– The GAP is encapsulated (notion DA = GAA, SA = SA_n, NGID = 1) and copies are passed to network 2 and 5;

Group address resolution takes place in network 2:

– GAPs are copied to the local members 4 and 5 in network 2;

Group address resolution takes place in network 5:

– GAPs are copied to the local members 12 and 13 in network 5;

– The GAP is encapsulated (notion DA = NGA3, SA = SA_n, NGID = 5) and passed to network 3;

Group address resolution takes place in network 3:

– GAPs are copied to the local members 6, 7 and 8 in network 3;

– The GAP is encapsulated (notion DA = NGA4, SA = SA_n, NGID = 3) and passed to network 4;

Group address resolution takes place in network 4:

– GAPs are copied to the local members 9, 10 and 11 in network 4.

7.3.3.3 Adding a new member to the group

This subclause describes the addition of a new member to the group by means of the example shown in Figure 26. Two cases may be distinguished.

– A member is added to an existing NGAA.

– A member leads to the creation of a new NGA.

- Case 1: Member 14 on network 4 is added to the GA. In the GA database in network 5 a new entry for member 14 is created. A new table entry in NGAA4 for member 14 is also created.
- Case 2: Member 15 on network 6 is added to the GA. In the GA database in network 5 a new entry for member 15 and NGAA5 is created. A new table entry in NGAA4 for NGAA5 is also created. A new entry for member 15 is created in NGAA5.

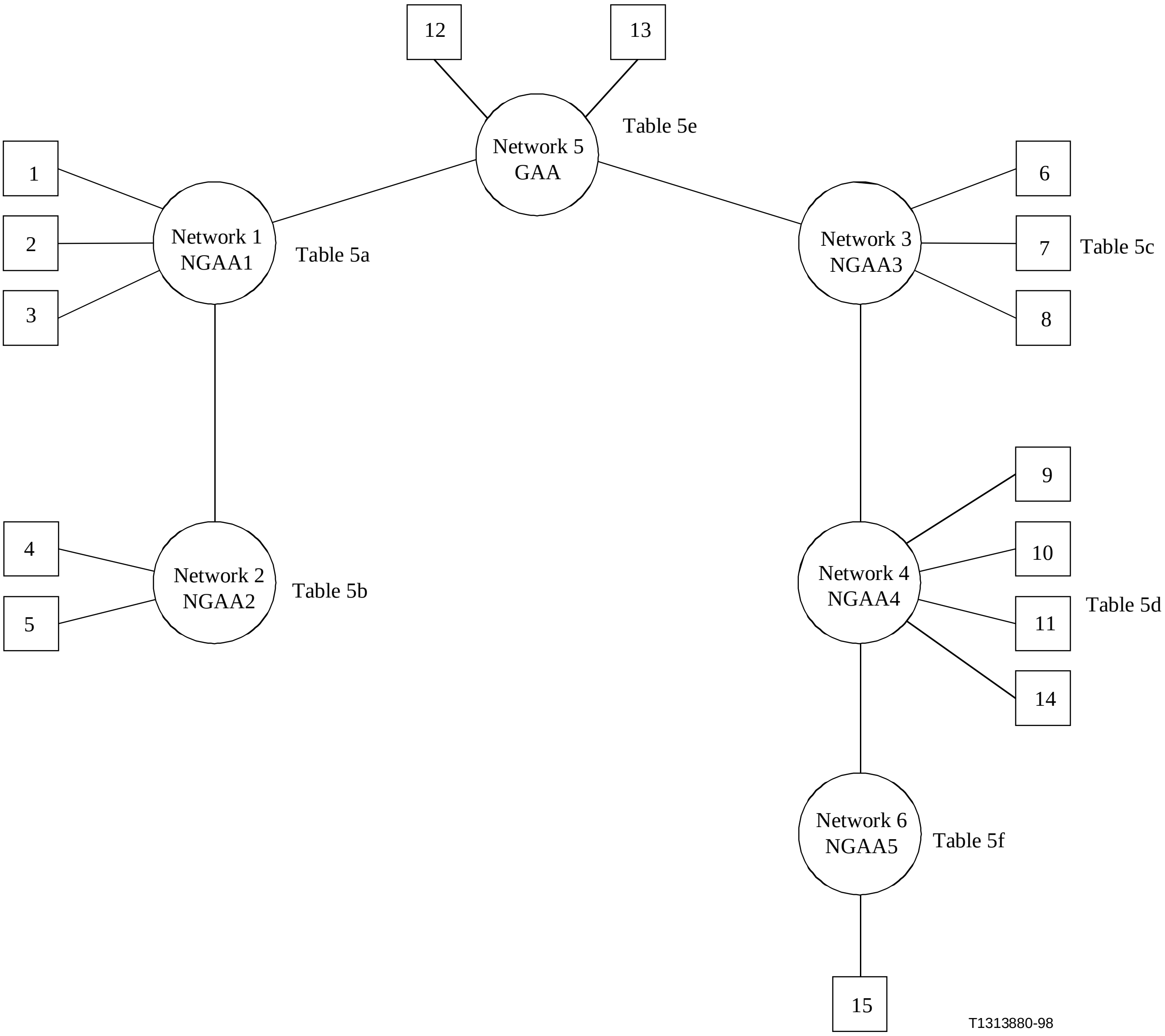


Figure 26/I.364 – Partial resolution before the GAA – Addition of a new member – An example

Table 5/I.364 – Reachability information after the addition of a new number

Table 5a

NGAA1 (G)	NGID1	GAA
		1, 2, 3, NGAA2

Table 5b

NGAA2 (G)	NGID2	NGAA1
		4, 5

Table 5c

NGAA3 (G)	NGID3	GAA
		6, 7, 8, NGAA4

Table 5d

NGAA4 (G)	NGID4	NGAA3
		9, 10, 11, 14, NGAA5

Table 5e

GAA (G)	NGID5	12, 13
	NGAA1	1, 2, 3, NGAA2
	NGAA2	4, 5
	NGAA3	6, 7, 8, NGAA4
	NGAA4	9, 10, 11, 14, NGAA5
	NGAA5	15

Table 5f

NGAA5 (G)	NGID6	NGAA4
		15

7.4 Combination of group address resolution mechanism

For further study.

ANNEX A

Encoding of the Destination Address field and Source Address field

Table A.1/I.364 – Encoding of the Destination Address field

Address type	Address structure/meaning
0100	Reserved (Note)
1000	Reserved (Note)
1100	E.164 publicly administered individual address
1101	Reserved (Note)
1110	E.164 publicly administered group address
1111	Reserved (Note)
All other codes	Reserved for future standardization
NOTE – The use of these values is defined for MAN application – see ISO/IEC 8802-6.	

Table A.2/I.364 – Encoding of the Source Address field

Address type	Address structure/meaning
0100	Reserved (Note)
1000	Reserved (Note)
1100	E.164 publicly administered individual address
1101	Reserved (Note)
All other codes	Reserved for future standardization
NOTE – The use of these values is defined for MAN application – see ISO/IEC 8802-6.	

The E.164 number carried in the 60-bit address subfield is the international ISDN number. The international ISDN number can be up to 15 decimal digits. When numbers are less than 15 decimal digits, the number is placed in the most significant bits of the address subfield. The remaining part of the address subfield is coded to all binary "1"s.

The E.164 numbers are coded using Binary Coded Decimal (BCD).

APPENDIX I

List of acronyms

For the purposes of this Recommendation, the following abbreviations are used:

AAL ATM Adaptation Layer

AATF ATM Access Termination Function

AL ALignment

ANTF ATM Network Termination Function

ATF Access Termination Function

ATM Asynchronous Transfer Mode

BAsize Buffer Allocation Size

BCD Binary Coded Decimal

BCDBS Broadband Connectionless Data Bearer Service

B-ISDN Broadband Integrated Services Digital Network

BOM Beginning Of Message

Btag Beginning tag

CF Connection Function

CIB CRC Indication Bit

CL ConnectionLess

CLAI ConnectionLess Access Interface

CLATF CL Access Termination Function

CLCP ConnectionLess Convergence Protocol

CLHF ConnectionLess Handling Function

CLL	ConnectionLess Layer
CLLR&R	ConnectionLess Layer Routing & Relaying
CLMF	ConnectionLess Mapping Function
CLNAP	ConnectionLess Network Access Protocol
CLNI	ConnectionLess Network Interface
CLNIP	ConnectionLess Network Interface Protocol
CLNTF	CL Network Termination Function
CLS	ConnectionLess Server
CLSF	ConnectionLess Service Function
COM	Continuation Of Message
CPCS	Common Part Convergence Sub-layer
CPE	Customer Premises Equipment
CPI	Common Part Indicator
CRC	Cyclic Redundancy Check
CS	Convergence Sub-layer
CTF	ConTrol Function
DA	Destination Address
EOM	End Of Message
Etag	End tag
GA	Group Address
GAA	Group Address Agent
GAHF	Group Address Handling Function
GAP	Group Addressed CLNAP-PDU
HE	Header Extension
HEL	Header Extension Length
HLPI	Higher-Layer-Protocol-Identifier
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
MAN	Metropolitan Area Network
MID	Multiplexing IDentification
MIR	Maximum Information Rate
NGA	Nested Group Address
NGAA	Nested Group Address Agent
NGID	NGAA Identifier
NNI	Network Node Interface
NPC	Network Parameter Control

NTF	Network Termination Function
OAM	Operation And Maintenance
PCF	Protocol Conversion Function
PDU	Protocol Data Unit
PI	Protocol Identifier
PPTU	PDUs per Time Unit
QOS	Quality of Service
SA	Source Address
SAP	Service Access Point
SAR	Segmentation And Reassembly
SDU	Service Data Unit
SIR	Sustained Information Rate
SSCS	Service Specific Convergence Sub-layer
SSM	Single Segment Message
UNI	User Network Interface
UPC	Usage Parameter Control
VC	Virtual Channel
VCI	Virtual Channel Identifier
VP	Virtual Path
VPI	Virtual Path Identifier

APPENDIX II

SDL diagrams

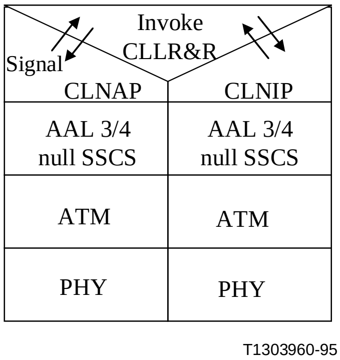
II.1 General description

The SDL diagrams serve formal and descriptive purposes; they do neither imply the existence of the primitives described in a specific implementation nor the explicit distribution of functions between CLNAP, CLNIP and CLLR&R entities as assumed for the purpose of this description.

The SDL diagrams do not preclude operation at the CLL in a streaming mode or on the fly fashion, i.e. when only virtual reassembly of PDUs is done at this level. Details of this mode are for further study.

Concerning multicasting mechanisms, this appendix covers only 7.2 and 7.3.1. Additions are required to cover 7.3.2, 7.3.3 and 7.4.

The CLLR&R is positioned as follows:



The arrows represent the signals exchanged between the CLLR&R and the CLNAP or CLNIP entities of the CLL.

The function of the CLLR&R entity is described in 2.3 and 2.4.

It is assumed that the protocol entity (CLNAP or CLNIP) checks the validity of any CLNAP/CLNIP-PDU it receives over a CLAI or CLNI; these controls are reflected in 5.5 (Error conditions). The received PDU in the CLLR&R is then assumed to be correct in relation to encapsulation/non-encapsulation.

It is assumed as well that the CLNIP and CLNAP functions belonging to the functional blocks ATF & NTF (see 2.3) perform formatting of the PDUs, i.e. encapsulation or decapsulation.

These SDL diagrams cover the case in which a received encapsulated PDU is transported encapsulated within a non-encapsulating domain up to the destination node and the case, when as a non-encapsulating domain option, a CLNIP-PDU encapsulating individually addressed CLNAP-PDU (notation IA, IAP) is transported decapsulated to the destination user served by this domain.

Interaction between entities

The description of the interaction is made in terms of primitives between the CLLR&R entity and the protocol entity but these primitives are named "invoke" (when initiated by the CLLR&R) and "signal" (when initiated by the protocol entity) to differentiate from layer interface primitives.

Interaction with management entities is not covered in the SDL diagrams.

II.2 Interaction between CLNAP entity and CLLR&R entity

A receiving CLNAP entity forwards each CLNAP-PDU with an EI (Encapsulating Indicator) parameter to the CLLR&R entity. The EI is set to FALSE, indicating that the CLNAP-PDU is not an encapsulating one.

A transmitting CLNAP entity receives from the CLLR&R entity the CLNAP-PDU to be transmitted over a CLAI.

II.3 Interaction between CLNIP entity and CLLR&R entity

A receiving CLNIP entity forwards each CLNIP-PDU with an EI parameter to the CLLR&R entity. The EI indicates whether or not the CLNIP-PDU is an encapsulating one.

A transmitting CLNIP entity receives from the CLLR&R entity a data parameter and the EI parameter indicating if the data parameter is a CLNIP-PDU to be kept as it is or has to be encapsulated.

If the data parameter has to be encapsulated, the CLNIP entity gets, in addition, DA, SA, QOS, HE, HE Post-PAD parameters to be used in the encapsulating header of the CLNIP-PDU. The CLNIP entity adds a CLNIP-PDU header and an Alignment Header at the beginning of the data parameter value. The values in the added CLNIP-PDU header are derived from the additional parameters and the data parameter.

A CLLR&R entity derives the EI parameter from the DA in the PDU and from the knowledge about the mechanism used in the domain for encapsuIation/non-encapsulation.

If encapsulation needs to be performed, the CLLR&R entity derives DA, HE and HE Post-PAD to be used in the encapsulating CLNIP-PDU and forwards the received PDU, the EI parameter and the additional parameter values to the appropriate transmitting CLNIP entity.

If decapsulation has to be performed, the CLLR&R entity strips the CLNIP-PDU header and the Alignment Header and forwards the CLNAP-PDU to the appropriate CLNAP entity.

If no encapsulation/decapsulation has to be performed, the CLLR&R entity forwards the PDU to the appropriate CLNAP entity, or to the appropriate CLNIP entity with the indication that no encapsulation is required.

Two types of CLNI are distinguished: intra-domain and inter-domain.

Process CLLR&R

Signals to/from CLNAP

CLNAP-UNITDATA.invoke (data)

data	CLNAP-PDU to be forwarded.

CLNAP-UNITDATA.signal (data, EI)

data	CLNAP-PDU received.
EI	false.

Signals to/from CLNIP

CLNIPI-UNITDATA.invoke (data, EI, DA, QOS, HE, HE Post-PAD)

data	CLNAP- or CLNIP-PDU to be forwarded.
EI	True when encapsulation has to be performed, false when encapsulation does not have to be performed which does not preclude PI to be adjusted when needed.

Other parameters are only present when EI is true:

DA	This parameter specifies the destination address to be used in the encapsulating CLNIP-PDU. It may be different from the destination address in the PDU contained in the data parameter (e.g. due to address resolution).
SA	This parameter is equal to the SA of the CLNAP-PDU.
QOS	This parameter is equal to "0".
HE	This parameter specifies the value to be transmitted in the encapsulating CLNIP-PDU.
HE Post-PAD	This parameter specifies the value to be transmitted in the encapsulating CLNIP-PDU; its first octet is set to "1".

CLNIPI-UNITDATA.signal (data, EI)

data	CLNIP-PDU received.
EI	True when CLNIP-PDU is encapsulating, false when it is not encapsulating.

CLNIPN-UNITDATA.invoke (data, EI, DA, SA, QOS, HE, HE Post-PAD)

data	CLNAP- or CLNIP-PDU to be forwarded.
EI	True when encapsulation has to be performed, false when encapsulation does not have to be performed.

Other parameters are only present when EI is true:

DA	This parameter specifies the destination address to be used in the encapsulating CLNIP-PDU. It may be different from the destination address in the PDU contained in the data parameter (e.g. due to address resolution).
SA	This parameter is equal to the SA of the CLNAP-PDU.
QOS	This parameter is equal to "0".
HE	This parameter specifies the value to be transmitted in the encapsulating CLNIP-PDU.
HE Post-PAD	This parameter specifies the value to be transmitted in the encapsulating CLNIP-PDU; its first octet is set to "1".

CLNIPN-UNITDATA.signal (data, EI)

data	CLNIP-PDU received.
EI	True when CLNIP-PDU is encapsulating, false when it is not encapsulating.

INTRA-DOMAIN

It is used when the received PDU is addressed to a user/CLAI of the domain in which this server is.

Parameters INTRA-DOMAIN

data	CLNAP/CLNIPN/CLNIPI-UNITDATA data parameter.
@	Destination address from BOM; can be an Individual Address (IA) or a Group Address (GA).
ingress IF type	Type of interface on which PDU entered the domain; can be a CLAI, a CLNIN or a CLNII.
egress IF type	Type of interface of the domain to which PDU is destined; it is a CLAI.
EI	Indicates if received PDU is encapsulated or not.

INTER-DOMAIN

It is used when the received PDU is destined to a domain different from the domain in which this server is.

Parameters INTER-DOMAIN

data	CLNAP/CLNIPN/CLNIPI-UNITDATA data parameter.
@	Destination address from BOM; can be an Individual Address (IA) or a Group Address (GA or a NGA).
ingress IF type	Type of interface on which PDU entered the domain; can be a CLAI, a CLNIN or a CLNII.

egress IF type	Type of interface of the domain to which PDU is destined; it is a CLNII.
EI	Indicates if received PDU is encapsulated or not.

GARFLOODING

It is used when the PDU received requires resolution (partial or not) of a GA/NGA.

Parameters GARFLOODING

data	CLNAP/CLNIPN/CLNIPI-UNITDATA data parameter.
@	Destination address from BOM; can be an Individual Address (IA) or a Group Address (GA or a NGA).
ingress IF type	Type of interface on which PDU entered the domain; can be a CLAI, a CLNIN or a CLNII.
egress IF type	Type of interface of the domain to which PDU is destined; the type is indifferent.
EI	Indicates if received PDU is encapsulated or not.

DELIVERY

It is used when PDU is to be delivered to a user of the domain or to another domain, which is directly connected/accessible to/by this server of the domain.

Parameters of DELIVERY

data	CLNAP/CLNIPN/CLNIPI-UNITDATA invoke parameter.
@	Destination address; can be an Individual Address (IA) or a Group Address (GA or a NGA).
ingress IF type	Type of interface on which PDU entered the domain; can be a CLAI, a CLNIN or a CLNII.
egress IF type	Type of interface of the domain to which PDU is destined; the type is CLAI or CLNII.
egress IF	It is the identification of the interface over which the PDU will be sent from this server.
EI	Indicates if the PDU is to be encapsulated or not.

FORWARD

It is used when PDU needs to be forwarded, from this server, inside the domain.

Parameters of FORWARD

data	CLNAP/CLNIPN/CLNIPI-UNITDATA invoke parameter.
@	Destination address; can be an Individual Address (IA) or a Group Address (GA or a NGA).
ingress IF type	Type of interface on which PDU entered the domain; can be a CLAI, a CLNIN or a CLNII.
egress IF type	Type of interface of the domain to which PDU is destined; the type is CLAI or CLNII.
egress IF	It is the identification of the interface over which the PDU will be sent from this server; it is a CLNIN.

EI Indicates if the PDU is to be encapsulated or not.

FLOODING

It is used by this server when resolution or partial resolution is done in the server and needs to be completed inside the domain.

Parameters of FLOODING

FFS

GA RESOLUTION

It is used to resolve the membership of the group. Parameters are for further study.

ROUTE AND LINK

It is used to derive the route and the link to be used by the PDU. Parameters are for further study.

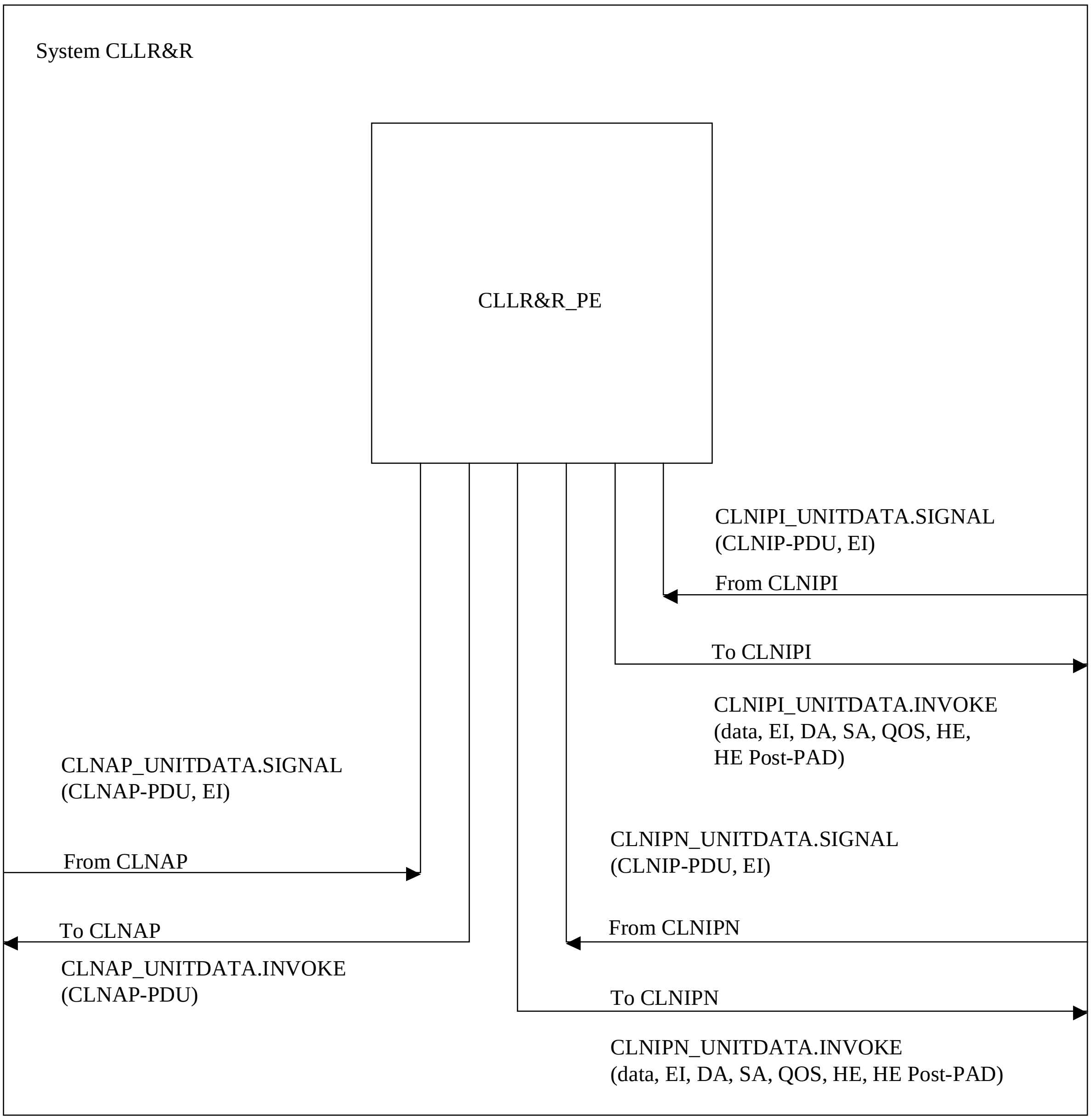


Figure II.1/I.364

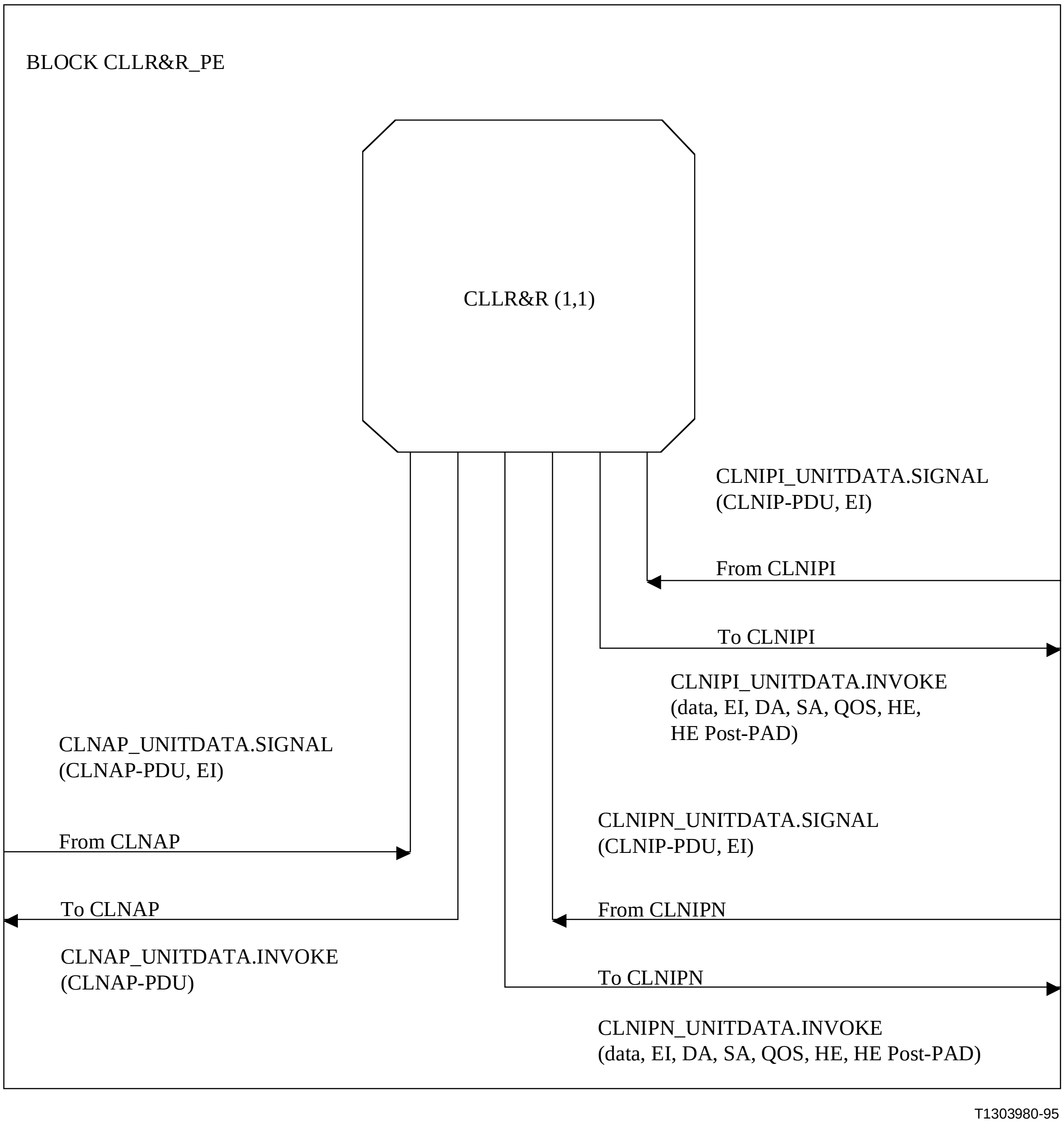


Figure II.2/I.364

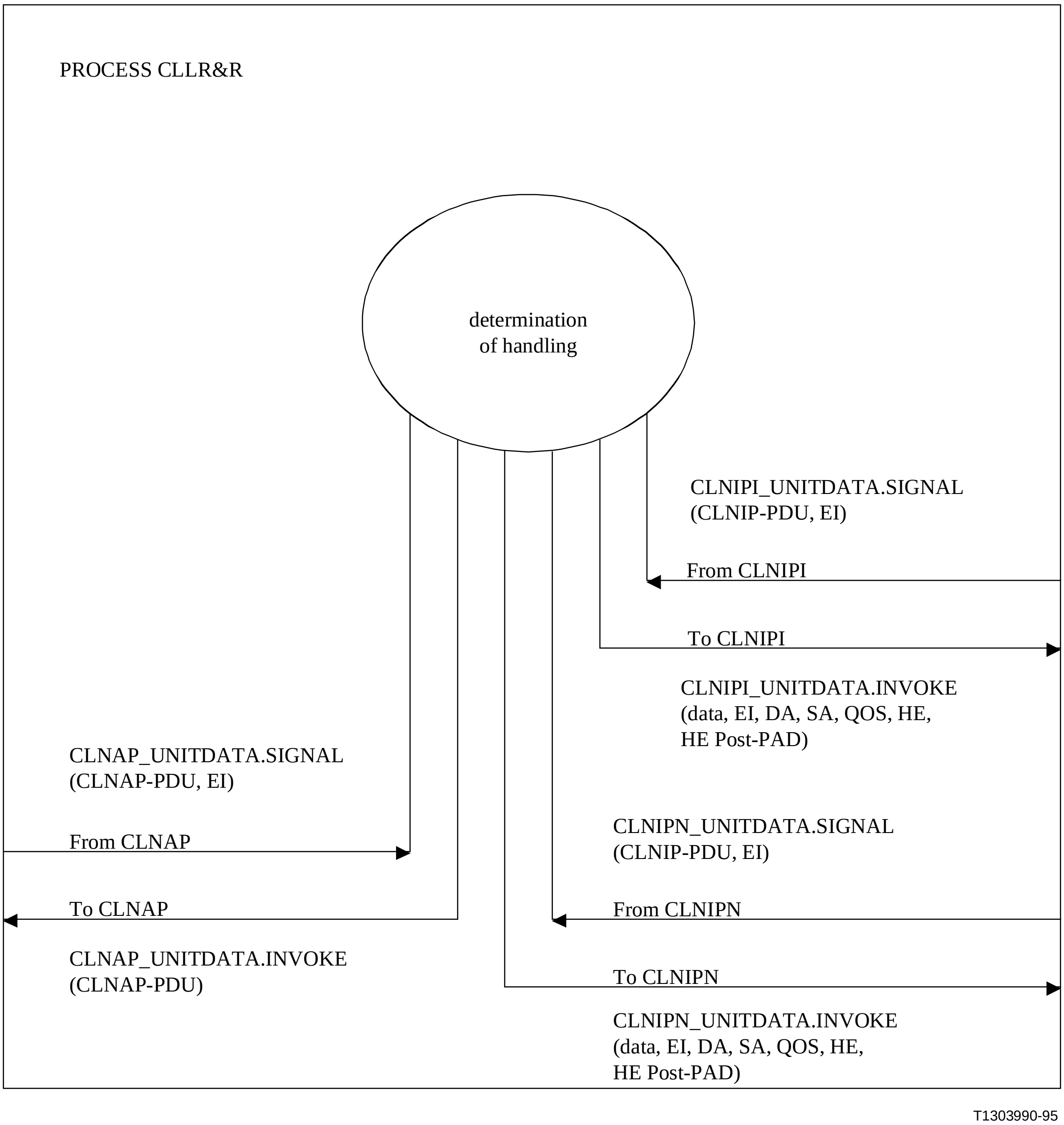


Figure II.3/I.364

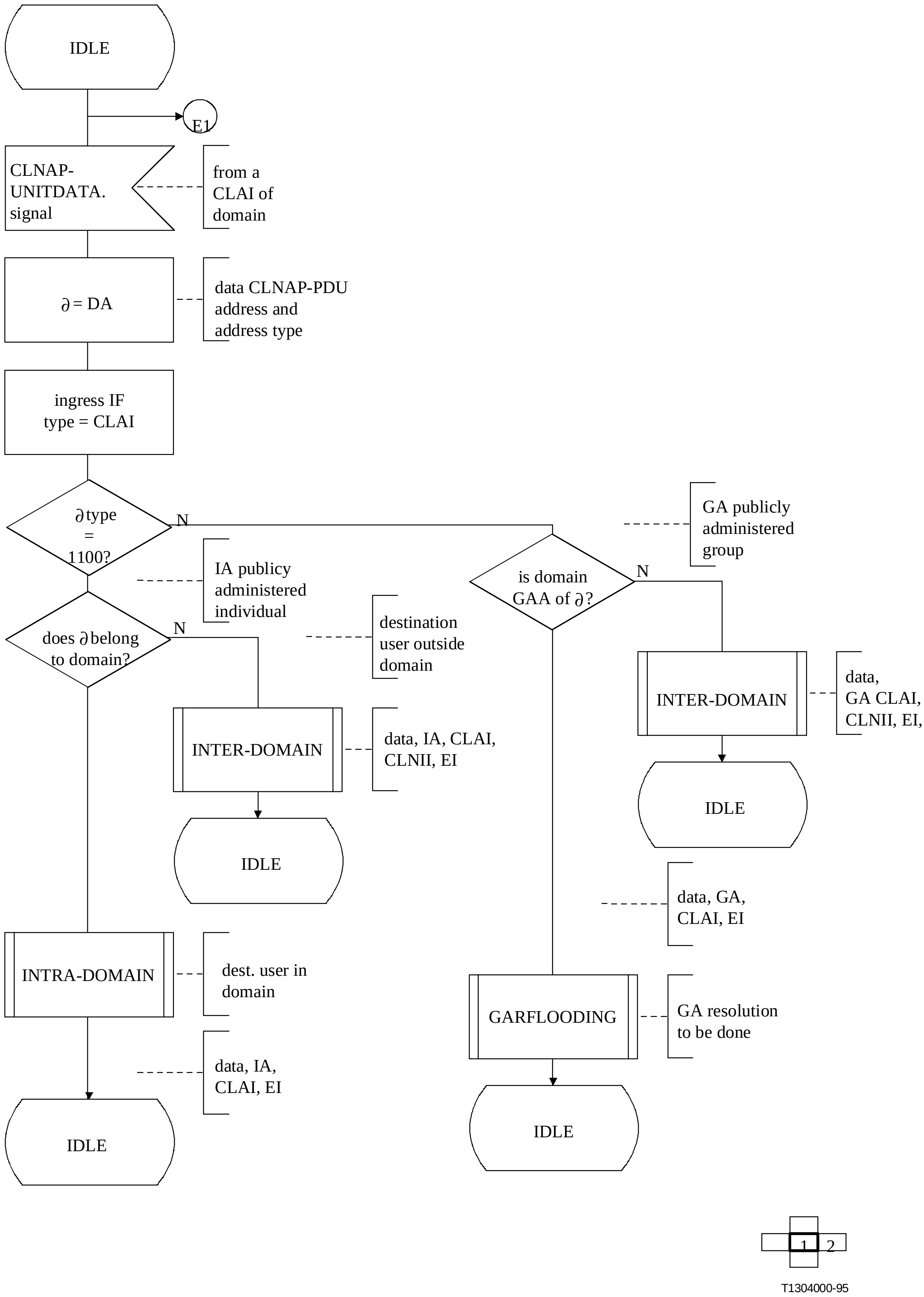


Figure II.4/I.364 ***(sheet 1 of 15)***

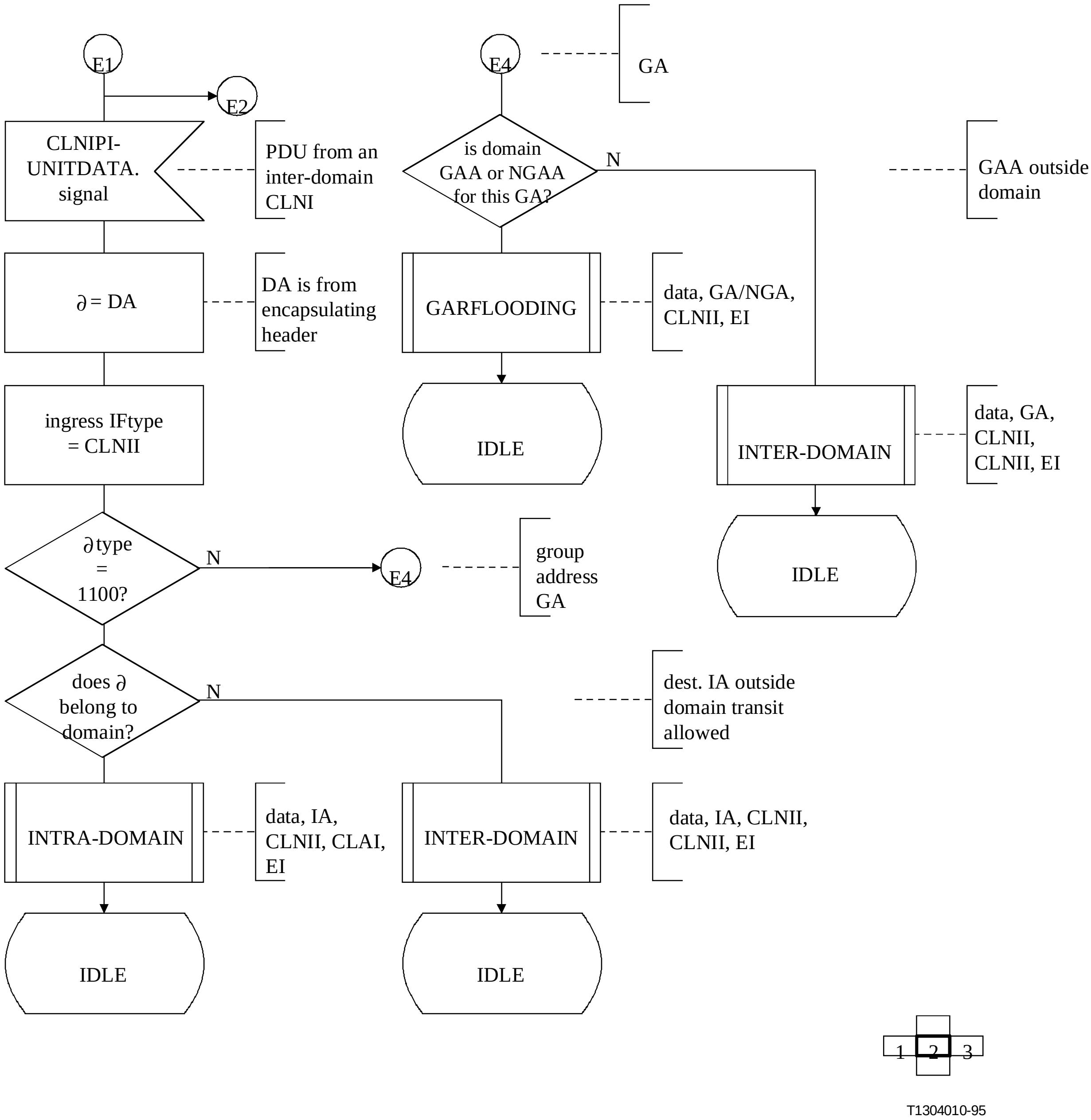


Figure II.4/I.364 ***(sheet 2 of 15)***

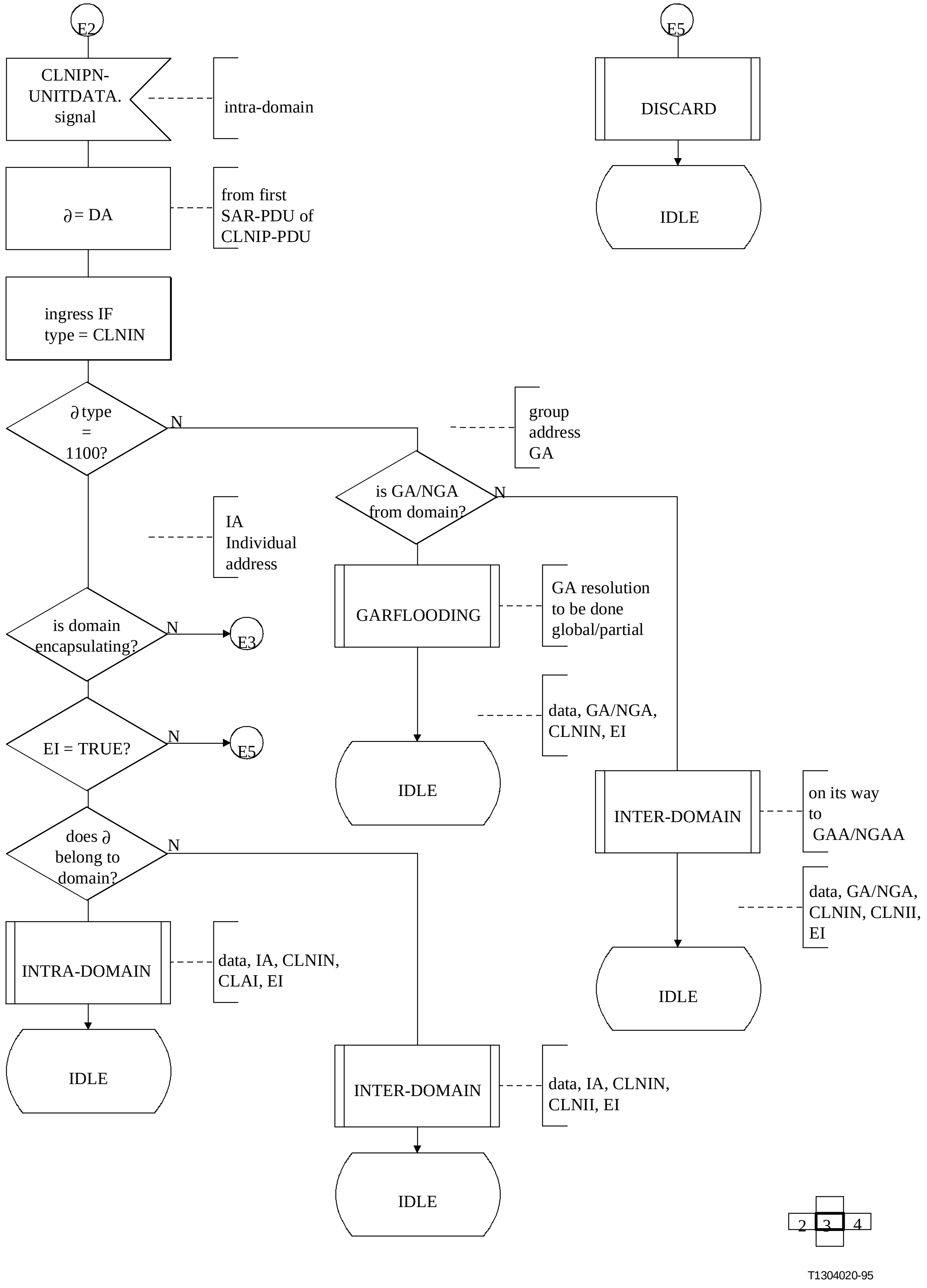


Figure II.4/I.364 ***(sheet 3 of 15)***

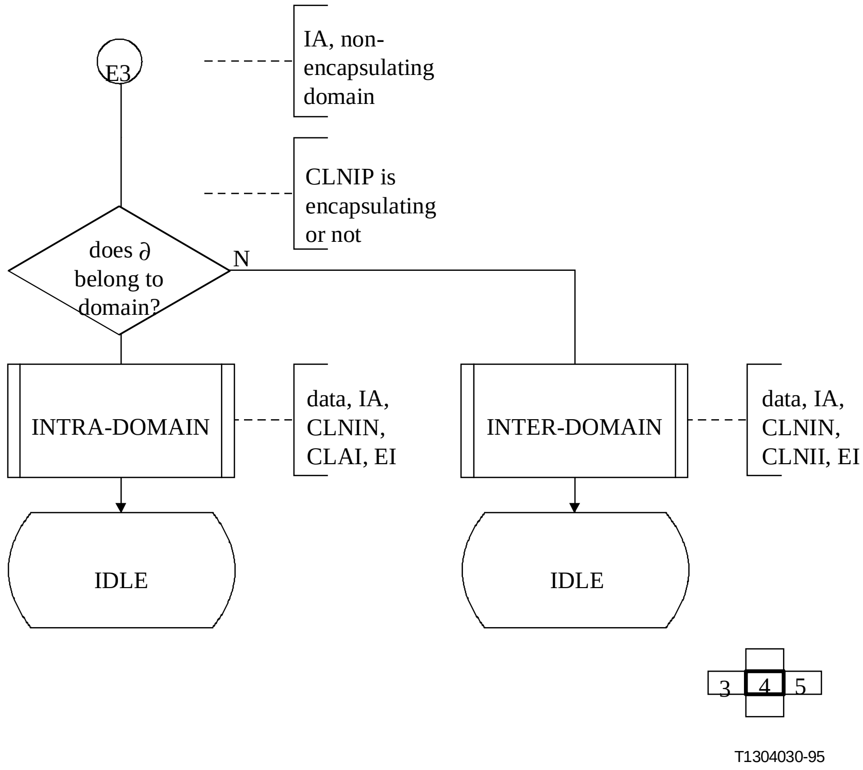


Figure II.4/I.364 ***(sheet 4 of 15)***

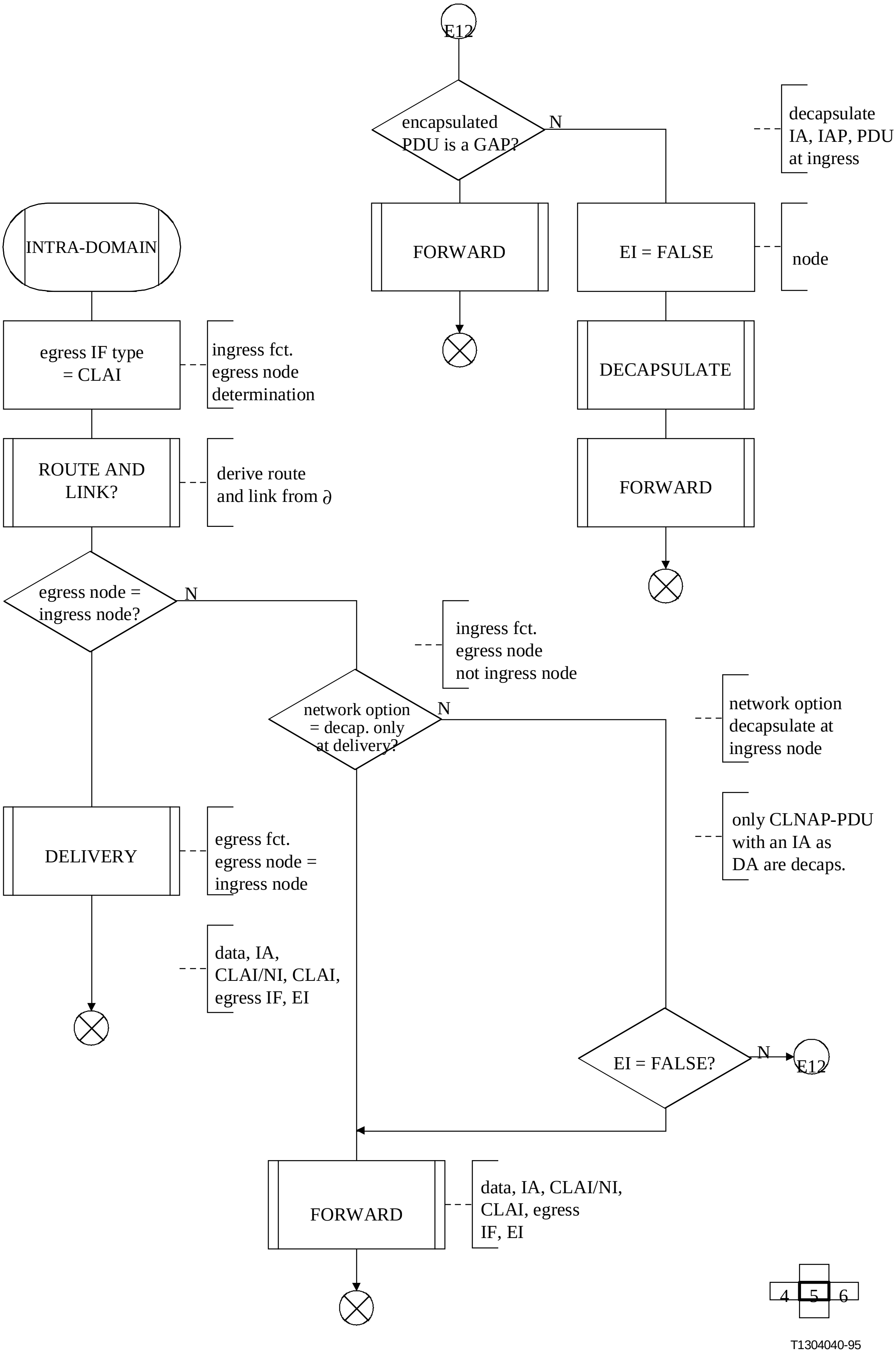


Figure II.4/I.364 ***(sheet 5 of 15)***

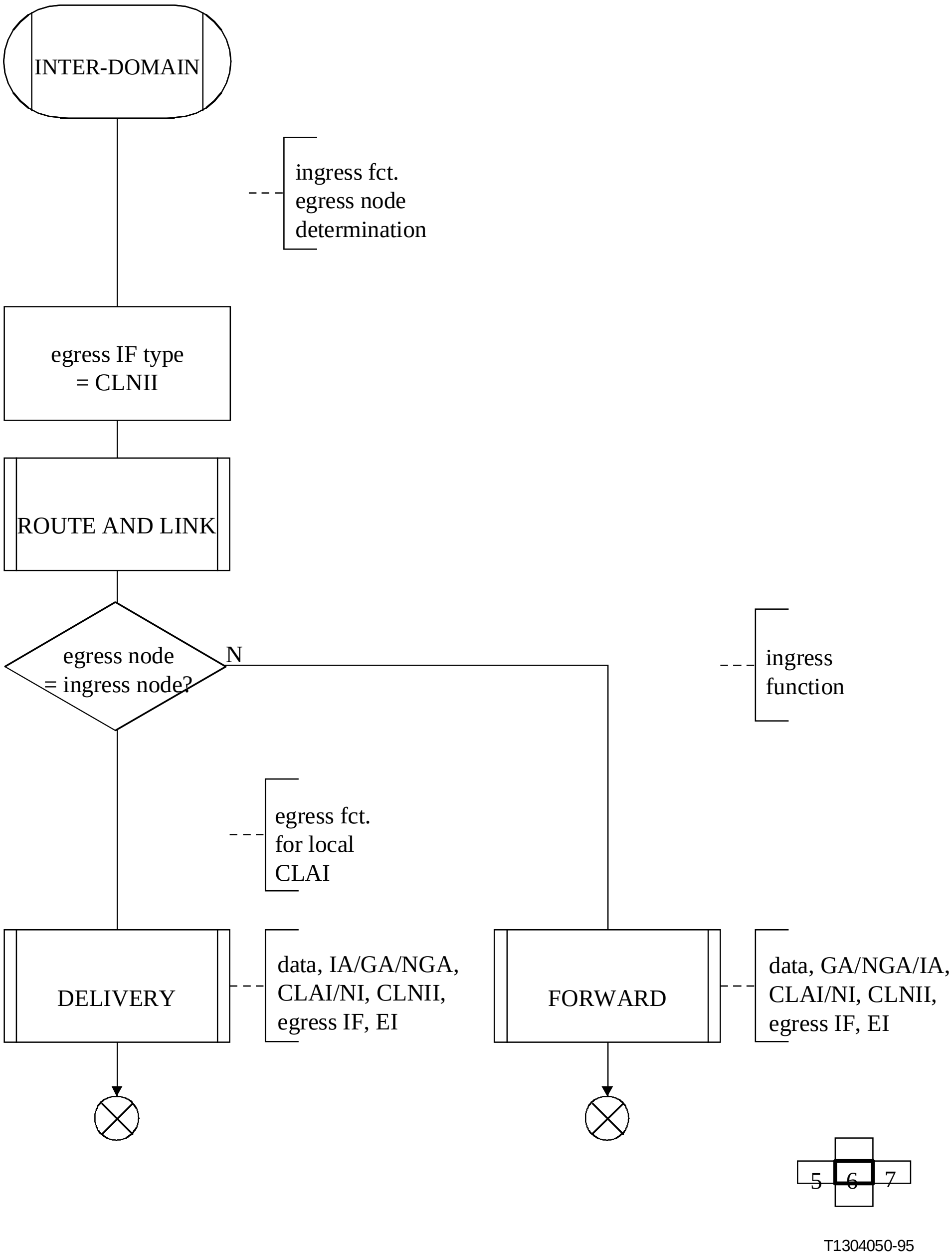


Figure II.4/I.364 ***(sheet 6 of 15)***

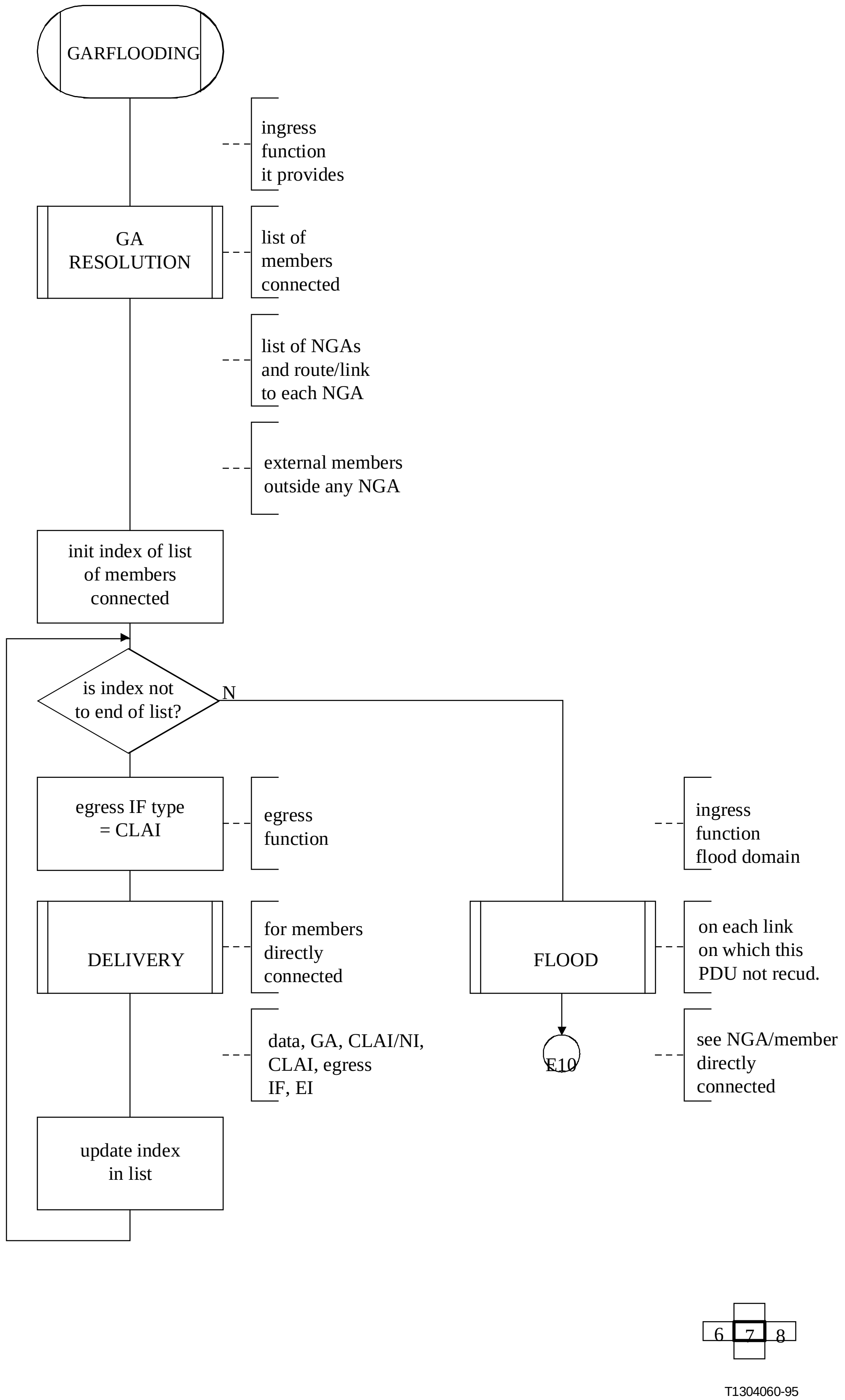


Figure II.4/I.364 ***(sheet 7 of 15)***

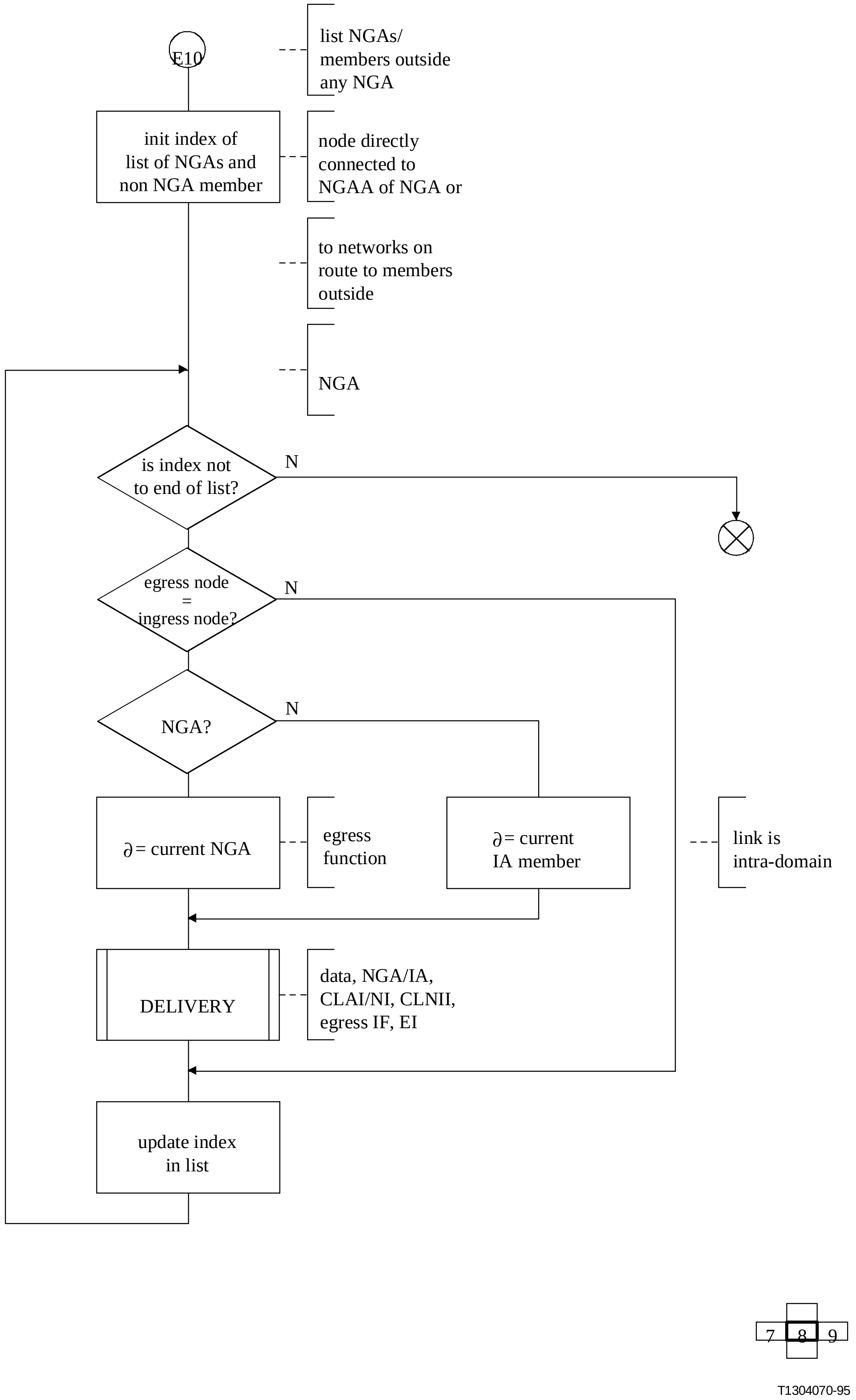


Figure II.4/I.364 ***(sheet 8 of 15)***

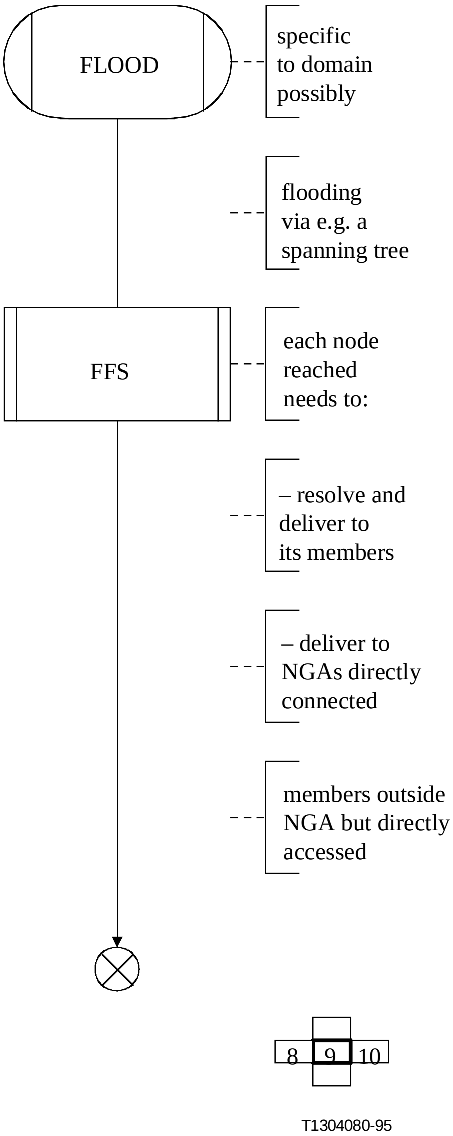


Figure II.4/I.364 ***(sheet 9 of 15)***

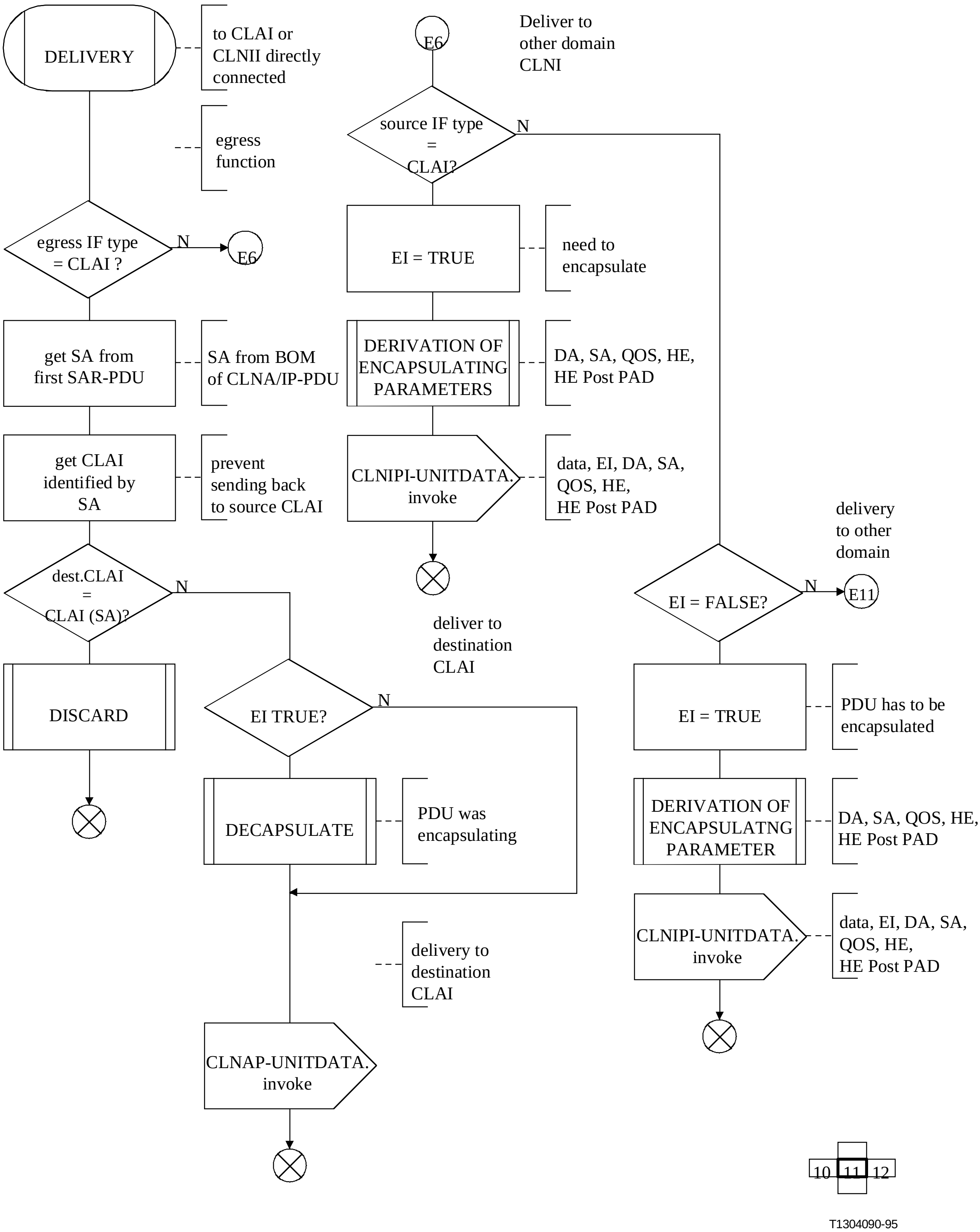


Figure II.4/I.364 ***(sheet 10 of 15)***

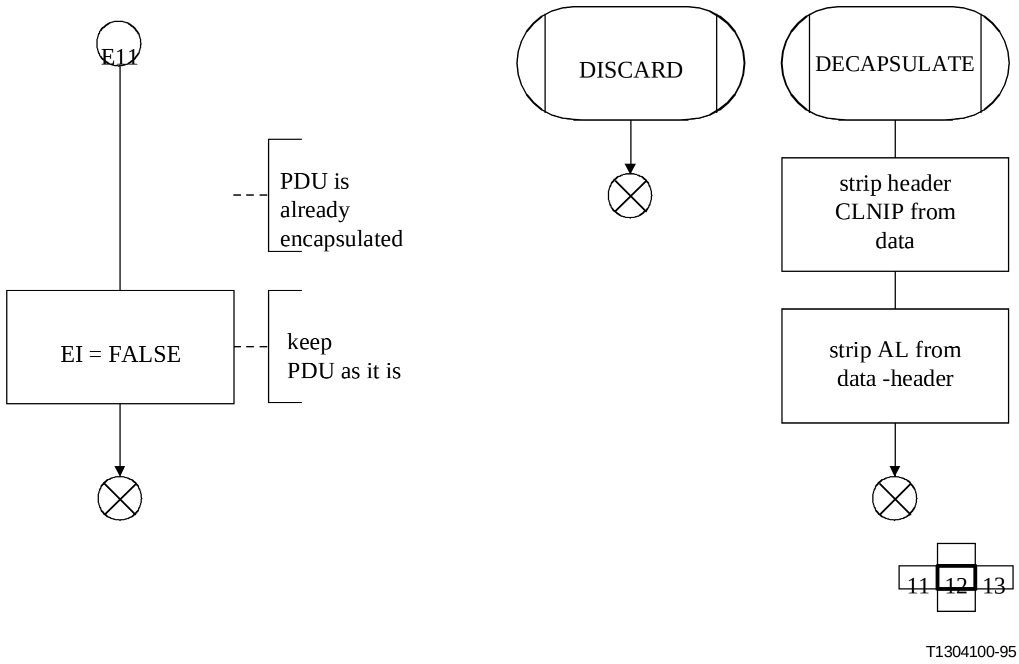


Figure II.4/I.364 ***(sheet 11 of 15)***

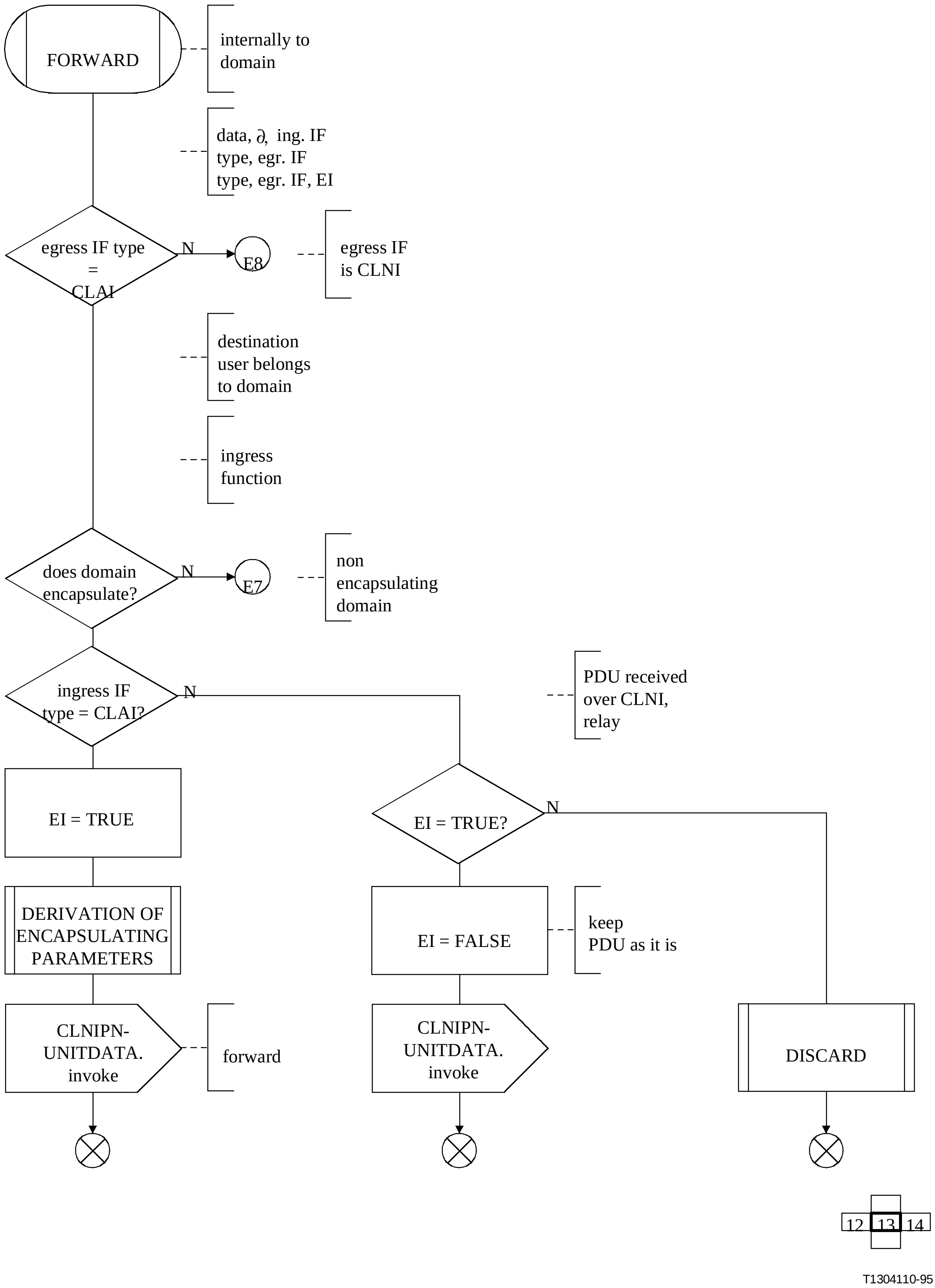


Figure II.4/I.364 ***(sheet 12 of 15)***

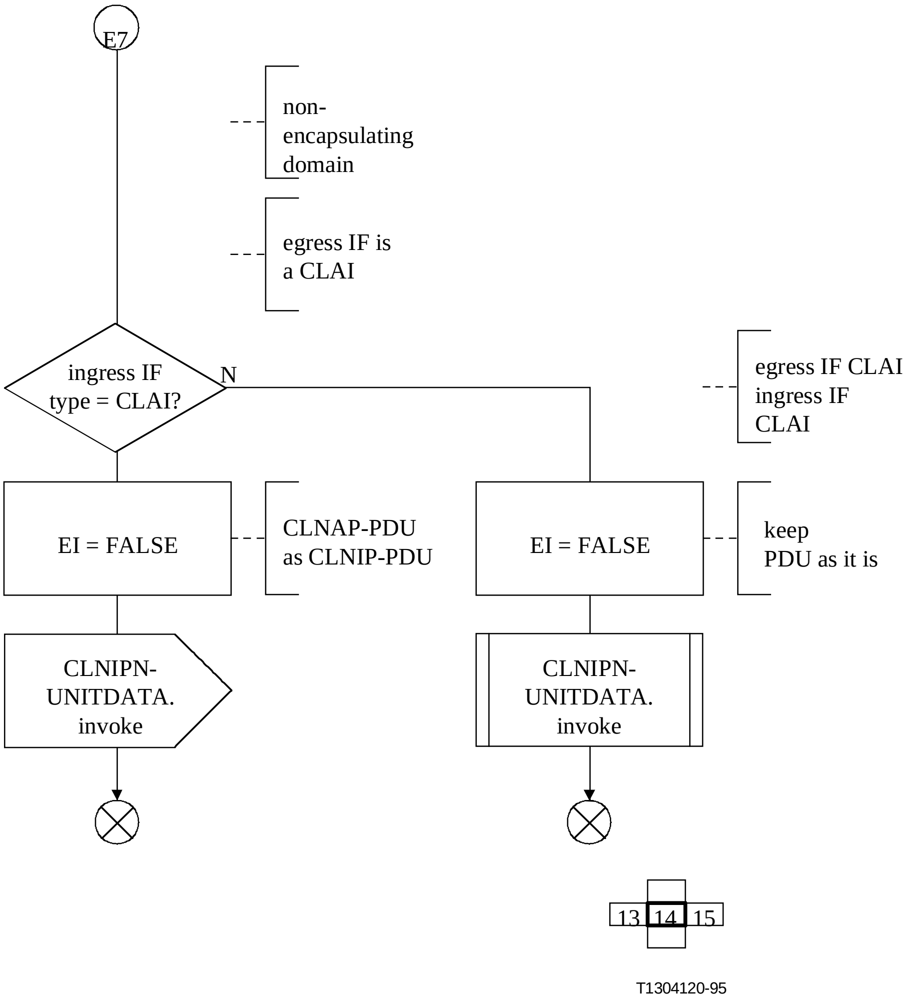


Figure II.4/I.364 ***(sheet 13 of 15)***

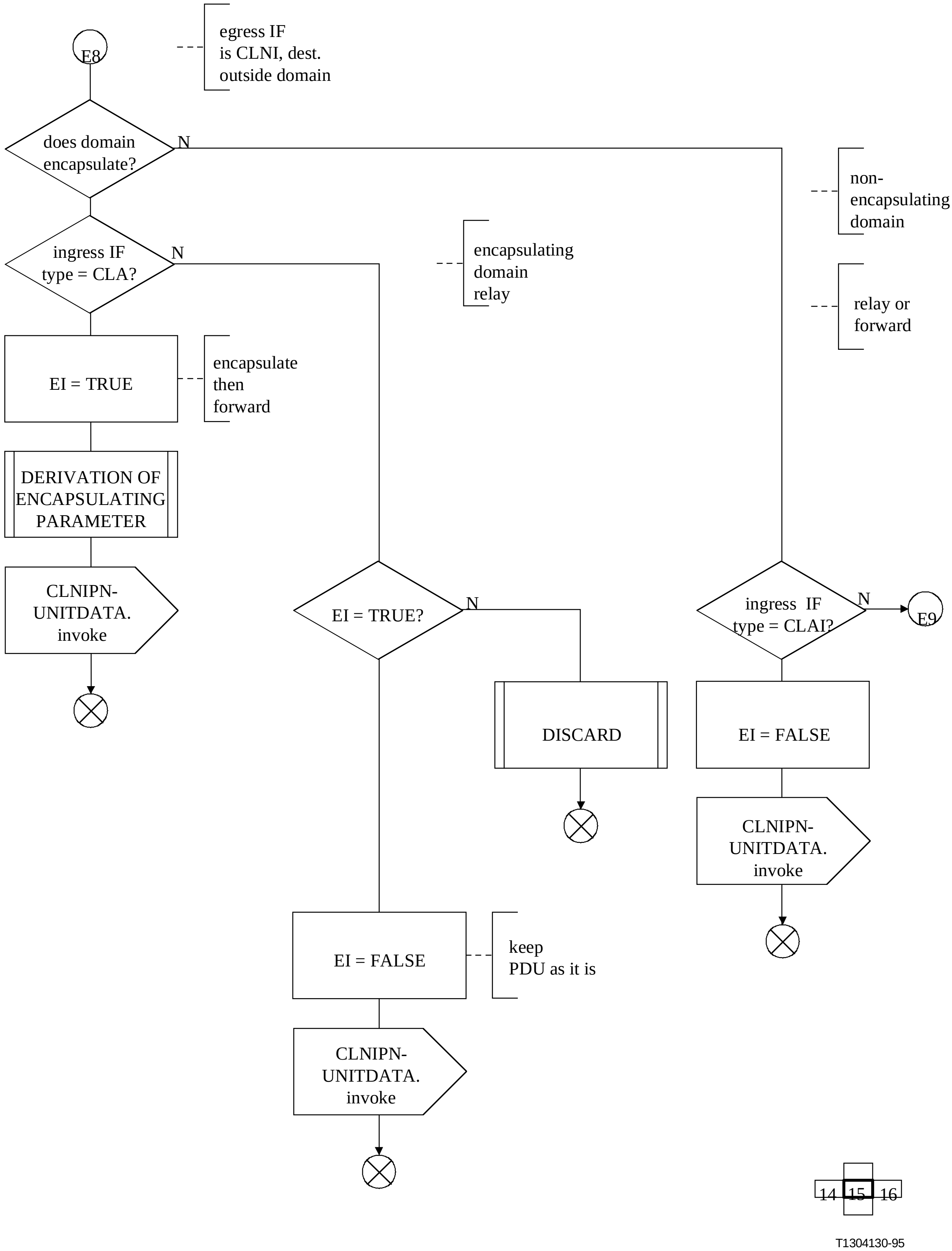


Figure II.4/I.364 ***(sheet 14 of 15)***

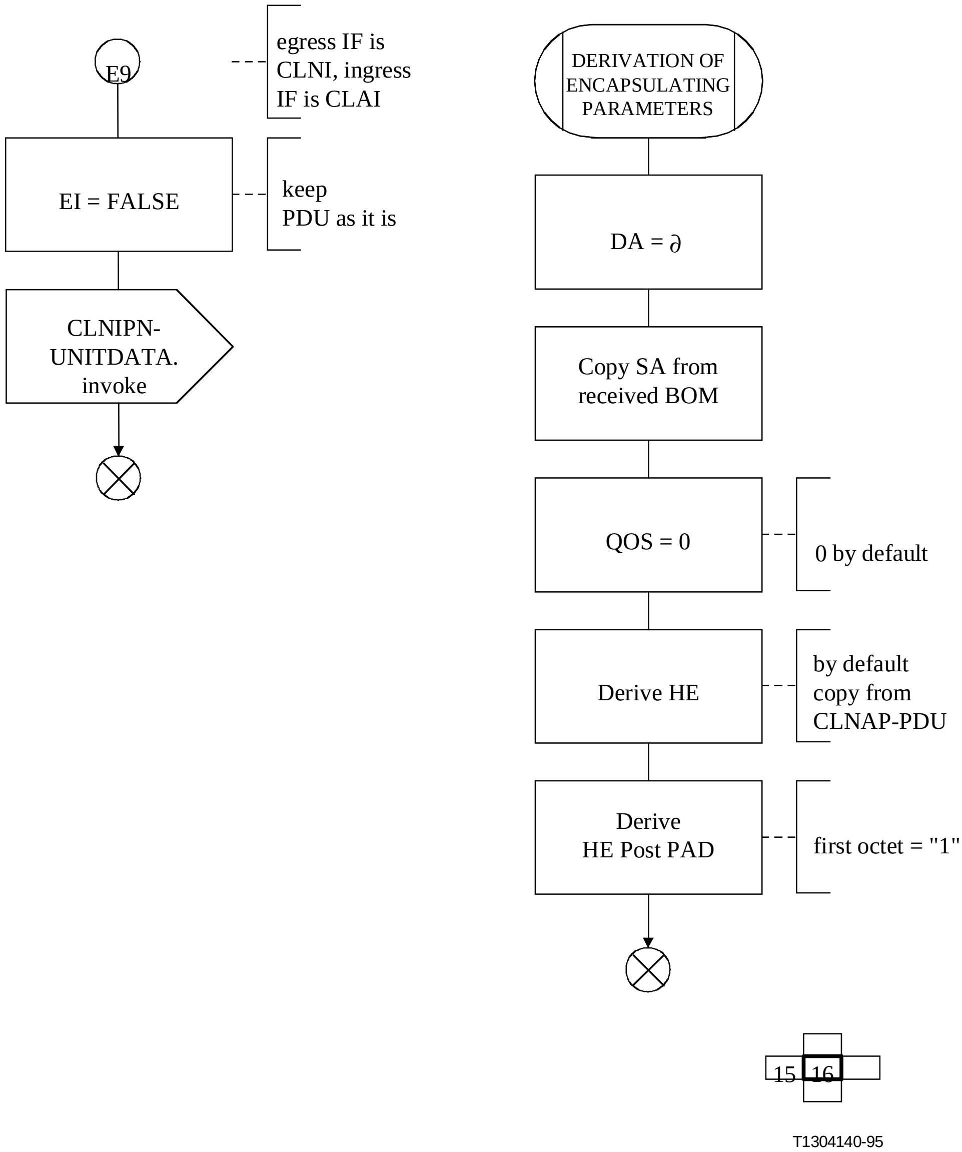


Figure II.4/I.364 ***(sheet 15 of 15)***

APPENDIX III

Example of a network operating with enhanced group address resolution

III.1 Introduction

A number of networks may participate in a group address resolution process. The GAA resolves either the complete or only part of the group address. In case of partial resolution by the GAA, the complete resolution is accomplished with the support of NGAAs.

The networks participating in the group address resolution process for a given group are interconnected in a tree-like structure (see Figure III.1). This structure is also known as a spanning tree. It has to be noted that this tree is fairly static and restructuring will be initiated from the root.

GAPn denotes a group addressed CLNAP-PDU. GAPe denotes an encapsulated CLNAP-PDU, i.e. CLNIP-PDU.

III.2 The algorithm used for enhanced group address resolution

The following algorithm describes the operation of the enhanced group address resolution process.

```
IF DA=α THEN
    // do the multicasting
    FOR each individual address associated with α
        Send a copy of the PDU
    END FOR
    FOR each NGA ν associated with α
        IF the LASTRES field from the PDU=NGID of ν THEN
            do nothing
        ELSE
            set DA to ν
            send a copy of the PDU to ν
        END IF
    END FOR
END IF
```

The NGAA's algorithm when its NGA is β

```
IF DA=β AND the LASTRES field of the PDU is different from the NGID of β THEN
    // do the multicasting:
    FOR each individual address associated with β
        send a copy of the PDU
    END FOR
    FOR each NGA associated with β
        IF the LASTRES field from the PDU is different from the NGID of ν THEN
            Set DA to ν
            Send a copy of the PDU to ν
        END IF
    END FOR
```

```
ELSE IF DA=β AND the LASTRES field of the PDU is equal to the NGID of β THEN
        discard the PDU
ELSE IF DA=α AND LASTRES is either 0, or the NGID of one of the NGAs ν associated with β
THEN
        // do the multicasting:
        FOR each individual address associated with β
            send a copy of the PDU
        END FOR
        FOR each NGA associated with β
            IF the LASTRES field from the PDU is different from the NGID of ν THEN
                set DA to ν
                send a copy of the PDU to ν
            END IF
        END FOR
        forward a copy of the PDU in the direction of the GAA:
            DA=α; //unchanged
            LASTRES field = NGID of β
ELSE
        forward a copy of the PDU in the direction of the GAA; //DA and LASTRES field
unchanged
ENDIF
```

III.3 Example operation

III.3.1 Network configuration

The tree contains several hierarchy levels. Each node in the tree owns a unique number (NGID) and represents either NGAA or at the root the GAA which participates in a given group address resolution process. Depending on the position of the node in the tree, the node has to support a number of distinct functions:

1) *Local group address resolution*

   The node receives a GAPn across one of its attached UNIs. The GA is served by the NGAA. The number of copies of the GAPn is determined by the number of IAs served by the NGAA. The determined numbers of copies of the GAPn are made and sent across the appropriate UNIs.

2) *Group address distribution function within the tree*

   The working node receives either a GAPe from any node connected to the working node or a GAPn across one of its attached UNIs. The GAPn is encapsulated. The necessary numbers of copies of the GAPe are made and sent to all nodes but the node from where the GAP was sent.

3) *Management of nested groups*

The NGAA maintains a list containing all IAs served by a particular GA. It has to be assured that this list is in accordance with the list maintained by the GAA.

4) *Management of the group*

Nodes numbered 1, 3, 4, 5 and 8 perform functions 1), 2) and 3).

Nodes 2, 6, 7, 9, 10 and 11 perform functions 2) and 3). In case the node serves members of the group, function 1) is also performed.

Node 12 performs functions 2) and 4). In case the node serves members of the group, function 1) is also performed.

Table III.1 shows the information which has to be stored in the GAA. The information contained in a row has to be stored in the respective NGAA. Furthermore, each NGAA knows the node number of the GAA for a particular GA.

Table III.1/I.364 – Reachability information for partial resolution – for example, configuration Figure III.1

Node number	Server type	Service supported	Members of the group to be locally served	Nodes of the group to be served
1	NGAA	1, 2, 3	IA1, IA2, IA3, IA4, IA5, IA6, IA7, IA8	2
2	NGAA	1, 2, 3	IA9, IA10	1, 6
3	NGAA	1, 2, 3	IA16, IA17, IA18, IA19, IA20, IA21	6
4	NGAA	1, 2, 3	IA11, IA12, IA13, IA14, IA15	6
5	NGAA	1, 2, 3	IA22	6
6	NGAA	1, 2, 3	IA23, IA24	2, 3, 4, 5, 7
7	NGAA	2, 3		6, 12
8	NGAA	1, 2, 3	IA25, IA26, IA27, IA28	9
9	NGAA	1, 2, 3	IA29, IA30, IA31, IA32, IA33, IA34	8, 12
10	NGAA	2, 3		12
11	NGAA	2, 3		12
12	GAA	1, 2, 4	IA35	7, 9, 10, 11

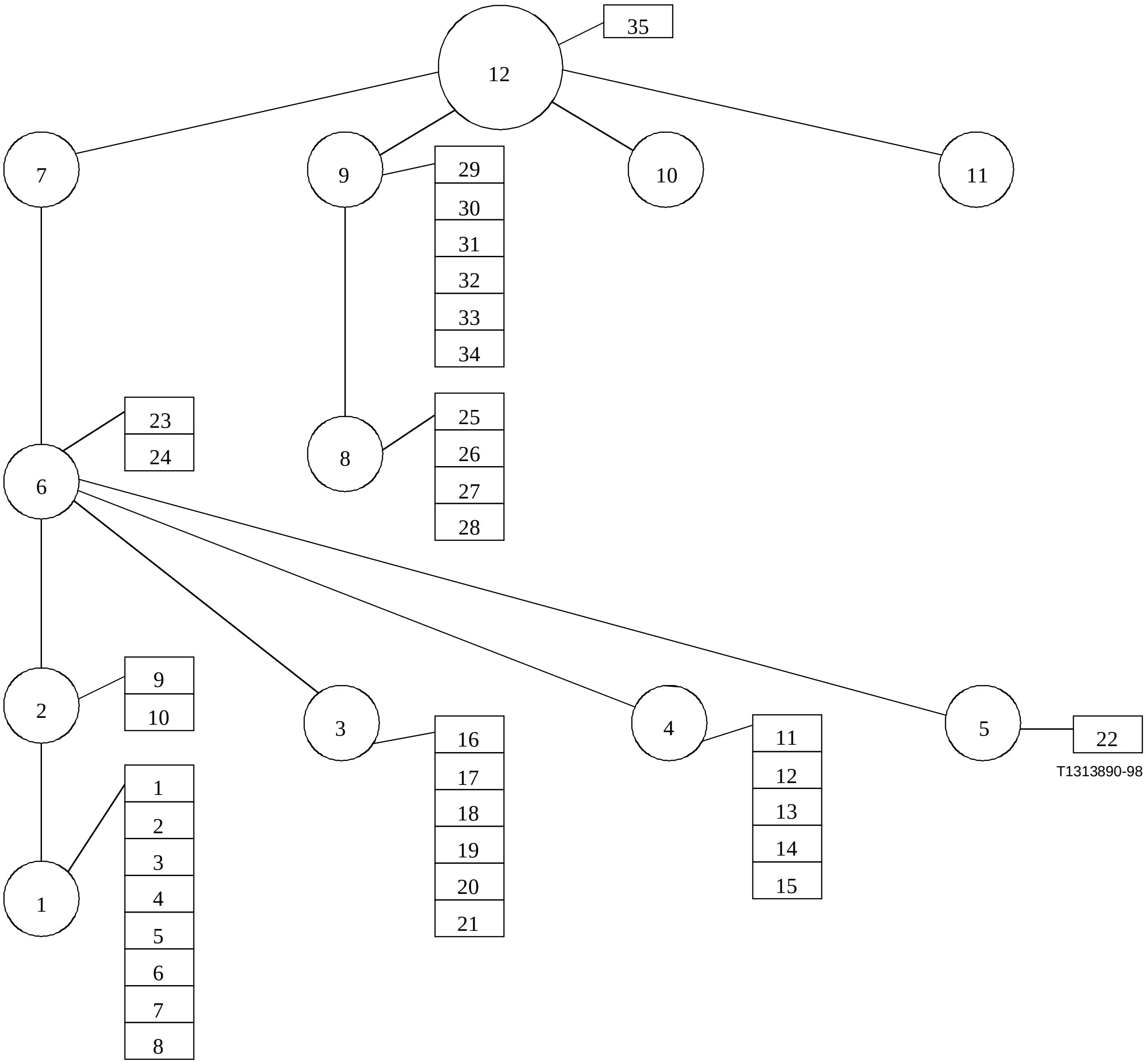


Figure III.1/I.364 – Tree structure interconnecting participating (N)GAAs

III.3.2 Description of the group address distribution process

As an example node 1 receives a GAPn.

Node 1

A GAPn is received and validated. The GAPn is copied eight times and a copy is sent across the UNIs belonging to IA1-8. The GAPn received is encapsulated as follows:

DAe = NGAA2
SAe = SAn
DAn = GA
SAn = SAn
NGID = 1

The resulting GAPe is sent across the link leading towards node 2.

Node 2

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed.

The GAPn is copied twice, and a copy is sent across the UNIs belonging to IA9 and IA10. The GAPn is encapsulated again. The copy carries the following information:

DAe = NGAA6
SAe = SAn
DAn = GA
SAn = SAn
NGID = 2

The resulting GAPe is sent across the link leading towards node 6.

Node 6

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied twice, and a copy is sent across the UNIs belonging to IA23 and IA24. The GAPn is encapsulated again. Four copies are made available and carry the following information:

DAe = NGAA7
SAe = SAn
DAn = GA
SAn = SAn
NGID = 6

The resulting GAPe is sent across the link leading towards node 7.

DAe = NGAA5
SAe = SAn
DAn = GA
SAn = SAn
NGID = 6

The resulting GAPe is sent across the link leading towards node 5.

DAe = NGAA4
SAe = SAn
DAn = GA
SAn = SAn
NGID = 6

The resulting GAPe is sent across the link leading towards node 4.

DAe = NGAA3
SAe = SAn
DAn = GA
SAn = SAn
NGID = 6

The resulting GAPe is sent across the link leading towards node 3.

Node 3

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied six times, and a copy is sent across the UNIs belonging to IA16-IA21. No further processing required.

Node 4

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied five times, and a copy is sent across the UNIs belonging to IA11-IA15. No further processing required.

Node 5

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied once, and the copy is sent across the UNI belonging to IA22. No further processing required.

Node 7

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is encapsulated again. The copy carries the following information:

DAe = NGAA12
SAe = SAn
DAn = GA
SAn = SAn
NGID = 7

The resulting GAPe is sent across the link leading towards node 12.

Node 12

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied once, and the copy is sent across the UNI belonging to IA35. The GAPn is encapsulated again. Three copies are made available and carry the following information:

DAe = NGAA9
SAe = SAn
DAn = GA
SAn = SAn
NGID = 12

The resulting GAPe is sent across the link leading towards node 9.

DAe = NGAA10
SAe = SAn
DAn = GA
SAn = SAn
NGID = 12

The resulting GAPe is sent across the link leading towards node 10.

DAe = NGAA11
SAe = SAn
DAn = GA
SAn = SAn
NGID = 12

The resulting GAPe is sent across the link leading towards node 11.

Node 9

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied six times, and a copy is sent across the UNIs belonging to IA29-IA34. The GAPn is encapsulated again. The copy carries the following information:

DAe = NGAA8
SAe = SAn
DAn = GA
SAn = SAn
NGID = 9

The resulting GAPe is sent across the link leading towards node 8.

Node 8

The first cell of the GAPe is received. End-user blocking may be performed. No blocking required. The NGID is saved and the first cell is discarded and the rest of GAPe (=GAPn) can be processed. The GAPn is copied four times, and the copy is sent across the UNIs belonging to IA25-IA28. No further processing required.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	**Integrated services digital network**
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure
Series Z	Programming languages