INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.32

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/93)

PUBLIC DATA NETWORKS: INTERFACES

INTERFACE BETWEEN DATA TERMINAL EQUIPMENT (DTE) AND DATA CIRCUIT-TERMINATING EQUIPMENT (DCE) FOR TERMINALS OPERATING IN THE PACKET MODE AND ACCESSING A PACKET SWITCHED PUBLIC DATA NETWORK THROUGH A PUBLIC SWITCHED TELEPHONE NETWORK OR AN INTEGRATED SERVICES DIGITAL NETWORK OR A CIRCUIT SWITCHED PUBLIC DATA NETWORK

ITU-T Recommendation X.32

(Previously "CCITT Recommendation")

FOREWORD

The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the International Telecommunication Union. 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, established the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

ITU-T Recommendation X.32 was revised by the ITU-T Study Group VII (1988-1993) and was approved by the WTSC (Helsinki, March 1-12, 1993).

NOTES

1 As a consequence of a reform process within the International Telecommunication Union (ITU), the CCITT ceased to exist as of 28 February 1993. In its place, the ITU Telecommunication Standardization Sector (ITU-T) was created as of 1 March 1993. Similarly, in this reform process, the CCIR and the IFRB have been replaced by the Radiocommunication Sector.

In order not to delay publication of this Recommendation, no change has been made in the text to references containing the acronyms "CCITT, CCIR or IFRB" or their associated entities such as Plenary Assembly, Secretariat, etc. Future editions of this Recommendation will contain the proper terminology related to the new ITU structure.

2 In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

© ITU 1993

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

			Page
Preface			1
1	Scope		2
2	Functional aspects		3
	2.1	Dial-in and dial-out considerations	3
	2.2	Identification	4
	2.3	Service aspects	5
	2.4	DTE identification methods	7
	2.5	DCE identification methods	9
	2.6	Dial-in-by-the-DTE and dial-out-by-the-PSPDN operation	10
	2.7	DTE service requirement	10
	2.8	Duplex and half-duplex operation	10
	2.9	Identification protocol	10
	2.10	Negotiation of values	10
3	DTE service descriptions		10
	3.1	DTE service attributes	10
	3.2	Summary of DTE services	15
	3.3	Non-identified DTE service	16
	3.4	Identified DTE service	16
	3.5	Customized DTE service	19
4	Interface characteristics (physical layer)		19
	4.1	X.21 interface	22
	4.2	X.21 *bis* interface	22
	4.3	V-series interface	23
5	Link access procedure across the DTE/DCE interface		24
	5.1	Introduction	24
	5.2	Data link layer address assignment	25
	5.3	Use of exchange identification (XID) frames	26
	5.4	Link set-up disconnection	29
	5.5	Multilink	29
	5.6	Half-duplex operation	29
6	Packet layer		35
	6.1	Scope and field of application	35
	6.2	Identification and authentication of the DTE using the NUI selection facility in call set-up packets	36
7	X.32 procedures, formats and facilities		36
	7.1	Identification protocol	36
	7.2	Procedures for X.32 optional user facilities	38
	7.3	Coding of the identification protocol elements	39
	7.4	Security grade 2 method	41
	7.5	DCE timers T14 and T14 *bis*	41
	7.6	DCE timer T15	42
Annex A – Actions taken by the DCE in the roles of questioning and challenged parties for security grade 1 and security grade 2 identifications			42
	A.1	Introduction	42
	A.2	Security grade 1 identification	43
	A.3	Security grade 2 identification	47

Page

Annex B – Abbreviations 52

Appendix I – Implementation of LAPX 54

I.1 Introduction 54

I.2 Control and status functions 54

I.3 Table of transitions between states 55

I.4 HDTM/physical layer control and status functions expressed in terms applicable to a modem interface 57

Appendix II – RSA public key algorithm 57

Appendix III – Relationship of timers T14 and T14 *bis* to the different methods of DTE identification 58

INTERFACE BETWEEN DATA TERMINAL EQUIPMENT (DTE) AND DATA CIRCUIT-TERMINATING EQUIPMENT (DCE) FOR TERMINALS OPERATING IN THE PACKET MODE AND ACCESSING A PACKET SWITCHED PUBLIC DATA NETWORK THROUGH A PUBLIC SWITCHED TELEPHONE NETWORK OR AN INTEGRATED SERVICES DIGITAL NETWORK OR A CIRCUIT SWITCHED PUBLIC DATA NETWORK

(Malaga-Torremolinos, 1984, amended at Melbourne, 1988 and Helsinki, 1993)

Preface

The establishment in various countries of packet switched public data networks (PSPDN) providing data services creates the need to produce Recommendations to facilitate access to the PSPDN through a public switched telephone network (PSTN) or an integrated services digital network (ISDN) or a circuit switched public data network (CSPDN).

The CCITT,

considering

(a) that Recommendation X.1 specifies the user classes of service for DTEs operating in the packet mode, that Recommendation X.2 defines user facilities provided by public data networks, that Recommendation X.10 defines categories of access, that Recommendations X.21 and X.21 *bis* define DTE/DCE physical level interface characteristics, that Recommendation X.25 defines the interface between the DTE and the DCE for terminals operating in the packet mode and connected to public data networks by dedicated lines, that Recommendation X.31 defines the support of packet mode terminal equipment by an ISDN, that Recommendation X.121 defines the international numbering plan for public data networks (PDNs), that Recommendation X.300 defines the principles and arrangements for interworking between PDNs and other public networks;

(b) that the V-Series Recommendations define modem and interface characteristics for use of data services on the PSTN;

(c) that Recommendation T.70 defines the procedures and interfaces to be used by telematic terminals, that Recommendation T.71 defines the extension of Link Access Procedure Balanced (LAPB) procedure to be used in half-duplex transmission facilities (LAPX);

(d) that a need has been identified to access a PSPDN through a PSTN, or an ISDN, or CSPDN, because a dedicated circuit to the PSPDN is not justified, or because global service availability is required with back-up network access via public switched networks; however permanent virtual circuits are not available in the types of access covered in this Recommendation;

(e) that some Administrations have considered the provision of Telematic services in different types of networks, e.g. PSPDN, PSTN, ISDN and CSPDN;

(f) that, when this Recommendation is used to provide the Network Service defined in Recommendation X.213, the physical, link and packet layers correspond to the Physical, Data link and Network layers respectively, as defined in Recommendation X.200,

(unanimously) recommends

that the functional and procedural aspects of packet mode DTEs accessing a PSPDN through a PSTN or an ISDN circuit switched bearer service, or CSPDN, are as specified in this Recommendation.

NOTE – Packet mode terminal (TE 1 or TE 2) conforming to the I-Series Recommendations may access a PSPDN through an ISDN circuit switched bearer service. In this case the functional and procedural aspects related to layer 2 and layer 3 in the B channel are as specified in this Recommendation.

1 Scope

This Recommendation defines the functional and procedural aspects of the DTE/DCE interface for packet mode user classes of service DTEs as defined in Recommendations X.1; for DTEs that access a PSPDN via public switched networks. In this Recommendation, a public switched network (PSN) is either a public switched telephone network (PSTN) or an integrated services digital network (ISDN) providing circuit switched bearer service or a circuit switched public data network (CSPDN).

NOTE – The ISDN interface specification for transparent circuit connection is described in Recommendation X.31. In this Recommendation only the DTE functionalities for the access to a PSPDN service through an ISDN are considered.

In the PSTN case, the X.32 DTE/DCE interface coincides with the interface between the DTE and the modem. In the ISDN case, the X.32 interface coincides with the R reference point (see Figure 1). In the CSPDN case, the X.32 DTE/DCE interface coincides with the X.21 or X.21 *bis* interface. This definition applies whether or not the Administration provides the DCE and regardless of how the interface is physically realized (e.g., whether or not the DTE and DCE are contained within the same enclosure). In either case the PSN is involved only:

a) in the establishment of the switched access path;

b) to provide a transmission medium; and

c) optionally, to provide a PSN number for purposes of identification and addressing.

Administrations may offer one or more of the following physical layer interfaces:

1) for access by way of a CSPDN, either Recommendation X.21 or Recommendation X.21 *bis* will be used, as described in 4.1 or 4.2, respectively;

2) for access by way of a PSTN, appropriate V-Series Recommendations will be used as described in 4.3;

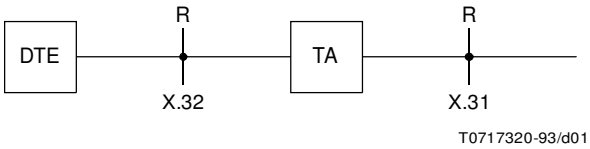
3) for access by way of an ISDN, refer to Recommendation X.31.

The exact use of the relevant points in these Recommendations is given in 4.

The transmission facility is duplex or, optionally, half-duplex. Specific procedures are defined in 5.6 for operation over a half-duplex transmission facility.

At the link layer, the LAPB link access procedure of Recommendation X.25 is used over a single switched physical circuit. The LAPB formats and procedures shall be in accordance with 2.2/X.25, 2.3/X.25 and 2.4/X.25, with additions as noted in 5 of this Recommendation.

The formats and the procedures at the packet layer shall be in accordance with 3/X.25, 4/X.25, 5/X.25, 6/X.25 and 7/X.25 with the additions noted in 6 of this Recommendation.



NOTE – The DTE and TA functionalities may be implemented in the same piece of equipment in the case of a TE1 terminal. In this case this Recommendation covers layers 2 and 3 operation in the B-channel while the S reference point procedures are described in Recommendation X.31.

FIGURE 1/X.32

ISDN reference point

2 Functional aspects

2.1 Dial-in and dial-out considerations

Dial-in operation allows a packet-mode DTE to access a PSPDN by means of selection procedures on a PSTN or CSPDN or ISDN (see Figure 2). This operation is termed "dial-in-by-the-DTE" within this Recommendation.

NOTE – In the ISDN case, the ISDN is accessed via TA functions that may be implemented in separate equipment (DTE and TA case) or in the same piece of equipment (TE1 case) as the DTE functions.

FIGURE 2/X.32

Dial-in-by-the-DTE operation

For performing this operation, the DTE may use an automatic or manual calling procedure.

Dial-out operation allows a PSPDN to access a packet-mode DTE by means of selection procedures on a PSTN or CSPDN or ISDN (see Figure 3). This operation is termed "dial-out-by-the-PSPDN" within this Recommendation.

NOTE – In the ISDN case, the ISDN is accessed via TA functions that may be implemented in separate equipment (DTE and TA case) or in the same piece of equipment (TE1 case) as the DTE functions.

FIGURE 3/X.32

Dial-out-by-the-PSPDN operation

For dial-out-by-the-PSPDN operation, the DTE should use the automatic answering procedure but may use manual answering.

Virtual call origination is independent of dial-in-by-the-DTE and dial-out-by-the-PSPDN operations. That is, a DTE that has been involved in a dial-in-by-the-DTE or dial-out-by-the-PSPDN operation may then initiate or receive virtual calls, subject to the limitations in specific situations as described in 3.

2.2 Identification

2.2.1 DTE identity

When a DTE accesses a PSPDN through a PSN (dial-in-by-the-DTE) or when a DTE is accessed by a PSPDN through a PSN (dial-out-by-the-PSPDN), there may be a requirement for identification of the DTE to the DCE.

The DTE "identity" is a means of referring to the DTE. The DTE identity is either explicitly agreed to between the DTE and the Administration or is implicitly acceptable to the Administration through agreements with other Administrations, organizations or authorities. It may be composed of different elements such as a number from a numbering plan, identification of the DTE service and authority, validity dates and period, public keys used for authentication, etc.

The characteristics of the service which a DTE obtains via dial-in-by-the-DTE or dial-out-by-the-PSPDN access depend upon whether the PSPDN considers the DTE identified for each particular switched access connection or virtual call. If the DTE is identified, then the PSPDN has a way to accrue charges to be paid on behalf of the DTE. That is, either the DTE or some other party is billable.

Two components are required in order for a DTE to be considered identified:

a) the DTE is administratively registered either:

   1) through direct arrangement with the PSPDN (i.e. explicitly); or

   2) through pre-arrangement between the PSPDN and a PSN or another authority, and direct arrangement between the DTE and that authority (i.e. not explicitly),

b) the DTE identity is made known to the DCE during the switched access connection using one of the methods described in 2.4.

A DTE may incur charges even if not identified because some Administrations collect charges via the PSTN, ISDN or CSPDN.

In any case, DTE identification is used for billing and accounting purposes. In addition to this basic function, DTE identification may optionally be used for one or both of the following purposes:

a) enabling the PSPDN to provide a calling DTE address to a called DTE, or

b) enabling the DTE to obtain a different service than that offered to DTEs which do not establish an identity (see 2.3).

2.2.2 DCE identity

When a network supports dial-out-by-the-PSPDN access to DTEs, there may be a requirement for identification of the network (i.e. DCE) to the DTE. In the case of dial-in-by-the-DTE access, although the identity of the DCE may already be known by the DTE (as the DTE originated the switched access connection), there may also be a DTE requirement for identification of the network. The identification of the DCE to the DTE may be used for different purposes, such as:

a) to enable the DTE to select the specific security related information (e.g. encrypted key, password, etc.) appropriate to that network for use in exchanges with the DCE;

b) to enable the DTE to select different parameters, procedures or profiles appropriate to that network;

c) to enable a DTE to ascertain by which PSPDN the switched access has been established, thus enabling proper operation of the optional *closed user group* facility and of the conveyance of the appropriate calling DTE address provided by the PSPDN, if applicable.

For each dial-in-by-the-DTE or dial-out-by-the-PSPDN access, the DCE may establish its identity by successfully completing one of the methods for DCE identification described in 2.5. The DCE identity is composed of the network's Data Network Identification Code (DNIC), and optionally, a DTE profile designator (see 3.1.11), except when the identity is provided by the PSN (see 2.5.1.1); in the latter case the identity is a number of the PSN numbering plan.

2.3 Service aspects

The switched access service given to a particular DTE is dependent upon:

a) the PSPDN;

b) the use/non-use of DTE identification; and

c) the DTE service available to and chosen by the DTE.

Three DTE service types are defined in this Recommendation (see 2.3.2). One of the DTE service types (*non-identified*) is independent of the specific DTE identity. One service type (*identified*) may or may not be independent of the specific DTE identity. The third type (*customized*) is related to the specific DTE identity in order to provide customization of some service aspects.

The types of DTE service are further distinguished by whether there is a number assigned by the network to be used to represent the DTE identity in the address fields of *call set-up* packets. This number is called a "DTE address" and is defined in 3.1.3.

2.3.1 Service attributes

"Attributes" are defined to describe each aspect of switched access service. However, the values of the attributes do not necessarily include all capabilities offered to PSPDN users that access the PSPDN via a leased line. The attributes are:

a) DTE identity;

b) DTE identification method;

c) DTE address;

d) registered address;

e) registered PSN number;

f) X.25 subscription set;

g) logical channels assignment;

h) dial-out-by-the-PSPDN availability;

i) dial-out access type;

j) X.32 optional user facilities;

k) DCE identity presentation, and

l) data link layer address assignment.

For each DTE service, each attribute is either provided or not provided; if it is provided it is either:

1) set to a default value specified by the network (Network Default); or

2) set to a value selected by the user from a set of values provided by the network (User Selectable).

NOTE – A network may define a default value for the attribute.

A *DTE profile* is the set of values of the Network Default and User Selectable attributes that have been selected for a particular DTE identity.

NOTE – In some networks, the DTE profile is stored in the PSTN.

Some networks may allow a subscriber to arrange for more than one *DTE profile* to meet different requirements for switched access service. Each *DTE profile* is independent. A "DTE profile designator" is used to differentiate the multiple profiles of the DTE.

2.3.2 DTE services

Some networks may offer service to unidentified DTEs, that is, to DTEs for which no identification is provided to the DCE.

Some networks may offer service to identified DTEs, that is, to DTEs for which an implicit or explicit *DTE identity* is provided to the DCE via one of the methods specified in 2.4. Different types of service are defined for use in different situations. The network may offer one or more of these services.

The three types of service defined in this Recommendation are called DTE services. One is a service for unidentified DTEs. The other two are services for identified DTEs. The three DTE services are:

a) non-identified;

b) identified; and

c) customized.

2.3.2.1 Service for unidentified DTEs

The service offered to unidentified DTEs is called *non-identified* DTE service and is detailed in 3.3. This DTE service may be offered as part of dial-in-by-the-DTE or dial-out-by-the-PSPDN operation or both.

For a dial-out-by-the-PSPDN operation using a single logical channel, the lifetime of a switched access path corresponds to the lifetime of the virtual call. That is, at the completion of the clearing procedures for the virtual call, the DCE initiates those procedures necessary to disconnect the switched access path.

For a dial-out-by-the-PSPDN operation using multiple logical channels, at the completion of the clearing procedures for the last virtual call, the DCE initiates those procedures necessary to disconnect the switched access path, taking into account the value of the T14 timer (see 7.5)

NOTE – In the case where the network provides the optional capability for multiple logical channels for dial-out-by-the-PSPDN to unidentified DTEs, the service is equivalent to the Registered Address service described in 3.1.4.2. In this case, however, the DTE and the network are not required to establish an agreement for the use of a registered address.

For a dial-in-by-the-DTE operation (and dial-out-by-the-PSPDN) using multiple logical channels), the switched access path shall not be disconnected for a period of time (T14), even in the absence of any virtual calls. This allows users a period of time to reestablish a virtual call (see 7.5).

For dial-in-by-the-DTE operation, the PSPDN may limit the number of unsuccessful attempts to reestablish a virtual call.

When a DTE uses the *non-identified* DTE service:

a) it is not required to use any optional procedures;

b) it is able to operate with different networks without having to subscribe to any of them (i.e. not administratively registered and/or assigned an identity with any PSPDN); and

c) it should not be permitted to make paid calls or receive reverse-charged calls (i.e. the *local charging prevention* facility is set by the network), thus allowing the Administration to guarantee collection of charges. However, some Administrations may permit non-identified DTEs to make free calls or may use other methods to collect charges, e.g. via the PSTN, ISDN or PSPDN).

2.3.2.2 Services for identified DTEs

The services offered to identified DTEs provide a set of capabilities/facilities different from and/or enhanced beyond the *non-identified* DTE service. In particular, on those networks which allow only identified DTEs to accrue charges, it is possible for DTEs to:

a) make calls for which the calling DTE assumes responsibility for the charges; and/or

b) receive reverse-charged calls.

2.3.2.2.1 Identified DTE service

The PSPDN may offer the *identified* DTE service in which:

a) the *DTE identity* has not been explicitly agreed to with the Administration, or

the *DTE identity* has been explicitly agreed to. In this case, allocation of *registered addresses*, to some DTEs, by the Administration is a network option;

b) the other attributes have the values set by the network as specified in 3.4.

The effect of the *identified* DTE service is that this DTE is billable but the service is otherwise similar to the *non-identified* DTE service. Note that the use of the *network user identification* (NUI) *subscription* facility provides a *DTE identity* used for billing purposes and may, in conjunction with the *NUI override* facility (6.3), override, for the specific

virtual call, the default set of X.25 subscription facilities. However, when using the *NUI override* facility feature, overridding the facilities is performed only when a Call Request is made by the switched access DTE and not for an Incoming Call to the switched access DTE.

The *identified* DTE service may be offered as part of dial-in-by-the-DTE or dial-out-by-the-PSPDN operation or both.

2.3.2.2.2 Customized DTE service

The PSPDN may offer the *customized* DTE service in which the *DTE identity* has been explicitly agreed to with the Administration, a *registered address* has been allocated and the other attributes are set according to the DTE profile which has been customized for the DTE according to the capabilities supported by the network as permitted within the specification given in 3.5. The effect is that this DTE is billable, has an X.121 address registered with the PSPDN, and is provided a service tailored in many aspects to its requirements. This DTE service may be offered as part of dial-in-by-the-DTE or dial-out-by-the-PSPDN operation or both.

2.4 DTE identification methods

This Recommendation provides three distinct methods for DTE identification. These methods are:

a) identification provided by the public switched network;

b) identification by means of a link layer Exchange Identification (XID) procedure;

c) identification by means of the *NUI selection* facility in *call set-up* packets.

NOTE – For an interim period, support of the use of a DTE identification method by means of the calling address field in *call request* packets is a national matter. It should be remembered that the use of the calling address field for conveying identification conflicts with the use of this field for addressing, and problems can arise if both uses are needed.)

A network may support any, all or none of these methods in conjunction with the DTE services offered (see 2.7).

The mechanisms in b) and c) may be used by some networks to offer functions other than, or in addition to, DTE identification.

The identity of the DTE becomes known to the network via one of the identification procedures at either or both of the following times:

1) prior to any virtual call establishment (see 2.4.1); or

2) on a per virtual call basis (see 2.4.2).

It is considered vital that a reasonable degree of protection be achieved in the DTE identification procedure so that Administrations and subscribers can prevent fraudulent DTE identification. Therefore, the identification procedure includes the capabilities to verify and/or authenticate the correctness of the DTE identification. The XID method obeys an "identification protocol" that has been defined in 2.9 and 7.1 for conveying the information necessary for the DCE to receive the DTE identity, verify it to the proper degree of authenticity, and to report on the success of the procedure. Two grades of security are defined in the identification protocol. Identification provided by the public switched network and the X.25 *NUI selection* facility do not use an explicit identification protocol. However, the success of authentication is implicit in the reception by the DTE of a *call connected* packet.

DCE identification may be achieved by using the identification protocol while it is simultaneously being used for DTE identification, but as an independent invocation of the protocol.

Networks may choose to offer "secure dial-back" as an additional means for authentication of the DTE identity. Secure dial-back, as specified in 7.2.1, uses physical location as a basis for DTE authentication by combining dial-in-by-the-DTE, dial-out-by-the-PSPDN, and DTE identification prior to virtual call establishment.

2.4.1 Identification prior to virtual call establishment

There are two methods by which the identity of the DTE can be determined by the DCE prior to the establishment of any virtual call. These methods are described in the following two subclauses. Both methods apply to both dial-in-by-the-DTE and dial-out-by-the-PSPDN operation.

The service that a DTE which is identified prior to virtual call establishment obtains is either the *identified* or the *customized* DTE service.

If the service obtained is the *customized* DTE service and includes customized values for link layer options and system parameters, the DTE identification must be performed at the link level (see 2.4.1.2) or be provided by the public switched network (see 2.4.1.1).

The DTE identification that is determined by any of the prior-to-virtual-call-establishment methods remains in effect even in the absence of any virtual calls.

2.4.1.1 Identity provided by the public switched network

In the case of dial-in-by-the-DTE operation, the *DTE identity* may be provided by the public switched network (i.e. PSTN, ISDN or CSPDN) to the PSPDN during the PSN connection establishment stage.

NOTE – The administrative arrangements described in 2.2.1 are necessary for the calling line identification to be used by the PSPDN as a *DTE identity*.

The DTE is a subscriber of the PSTN, ISDN or CSPDN network, and, therefore, the PSTN number, the ISDN number or the CSPDN number (as well as some additional management information in some circumstances) may be available and will be signalled to the PSPDN.

In the case of dial-out-by-the-PSPDN, the PSPDN uses, as the DTE identification, the information which has been provided to the PSN in order to do the dial-out-by-the-PSPDN operation.

NOTE – This method of identification may be used in the case of dial-out-by-the-PSPDN operation even when the PSN does not provide calling line identification.

As the PSN is providing the identification information, the DTE is not required to use any optional user procedures in order to accomplish DTE identification.

The DTE identification determined by means of this method remains in effect until the switched access path is disconnected.

NOTE – Although the operational requirements for a DTE which is not identified or which is identified via the "provided-by-public-switched-network" method are the same, the capabilities/facilities available to DTEs using these methods can be very different. This may result in differences in general DTE operation, especially in regard to reverse charging. In particular, the differences are those between the *non-identified* DTE service and the *identified* or *customized* DTE services.

2.4.1.2 Identity provided by means of the link layer XID procedure

Identification of the DTE may be provided by a link layer procedure, as described in 5 and 7, based on exchanges of XID frames between the DTE and the DCE before the logical link is established (*disconnected* phase of Recommendation X.25).

This procedure may be optionally offered by networks depending, in part, on the offering by the network of the optional frames that this procedure uses. When it is offered by the network, use of this identification procedure by DTEs is optional.

The XID frame used in this method may also be used for other link layer functions.

The DTE identification determined by means of this method remains in effect until the switched access path is disconnected or the link layer has left the information transfer phase and has entered the *disconnected* phase.

2.4.2 Identification per virtual call by means of network user identification facility

There is a method, using the *network user identification selection* facility, by which the identity of the DTE can be determined on a per-virtual-call basis.

The identification of the DTE is provided in the facility field of the *call request* packet via the use of the optional *NUI selection* facility. Use of NUI in the facility field in a *call accepted* packet allows a modification of billing (e.g. subaccount billing) to be carried out and has no effect on the values of the *DTE profile* in use for this DTE.

This procedure may be optionally offered by networks depending, in part, on the offering by the network of the optional *NUI selection* facility that this procedure uses. When it is offered by the network, use of this identification procedure by DTEs is optional.

The identification established by this method is accomplished at the same time as virtual call set-up and remains in effect until the virtual call is cleared.

The *NUI selection* facility may also be used when a prior-to-virtual-call-establishment identification method has been used. In this case, the service obtained by the DTE using the *NUI selection* facility in a *call request* packet is detailed in 6.3 concerning operation of the *NUI selection* facility.

The service that a DTE using the NUI method obtains is the *identified* DTE service. Upon termination of the virtual call:

a) if no prior-to-virtual-call-establishment DTE identification had been accomplished, the logical channel is usable again for a *non-identified* call or a DTE-identification-via-NUI call; or

b) if a prior-to-virtual-call-establishment DTE identification had been accomplished, the logical channel is usable again under the conditions of the DTE service that the prior-to-virtual-call *DTE identity* had invoked.

2.5 DCE identification methods

This Recommendation provides two methods for DCE identification. These methods are:

a) identification provided by the public switched network; and

b) identification by means of a link layer XID procedure.

When a network provides dial-in-by-the-DTE access and/or dial-out-by-the-PSPDN access, it need not provide the DCE identification to the DTE. Some networks may not provide the DCE identification to the DTE regardless of the approach used for the DTE identification.

However, for the networks that choose to provide the DCE identification to the DTE using one of the optional identification procedures, it is possible that the DTE may not use that optional identification procedure and, therefore, may not recognize the DCE identification. Additionally, networks are not required to provide DCE identification on dial-in-by-the-DTE operation.

There is a need to provide a reasonable degree of protection in the identification procedure so that Administrations and subscribers can prevent inaccurate DCE identification. Therefore, the identification procedure incorporates the functions of authentication and verification of the DCE's identity. The XID method of DCE identification obey an "identification protocol" that has been defined in 2.9 and 7.1 for conveying the information necessary for the DTE to recognize the DCE identity, including verifying the identity to the proper degree of authenticity and reporting on the success of the procedure.

When no DCE identification is received by the DTE, it is the responsibility of the DTE to decide if the level of security is sufficient to continue operation.

DTE identification may be achieved by using the identification protocol while it is simultaneously being used for DCE identification, but as an independent invocation of the protocol.

2.5.1 Identification prior to virtual call establishment

2.5.1.1 Identity provided by the public switched network

In the case of dial-out-by-the-PSPDN, the PSTN number, the ISDN number or the CSPDN number identifying the DCE may be provided by the public switched network (as well as some additional network management information from the PSPDN in some circumstances).

When identification is provided by the PSN, the DCE is not required to use any optional packet/frame types or any optional packet/frame fields defined in 5, 6 or 7 or in Recommendation X.25.

2.5.1.2 Identity provided by means of the link layer XID procedure

DCE identification can be optionally provided to the DTE by means of the exchange of XID frames prior to the link set-up. The detailed procedure to provide such information is the identification protocol given in 2.9 and 7.1.

2.5.2 Identification per virtual call

Identification of the DCE to the DTE on a per-virtual-call basis is currently not provided. The need for such a capability has been left for further study.

2.6 Dial-in-by-the-DTE and dial-out-by-the-PSPDN operation

All PSPDNs conforming to this Recommendation shall provide dial-in-by-the-DTE operation. Provision of dial-out-by-the-PSPDN operation is optional.

2.7 DTE service requirement

To provide a switched access service to DTEs, without introducing additional procedures, all PSPDNs conforming to this Recommendation shall offer the *non-identified* DTE service and/or support use of the provided-by-the-PSN DTE identification method.

Networks may also provide access to and/or from DTEs through a PSN, with the DTE being identified to the network using one of the optional identification procedures (see 2.4.1.2 and 2.4.2).

2.8 Duplex and half-duplex operation

If CSPDN access is used, the transmission facility is duplex. If PSTN access is used, the transmission facility operation is duplex, or, optionally, some networks may also provide for half-duplex operation. The additional procedures necessary for half-duplex operation are described in 5.6. If an ISDN transparent circuit connection is used, the transmission facility is duplex.

2.9 Identification protocol

The "identification protocol" consists of exchanges between the "challenged" party and the "questioning" party. The "challenged" party provides and, optionally, certifies its identity and the "questioning" party checks and authenticates this identity.

The DTE and DCE, either calling or called, may be questioning, challenged, or both questioning and challenged. This is the result of the identification protocol being used independently for DTE identification and DCE identification, possibly simultaneously.

The identification protocol provides two grades of security characterized by how many operations are needed and which elements are needed in each direction.

The operational details of the identification protocol are given in 7.1.

2.10 Negotiation of values

Negotiation of link layer parameters is left for further study. Presently, DCE parameters are set to specific values according to the *DTE profile* as outlined in 2.3 and 3.

Some networks may provide the capability for negotiation of packet layer facilities by means of the *on-line facility registration* facility. When provided, this negotiation takes as a starting point the values established in the *DTE profile* and, as a result, may override them.

Packet layer facilities may also be overridden by using the *NUI selection* facility when the *NUI override* facility is in effect.

3 DTE service descriptions

3.1 DTE service attributes

3.1.1 DTE identity

The *DTE identity* attribute, when provided, defines the identity of the DTE.

3.1.2 DTE identification method

The *DTE identification method* attribute, when provided, defines the DTE identification method used for establishing the *DTE identity* (see 2.4). The method is the same for dial-in-by-the-DTE and dial-out-by-the-PSPDN operation unless the provided-by-PSN method is selected for one operation, in which case the methods may be different.

3.1.3 DTE address

When this attribute is provided, a *DTE address* is assigned by the network for a given DTE identity.

The *DTE address* can be derived and validated from the DTE identification.

This *DTE address* may be, as a network option, either an X.121 number from the PSPDN numbering plan (see 2.3/X.121) or a number in the X.121 format from the PSN numbering plan. The number in the X.121 format from the PSN numbering plan for CSPDN is according to 2.3/X.121. The number in the X.121 format from the PSN numbering for PSTN and for ISDN is either according to 2.2.1.3/X.121 or to 2.6/X.121. The possible formats of the DTE address are given in 6.6/X.301.

NOTE – The inclusion or application of the Type of Address/Numbering Plan Identification (TOA/NP1) address format as defined in 5.2.1.2.2/X.25 requires further study.

3.1.3.1 DTE address not provided

In the case of dial-in-by-the-DTE, when the DTE makes a call request, the contents of the calling address field in the corresponding *incoming call* packet are either:

a) incomplete X.121 PSN format; this means the contents of the calling address field are not valid with respect to the definition of a "valid number" in the various Recommendations (e.g. a four digit number representing a DNIC that is assigned to a PSN; a number in the form 0 + CC; and a number in the form 9 + TCC are not valid numbers as defined in Recommendations X.121, E.164 and E.163 respectively); or

b) temporary number from the PSPDN numbering plan; this corresponds to the address of the dial-in port used for a particular call.

It is a network option whether the incomplete X.121 PSN format or the temporary number is used; however only the incomplete X.121 format is permitted at internetwork interfaces.

Moreover, when the PSN implements calling line identification but there is no arrangement between the PSN and PSPDN to use the number provided by the PSN as DTE identification and when no other DTE identification method is used, the PSPDN may include the PSN-provided number in the calling address field of the *incoming call* packet.

3.1.3.2 DTE address provided

When an identified DTE makes a call request, the contents of the calling DTE address field in the *incoming call* packet given to the called DTE is the *DTE address*. This applies even if the *temporary location* facility has been used to change the *registered PSN number* (see 7.2).

3.1.4 Registered address

This attribute, when provided, permits the DCE to be aware of a possible already established PSN connection with the DTE. The value of the *registered address* is always identical to the value of the *DTE address*.

3.1.4.1 Registered address not provided

When the network only provides a single logical channel for dial-out-by-the-PSPDN to a DTE that has no *registered address*, if the called DTE address field in a *call request* packet contains an X.121 number from the PSN numbering plan which is not a *registered address*, a dial-out-by-the-PSPDN operation will result in a busy signal. Therefore the incoming virtual call is cleared.

When the network provides multiple logical channels for dial-out-by-the PSPDN to a DTE that has no registered address, the PSPDN always checks if a switched connection already exists to the called DTE (see 2.3.2.1, this switched connection is then used by the PSPDN.

3.1.4.2 Registered address provided

Upon receiving a call request with a called DTE address, that is the *registered address*, the PSPDN needs to determine whether or not to perform a dial-out-by-the-PSPDN operation. If there is a switched connection in existence on which the *DTE identity* that corresponds to the *registered address* has been established, that switched connection will be used by the PSPDN. Otherwise, the PSPDN will perform the dial-out-by-the-PSPDN operation.

NOTE – This dial-out-by-the-PSPDN will not be successful if there is already a switched connection to the DTE when there has not been an establishment of a *DTE identity* or there has been a *DTE identity* established that does not correspond to the *registered address*.

The PSN number used for the dial-out-by-PSPDN is the *registered PSN number.*

NOTE – In some networks, if the called address used in a call request packet to call a switched access DTE is not the *registered address* for a *DTE identity* but is a *registered PSN number*, the PSPDN will not recognize this as a *registered address* and may treat the call according to the *non-identified* DTE service (see 3.5 and 3.3).

3.1.5 Registered PSN number

When the *registered PSN number* attribute is provided, its value is used by the PSPDN for dialing out to that DTE. If a *call request* packet contains a *registered address* which is not X.121 PSN number, the PSPDN uses the *registered PSN number* in order to perform the dial-out-by-the-PSPDN operation. If the *registered address* is an X.121 PSN number, then it is considered to be the *registered PSN* number.

If a DTE does not have a *registered address*, then the *registered PSN number* attribute does not apply.

3.1.6 X.25 subscription set

The *X.25 subscription set* attribute defines values for the X.25 link layer options and system parameters and the X.25 packet layer subscription-time optional user facilities which apply to switched access operation. Networks are not required to support all of the link layer options and packet layer subscription-time facilities, except as required in Recommendation X.2. The list of link layer options and system parameters and packet layer optional user facilities in the *X.25 subscription set* is given in Table 3 (see 3.3).

NOTE – As defined in Recommendation X.25, the throughput class values are, at most, the speed of the access line (see the *dial-out access type* attribute, 3.1.9). However, in the case of a modem with automatic fall-back capability, the DCE shall set the default throughput class values to the maximum signalling rate of the modem used, unless the user has selected lower values for the *default throughput classes assignment* facility. Some networks may take into account the signalling rate selected by the modems in fixing the default throughput class.

3.1.6.1 Network default

When the *X.25 subscription set* is specified as network default, the value of each of the options, parameters and facilities is a default value that is set by the PSPDN. Different defaults may apply according to the DTE service invoked.

The value of the *local charging prevention* facility is closely related to the policy of the PSPDN regarding accrual of charges by a non-identified DTE (see 3.3).

3.1.6.2 User selectable

When the *X.25 subscription set* is specified as user selectable, the value of each of the options, parameters, and facilities is available for customization by the user to a value from the set of values offered by the PSPDN.

3.1.7 Logical channels assignment

The logical channels assignment attribute defines the number of logical channels of each type assigned for a particular DTE.

There is a default value assigned by the PSPDN for non-identified DTEs (see below). A different default value may be set by the PSPDN for use in cases where the *DTE identity* is established.

3.1.7.1 Network default

When the logical channels assignment is specified as network default, for Dial-out-by-the-PSPDN operation the network default may be either one virtual call logical channel or more than one virtual call logical channels. Which default is offered by the network is a network operation. For dial-in-by-the-DTE operation, there may be one or more virtual call logical channels; the specific number is a network option. The direction of virtual call placement that is allowed on the logical channel(s) is governed by the direction of the dial operation as shown in Table 1.

TABLE 1/X.32

Direction of virtual call placement allowed as related to direction of the dial operation when logical channels assignment is by network default

Dial operation	Capabilities for DTE originating/receiving virtual calls	Equivalent X.25 optional user facilities (see Note)
Dial-in-by-the-DTE	Originating virtual calls	– Incoming calls barred – 1-way logical channel outgoing
Dial-out-by-the-PSPDN	Receiving virtual calls	– Outgoing calls barred – 1-way logical channel incoming
NOTE – The association of the dial operation with one or both of the optional user facilities is network-dependent.		

3.1.7.2 User selectable

When the *logical channels assignment* is specified as user selectable, the number of logical channels of each type is set by the user, for the particular *DTE identity*, from the values supported by the network.

3.1.8 Dial-out-by-the-PSPDN availability

The *dial-out-by-the-PSPDN availability* attribute allows the use of dial-out-by-the-PSPDN operation.

3.1.8.1 Network default

When the *dial-out-by-the-PSPDN availability* is specified as network default, the network chooses whether or not to offer dial-out-by-the-PSPDN operation. When dial-out-by-the-PSPDN operation is offered, the PSPDN attempts to establish a switched access path to the PSN number given in a *call request* packet.

3.1.8.2 User selectable

When the *dial-out-by-the-PSPDN availability* is specified as user selectable, the capability to have dial-out-by-the-PSPDN availability operation with a particular DTE is chosen by the user. When the *dial-out-by-the-PSPDN availability* is selected, the *registered PSN number* attribute must also be selected. Then the network dials out to the DTE whenever the *registered address* is used in a *call request* packet and there is not already a switched access path.

3.1.9 Dial-out access type

The *dial-out access type* attribute applies to dial-out-by-the-PSPDN operation and allows a DTE to choose modem characteristics or a user class of service or characteristics of an ISDN connection, possibly other than the national default, from those offered by the network. *Dial-out access type* refers to the modem characteristics (in the case of the PSTN) or the Recommendation X.1 user class (in the case of the CSPDN) or the characteristics of an ISDN connection (in the case of ISDN) that are used for switched access line operation at the physical layer, see 4. A national default dial-out access type is made by the PSPDN for each PSN through which access is permitted.

Note that for dial-in-by-the-DTE through the PSTN, the modem characteristics of the PSPDN port dialled into are used. For dial-in-by-the-DTE through the CSPDN, the Recommendation X.1 user class of the PSPDN port called is used.

NOTES

1 Some networks may use the procedures of Recommendation V.100 to perform modem selection.

2 The modem used determines whether the transmission facility is full or half duplex. Therefore, there is no attribute for the type of transmission facility operation.

3.1.9.1 Network default

When the *dial-out access type* is specified as network default, the national default modem characteristics are used for dial-out-by-the-PSPDN through the PSTN. For dial-out-by-the-PSPDN through the CSPDN, the national default Recommendation X.1 user class is used. For dial-out-by-the-PSPDN through an ISDN, the national default for rate adaption method is used, see Recommendation X.31 for the applicable method.

3.1.9.2 User selectable

When the *dial-out access type* is specified as user selectable, the modem characteristics selected for this *DTE identity*, from those offered by the network, are used for dial-out-by-the-PSPDN through the PSTN. For dial-out-by-the-PSPDN through the CSPDN, the Recommendation X.1 user class, selected for this *DTE identity* from those offered by the network, is used. For dial-out-by-the-PSPDN through an ISDN, the Recommendation X.1 user class, selected for this *DTE identity* from those offered by the network, is used.

3.1.10 X.32 optional user facility

The secure dial-back X.32 optional user facility is included within this attribute and is defined in 7.2. It is optional for the PSPDN to offer this facility.

3.1.11 DCE identity presentation

The PSPDN chooses whether or not to offer DCE identity presentation. When DCE identity presentation is offered, the *DCE identity presentation* attribute defines the DCE identification method used by the PSPDN. The PSPDN may choose to use a DCE identification method for both dial-in-by-the-DTE operation and dial-out-by-the-PSPDN operation or for only dial-out-by-the-DTE operation. When the DCE identification is done for both operations, the method is the same for dial-in-by-the-DTE operation and dial-out-by-the-PSPDN operation. The PSPDN selects one of the DCE identification methods given in 2.5.

Some networks may include a DTE profile designator as part of the DCE identity in order to inform the DTE of the *DTE profile* applicable to the DTE/DCE interface during this instance of switched access. The DTE profile designator is a string of octets that may be assigned by the PSPDN to the *DTE identity* as a name for the specific *DTE profile*.

3.1.12 Data link layer address assignment

The *data link layer address assignment* attribute defines the mechanism used to determine the data link layer addresses.

NOTE – Other methods of data link layer address assignment different from those described below, are for further study.

3.1.12.1 Network default

When the *data link layer address assignment* is specified as network default, the data link level addresses are assigned depending on the direction of the switched access call as defined in 5.2 (same as Recommendation T.70).

Alternatively, *data link layer address assignment* that is dependent on the roles of the equipment as DTE and DCE, as defined in 5.2 (same as 2.4.2/X.25), may be provided by some networks.

NOTES

1 The dial-out-by-the-PSPDN operation will only operate properly when the DTE and the PSPDN implement the same *data link layer address assignment* method.

2 Assigning the data link layer addresses according to the roles of the equipment as DTE and DCE does not allow for two DTEs to interoperate directly without an intervening PSPDN.

3.1.12.2 User selectable

When the *data link layer address assignment* is specified as user selectable, the user designates whether the link level addresses are assigned depending on the direction of the switched access call or depending on the roles of the equipment as DTE and DCE (see 5.2).

3.2 Summary of DTE services

The type of each attribute is given for the three DTE services in Table 2.

TABLE 2/X.32

Summary of DTE services

Services / Attributes	Non-identified	Identified	Customized
DTE identity	–	Yes	Yes
DTE identification method	–	Any (ND)	Prior to virtual circuit establishment (ND)
DTE address	–	(See Note 4)	Yes
Registered address	–	(See Note 1)	Yes
Registered PSN number	–	–	User selectable
X.25 subscription set	ND	(See Note 1)	User selectable
Logical channel assignment	ND	ND	User selectable
Dial-out-by-the-PSPDN availability	ND	(See Note 1)	User selectable
Dial-out access type	ND	ND	User selectable
X.32 optional user facilities	–	–	User selectable
DCE identity presentation	ND	ND	ND
Data link layer address assignment	ND	ND	User selectable (See Note 3)

– Not provided

ND Network default

Yes Provided

NOTES

1 In this DTE service, the use of *registered addresses* for some DTEs is a network option. When the DTE is assigned a *registered address*, the value of the *dial-out-by-the-PSPDN availability* attribute is user selectable. Otherwise, (if no *registered address* is assigned to the DTE), the availability of dial-out-by-the-PSPDN operation is by network default.

2 ND or, if *NUI override* is in effect, user selectable packet layer facility values (Annex H/X.25).

3 In the case of dial-in-by-the-DTE operation, the link layer address values assigned are the same for both assignment methods and, therefore, the values are not dependent on the assignment method selected by the user.

4 In this DTE service, the use of *DTE addresses* for some DTEs is a network option.

3.3 Non-identified DTE service

The values of the attributes for the *non-identified* DTE service defined in 2.3.2.1 are shown in the "non-identified" column of Table 2:

– no *DTE identity* is established;

– no *DTE identification* method is used.

Generally, no optional user facilities are available except those governing the direction of virtual call placement (i.e. incoming calls barred, outgoing calls barred, one-way logical channel outgoing, and one-way logical channel incoming) and those that can be used on a per-virtual-call basis without prior subscription. In addition, some networks may allow the use of:

a) some subscription-time optional user facilities without prior subscription. (The network may make these known by publication or through the use of the *on-line facility registration* facility; in such cases, a PSPDN should consider making its identity known non-identified DTEs); and

b) some subscription-time optional user facilities that must be requested by the DTE through the use of the *on-line facility registration* facility.

The X.25 data link layer options and system parameters and the X.25 subscription-time optional user facilities are categorized for dial-in-by-the-DTE and dial-out-by-the-PSPDN operation in Table 3 as:

– an "AVAIL-NS" data link layer system parameter, which is set by the network on all networks offering *non-identified* DTE service;

– an "AVAIL-BAS" optional user facility or data link layer option, which is available on all networks offering *non-identified* DTE service. This facility is in effect even if not requested;

– an "AVAIL-OPT" optional user facility, which is available on some networks offering the *non-identified* DTE service and the availability of which is made known through either publication or use of the *on-line facility registration* facility. These facilities can be used without further request when operating on these networks;

– an "AVAIL-RQ" optional user facility, which is available on some networks offering the *non-identified* DTE service and the use of which must be requested through the *on-line facility registration* facility; or

– a "No" optional user facility or data line level option, which is not available on any network offering *non-identified* DTE service.

The DTE may use any per-call X.25 facility that is supported by the PSPDN and that does not require prior subscription.

3.4 Identified DTE service

The values of the attributes for the *identified* DTE service (defined in 2.3.2.2) are shown in the "identified" column of Table 2.

– A *DTE identity* that has been agreed to explicitly or implicitly is provided to the network.

– The *X.25 subscription* set is the same as in the *non-identified* DTE service except that:

  a) for dial-in-by-the-DTE operation, in which the *NUI override* facility is in effect at the DTE/DCE interface, the *NUI selection* facility, as defined in Recommendation X.25, can be used to invoke user selected packet layer facility values (see 6.3 of this Recommendation and Annex H/X.25); and

  b) the *local charging prevention* facility is not in effect.

The DTE may use any per-call X.25 facility which is supported by the PSPDN and which does not require prior subscription.

TABLE 3/X.32

Availability of data link layer options and system parameters and packet level subscription-time facilities in the non-identified DTE service

Option, parameter or facility (applicable to all assigned logical channels)	Available with Dial-in-by-the-DTE operation	Available with Dial-out-by-the-PSPDN operation
Data Link layer		
K	AVAIL-NS	AVAIL-NS
T1	AVAIL-NS	AVAIL-NS
T2	AVAIL-NS	AVAIL-NS
T3	AVAIL-NS	AVAIL-NS
N1	AVAIL-NS	AVAIL-NS
N2	AVAIL-NS	AVAIL-NS
Multilink	No	No
MT1	No	No
MT2	No	No
MT3	No	No
Extended frame sequence numbering	No	No
Packet layer		
On-line facility registration	AVAIL-OPT	AVAIL-OPT
Extended packet sequence numbering	AVAIL-RQ (Note 1)	AVAIL-RQ
D-bit Modification	AVAIL-RQ	AVAIL-RQ
Packet retransmission	AVAIL-OPT	AVAIL-OPT
Incoming calls barred	AVAIL-BAS	No
Outgoing calls barred	No	AVAIL-BAS
One-way logical channel outgoing	AVAIL-BAS	No
One-way logical channel incoming	No	AVAIL-BAS
Non-standard default packet sizes	AVAIL-RQ	AVAIL-RQ
Non-standard default window sizes	AVAIL-RQ (Note 2)	AVAIL-RQ (Note 2)

TABLE 3/X.32 *(cont.)*

Availability of data link layer options and system parameters and packet level subscription-time facilities in the non-identified DTE service

Option, parameter or facility (applicable to all assigned logical channels)	Available with Dial-in-by-the-DTE operation	Available with Dial-out-by-the-PSPDN operation
Data Link layer		
Default throughput classes assignment	AVAIL-RQ	AVAIL-RQ
Flow control parameter negotiation	AVAIL-RQ (Note 1)	AVAIL-RQ
Basic throughput class negotiation	AVAIL-OPT (Note 1)	AVAIL-OPT
Extended throughput class negotiation	(Note 1)	(Note 1)
Closed user group related facilities – Closed user group – Closed user group with outgoing access – Closed user group with incoming access – Incoming calls barred within a closed user group – Outgoing calls barred within a closed user group	 No No No No No	 No No No No No
Bilateral closed user group related facilities – Bilateral closed user group – Bilateral closed user group with outgoing access	 No No	 No No
Fast select acceptance	No	AVAIL-OPT
Reverse charging acceptance	No	No
Local charging prevention (See Note 3)	Yes	Yes
Network user identification subscription	No	No
NUI override	No	No
Charging information subscription	No	No
ROA subscription	No	No
Hunt group	No	No
Call redirection	No	No
Call deflection subscription	No	No

TABLE 3/X.32 *(end)*

Availability of data link layer options and system parameters and packet level subscription-time facilities in the non-identified DTE service

Option, parameter or facility (applicable to all assigned logical channels)	Available with Dial-in-by-the-DTE operation	Available with Dial-out-by-the-PSPDN operation
TOA/NPI address subscription	(See Note 4)	(See Note 4)
Interface specific alternative address registration	No	No
Packet layer *(end)*		
Alternative address usage subscription	AVAIL-OPT	No

NOTES

1 Further study is required to determine whether subscription should be equivalent to use in a *call set-up* packet (either in the general format identifier for the *extended packet sequence numbering* facility or in the facility field for other facilities) under the *non-identified* DTE service.

2 Some networks offering half-duplex operation as part of the *non-identified* DTE service may set the default window size to a single non-standard default window size value.

3 The *local charging prevention* facility is in effect unless the PSPDN permits unidentified DTEs to accrue charges.

4 The application of TOA/NPI address subscription is for further study.

3.5 Customized DTE service

The values of the attributes for the *customized* DTE service (defined in 2.3.2.2) are shown in the "customized" column in Table 2.

NOTE – If a public port is used, the values in the customized *DTE profile* may not all be supported. (The characteristics available may vary from one public port to another). The result may be service according to network default values or refusal of service.

A *DTE identity* that has been explicitly agreed to with the PSPDN for obtaining the *customized* DTE service is provided to the PSPDN.

The availability for customization of each X.25 link layer option and system parameter and X.25 packet layer subscription-time facility is given in Table 4.

The DTE may use any per-call X.25 facility which is supported by the PSPDN and which does not require prior subscription.

The DTE may use any per-call X.25 facility which is supported by the PSPDN and which requires a corresponding subscription-time facility to be selected, provided that the corresponding subscription-time facility has been selected.

4 Interface characteristics (physical layer)

Administrations may offer one or more of the physical layer interfaces specified below.

For a description of the physical layer interface for the case of ISDN transparent circuit connection, see Recommendation X.31.

TABLE 4/X.32

Availability for customization in the customized DTE service of the X.25 data link layer options and system parameters and the X.25 subscription-time facilities

Option, parameter or facility	Customization available
Data Link layer	
K	CUSTOM
T1	CUSTOM
T2	CUSTOM
T3	CUSTOM
N1	CUSTOM
N2	CUSTOM
Multilink	(Note 1)
MT1	(Note 1)
MT2	(Note 1)
MT3	(Note 1)
Extended frame sequence numbering	CUSTOM
Packet layer	
On-line facility registration	CUSTOM
Extended packet sequence numbering	CUSTOM
D-bit modification	CUSTOM
Packet retransmission	CUSTOM
Incoming calls barred	CUSTOM
Outgoing calls barred	CUSTOM
One-way logical channel outgoing	CUSTOM
One-way logical channel incoming	CUSTOM
Non-standard default packet sizes	CUSTOM
Non-standard default window sizes	CUSTOM
Default throughput classes assignment	CUSTOM
Flow control parameter negotiation	CUSTOM
Basic throughput class negotiation	CUSTOM
Extended throughput class negotiation	CUSTOM

TABLE 4/X.32 *(end)*

Availability for customization in the customized DTE service of the X.25 data link layer options and system parameters and the X.25 subscription-time facilities

Option, parameter or facility	Customization available
Packet layer *(end)*	
Closed user group related facilities – Closed used group – Closed user group with outgoing access – Closed user group with incoming access – Incoming calls barred within a closed user group – Outgoing calls barred within a closed user group	 CUSTOM CUSTOM CUSTOM CUSTOM CUSTOM
Bilateral closed user group related facilities – Bilateral closed user group – Bilateral closed user group with outgoing access	 CUSTOM CUSTOM
Fast select acceptance	CUSTOM
Reverse charging acceptance	CUSTOM
Local charging prevention	CUSTOM
Network user identification subscription	CUSTOM
NUI override	CUSTOM
Charging information subscription	CUSTOM
ROA subscription	CUSTOM
Hunt group	CUSTOM
Call redirection	CUSTOM (See Note 2)
Call deflection subscription	CUSTOM
TOA/NPI address subscription	(See Note 3)
Interface specific alternative address registration	CUSTOM
Alternative address usage subscription	CUSTOM

CUSTOM Can be chosen or set to a non-default value by the DTE, if supported by the PSPDN.

NOTES

1 The need for multilink procedures over switched access paths is left for further study.

2 The criteria for determining that the DTE is out of order (for the purposes of call redirection) have been left for further study.

3 The application of TOA/NPI address subscription is for further study.

4.1 X.21 interface

For establishment, maintenance, and disestablishment of a switched access path between a DTE and a PSPDN by way of a CSPDN, the interface at the physical layer shall be in accordance with Recommendation X.21, as described in the following clauses.

4.1.1 DTE/DCE physical interface elements

The DTE/DCE physical interface elements shall be according to 2.1/X.21 through 2.5/X.21.

4.1.2 Alignment of call control characters and error checking

Alignment of call control characters and error checking shall be in accordance with 3/X.21.

4.1.3 Procedures for entering operational phases

The *call control* phase shall be required prior to entering the data transfer phase and shall be in accordance with 4/X.21.

After a call is established within the CSPDN, the physical layer interface will enter the *data transfer* phase, as described in 5.1/X.21. While in the *data transfer* phase (state 13), data exchanged on circuits T and R will be as described in subsequent clauses of this Recommendation.

The *Not ready* states given in 2.5/X.21 are considered to be non-operational states, and may be considered by higher layers to be out-of-order states.

4.1.4 Clearing procedures

Clearing procedures shall be according to 6/X.21.

4.1.5 Failure detection principles and test loops

Failure detection principles shall be according to 2.6.1/X.21 and 2.6.2/X.21.

The definitions of test loops and the principles of maintenance testing using test loops are provided in Recommendation X.150.

A description of the test loops and the procedures for their use are given in 7/X.21.

Automatic activation by a DTE of test loop 2 in the DCE at the remote DTE/DCE interface is not possible. However, some Administrations may permit the DTE to control the equivalent of a test loop 2 at the local data switching exchange (DSE) to verify the operation of the subscriber line, the switched access path and all or part of the DCE or line terminating equipment. Subscriber control of the loop, if provided, may be manual or automatic as described in Recommendations X.150 and X.21, respectively.

4.1.6 Signal element timing

The signal element timing shall be in accordance with 2.6.3/X.21.

4.2 X.21 *bis* interface

For establishment, maintenance, and disestablishment of a switched access path between a DTE and a PSPDN by way of a CSPDN, the interface at the physical layer shall be in accordance with Recommendation X.21 *bis*, as described in the following clauses.

4.2.1 DTE/DCE physical interface elements

The DTE/DCE physical interface elements shall be in accordance with 1.2/X.21 *bis*.

4.2.2 Procedures for entering operational phases

The procedures for entering operational phases shall be in accordance with 2/X.21 *bis*. When circuit 107 is in the ON condition, and when circuits 105, 106, 108, and 109, if provided, are in the ON condition, data exchange on circuits 103 and 104 will be as described in subsequent clauses.

When circuit 107 is in the OFF condition, or any of circuits 105, 106, 108 or 109, if provided, is in the OFF condition, the interface is considered to be in a non-operational state and may be considered by the higher layers to be in an out-of-order state.

4.2.3 Failure detection and test loops

Failure detection principles, the description of the test loops and the procedures for their use are given in 3.1 through 3.3/X.21 *bis*.

Automatic activation by a DTE of test loop 2 in the DCE at the remote DTE/DCE is not possible. However, some Administrations may permit the DTE to control the equivalent of a test loop 2 at the local DSE to verify the operation of the subscriber line, the switched access path, and all or part of the DCE or line terminating equipment. Subscriber control of the loop, if provided, may be manual or automatic as described in Recommendations X.150 and X.21 *bis*, respectively.

4.2.4 Signal element timing

Signal element timing shall be in accordance with 3.4/X.21 *bis*.

4.3 V-series interface

For establishment, maintenance, and disestablishment of a switched access path between a DTE and a PSPDN by way of a PSTN, the physical layer interface shall be as described in the following clauses.

4.3.1 Modem characteristics

Administrations may choose to offer modem characteristics in accordance with any or all of the following:

a) 1200 bit/s V.22, Alternatives A, B or C, Mode i)

b) 2400/1200 bit/s V.22 *bis*, Modes i) or iii), or

V.26 *ter*, Mode i) or iii)

c) 9600/4800 bit/s V.32, Synchronous Modes

d) 14 400 bit/s V.32 *bis* Synchronous Mode.

In addition, those Administrations which offer half-duplex operation may choose to offer modem characteristics in accordance with any or all of the following:

e) 2400 bit/s V.26 *bis*, Alternative B

f) 4800/2400 bit/s V.27 *ter*

NOTE – In the future it is desirable that one modem characteristic should be available in all network implementations of this Recommendation. However, for the time being, it has not been possible to select a single modem type.

Other modem characteristics are left for further study or are a national matter.

Use of the backward channel, if allowed, is outside the scope of this Recommendation.

4.3.2 Procedures for full duplex operational phases

When circuit 107 is in the ON condition, and when circuits 105, 106, 108 and 109, if provided, are in the ON condition, data exchanged on circuits 103 and 104 will be as described in subsequent clauses.

Circuits 106 and 109 may enter the OFF condition due to momentary transmission failures of modem retraining. Higher layers should delay for several seconds before considering the interface to be non-operational.

4.3.3 Procedures for half-duplex operational phases

The states of circuits 103, 104, 105, 106 and 107 shall be according to 5.6.8.

4.3.4 Origination procedures

DTEs may use either:

a) the automatic origination procedures described in 3/V.25;

b) the automatic origination procedures described in 4 or 5/V.25 *bis*;

c) the manual origination procedures of 6/V.25.

Networks will use automatic origination procedures only.

NOTE – Other origination procedures may be used provided that no special requirements are placed on DTEs (including DTEs having integral modems and diallers) using only V.25 or V.25 *bis* procedures.

4.3.5 Answering procedures

For dial-out-by-the-PSPDN procedures, DTEs should use the automatic answering procedures of Recommendations V.25 and V.25 *bis*. Some Administrations may also allow use of manual answering procedures, provided that doing so does not affect DTEs using automatic answering procedures.

For dial-in-by-the-DTE, networks will use automatic answering procedures only.

4.3.6 Disconnection procedures

DTEs and networks shall use the disconnection procedures specified in Recommendation V.24.

4.3.7 Test loops

The definitions of test loops and the principles of maintenance testing using test loops are provided in Recommendation V.54.

Descriptions of the test loops and the procedures for their use are given in the appropriate modem Recommendations. It should be noted that the procedures for loop testing vary among the several modem Recommendations.

Automatic activation by a DTE of test loops 2 and 4 in the DCE at the remote DTE/DCE interface is not possible. However, some Administrations may permit the DTE to control the equivalent of a test loop 2 or 4 at the local DSE to verify the operation of the subscriber line, the switched access path, and all or part of the DCE or line terminating equipment. Subscriber control of the loop, if provided, may be manual or automatic as described in Recommendation V.54 and the appropriate modem Recommendations, respectively.

5 Link access procedure across the DTE/DCE interface

5.1 Introduction

This clause specifies the mandatory and optional data link layer procedures that are employed to support switched access data interchange between a DCE and a DTE.

5.1.1 Compatibility with the ISO balanced classes of procedure

The switched access data link layer procedures defined in this Recommendation use the principles and terminology of the High-level Data Link Control (HDLC) procedures specified by the International Organization for Standardization.

DCE compatibility of operation with the ISO balanced classes of procedure (Class BA with options 2 and 8 and Class BA with options 2, 8 and 10) is achieved using the LAPB procedure described in 2.2/X.25, 2.3/X.25, and 2.4/X.25. Class BA with options 2 and 8 (LAPB modulo 8) is available in all networks for switched access.

Class BA with options 2, 8 and 10 (LAPB modulo 128) may also be offered for switched access by some networks.

NOTE – The operating conditions under which modulo 128 sequence numbering applies are left for further study.

Class BA 1, 2, 8 and Class BA 1, 2, 8 and 10 provide for the additional use of the unnumbered format Exchange Identification (XID) command and response. This additional capability may be used in the performance of DTE/DCE identification and authentication and in the selection of X.32 optional user facilities (see 7.2) by the application of the proposed HDLC standard – General purpose XID frame information field content and format (ISO International Standard 8885).

5.1.2 Underlying transmission facility

The underlying transmission facility is duplex or, optionally, half-duplex (see 2.8). Specific procedures are defined in 5.6 for operation over a half-duplex transmission facility.

5.2 Data link layer address assignment

Two alternative mechanisms for assigning the data link layer addresses are included in the procedures of this Recommendation. The conditions under which each mechanism applies are specified in the *data link layer address assignment* attribute (see 3.1.12).

It should be noted that the alternative mechanisms result in the assignment of identical values in dial-in-by-the-DTE operation.

5.2.1 Assignment depending on switched access call direction

In accordance with Recommendation T.70, data link layer address assignment for dial-in-by-the-DTE and dial-out-by-the-PSPDN operation depends on the direction of the switched access call as specified in Figure 4.

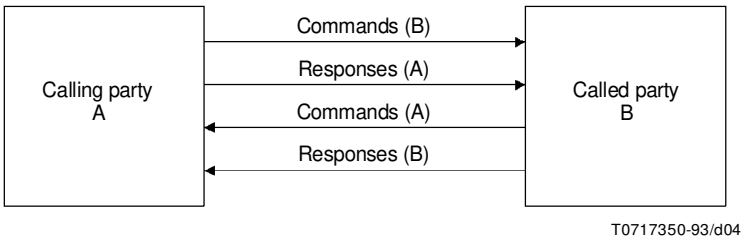
The DCE is always aware of whether the switched access path is established by the DTE (dial-in-by-the-DTE) or the DCE (dial-out-by-the-PSPDN). The DTEs that are not or cannot be aware of this situation shall initiate the appropriate address resolution procedures to determine the individual address of the DCE. These procedures are left for further study. However, it is intended that these procedures will not affect DTEs using the data link layer address assignment described in Figure 4.

Link addresses, A and B, shall be assigned according to the following rules:

1) the calling party shall take address A;

2) the called party shall take address B;

3) commands and responses shall be transferred as shown in Figure 4.



NOTE – For dial-in-by-the-DTE, the DTE is the calling party A; for dial-out-by-the-PSPDN, the DCE is the calling party A.

FIGURE 4/X.32

Data link layer address assignment depending on switching access call direction

5.2.2 Assignment depending on roles of equipment as DTE and DCE

In accordance with the specifications in 2.4.2/X.25, the data link layer address assignment depends on the roles of the equipment as DTE and DCE such that the DCE transmits to the DTE the address A in command frames and the address B in response frames and the DTE does the opposite (i.e. transmits to the DCE address B in command frames and address A in response frames).

5.3 Use of exchange identification (XID) frames

5.3.1 General

XID frames may be used by the DCE and DTE in the performance of either DTE or DCE identification and authentication, and/or by the DTE and DCE to convey X.32 optional user facilities (see 7.2).

NOTE – The use of the XID command/response for address negotiation and the negotiation of link layer parameters is left for further study.

5.3.1.1 XID command

The XID command is used by the DTE/DCE to cause the DCE/DTE to identify itself, and, optionally, to provide DTE/DCE identification and/or characteristics to the DCE/DTE. An information field is optional with the XID command.

5.3.1.2 XID response

The XID response is used by the DTE/DCE to reply to a XID command. An information field containing the DTE/DCE identification and/or characteristics may be optionally present in the XID response.

5.3.2 Format of XID frame

The format of the address field of the XID frame is as defined in 5.2.

The format of the control field of the XID frame is given in Figure 5.

NOTE – The first bit transmitted is bit 1, the low order bit.

Format	Command	Response	Encoding			
			1 2	3 4	5	6 7 8
Unnumbered	XID	XID	1 1	1 1	P/F	1 0 1

FIGURE 5/X.32

XID command and response control field bit encoding

After the XID control field there may be an XID information field. The general format of the XID information field, when present, is shown in Figure 6.

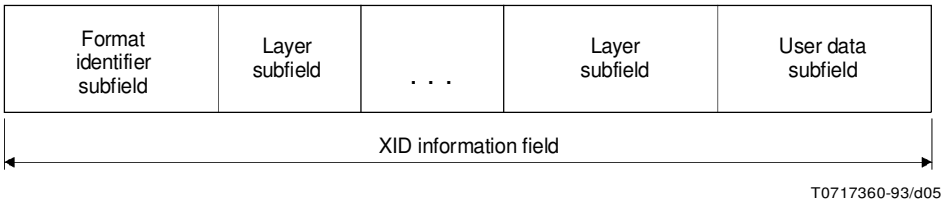


FIGURE 6/X.32

General structure of the XID information field

The XID information field is composed of a number of subfields. These subfields are a format identifier (FI) subfield, several layer subfields, and a user data subfield.

The FI subfield is a fixed one-octet field. This field is encoded to have a capacity of designating 128 different ISO standardized formats and 128 different user-defined formats. The format identifier in this Recommendation is one of the ISO standardized format identifiers. The FI subfield is present if there is a layer subfield and/or a user data subfield present. The FI subfield need not be present if there is no layer subfield or data user subfield present. The format identifier is encoded as shown in Figure 7.

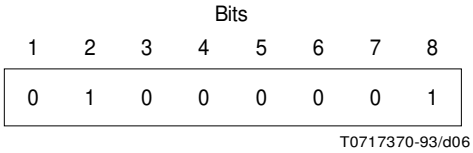


FIGURE 7/X.32

XID format identifier subfield

The layer subfields are permitted to be present in the information field of either XID command or XID response frames for the purposes of link layer address resolution and link level parameter negotiation. The use of these subfields within the scope of this Recommendation is left for further study.

The user data subfield contains data link user information to be transferred during XID interchange. This data link user information is transported transparently across the data link and passed to the user of the data link. The user data subfield is composed of the two elements illustrated in Figure 8.

The user data identifier element identifies the subfield as the user data subfield. Its encoding is shown in Figure 9.

The length of the user data field is the number of octets between the user data identifier and the frame check sequence of the XID frame. The user data field element contains the X.32 identification protocol elements or X.32 optional user facilities which are described in 7 (see Table 7).

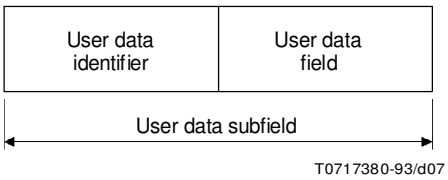


FIGURE 8/X.32

User-data subfield

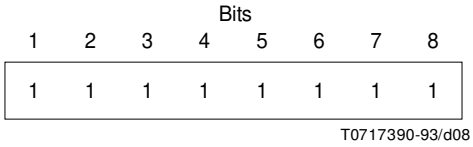


FIGURE 9/X.32

User data identifier element

In the scope of this Recommendation, the user data subfield should only be used in XID command frames, and while in the disconnected phase.

Since the use of layer subfields is for further study within the scope of this Recommendation, the format of the information field of the XID command frames is summarized in Figure 10.

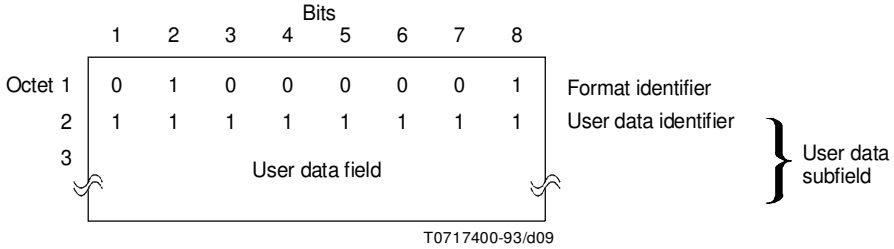


FIGURE 10/X.32

XID information field format

5.3.3 XID procedures for identification and X.32 optional user facilities

5.3.3.1 General

When a DTE/DCE determines that it is not able to act upon a received XID command, it will consider this XID command as not implemented and will act as specified in Recommendation X.25 (see 2.4.4.4.1/X.25 for the *disconnected* phase, and 2.4.6.1/X.25 for the *information transfer* phase).

When a DTE/DCE determines that it is able to act upon a received XID command, it shall process this command and acknowledge it by transmitting an XID response with the F bit set to the value of the P bit received in the XID command in any phase (*disconnected* phase or *information transfer* phase). The DCE shall and the DTE should set the P bit to 1 in the XID command frame.

For purposes of this Recommendation, the user data subfield shall only be used in XID command and while in the disconnected phase. A user data subfield will be ignored by the DCE when received in an XID response and/or while in the *information transfer* phase.

When transmitting an XID command, the DTE/DCE shall start timer T1. Timer T1 is stopped upon reception of the XID response with the F bit set to the value of the P bit sent in the XID command.

If timer T1 expires before the XID response (which has the F bit set to the value of the P bit sent in the XID command) is received by the DTE/DCE, the DTE/DCE retransmits the XID command and restarts timer T1. The maximum number of attempts made by the DTE or DCE to complete successful transmission of the XID command is defined by N2.

5.3.3.2 Identification, authentication and selection of X.32 optional user facilities using XID frames

The reception of an XID response by the DTE/DCE only means that the corresponding XID command has been correctly received by the DCE/DTE. If the DCE/DTE needs to transmit an identification protocol element or an X.32 facility element to the DTE/DCE, it shall transmit the element in an XID command.

Following successful identification/authentication and/or selection of X.32 optional user facilities using an XID exchange(s), the data link will be established under normal LAPB procedures (see 5.4.1). If these procedures are not successful, the switched access path is disconnected (see 5.4.2).

The identification of the DTE and/or DCE remains in effect until the link layer or the switched access path is disconnected.

5.4 Link set-up disconnection

5.4.1 Link set-up

The initiative of the link set-up is in the charge of the DTE in dial-in-by-the-DTE operation and of the DCE in dial-out-by-the-PSPDN operation. The DCE may also initiate link set-up in the case of dial-in-by-the-DTE operation; likewise, the DTE may also initiate link set-up in the case of dial-out-by-the-PSPDN operation.

When receiving a Set Asynchronous Balanced Mode (SABM) or Set Asynchronous Balanced Mode Extended (SABME) (if supported) command during the identification procedure with XID frames, the DCE/DTE shall consider that the DTE/DCE does not want to complete the identification procedure. The DTE/DCE may then accept the link set-up initiation or may disconnect the link and the switched access path, depending on whether or not the DCE/DTE considers the completion of the identification process as mandatory.

During the period between transmitting an SABM/SABME command and receiving the UA response, the DCE/DTE shall discard any frame (including XID) except SABM/SABME, Disconnect (DISC), Unnumbered Acknowledge (UA) and Disconnected Mode (DM) as specified in 2.4.4.1/X.25.

5.4.2 Disconnection

Whenever the DCE needs to disconnect the switched access path and the link is not already in the *disconnected* phase, it should first disconnect the link.

5.5 Multilink

The need for multilink procedures over switched access paths is left for further study.

5.6 Half-duplex operation

Figure 11 shows the half-duplex transmission module (HDTM) for extending LAPB for operation over the PSTN where half-duplex circuits are used. The signals which the two LAPX modules use in controlling the direction of the line are described.

Before the HDTM begins operation the physical circuit must be established by the appropriate PSTN call control procedures. The HDTM in the DTE or DCE which has established the switched access path will initially have the right to transmit. The DTE or DCE which originated the switched access path is the "calling DTE/DCE". The other DTE or DCE is the "called DTE/DCE".

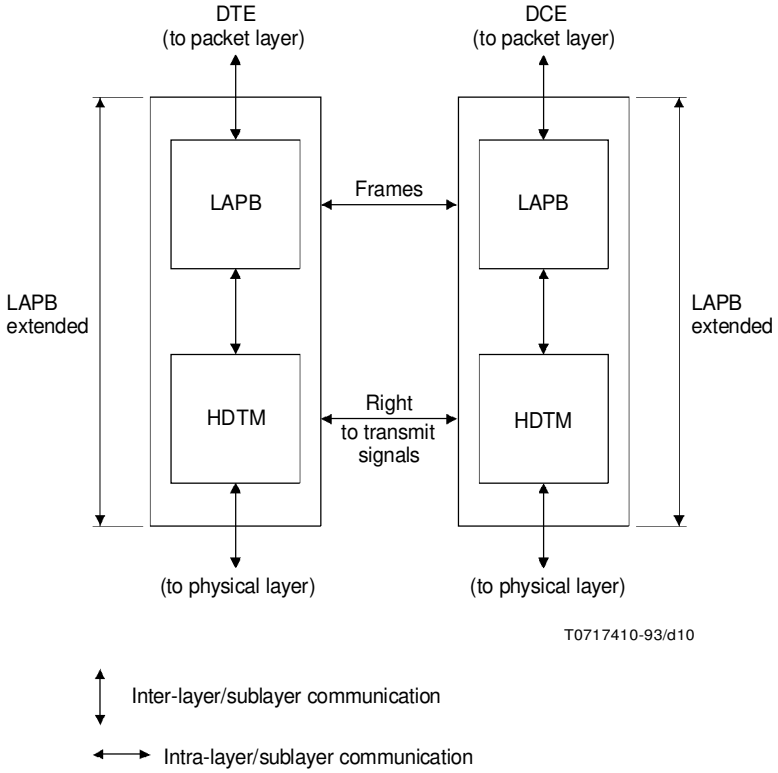


FIGURE 11/X.32

Link layer for PSTN access based on LAPB plus the HDTM

5.6.1 Right to transmit

The purpose of the HDTM is to coordinate the use of the half-duplex line between the DTE and DCE. It must exchange signals with the remote HDTM, interact with LAPB, and direct the physical level. The HDTM has the responsibility for deciding when to give up the right to transmit.

The right to transmit is exchanged between the DTE and DCE by using the idle channel state condition and flags as signals. Initially, the DTE or DCE which initiated establishing the physical connection has the right to transmit. That DTE or DCE sends the idle channel state condition when it has finished transmitting frames. After the line has been turned around, the other DTE/DCE sends flags to confirm the exchange of the right to transmit, until it has a frame to send. If the confirmation is not received in a certain amount of time, the DTE or DCE which gave up the right to transmit may take it again by sending flags.

NOTE – If no frame is sent, at least five flags must be sent as the minimum signal between receiving the right to transmit and relinquishing it again.

The meaning of the idle channel state condition in this Recommendation is different from that of Recommendation X.25. As a result, the T3 timer does not apply to half-duplex operation.

An optional alternative to the detection of the idle channel state condition is to use the detection of the carrier going OFF as the signal that the sending device is giving up the right to transmit. Also, an optional alternative to the detection of flags is to use the detection of the carrier going ON as the signal that the remote device has accepted the right to transmit. This alternative behavior should only be used with modems that give substantial protection from transient errors on the line.

In those situations where the physical layer cannot detect that the connection has been cut-off, an optional procedure, which detects the absence of any activity over a period of time and then disconnects the link, should be used.

5.6.2 Layer relationships

In adapting LAPB for half-duplex operation, modifications have been kept to a minimum. However, there is a functional requirement that the HDTM inhibit LAPB from sending frames during certain phases of the half-duplex procedure. The means of accomplishing this functional requirement are not defined in this Recommendation. Some considerations in implementing the HDTM are discussed in Appendix I.

The logical relationships among LAPB, the HDTM, and the physical layer are as shown in Figure 12.

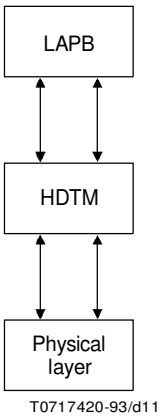


FIGURE 12/X.32

Layer relationships

5.6.3 State definitions

Five states of the HDTM are defined for describing the procedure used to keep track of the right to transmit.

5.6.3.1 Idle state (state 0)

The DTE/DCE is in an inactive state. This is the initial state prior to the establishment of the switched access path and the final state after termination of the switched access path.

5.6.3.2 Half-duplex sending state (state 1)

The DTE/DCE is in a half-duplex sending state, so that all signals generated by LAPB are passed to the physical layer. The calling DTE/DCE enters this state upon establishment of the switched access path.

5.6.3.3 Wait for receiving state (state 2)

The DTE/DCE is waiting for an indication that the remote DTE/DCE has entered the half-duplex sending state. No signals generated by LAPB are passed to the physical layer.

5.6.3.4 Half-duplex receiving state (state 3)

The DTE/DCE is in a half-duplex receiving state, so that no signals generated by LAPB are passed to the physical layer. The remote DCE/DTE is considered to be in the half-duplex sending state. The called DTE/DCE enters this state upon establishment of the switched access path.

5.6.3.5 Wait for sending state (state 4)

The DTE/DCE is awaiting indication of the availability of the physical layer for transmission of frames to the remote DCE/DTE. Flag, idle channel state condition, and abort signals are passed to the physical layer, but sending of frames is inhibited.

5.6.4 Timer XT1

A timer, XT1, is defined for use in recovering from an apparent failure of the remote DTE/DCE to take the right to transmit. To avoid a contention condition during this recovery process, different values of timer XT1 are to be used by the called and calling DTE/DCE. A calling DTE/DCE uses the value XT1a, and a called DTE/DCE uses the value XT1b.

The values of XT1a and XT1b are system parameters and have been left for further study.

5.6.5 Counter XC1

An optional counter, XC1, is defined for use in determining that the connection has been cut-off. It is incremented when the DTE or DCE is given the right to transmit or seizes the right to transmit and has not received a frame or at least five continuous flags. This counter is decremented if its value is greater than zero and the flags or a frame have been received. If the counter reaches a certain level, the switched call is assumed to be cut-off. The minimum value of this cut-off level is four.

5.6.6 State diagram and descriptions

The state diagram shown in Figure 13 describes the procedure used by the HDTM for controlling the right to transmit. The number in each ellipse is the state reference number. The transitions are caused by interactions between LAPB and the HDTM, interactions between the HDTM and the physical layer, signals from the remote HDTM, and timer expiration within the HDTM.

5.6.7 State definitions expressed in terms applicable to a modem interface

Taking the use of the HDTM with a V-series modem interface as an example, the following expressions of the state definitions can be made:

5.6.7.1 Idle state (state 0)

Circuit 107 is OFF. Circuit 105 is OFF. LAPB is inhibited from sending frames and is disconnected from circuit 103.

5.6.7.2 Half-duplex sending state (state 1)

Circuit 105, circuit 106 and circuit 107 are ON. LAPB is connected to circuit 103 and enabled to send frames.

5.6.7.3 Wait for receiving state (state 2)

Circuit 107 is ON, circuit 105 is OFF. LAPB is inhibited from sending frames and disconnected from circuit 103, which is held in the binary 1 condition. Timer XT1 is running.

5.6.7.4 Half-duplex receiving state (state 3)

Circuit 107 is ON, circuit 105 is OFF. LAPB is inhibited from sending frames and disconnected from circuit 103, which is held in the binary 1 condition.

5.6.7.5 Wait for sending state (state 4)

Circuit 105 and circuit 107 are ON, and circuit 106 is OFF. LAPB is connected to circuit 103 but is inhibited from sending frames.

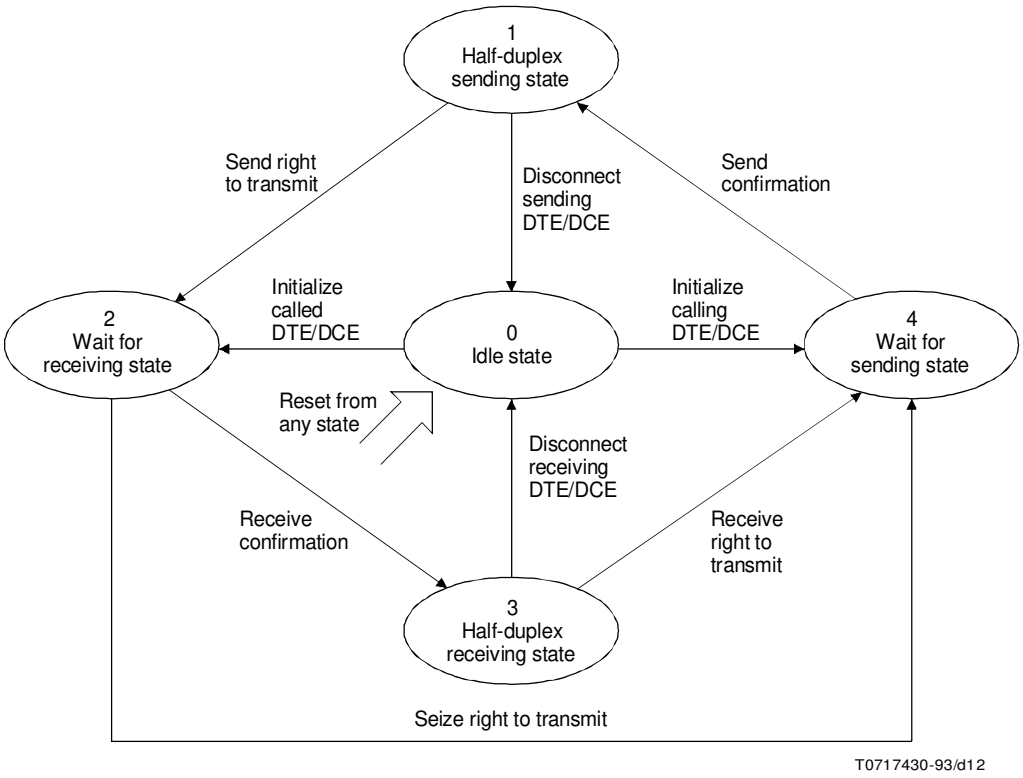


FIGURE 13/X.32

State diagram

5.6.8 Table of transitions between states expressed in terms applicable to a modem interface

Continuing the example, Table 5 shows, in terms of a V-series modem interface, the events that cause a state transition and the resulting action(s).

5.6.9 Turnaround checkpoint retransmission

In order to improve the efficiency of the LAPB procedure when using half-duplex circuits, it is highly recommended that an additional mechanism be implemented. It is called "turnaround checkpoint retransmission" and is described as follows:

– before a DTE/DCE gives the turn back (i.e. goes from state 1 to state 2 of Figure 13), it acknowledges all frames that were received and accepted during the time it was in state 3 (*Half-duplex receiving* state) before it got the turn;

– if a DTE/DCE gets the turn (i.e. transition from state 3 to state 4) or takes the turn (i.e. transition from state 2 to state 4 of Figure 13) then this DTE/DCE will first retransmit all I-frames that have not been acknowledged.

5.6.10 Interworking with a DTE/DCE without turnaround checkpoint additional procedures

The above procedure allows for interworking between a DTE/DCE having implemented the above additional mechanisms and a DCE/DTE not having implemented them.

TABLE 5/X.32

Description of state transitions in terms of a V-series modem interface

Present state	Transition name		New state
	Event	Action	
0	Initialize calling DTE/DCE		4
Idle state	Calling DTE/DCE: circuit 107 ON	Turn circuit 105 ON. Connect LAPB to circuit 103	Wait for sending state
0	Initialize called DTE/DCE		2
Idle state	Called DTE/DCE: circuit 107 ON	Start timer XT1.	Wait for receiving state
1	Send right to transmit		2
Half-duplex sending state	Transmission concluded (see Note 1)	Inhibit sending of LAPB frames. Disconnect LAPB from circuit 103. Hold circuit 103 in the binary 1 condition. Turn circuit 105 OFF (see Note 2). Start timer XT1.	Wait for receiving state
1	Disconnect sending DTE/DCE		0
Half-duplex sending state	LAPB has entered a disconnected phase	Turn circuits 105 and 107 OFF.	Idle state
2	Receive confirmation		3
Wait for receiving state	Reception of a flag or detection of carrier ON (see Note 3)	Stop timer XT1.	Half-duplex receiving state
2	Seize right to transmit		4
Wait for receiving state	Expiry of timer XT1	Turn circuit 105 ON. Release circuit 103 from binary 1 condition. Connect LAPB to circuit 103	Wait for sending state
3	Receive right to transmit		4
Half-duplex receiving state	Reception of 15 continuous 1 bits or detection of carrier OFF (see Notes 4 and 5)	Turn circuit 105 ON. Release circuit 103 from binary 1 condition. Connect LAPB to circuit 103.	Wait for sending state
3	Disconnect receiving DTE/DCE		0
Half-duplex receiving state	LAPB has entered a disconnected phase	Turn circuit 107 OFF.	Idle state
4	Send confirmation		1
Wait for sending state	Circuit 106 ON	Enable sending of LAPB frames (see Note 6)	Half-duplex sending state

TABLE 5/X.32 *(end)*

Description of state transitions in terms of a V-series modem interface

Present state	Transition name		New state
	Event	Action	
Any	Reset from any state		0
	Circuit 107 OFF	Inhibit sending of LAPB frames. (Turn circuit 105 OFF)	Idle state

NOTES

1 The HDTM may determine that a transmission by the LAPB module has been concluded by either of the following:

- counting a sequence of continuous flags on circuit 103 while in state 1;
- a time-out;
- a signal from another source, e.g. from a higher level.

However, if no frame is transmitted while in state 1, not less than five continuous flags shall be sent in state 1 before entry into state 2.

2 It is recommended that circuit 105 not be turned OFF until 15 bit times after the binary 1 condition is established on circuit 103. This will assure transmission of an idle sequence to the remote DTE/DCE.

3 It is understood that circuit 109 will go ON. Entry into state 3 may be dependent on this condition as an implementation option.

4 It is recognized that whether or not an idle channel state condition sequence is sent by the remote DTE/DCE, the DTE/DCE will detect an idle channel state condition after circuit 109 goes OFF, since according to 4.3/V.24, this will hold circuit 104 in the binary 1 condition.

5 It is understood that circuit 109 will go OFF. Entry into state 4 may be made dependent on this OFF condition as an implementation option.

6 It is necessary to ensure that at least one full flag is transmitted after circuit 106 comes ON. This flag may be the opening flag of the first frame.

In order to improve the efficiency of the procedure in such a case:

- a DTE/DCE having implemented the *turnaround checkpoint retransmission* is advised to replace the last RR frame of the transmit sequence, if any, by a REJ frame carrying the appropriate N(R).

- a DTE/DCE not having implemented *turnaround checkpoint retransmission* nevertheless acknowledges during a turn all frames which have been correctly received during the previous turn.

6 Packet layer

6.1 Scope and field of application

The formats and the procedures at the packet layer shall be in accordance with 3/X.25, 4/X.25, 5/X.25, 6/X.25 and 7/X.25 with additions as noted in this clause and in 7 of this Recommendation. The disconnected condition of the link layer is recognized as the same condition as an out-of-order condition defined in 4.6.2/X.25. (Definition of an out-of-order condition.) Therefore after the link layer establishment, the DCE will send a restart indication packet with the cause "Network operational" to the local DTE.

If identification and authentication are done at the packet layer, identification and authentication of the identity of both the DTE and DCE will cease to apply when a failure on the physical layer and/or link layer is detected.

Some DTEs may choose to use the registration procedure for *on-line facility registration* immediately after the switched access path has been established and the link has been set up.

6.2 Identification and authentication of the DTE using the NUI selection facility in call set-up packets

The *NUI selection* facility in *call set-up* packets can be used for DTE identification on a per virtual call basis. It can also be used in addition to one of the prior-to-virtual-call DTE identification methods. This NUI identification remains in effect for the lifetime of the virtual call and is independent of any previous NUI identification on the interface. Subsequent call requests on the switched access path will either revert to the prior DTE service on the interface or receive a DTE service associated with a NUI.

The *NUI selection* facility parameter may contain as the *DTE identity* either a user identifier plus a password assigned by the network to the DTE, or only a password assigned by the network to the DTE. The formats of the user identifier and the password are national matters. The following cases describe the operation of the *NUI selection* facility:

1) When a *DTE identity* has been established using a prior-to-virtual-call DTE identification method, the *NUI selection* facility may be used if the *NUI subscription* and/or the *NUI override* facilities are set by the network. In this case, the *NUI selection* facility applies conforming to the procedures described in Recommendation X.25 (see 6.21/X.25).

2) When a *DTE identity* has not been established using a prior-to-virtual-call identification method and the *NUI selection* facility is used, the *identified DTE* service (see 3.4) is selected (when supported by the network). Two subcases are possible:

   a) *NUI override* facility is set by the network when a *call request* packet containing a valid NUI is sent, the features subscribed to by the DTE identified by that NUI and associated with that NUI apply to the virtual call;

   b) *NUI override* facility is not set by the network when a *call request* packet containing a valid NUI is sent, the default *X.25 subscription set* applies to the virtual call.

In both cases 2a) and 2b), the NUI remains in effect only for the lifetime of the virtual call.

7 X.32 procedures, formats and facilities

7.1 Identification protocol

7.1.1 Protocol elements

The identification protocol is for exchanging identification and authentication information in one or more pairs of messages. The two parties involved in this protocol are called the questioning party and the challenged party.

Two security options are defined: the basic option described as *security grade 1* and an enhanced option described as *security grade 2*. The identification and authentication information are encoded in the following protocol elements:

a) The identity element (ID) is a string of octets representing the DTE or DCE identity (see 2.2.1 and 2.2.2, respectively) of the challenged party.

b) The signature element (SIG) of the identity is a string of associated with the identity and used for authentication of the identity. It is assigned for a period of time by the authority that assigns the identity and may be changed from time to time. For example, the SIG may be a password or the result of an encryption process applied to the identity element (ID) of the challenged party.

c) The random number element (RAND) is a string of octets which is unpredictable for each identification exchange. It is used only in the security grade 2 option.

d) The signed response element (SRES) of the challenged party is the reply to the RAND protocol element by the questioning party. It is used only in the security grade 2 option.

e) The diagnostic element (DIAG) is the result of the identification process and is transmitted by the questioning party at the end of the process.

The format of these elements is shown in 7.3.

The sizes of values of the identity, signature and random number elements are a national matter and depend on a number of factors including:

a) whether the authentication is of DTE identity or DCE identity;

b) the grade of security;

c) the method of identification;

d) the possibilities of future improvements in computational techniques; and

e) whether the PSPDN directly assigns DTE identities or adopts, through pre-arrangement, the DTE identities assigned by the PSN or another authority.

7.1.2 Identification protocol procedure

The first message of a pair is transmitted by the challenged party. The second message of the pair is transmitted by the questioning party. Security grade 1 provides a single exchange of elements ID [, SIG] and DIAG, whereas security grade 2 uses an additional exchange of RAND and SRES elements to provide a greater degree of security.

NOTE – In both security grades 1 and 2, SIG may be omitted if not required by the questioning party. If it is not required, its presence is not considered in error.

The identification protocol elements are passed between the parties in a sequence of XID command frames.

The identification protocol may be used for DTE identification simultaneously but independently of its use for DCE identification. When this occurs, the XID frame may carry elements for both directions of identification simultaneously.

The identification established using the identification protocol applies for the duration of the switched access. That is, once the DIAG element indicating acceptance of the DTE/DCE identity has been sent, the switched access path must be disconnected before another attempt to use the identification protocol to identify that challenged party can be made.

If the identification protocol is not successful, that is, the DIAG element indicates refusal of the DTE/DCE identity, the questioning party should disconnect the switched path. In the case of security grade 1, a network may allow up to three retries of the identification protocol (i.e. the DIAG element indicates refusal of the DTE/DCE identity) before the switched access path is disconnected when the network is the questioning party. For security grade 2, only one attempt to perform the identification protocol is permitted when the network is the questioning party.

The actions of the DCE when acting as the challenged or questioning party are further described by the state diagrams and tables in Annex A.

The security grade applied on a particular switched connection is determined by the subscription of the DTE with the Administration. It is not negotiable on a per call basis. Not all networks will offer both security grade options. The use of certain optional features may be restricted to a particular security grade. A positive and secure DTE identification is limited to the security of the switched access path, particularly in dial-out-by-the-PSPDN operation.

In order to avoid situations in which both parties are waiting for the other to identify first, these principles will be followed:

a) Each party should send its identity, if capable and willing, at the earliest opportunity. However, the called party is not required to send its own identity before complete identification of the calling party.

b) If the calling party does not send its identity, the called party has a choice of operating a service not requiring identification or disconnecting the switched connection.

Security grade 1 involves a single pair of messages as shown in Figure 14. First, the challenged party sends its identity (ID) and, if required, its signature (SIG). The questioning party responds with the diagnostic (DIAG).

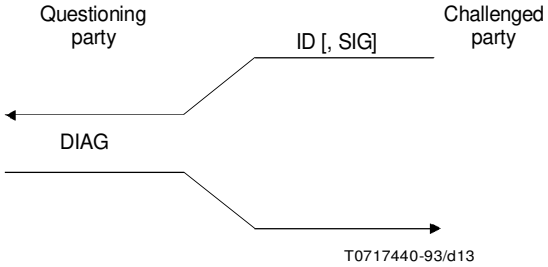


FIGURE 14/X.32

Security grade 1

As shown in Figure 15, security grade 2 involves an additional authentication exchange if the initial response (ID [, SIG]) of the challenged party is valid. If ID is an identity unknown to the questioning party or if the SIG element is required by the questioning party but either it is not present or is inconsistent with the claimed identity, then an error diagnostic (DIAG) is issued and the access path is disconnected. Otherwise, the questioning party will generate and send a random number (RAND) which the challenged party will encrypt and return as its signed response (SRES). The questioning party will then decrypt SRES and, if this operation results in a value identical to RAND, the appropriate diagnostic (DIAG) is sent to the challenged party and the identification process is successfully completed. Otherwise, an error diagnostic (DIAG) is returned and the access path is disconnected.

NOTES

1 It is left for further study whether or not to define, as a mechanism for protecting against specific forms of intrusion, that the value of RAND is odd or even depending on the direction of the switched access call.

2 If the network does not store the public keys of DTEs, the SIG can be used to convey the public key and other information characteristics of the DTE (e.g. indication of security level two is to be used). Private keys of the DTE, if any, are not included in the SIG information. In order to add to the protection, this information can be encrypted via the private key of the network.

7.1.3 Identification protocol formats

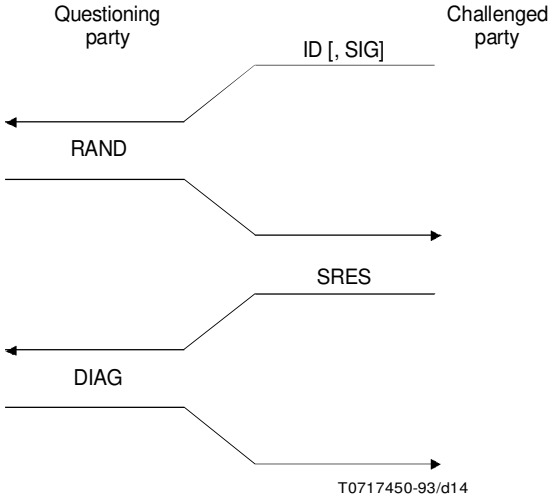
The formats for the identification protocol elements are defined in 7.3 of this Recommendation in accordance with 6/X.25 and 7/X.25.

7.2 Procedures for X.32 optional user facilities

7.2.1 Secure dial-back facility

Networks that implement both the dial-in-by-the-DTE and dial-out-by-the-PSPDN operations may provide, as an optional user facility agreed for a period of time, a dial-back procedure. This facility, if subscribed to, combines the dial-in-by-the-DTE operation with the dial-out-by-the-PSPDN operation to offer additional protection when the identity of the DTE becomes known to the network. This procedure allows, in the *customized* DTE service, a DTE to use the dial-in-by-the-DTE operation, identifies itself, and disconnect. Security is achieved in using the *identity element* of the identification protocol and a dial-out-by-the-PSPDN to the *registered PSN number.* The network uses the dial-out-by-the-PSPDN operation to dial back the DTE using the *registered PSN number.* The DCE identifies itself and the DTE identifies itself again. Some networks may offer the additional feature of limiting the use of the *secure dial-back* facility to specific hours of operation of the DTE.

The grade of security for *secure dial-back* is not negotiable per switched access call. It is one aspect of the identity and its value is set when pre-registering to the authority that defines the identity.



NOTE – The exchange depicted illustrates the case where the initial ID [, SIG] message was valid.

FIGURE 15/X.32

Security grade 2

After the DTE has correctly identified itself to the DCE during dial-in-by-the-DTE, the DCE sends a *request for dial-back confirmed* via the *diagnostic element* of the identification protocol. Then the DTE and network should disconnect the link, if necessary, and then the switched access path as soon as possible. The network should then initiate the dial-back to the DTE as soon as possible by using dial-out-by-the-PSPDN.

If, during the dial-in-by-the-DTE operation, the DCE is aware that it cannot perform the dial-back, the DCE will indicate to the DTE that dial-back is not possible. This indication is given via the *diagnostic element* of the identification protocol.

When the DCE disconnects the switched access path on the dial-in-by-the-DTE it starts DCE timer T15. The DCE then attempts the dial-out-by-the-PSPDN operation as soon as possible. The period of timer T15, at the end of which the DCE abandons the attempt to dial out to the DTE, is a system parameter agreed for a period of time with the Administration.

When the network dials out, the DCE includes a "dial-back indication" to the DTE via the *diagnostic element* of the identification protocol.

If the DTE receives an unsolicited dial-back from the DCE, the switched access path may be disconnected.

NOTE – As some PSTN networks implement *calling party clear,* a PSPDN may wish to restrict dial-back to an outgoing only PSTN port.

7.3 Coding of the identification protocol elements

7.3.1 General

The general principles for coding of the identification protocol elements are the same as the ones specified for the registration field in 7.1/X.25. The statements of 7.1/X.25 concerning facilities do not apply to this clause. The statements of 7.1/X.25 concerning registration elements apply to the identification protocol elements in this clause.

7.3.2 Coding of the identification protocol element code fields

Table 6 gives the list of the identification protocol element codes, the coding for each, and, where applicable, whether this code may be sent by the challenged or the questioning party.

TABLE 6/X.32

Identification protocol element codes

Identification element code	May be sent by		Bits							
	Challenged party	Questioning party	8	7	6	5	4	3	2	1
Identity element	X		1	1	0	0	1	1	0	0
Signature element	X		1	1	0	0	1	1	0	1
Random number element		X	1	1	0	0	1	1	1	0
Signed response element	X		1	1	0	0	1	1	1	1
Diagnostic element		X	0	0	0	0	0	1	1	1

7.3.3 Coding of the identification protocol element parameter fields

7.3.3.1 Identity element

The octet following the code field indicates the length, in octets, of the parameter field. The following octets contain the string of octets composing the identity.

7.3.3.2 Signature element

The octet following the code field indicates the length, in octets, of the parameter field. The following octets contain the string of octets composing the signature.

7.3.3.3 Random number element

The octet following the code field indicates the length, in octets, of the parameter field. The following octets contain the string of octets composing the number wich is the random number element. It is binary coded with bit 8 of the first octet following the parameter length being the high order bit and bit 1 of the last octet being the low order bit. If the number of significant bits of the random number is not octet-aligned, then zeroes precede the most significant bit to make it octet-aligned.

7.3.3.4 Signed response element

The octet following the code field indicates the length, in octets, of the parameter field. The following octets contain the string of octets composing the number which is the signed response. It is binary coded with bit 8 of the first octet following the facility parameter length being the high order bit and bit 1 of the last octet being the low order bit. If the number of significant bits of the signed response is not octet-aligned, then zeroes precede the most significant bit to make it octet-aligned.

7.3.3.5 Diagnostic element

The coding of the parameter field for the *diagnostic element* is shown in Table 7.

TABLE 7/X.32

Coding of the parameter field for the diagnostic element

	Bits							
	8	7	6	5	4	3	2	1
Identification/authentication confirmed	0	1	1	1	1	1	1	1
Identification or authentication failed (Note 1)								
– general	1	0	0	0	0	0	0	0
– additional	1	X	X	X	X	X	X	X
Network congestion (Note 2)	0	0	0	0	0	1	0	1
Identification in use (Note 3)	0	0	0	1	0	1	1	1
Dial-back indication (Note 4)	0	0	1	1	1	1	1	1
Network congestion for dial-back (Note 4)	0	0	0	1	1	0	1	1
Request for dial-back confirmed (Note 4)	0	0	0	1	1	1	1	1

NOTES

1 Bits 7 to 1 are for maintenance purposes and are a national matter. Complete specification and provision of this information to a user represents a possible compromise of security by providing details of authentication failure.

2 Replacement of this *call progress* signal is for further study in close liaison with the revision of Recommendation X.96.

3 Whether multiple switched connections can be simultaneously active using the same *DTE identity* is for further study.

4 Used only in conjunction with the *secure dial-back* facility (see 7.2.1).

7.4 Security grade 2 method

The authentication method in security grade 2 provides for the use of encryption to prevent unauthorized access subject to the constraints of unit cost and computation time. One example of a public key encryption technique which could be used for this purpose is given in Appendix II. The selection and use of security grade 2 algorithms is a national matter.

NOTE – Further study, in close cooperation with ISO/TC 97/SC20, will define the characteristics and length constraints of the various numbers and parameters to be used in security grade 2 algorithms. The definition of the parameters of an algorithm should strike a balance between the cost and the complexity of the algorithm, and the value of that which is protected. The goal is to make the cost of breaking the code exceed the cost of obtaining the network resources by authorized means.

7.5 DCE timers T14 and T14 *bis*

7.5.1 DCE timer T14

The DCE may support a timer T14, the value of which should be made known to the DTE.

At the expiration of timer T14, the DCE will disconnect the link, if connected, then the switched access path.

Timer T14 is started whenever a switched access path is established. Timer T14 is stopped when either the *DTE identity* is established or a virtual call(s) is established which is not to be charged to the local DTE. In the latter case, timer T14 will be restarted when no assigned logical channels are active.

The relationships of timer T14 to the different methods of DTE identification are illustrated in Appendix III.

The period of timer T14 shall be network dependent.

7.5.2 DCE timer T14 *bis*

The DCE may support a timer T14 *bis*, the value of which should be made known to the DTE.

At the expiration of timer T14 *bis*, the DCE will disconnect the link, if connected, then the switched access path.

NOTE – The T14 *bis* timer does not apply to the per-virtual-call DTE identification by means of NUI selection facility, or provided by the public switched network.

Timer T14 *bis* is started whenever a DTE identity has been established or when there are no virtual calls at the completion of clearing procedures. Timer T14 *bis* is stopped when a virtual call is established.

The relationships of timer T14 *bis* to the different methods of DTE identification are illustrated in Appendix III.

The period of timer T14 *bis* shall be network dependent.

7.6 DCE timer T15

Timer T15 is used in conjunction with the secure dial-back facility (see 7.2.1).

The period of timer T15 is left for further study.

Annex A

(to Recommendation X.32)

Actions taken by the DCE in the roles of questioning and challenged parties for security grade 1 and security grade 2 identifications

(This annex forms an integral part of this Recommendation)

A.1 Introduction

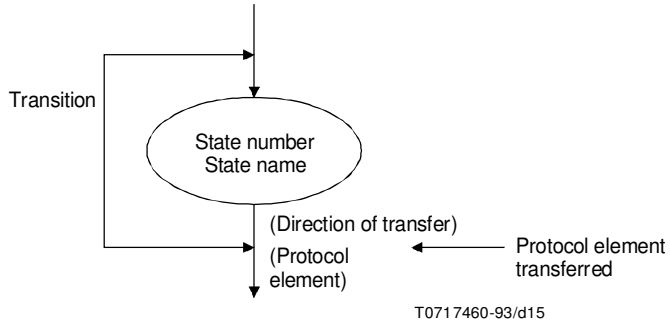
This annex specifies the actions taken by the DCE when it acts as the questioning and challenged parties for security grade 1 and security grade 2 identifications. When performing the identification procedure described in 7.1.2, the DCE shall act as described in this annex.

NOTE – As the identification protocol is symmetrical and should be used by the DTE in the same manner as the DCE, the actions of the DTE should correspond directly to the actions defined for the DCE.

The identification protocol is presented as a succession of state diagrams and corresponding tables.

In this annex, a DIAG element is considered is positive when its parameter field means *identification/authentication confirmed, request for dial-back confirmed,* or *dial-back indicator* (see 7.3.3.5). It is considered as negative in other cases.

A.1.1 Symbol definition of state diagrams



NOTES

1 Each state is represented by an ellipse wherein the state name and number are indicated.

2 Each state transition is represented by an arrow. The direction of transfer and the protocol element that has been transferred are indicated beside that arrow.

A.1.2 Definition of actions

In each table, the actions taken by the DCE as the questioning party or the challenged party are indicated in the following way:

NORMAL	Normal event; protocol elements received are handled as described in 7.1.2.
DISCARD	Received message is discarded.
RAND	RAND transmitted.
Positive DIAG	Positive DIAG transmitted.
Negative DIAG	Negative DIAG transmitted.
ID [, SIG]	ID [, SIG] transmitted.
SRES	SRES transmitted.

Each entry in the tables in this annex gives, first, the action taken, if any, then an arrow indicating the transition, and finally, the state that the DCE as the questioning or challenged party will enter.

A.2 Security grade 1 identification

A.2.1 DCE acting as the questioning party

The DCE acts as the questioning party for security grade 1 when it offers *identified* or *customized* DTE service via the XID DTE identification method with grade 1 authentication. Four states are defined for describing the procedures the DCE uses:

a) *q11 – Waiting for ID [, SIG] (grade 1)*

This is the initial state of the DTE identification process. It is entered after the switched connection is established. In this state, the DCE expects to receive the ID (and possibly SIG) element(s) from the DTE. If the DCE allows retrying the identification protocol, this state is also entered when a DTE identification attempt has failed and the limit of retries has not been exhausted.

b) *q12 – Evaluating ID [, SIG] (grade 1)*

In this state, the DCE determines whether or not the DTE identity that was presented in the ID (and possibly SIG) element(s) is acceptable. The result is the transmission by the DCE to the DTE of the DIAG element, which has as its value the success or not of the acceptability evaluation.

c) *q13 – DTE identification successful (grade 1)*

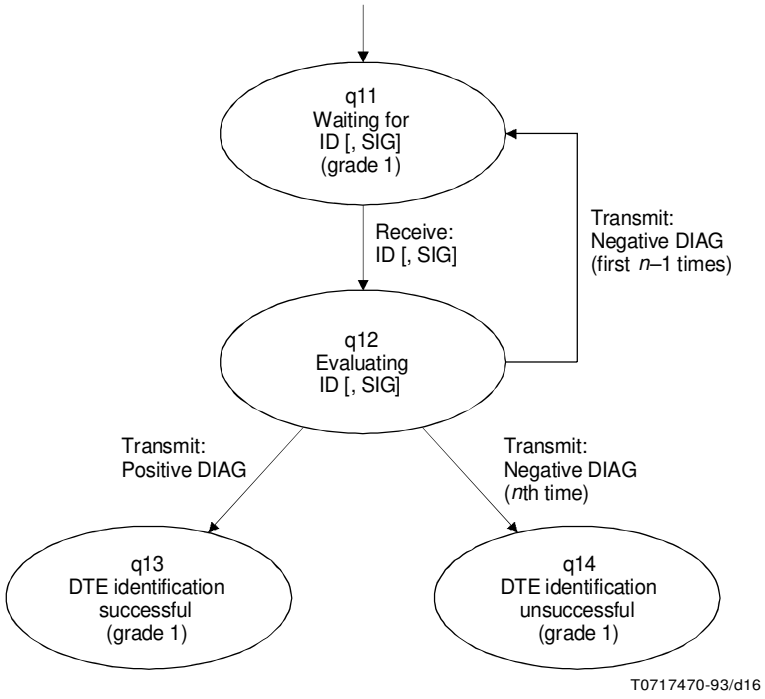
In this state, the DCE provides the identified or customized DTE service to the identified DTE. The DCE remains in this state until the switched connection is disconnected.

d) *q14 – DTE identification unsuccessful (grade 1)*

In this state, the DCE does not provide the identified or customized DTE service (unless NUI is used on a per virtual call basis for the identified DTE service) but may provide the non-identified DTE service if it is supported. The DCE enters this state, when the last DTE identification attempt allowed by the retry limit has failed. The DCE remains in this state until the switched connection is disconnected.

Figure A.1 provides the state diagram for the DCE acting as the questioning party in the case of security grade 1 identification.

The actions to be taken by the DCE acting as the questioning party for security grade 1 identification, when one of the listed events occurs, are indicated in Table A.1.



n Number of DTE identification attempts permitted

FIGURE A.1/X.32

Diagram of states for DCE acting as questioning party for security grade 1 identification

TABLE A.1/X.32

Actions taken by the DCE as the questioning party (security grade 1)

State of the DCE acting as the questioning party / Protocol element received by the DCE or decision by the DCE	q11 Waiting for ID [, SIG] (grade 1)	q12 Evaluating ID [, SIG] (grade 1)	q13 DTE Identification successful (grade 1)	q14 DTE Identification unsuccessful (grade 1) (see Note 1)
ID [, SIG]	NORMAL → q12	DISCARD → q12	DISCARD → q13	DISCARD → q14
DCE checking of the ID [, SIG] is complete	Not applicable	Positive DIAG → q13 or negative DIAG → q14 or → q11 (see Note 2)	Not applicable	Not applicable

NOTES

1 When in this state, the DCE should disconnect the switched access path when it is sure that the DIAG element has been received by the challenged party or the challenged party is out-of-order.

2 Depending on whether or not ID and/or SIG are recognized as correct by the DCE. When negative DIAG, go to q11 until the retry limit has been reached.

A.2.2 DCE acting as the challenged party

The DCE acts as the challenged party for security grade 1 when it identifies itself to the DTE via the XID DCE identification method with grade 1 authentication. Four states are defined for describing the procedures the DCE uses:

a) *c11 – Initial challenged (grade 1)*

This is the initial state of the DCE identification process. It is entered after the switched connection is established. In this state, the DCE transmits the ID (and possibly SIG) element(s) to the DTE.

b) *c12 – Waiting for DIAG (grade 1)*

In this state, the DCE expects to receive the DIAG element which has as its value the acceptability or not of the DCE identity.

c) *c13 – DCE Identification successful (grade 1)*

In this state, the DCE has completed its identification successfully. The DCE remains in this state until the switched connection is disconnected.

d) *c14 – DCE Identification unsuccessful (grade 1)*

The DCE enters this state when the DCE identification attempt has failed. The DCE remains in this state until the switched connection is disconnected.

Figure A.2 provides the state diagram for the DCE acting as the challenged party in the case of security grade 1 identification.

The actions to be taken by the DCE as the challenged party for security grade 1 identification, when one of the listed events occurs, are indicated in Table A.2.

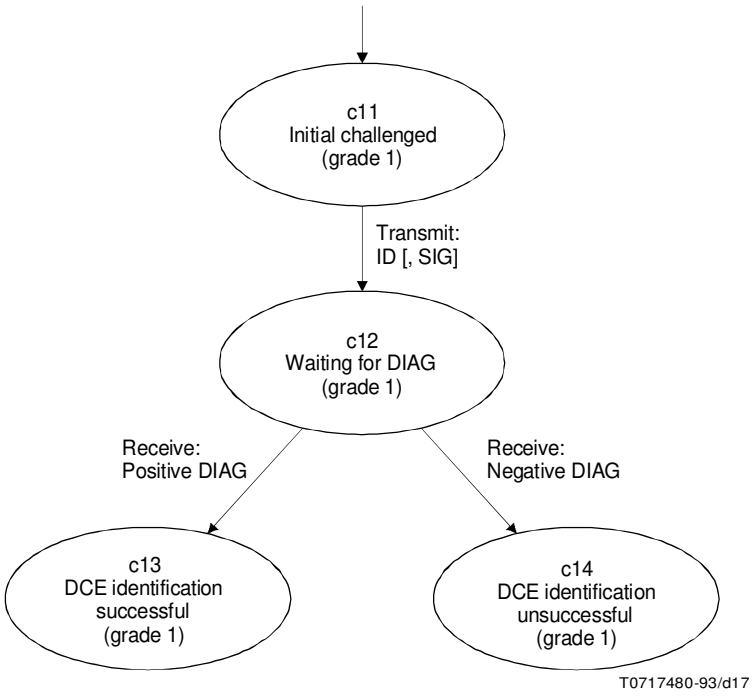


FIGURE A.2/X.32

Diagram of states for DCE acting as challenged party for security grade 1 identification

TABLE A.2/X.32

Actions taken by the DCE as the challenged party (security grade 1)

State of the DCE acting as the challenged party Protocol element received by the DCE or decision by the DCE	c11 Initial challenged (grade 1)	c12 Waiting for DIAG (grade 1)	c13 Identification successful (grade 1)	c14 Identification unsuccessful (grade 1) (see Note 1)
DCE decides it wants to be identified	ID [, SIG] → c12	Not applicable	Not applicable	Not applicable
Positive DIAG	NORMAL → c13 or c14 (see Note 2)	NORMAL → c13	DISCARD → q13	DISCARD → q14
Negative DIAG	NORMAL → c14	NORMAL → c14	DISCARD → q13	DISCARD → q14

NOTES

1 In this state, the DCE shall disconnect the switched access path.

2 c13 or c14 depending on whether or not the DCE wants to be identified.

A.3 Security grade 2 identification

A.3.1 DCE acting as the questioning party

The DCE acts as the questioning party for security grade 2 when it offers *identified* or *customized* DTE service via the XID DTE identification method with grade 2 authentication. Six states are defined for describing the procedures the DCE uses:

a) *q21 – Waiting for ID [, SIG] (grade 2)*

This is the initial state of the DTE identification process. It is entered after the switched connection is established. In this state, the DCE expects to receive the ID (and possibly SIG) elements) from the DTE.

b) *q22 – Evaluating ID [, SIG] (grade 2)*

In this state, the DCE begins determining whether or not the DTE identity that was presented in the ID (and possibly SIG) element(s) is acceptable. If the DTE identity is acceptable or the acceptability is not fully determined in this state, the DCE generates the value for the RAND element and transmits it to the the DTE. If the DTE identity is unacceptable, the DCE transmits to the DTE the DIAG element with a negative value.

c) *q23 – Waiting for SRES*

In this state, the DCE expects to receive SRES element from the DTE. The DCE may continue to evaluate the ID (and possibly SIG) element(s) and, if the DTE identity is unacceptable, the DCE transmits to the DTE the DIAG element with a negative value.

d) *q24 – Evaluating SRE*S

In this state, the DCE determines if the value presented in the SRES element is correct for the DTE identity. If the evaluation of the ID [, SIG] element(s) has not already been completed, it is completed in this state. The results of the SRES check (and the last of the ID [, SIG] check) is transmitted by the DCE to the DTE as the value of the DIAG element.

e) *q25 – DTE identification successful (grade 2)*

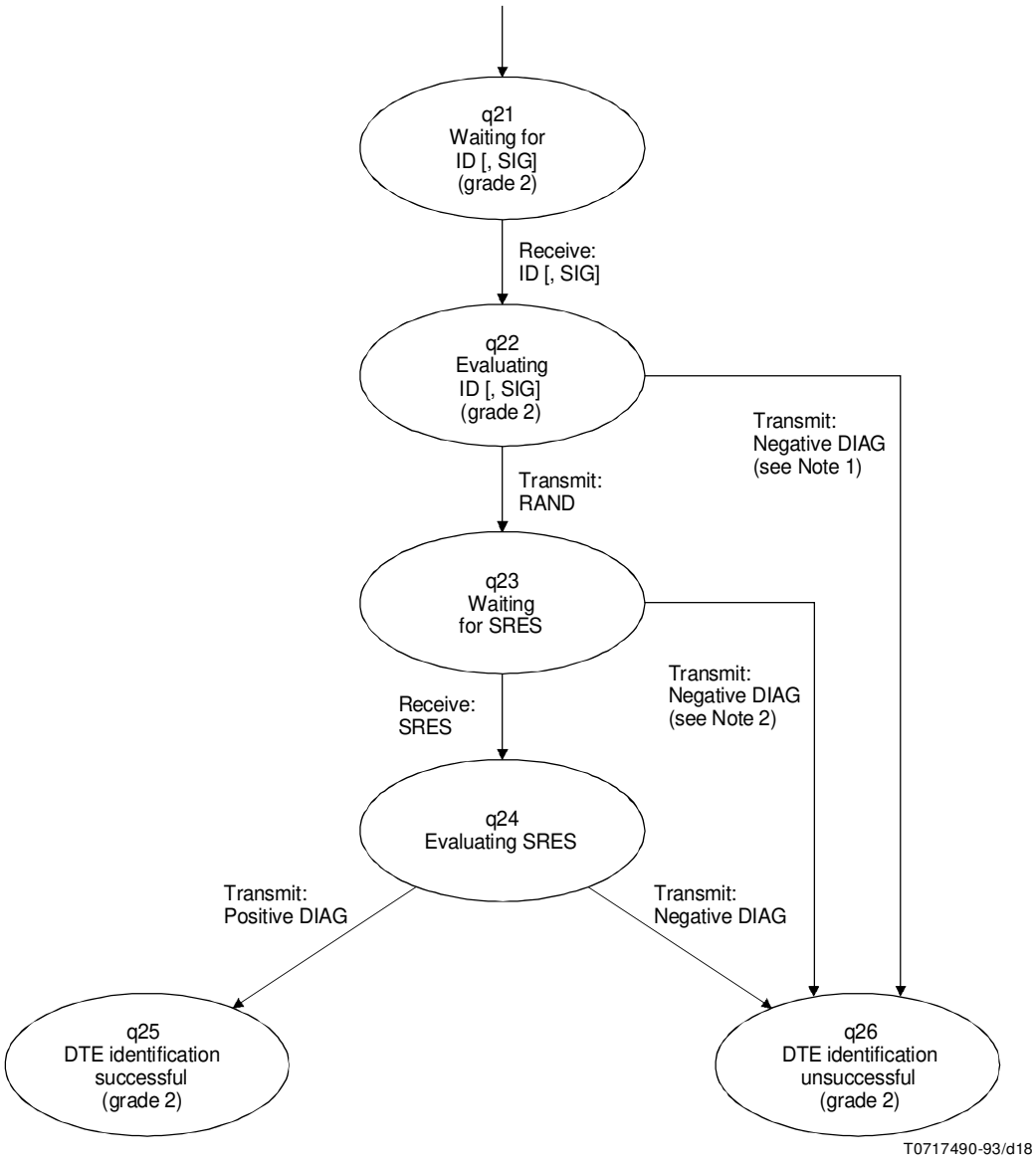
In this state, the DCE provides the identified or customized DTE service to the identified DTE. The DCE remains in this state until the switched connection is disconnected.

f) *q26 – DTE identification unsuccessful (grade 2)*

In this state, the DCE does not provide the identified or customized DTE service (unless NUI is used on a per virtual call basis for the identified DTE service) but may provide the non-identified DTE service if it is supported. The DCE remains in this state until the suitched connection is disconnected.

Figure A.3 provides a state diagran for the DCE acting as the questioning party in case of security grade 2 identification.

The actions to be taken by the DCE as the questioning party for security grade 2 identification, when one of the listed events occurs, are indicated in Table A.3.



NOTES

1 If an error in the ID and/or SIG is found before RAND is transmitted.

2 If an error in the ID and/or SIG is found after RAND is transmitted.

FIGURE A.3/X.32

Diagram of states for DCE acting as the questioning party for security grade 2 identification

TABLE A.3/X.32

Actions taken by the DCE as the questioning party (security grade 2)

State of the DCE acting as the questioning party / Protocol element received by the DCE or decision by the DCE	q21 Waiting for ID [, SIG] (grade 2)	q22 Evaluating ID [, SIG] (grade 2)	q23 Waiting for SRES	q24 Evaluating SRES	q25 DTE identification successful (grade 2)	q26 DTE identification unsuccessful (grade 2) (see Note 1)
ID [, SIG]	NORMAL → q22	DISCARD → q22	DISCARD → q23	DISCARD → q24	DISCARD → q25	DISCARD → q26
At least initial DCE checking of the ID [, SIG] is complete	Not applicable	RAND → q23 or Negative DIAG → q26 (see Note 2)	Not applicable	Not applicable	Not applicable	Not applicable
Further DCE checking (if any) of the ID [, SIG] is complete	Not applicable	Not applicable	NORMAL → q23 or Negative DIAG → q26 (see Note 3)	Not applicable	Not applicable	Not applicable
SRES	Negative DIAG → q26	Negative DIAG → q26	NORMAL → q24	DISCARD → q24	DISCARD → q25	DISCARD → q26
DCE checking of the SRES is complete	Not applicable	Not applicable	Not applicable	Positive DIAG → q25 or Negative DIAG → q26 (see Note 4)	Not applicable	Not applicable

NOTES

1 When in this state, the DCE should disconnect the switched access path when it is sure that the DIAG element has been received by the challenged party, or the challenged party is out-of-order.

2 As negative DIAG is sent if the DCE has detected ID [, SIG] as incorrect. RAND is sent if the DCE has detected ID [, SIG] as correct or if it has not yet checked ID [, SIG].

3 After having transmitted RAND, if the DCE detects that the ID [, SIG] received when in state q2l was incorrect, it transmits a negative DIAG and goes into state q26. Otherwise, the DCE continues with the normal process of waiting to receive the SRES element.

4 q25 or q26 depending on whether or not the SRES is recognized as correct by the DCE.

A.3.2 DCE acting as the challenged party

The DCE acts as the challenged party for security grade 2 when it identifies itself to the DTE via the XID DCE identification method with grade 2 authentication. Six states are defined for describing the procedures the DCE uses:

a) *c21 – Initial challenged (grade 2)*

This is the initial state of the DCE identification process. It is entered after the switched connection is established. In this state, the DCE transmits the ID (and possibly SIG) element(s) to the DTE.

b) *c22 – Waiting for RAND*

In this state, the DCE expects to receive, the RAND element. If the ID (and possible SIG) are not acceptable to the DTE, the DCE may receive the DIAG element with a negative value.

c) *c23 – Calculating SRES*

Using the value of the RAND element, the DCE calculates the value for the SRES element and transmits it to the DTE. If the DTE has continued to evaluate the ID (and possibly SIG) and determined that it is not acceptable, the DCE may receive the DIAG element with a negative value.

d) *c24 – Waiting for DIAG (grade 2)*

In this state, the DCE expects to receive the DIAG element which has as its value the acceptability or not of the DCE identity and SRES value.

e) *c25 – DCE identification successful (grade 2)*

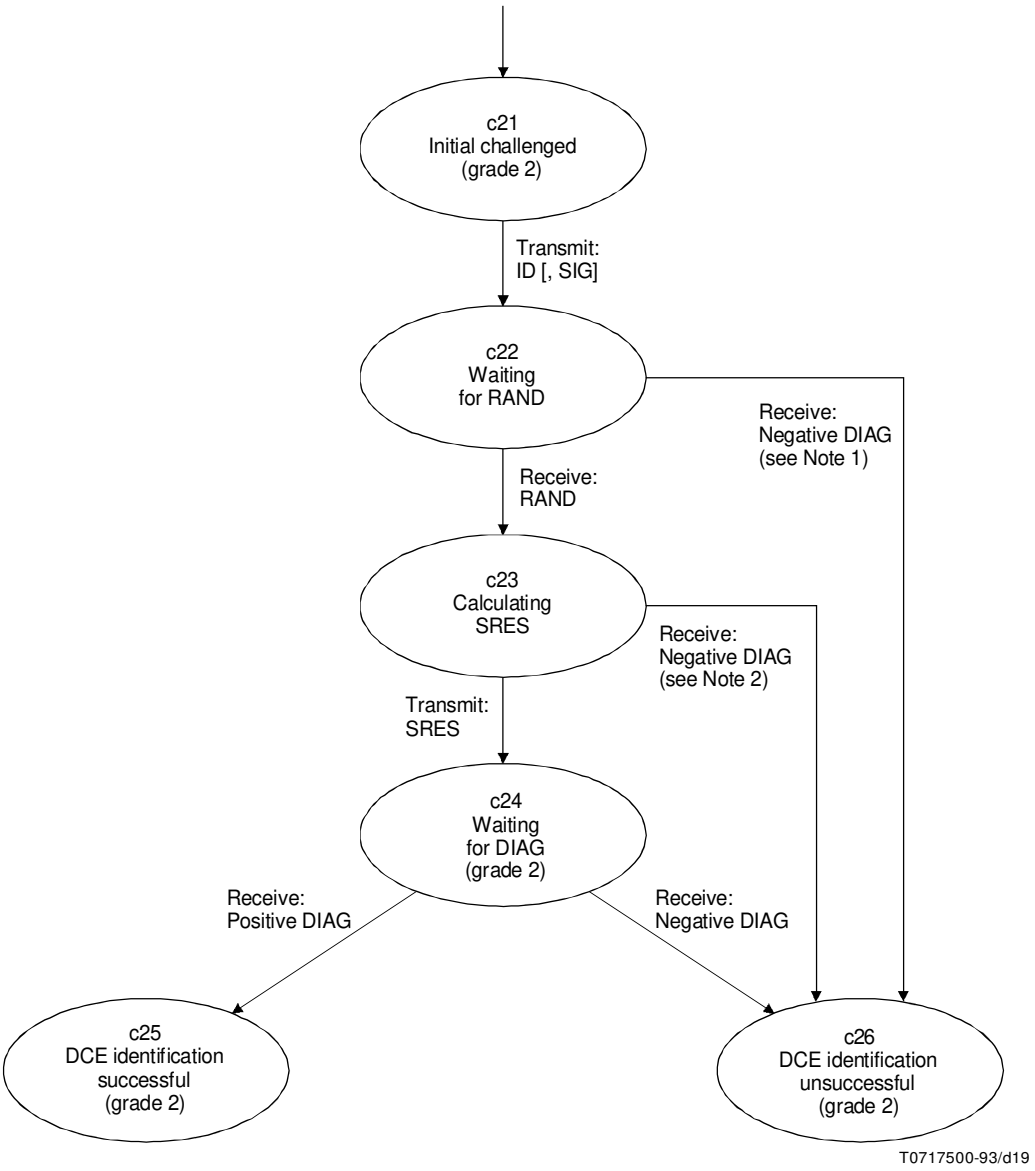
In this state, the DCE has completed its identification successfully. The DCE remains in this state until the switched connection is disconnected.

f) *c26 – DCE identification unsuccessful (grade 2*)

The DCE enters this state when the DCE identification attempt has failed. The DCE remains in this state until the switched connection is disconnected.

Figure A.4 provides a state diagram for the DCE acting as the challenging party in case of security grade 2 identification.

The actions to be taken by the DCE for security grade 2 identification, when one of the listed events occurs, are indicated in Table A.4



NOTES

1 If an error in the ID and/or SIG is found before RAND is transmitted.

2 If an error in the ID and/or SIG is found after RAND is transmitted.

FIGURE A.4/X.32

Diagram of states for DCE acting as the challenged party for security grade 2 identification

TABLE A.4/X.32

Actions taken by the DCE as the challenged party (security grade 2)

State of the DCE acting as the challenged party / Protocol element received by the DCE or decision by the DCE	c21 Initial challenged (grade 2)	c22 Waiting for RAND	c23 Calculating SRES	c24 Waiting for DIAG (grade 2)	c25 DCE identification successful (grade 2)	c26 DCE identification unsuccessful (grade 2) (see Note 1)
DCE decides it wants to be identified	ID [, SIG] → c22	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
RAND	DISCARD → c26	NORMAL → c23	DISCARD → c23	DISCARD → c24	DISCARD → c25	DISCARD → c26
DCE calculation of SRES from RAND is complete	Not applicable	Not applicable	SRES → c24	Not applicable	Not applicable	Not applicable
Positive DIAG	NORMAL → c26 or c25 (see Note 2)	NORMAL → c25 or c26 (see Note 2)	DISCARD → c26	NORMAL → c25	DISCARD → c25	DISCARD → c26
Negative DIAG	NORMAL → c26	NORMAL → c26	NORMAL → c26	NORMAL → c26	DISCARD → c25	DISCARD → c26

NOTES

1 In this state, the DCE shall disconnect the switched access path.

2 c26 or c25 respectively depending on whether or not the DCE wants to be identified.

Annex B

(to Recommendation X.32)

Abbreviations

(This annex forms an integral part of this Recommendation)

For the purpose of this Recommendation the following abbreviations are used:

ADM	Asynchronous disconnected mode
AVAIL-BAS	Available on all networks
AVAIL-NS	Available and selected by the network
AVAIL-OPT	Available on some networks
AVAIL-RQ	Available on some networks and must be requested
BA	Class of HDLC
CSPDN	Circuit switched public data network

CUSTOM	Customized
DCE	Data circuit-terminating equipment
DIAG	Diagnostic element
DISC	Disconnect
DM	Disconnected mode
DNIC	Data network identification code
DSE	Data switching equipment
DTE	Data terminal equipment
FI	Format identifier
HDLC	High-level data link control
HDTM	Half-duplex transmission module
ID	Identity element
ISDN	Integrated services digital network
ISO	International organization for standardization
k	Number of outstanding I frames
LAPB	Link access procedure B
LAPX	Link access procedure - Half-duplex
MT...	Parameter...
N...	Parameter...
ND	Network default
NN	National number
NTN	Network terminal number
NUI	Network user identification
PDN	Public data network
PSN	Public switched network
PSPDN	Packet switched public data network
PSTN	Public switched telephone network
RAND	Random number element
REJ	Reject
ROA	Recognized operating agency
RR	Receive ready
RSA	Rivest, Shamir, Adleman algorithm
SABM	Set asynchronous balanced mode
SABME	Set asynchronous balanced mode extended
SIG	Signature element
SRES	Signed response element
TCC	Telephone country code
T...	Timer...
UA	Unnumbered acknowledge

UTC	Coordinated universal time
XC	Counter...
XID	Exchange identification (Unnumbered Format)
XT...	Timer...

Appendix I

(to Recommendation X.32)

Implementation of LAPX

(This appendix does not form an integral part of this Recommendation)

I.1 Introduction

Considerations are given here for defining the signals needed between the HDTM and the LAPB and physical layer modules in implementing LAPX.

I.2 Control and status functions

The following logical functions describe interactions between LAPB and the HDTM:

– C*ontrol [TERM]*

LAPB has entered the disconnected phase.

– *Control [CONCLUDE]*

LAPB has finished transmitting one or more frames.

– *Status [OP-T]*

Enable LAPB to send frames.

– *Status [INOP-T]*

Inhibit LAPB from sending frames.

If the idle channel state condition detection mechanism of LAPB is not disabled, then the HDTM needs to protect LAPB from the use of idle channel state condition in turning around the line. This protection is done by having the HDTM present constant flags to LAPB except in the *half-duplex receiving* state (state 3). It may be desirable to define additional logical functions in doing this.

The following logical functions describe interactions between the HDTM and the physical layer:

– *Control [SEIZE]*

The HDTM has stopped waiting for data to be received and is waiting to transmit date.

– *Control [RELEASE]*

The HDTM has stopped sending data and is requesting the physical layer to release the right to transmit.

– *Control [DISCON]*

The HDTM is requesting the physical layer to disconnect the physical connection because LAPB is disconnected.

– *Status [CALLING]*

The physical connection originated by this DTE/DCE is established.

– *Status [CALLED]*

The physical connection originated by the other DTE/DCE is established.

– *Status [UNCON]*

There is no physical connection.

– *Status [XMT]*

The physical connection is able to transmit data.

– *Status [REMOTE]*

This is an optional function used if the physical layer, instead of the HDTM, detects the indication that the remote DTE/DCE accepts the right to transmit (remote is in the half-duplex sending state).

– *Status [LOCAL]*

This is an optional function used if the physical layer, instead of the HDTM, detects the request for change in the direction of transmission that gives the local DTE/DCE the right to transmit (remote is in the wait or receiving state).

The forms of these interactions are not defined. However, an example of the HDTM physical layer interactions is given in 5.6.7 and 5.6.8.

I.3 Table of transitions between states

Table I.1 shows the events that cause a state transition and the resulting action(s). This provides a generalized description of operation of the HDTM.

TABLE I.1/X.32

Description of state transitions

Present state	Transition name		New state
	Event	Action	
0	Initialize calling DTE/DCE		4
Idle state	Calling DTE/DCE: data circuit established (e.g. data set ready, ready for data) (i.e. status [CALLING])	Do function control [SEIZE]	Wait for sending state
0	Initialize called DTE/DCE		2
Idle state	Called DTE/DCE: data circuit established (e.g. data set ready, ready for data) (i.e. status [CALLED])	Start timer XT1	Wait for receiving state
1	Send right to transmit		2
Half-duplex sending state	Conclusion of transmission (i.e. control [CONCLUDE])	Send request that remote DTE/DCE enter the half-duplex sending state (see Note 1). Start timer XT1. Do function status [INOP-T] (see Note 2). Do function control [RELASE]	Wait for receiving state
1	Disconnect sending DTE/DCE		0
Half-duplex sending state	LAPB has entered a disconnected phase (i.e. control [TERM] (see Note 3)	Do function control [DISCON]	Idle state

TABLE I.1/X.32 *(end)*

Description of state transitions

Present state	Transition name		New state
	Event	Action	
2	Receive confirmation		3
Wait for receiving state	Reception of indication that the remote DTE/DCE has entered the half-duplex sending state (see Note 4) (i.e. status [REMOTE])	Stop timer TX1	Half-duplex receiving state
2	Seize right to transmit		4
Wait for receiving state	Expiry of timer XT1 or has frame to send (i.e. a LAPB/HDTM transmit data function) (see Note 5)	Do function control [SEIZE]	Wait for sending state
3	Initialize calling DTE/DCE		4
Half-duplex receiving state	Reception of notification that the remote DTE/DCE is requesting a change in the direction of transmission (i.e. status [LOCAL]) (see Note 6)	Do function control [SEIZE]	Wait for sending state
3	Receive right to transmit		2
Half-duplex receiving state	Reception of notification that the remote DTE/DCE is requesting a change in the direction of transmission (i.e. status [LOCAL]) (see Note 6)	Start timer XT1	Wait for receiving state
3	Disconnect receiving DTE/DCE		0
Half-duplex sending state	LAPB has entered a disconnected phase (i.e. control [TERM]) (see Note 3)	Do function control [DISCON]	Idle state
4	Send confirmation		1
Half-duplex sending state	Indication of availability of the physical layer for transmission (i.e. status [XMT])	Send indication to the remote DTE/DCE that the half-duplex sending state has been entered. Do function status [OP-T] (see Note 7)	Half-duplex sending state
Any	Reset from any state		0
	Physical layer has no circuit to a remote DTE/DCE (i.e. status [UNCON])	Do function status (INOP-T]	Idle state

NOTES

1 HDTM uses the idle data link channel state indication (at least 15 continuous 1's) for requesting that the remote DTE enter the *half-duplex sending* state.

2 Status [INOP-T] indicates to LAPB that the sending of frames is inhibited.

3 Control [TERM] indicates that LAPB has entered the disconnected phase (equivalent to ADM of HDLC).

4 Reception of a flag or detection of carrier ON (circuit 109 = 1) is this indication.

5 One timer XT1 expiration must occur before a frame may be sent.

6 HDTM uses the idle data link channel state indication (at least 15 continuous 1's) or detection of carrier OFF (Circuit 109 = 0) for detecting that the remote DTE is requesting a change in the direction of transmission.

7 Status [OP-T] indicates to LAPB that the sending of frame is enabled.

I.4 HDTM/physical layer control and status functions expressed in terms applicable to a modem interface

Continuing the example of 5.6.7, the HDTM/physical layer logical functions may be described as shown below as they apply to the use of the HDTM with a V-Series modem interface:

– *Control [SEIZE]*

  Request turning circuit 105 ON and, if necessary, releasing circuit 103 from binary 1 condition.

– *Control [RELEASE]*

  Request holding circuit 103 in the binary 1 condition and turning circuit 105 OFF.

– *Control [DISCON]*

  Request turning circuit 107 OFF and, if necessary, turning circuit 105 OFF.

– *Status [CALLING]*

  As the calling DTE/DCE, report circuit 107 ON.

– *Status [CALLED]*

  As the called DTE/DCE, report circuit 107 ON.

– *Status [UNCON]*

  Report circuit 107 OFF.

– *Status [XMT]*

  Report circuit 106 ON.

– *Status [REMOTE]*

  Report carrier ON.

– *Status [LOCAL]*

  Report carrier OFF.

Appendix II

(to Recommendation X.32)

RSA public key algorithm

(This appendix does not form an integral part of this Recommendation)

The Rivest, Shamir, Adleman (RSA) algorithm defines a public key cryptography system. Each subscriber to an RSA cryptosystem generates a public modulo key (n), a public exponential key (e), and a secret exponential key (d), which conform to certain consistency rules to be subsequently described. The subscriber can publish and disclose its public keys *(n, e)* but it will never reveal its secret exponential key (d). The exchange of information via the RSA algorithm involves the successive transformations and decryption. The form of encryption and decryption transformations are mathematically identical but differ only in the values of the exponential keys used. Each RSA transformation is of the form:

$$X' = X^k \text{ (modulo } n)$$

where

X is the integer to be transformed

X' is the transformed integer

n is the public modulo key

k is the exponential key which is either the public exponential key e, or the secret exponential key d.

The RSA keys for a subscriber are generated subject to the following two constraints:

$n = p \cdot q$ (p and q are large prime numbers)

$(d \cdot e)$ modulo $[(p''1) \cdot (q''1)] = 1$

The encryption operation can use either e or d as the exponential key. However, the decryption operation must use the exponential key (d or e) that was *not* used in the encryption process. Both processes must use the same modulo key, n.

As applied to the security grade 2 identification process described in 7.1.2, the challenged party will generate SRES by encrypting RAND using its secret exponential key, d, so that the questioning party can decrypt SRES using the public keys of the challenged party (e and n).

Appendix III

(to Recommendation X.32)

Relationship of timers T14 and T14 *bis* to the different methods of DTE identification

(This appendix does not form an integral part of this Recommendation)

Figure III.1 illustrates the points in the general sequence of events defined in this Recommendation at which timers T14 and T14 *bis* are started or stopped.

NOTE – The Tl4 *bis* timer does not apply to the per-virtual-call DTE identification by means of network user identification facility, or provided by the public switched network identification.

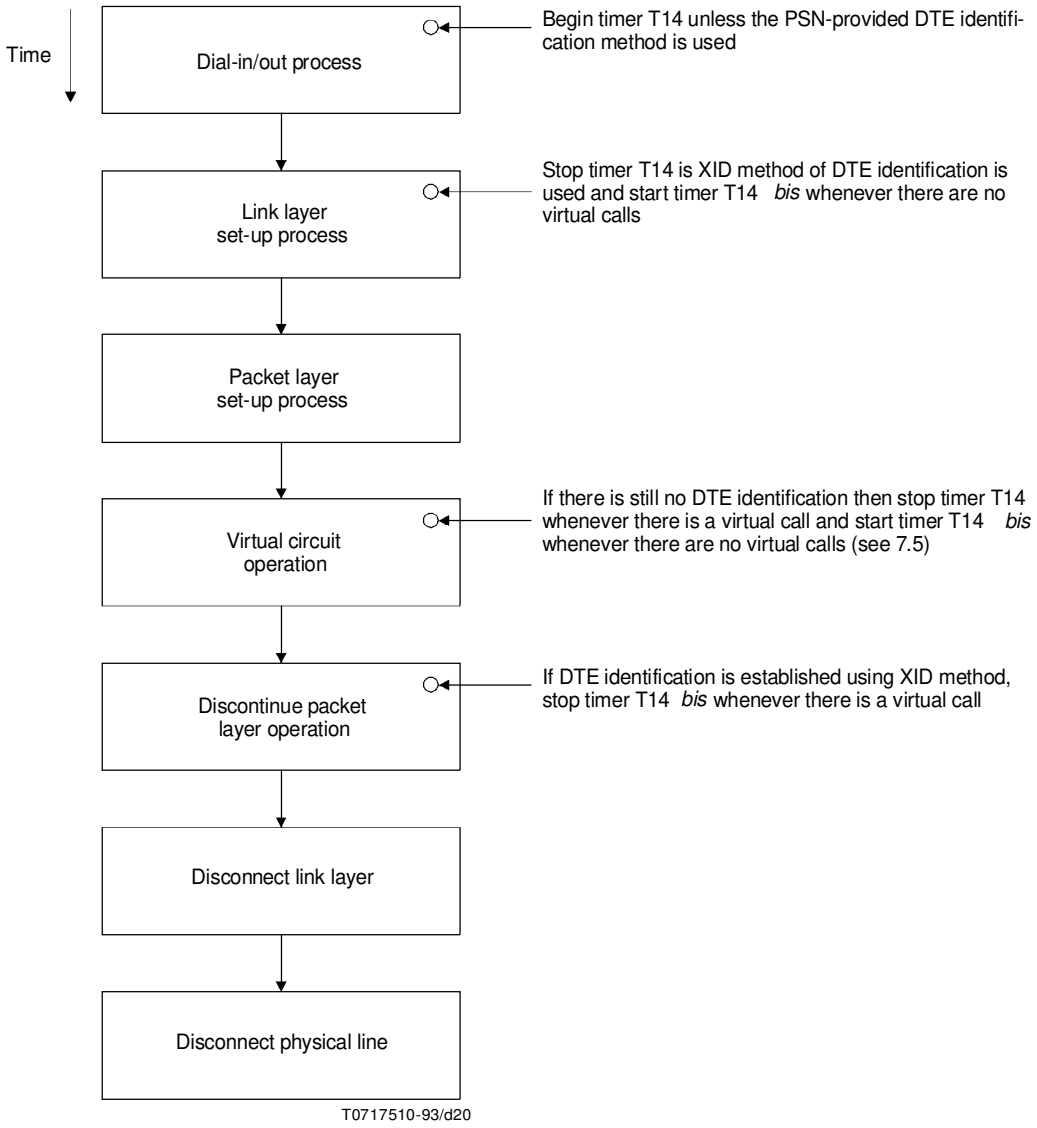


FIGURE III.1/X.32

Relationship between timers T14, T14 *bis* and DTE identification methods