

## 5 Link access procedure across the DTE/DCE interface

### 5.1 Introduction

This section specifies the mandatory and optional 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 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, 2.3, and 2.4 of Recommendation 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, 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 (Draft 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 Link layer address assignment

Two alternative mechanisms for assigning the link layer addresses are included in the procedures of this Recommendation. The conditions under which each mechanism applies are specified in the *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, 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 Table 5/X.32.

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 link level address assignment described in Table 5/X.32.

TABLE 5/X.32

## Link layer address assignment

Station 1  
Link layer address assignment

	Calling A	Called B
Command	B	A
Response	A	B

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

### 5.2.2 Assignment depending on roles of equipment as DTE and DCE

In accordance with the specifications in § 2.4.2 of Recommendation X.25, the 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 above.

The format of the control field of the XID frame is given in Table 6/X.32.

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

TABLE 6/X.32 (traité comme figure)

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 4/X.32.

FIGURE 4/X.32 - T0706470-88

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 5/X.32.

FIGURE 5/X.32 T0706480-88

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 6/X.32.

FIGURE 6/X.32 t0706490-88

The user data identifier element identifies the subfield as the user data subfield. Its encoding is shown in Figure 7/X.32.

FIGURE 7/X.32 -- T0706500-88

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 9/X.32).

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 8/X.32.

FIGURE 8/X.32 T0706510-88

### 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 Recommendation X.25, § 2.4.4.4.1 for the *disconnected* phase, and Recommendation X.25, § 2.4.6.1 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 of Recommendation 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 9/X.32 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 9/X.32 - T0706520-88

### 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 10/X.32.

FIGURE 10/X.32 - T0706530-88

### 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 XT1 a, and a called DTE/DCE uses the value XT1 b.

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 11/X.32 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.

FIGURE 11/X.32 - T0706540-88

#### 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.

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

Continuing the example, Table 7/X.32 shows, in terms of a V-series modem interface, the events that cause a state transition and the resulting action(s).

TABLE 7/X.32

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

Present state	Transition name		New state
	Event	Action	
0  Idle state	Initialize calling DTE/DCE		4
	Calling DTE/DCE: circuit 107 ON	Turn circuit 105 ON. Connect LAPB to circuit 103.	Wait for sending state
0  Idle state	Initialize called DTE/DCE		2
	Called DTE/DCE: circuit 107 ON	Start timer XT1.	Wait for receiving state
1  Half-duplex sending state	Send right to transmit		2
	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	Wait for receiving state

		105 OFF (see Note 2). Start timer XT1.	
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	Reception of 15 continuous 1 bits or	Turn circuit 105 ON. Release circuit 103	Wait for sending

receiving state	detection of carrier OFF (see Note 4 and 5)	from binary 1 condition. Connect LAPB to circuit 103.	state
-----------------	--	---	-------

TABLE 7/X.32 (cont.)

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

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

		circuit 105 OFF.)
--	--	-------------------

*Note 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.

*Note 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.

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

*Note 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 Recommendation V.24, § 4.3, this will hold circuit 104 in the binary 1 condition.

*Note 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.

*Note 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.

### 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 11/X.32), 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 11/X.32) 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.

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, 4, 5, 6 and 7 of Recommendation X.25 with additions as noted in this section and in § 7 of this Recommendation.

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 *Use of registration packets for identification of DTE and/or DCE and for conveyance of X.32 optional user facilities*

The registration procedure can be used for DTE and DCE identification at the packet layer. The *registration request* packet is used to convey identification protocol elements from the DTE to the DCE. The *registration confirmation* packet is used to convey identification protocol elements from the DCE to the DTE.

When using *registration* packets for DCE identification, it is necessary for the DTE to send a *registration request* packet in order to give the DCE an opportunity to identify itself.

Whenever DCE identification is being done via the registration procedure, a *registration confirmation* packet must be sent after the identification protocol has been completed in order for the registration procedure to be completed. If the DCE identification was not successful, this packet may contain identification protocol elements to begin the DCE identification procedure again, if allowed.

The identification protocol may be used for DTE identification and DCE identification at the same time. When this occurs, a registration packet may carry elements for both directions of identification simultaneously.

A DTE may specify X.32 optional user facilities in registration packets.

Descriptions of the identification protocol elements and X.32 facilities are listed in § 7.2.

When the *registration request* or the *registration confirmation* packet is used for identification and/or the conveyance of X.32 optional user facilities, the elements and/or facilities (see § 7.3) are carried in the registration field.

Registration packets may be used to perform identification, conveyance of X.32 facilities, and on-line facilities negotiation in the same packets, subject to the restriction of § 7.1.2, below (see § 7.3 of Recommendation X.25).

### 6.3 *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 a) and b), 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 octets 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 either a sequence of XID command frames or registration packets. Networks may offer either or both methods of security exchange, but an entire identification exchange must be done entirely with only one method.

The identification protocol may be used for DTE identification simultaneously but independently of its use for DCE identification. When this occurs, a registration packet or 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 access 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 12/X.32. First, the challenged party sends its identity (ID) and, if required, its signature (SIG). The questioning party responds with the diagnostic (DIAG).

FIGURE 12/X.32 - T0706550-88

As shown in Figure 13/X.32, 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.

*Note 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.

*Note 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.

If on-line facility registration is done simultaneously with identification, the DTE shall do so only in the packet containing SRES. If on-line facility registration is attempted prior to SRES, it will be refused by the network with a cause code value of *local procedure error*.

FIGURE 13/X.32 - T0706560-88

### 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 and 7 of Recommendation X.25. The elements are coded identically in registration packets and XID frames.

## 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, identity 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.

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.

### 7.2.2 Temporary location facility

*Temporary location* is an optional user facility that applies to the DTE/DCE interface for registered DTEs that accept dial-out calls from the PSPDN.

This facility can be used to substitute a different switched access number for dial-out-by-the-PSPDN to the DTE other than the *registered PSN number*. The switched access number specified is an X.121 number from the PSN numbering plan.

*Note* – Extension of a switched access number to accommodate additional digits, secondary digits, secondary dial tone, or dialling delays as allowed by V.25 and/or X.24 is left for further study.

In addition, a DTE may specify, by means of this facility, the periods of time during which it may be reached at a valid number for the PSN.

During those periods not identified by this facility, the number used to reach the DTE will be its *registered PSN number*.

The substitute number goes into effect at the “stay initiation” data and time. The substitute

number is no longer in effect at the “stay termination” date and time.

At the expiration of the time given in the *temporary location* facility, the number used for dial-out-by-the-PSPDN reverts to the *registered PSN number*.

Use of the *temporary location* facility by the called DTE will not cause the *called line address modified notification* facility to be inserted in the Call Connected packet. However, the *called line address modified notification* facility will appear in the Call Connected packet according to normal conditions of Recommendation X.25.

## 7.3 Coding of the identification protocol elements and X.32 facilities

### 7.3.1 General

The general principles for coding of the identification protocol elements and X.32 facilities are the same as the ones specified for the registration field in § 7.1 of Recommendation X.25. The statements of § 7.1 of Recommendation X.25 concerning facilities do not apply to this section. The statements of § 7.1 of Recommendation X.25 concerning registration elements apply to the identification protocol elements and X.32 facilities in this section.

### 7.3.2 Coding of the identification protocol element and X.32 facility code fields

Table 8/X.32 gives the list of the identification protocol element and X.32 facility codes, the coding for each, and, where applicable, whether this code may be sent by the challenged or the questioning party.

TABLEAU 8/X.32

#### Identification protocol element and X.32 facility codes

Identification element  or facility code	May be sent by		Bits
	challenged party	questioning party	
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
Temporary location			1 1 0 1 0 0 0 0

### 7.3.3 Coding of the identification protocol element and X.32 facility 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 which 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 9/X.32.

TABLE 9/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

*Note 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.

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

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

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

### 7.3.3.6 *Temporary location facility*

The octet following the code field indicates the length, in octets, of the parameter field.

The parameter field consists of one or more instances of temporary location requested by the DTE.

For each instance of temporary location, the first 5 octets indicate the date and time of the stay initiation. The next 5 octets indicate the date and time of the stay termination. The octet following the stay termination indicates the number of semi-octets in the switched access number and is binary encoded. The following octets contain the switched access number.

Date and time of initiation/termination is a string of 10 decimal digits expressing the coordinated universal time (UTC) and has the form YYMMDDhhmm. YY is the two low-order

digits of the Christian era year, and MM, DD, hh, and mm are the month, day, hour, and minute, respectively. The 10 decimal digits are BCD encoded in 5 octets with the first digit of the year encoded into bits 8 to 5 of the first octet and the last digit of the minute encoded into bits 4 to 1 of the fifth octet.

A value of all zeros for stay initiation will indicate the DTE's desire for immediate initiation.

A value of all zeros for stay termination will indicate the DTE's desire for the switched number to remain in effect until subsequent replacement (i.e., permanently).

*Note* – Some networks may only permit the stay termination and/or stay initiation fields to contain all zeros. In that case, the number of instances of temporary location is limited to one.

The switched access number is coded as a series of semi-octets. Each semi-octet contains either a digit in binary coded decimal or a special value in the range 1010–1111 binary.

*Note* – The special values may be used to accommodate the capabilities of V.25 and/or X.24, particularly in specifying secondary dial tone and dialling delays. Such use is left for further study.

If the switched access number contains an odd number of semi-octets, it is followed by a semi-octet containing zeros.

A switched number length of zero will indicate that the DTE is unavailable.

## 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/SC 20, 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 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.



## 7.6 *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.