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

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.

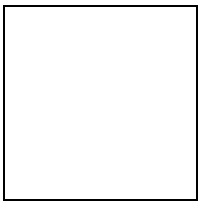
Note – As the identification protocol is symmetrical and should be used by the DTE in the same manner as the DCE, the actions of the DTE should correspond directly to the actions defined for the DCE.

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

In this annex, a DIAG element is considered as 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*

FIGURE T0706570-88



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] transmittted.

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 or registration 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 and, when the registration procedure DTE identification method is used, after the link layer is set up. 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 Nonidentified 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/X.32 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/X.32.

FIGURE A-1/X.32 T0706580-88

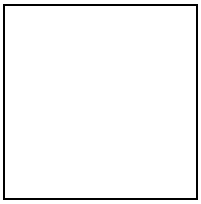


TABLE A–1/X.32

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 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	////////////////	Positive DIAG ->q13 or negative DIAG ->q14 or ->q11 (see Note 2)	////////////////	////////////////

Note 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.

Note 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 or registration 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, and, when the registration procedure DCE identification method is used, after the link layer is set up. 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/X.32 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/X.32.

FIGURE A-2/X.32 T0706590-88

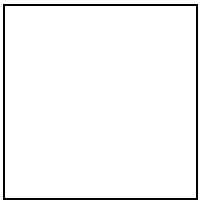


TABLE A–2/X.32

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	//////////////// ////////////////	//////////////// ////////////////	//////////////// ////////////////
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

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

Note 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 or registration 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 and, when the registration procedure DTE identification method is used, after the link layer is set up. In this state, the DCE expects to receive the ID (and possibly SIG) element(s) 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 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 the 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 SRES

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 nonidentified DTE service if it is supported. The DCE remains in this state until the switched connection is disconnected.

Figure A–3/X.32 provides a state diagram 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/X.32.

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 or registration 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, and, when the registration procedure DCE identification method is used, after the link layer is set up. 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-3/X.32 T0706600-88

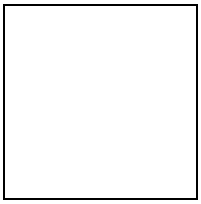


TABLE A–3/X.32

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 forID [, 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	//////////////	RAND ->q23 or Negative DIAG ->q26 (see Note 2)	//////////////	//////////////	//////////////	//////////////
Further DCE checking (if any) of the ID [, SIG] is complete	//////////////	//////////////	NORMAL ->q23 or Negative DIAG ->q26 (see Note 3)	//////////////	//////////////	//////////////
SRES	Negative DIAG->q26	Negative DIAG->q26	NORMAL ->q24	DISCARD ->q24	DISCARD ->q25	DISCARD ->q26
DCE checking of the SRES is complete	//////////////	//////////////	//////////////	Positive DIAG ->q25 or Negative DIAG ->q26 (see Note 4)	//////////////	//////////////

Note 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.

Note 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].

Note 3 – After having transmitted RAND, if the DCE detects that the ID [, SIG] received when in state q21 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.

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

Figure A–4/X.32 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/X.32.

FIGURE A-4/X.32 T-0706610-88

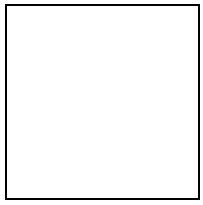


TABLE A–4/X.32

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	////////////// //////////////	////////////// //////////////	////////////// //////////////	////////////// //////////////	////////////// //////////////
RAND	DISCARD ->c26	NORMAL ->c23	DISCARD ->c23	DISCARD ->c24	DISCARD ->c25	DISCARD ->c26
DCE calculation of SRES from RAND is complete	////////////// ////////////// //////////////	////////////// ////////////// //////////////	SRES ->c24	////////////// ////////////// //////////////	////////////// ////////////// //////////////	////////////// ////////////// //////////////
Positive DIAG	DISCARD ->c26	NORMAL ->c25 or c26 (see Note 2)	DISCARD ->c26	NORMAL ->c25	DISCARD ->c25	DISCARD ->c26
Negative DIAG	DISCARD ->c26	NORMAL ->c26	NORMAL ->c26	NORMAL ->c26	DISCARD ->c25	DISCARD ->c26

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

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

ANNEX B

(to Recommendation X.32)

ABBREVIATIONS

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
RPOA	Recognized private 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...e
XID	Exchange identification (Unnumbered Format)
XT...	Timer...

APPENDIX I

(to Recommendation X.32)

IMPLEMENTATION OF LAPX

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:

– control [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 data.

– 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/X.32 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 Idle state	Initialize calling DTE/DCE		4 Wait for sending state
	Calling DTE/DCE: data circuit established (e.g. data set ready, ready for data) (i.e. status [CALLING])	Do function control [SEIZE]	
0 Idle state	Initialize called DTE/DCE		2 Wait for receiving state
	Called DTE/DCE: data circuit established (e.g. data set ready, ready for data) (i.e. status [CALLED])	Start timer XT1	
1 Half–duplex sending state	Send right to transmit		2 Wait for receiving 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 TX1. Do function status [INOP–T] (see Note 2). Do function control [RELEASE]	
1 Half–duplex sending state	Disconnect sending DTE/DCE		0 Idle state
	LAPB has entered a disconnected phase (i.e. control [TERM]) (see Note 3)	Do function control [DISCON]	
2 Wait for receiving state	Receive confirmation		3 Half–duplex receiving state
	Reception of indication that the remote DTC/DCE has entered the half–duplex sending state (see Note 4) (i.e. status [REMOTE])	Stop timer XT1	
2 Wait for receiving state	Seize right to transmit		4 Wait for sending 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]	

TABLE I–1/X.32 *(continued)*

Description of state transitions

Present state	Transition name		New state
	Event	Action	
3 Half–duplex receiving state	Initialize calling DTE/DCE		4 Wait for sending 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]	
3 Half–duplex receiving state	Receive right to transmit		2 Wait for 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	
3 Half–duplex sending state	Disconnect receiving DTE/DCE		0 Idle state
	LAPB has entered a disconnected phase (i.e. control [TERM]) (see Note 3)	Do function control [DISCON]	
4 Half–duplex sending state	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)	
Any	Reset from any state		0 Idle state
	Physical layer has no circuit to a remote DTE/DCE (i.e. status [UNCON])	Do function status [INOP–T]	

Note 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.

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

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

Note 4 – Reception of a flag or detection of carrier ON (circuit109 = 1) is this indication.

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

Note 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.

Note 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

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:

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

where

X is the integer to be transformed

$X\hat{}$ 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:

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

$(d \,.\, e)$ modulo $[(p - 1) \,.\, (q - 1)] = 1$

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 TIMER T14 TO THE DIFFERENT METHODS OF DTE IDENTIFICATION

Figure III–1/X.32 illustrates the points in the general sequence of events defined in this Recommendation at which timer T14 is started or stopped.

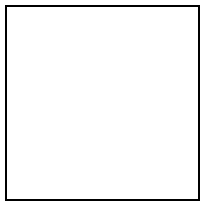



FIGURE III-1/X.32 T0706620-88