International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

T.123

(01/2007)

SERIES T: TERMINALS FOR TELEMATIC SERVICES

Network-specific data protocol stacks for multimedia conferencing

ITU-T Recommendation T.123

ITU-T Recommendation T.123

Network-specific data protocol stacks for multimedia conferencing

~~*(revised in 1999)*~~

Summary

ITU-T Recommendation T.123 specifies network-specific aspects of the T.120-series data protocols for multimedia conferencing. The networks currently identified are ISDN, CSDN, PSDN, PSTN, B-ISDN, and LAN. Communication profiles are specified which provide reliable point-to-point connections between a terminal and a multipoint control unit, between pairs of terminals or between pairs of MCUs. In some cases, a lower protocol layer allows the multiplexing of audio and video signals in addition to data connections. In other cases, separate calls, over the same or a different network, may be established to carry audio or video signals.

In addition, Annex B specifies a protocol that may be used to negotiate connection services beyond reliable data transfer. This protocol also provides for the use of alias address lists when making a connection. Alias lists will allow proxy services for T.120 communications to be created and used.

This revised version of ITU-T Recommendation T.123 introduces a number of clarifications to the previous version.

Source

ITU-T Recommendation T.123 was approved on 13 January 2007 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

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

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation T.123

Network-specific data protocol stacks for multimedia conferencing

~~(revised in 1999)~~

1 Scope

This Recommendation, which defines protocol stacks for terminals and MCUs, specifies network-specific aspects of the T.120 protocol suite in the form of profiles for each network identified. Each profile specifies a set of protocols that extend to layer 4 of the OSI reference model.

The rationale for this Recommendation is as follows: audiographic and video conferencing are intended to form part of the repertoire of ISDN services. Teleconferencing via ISDN involves the integration of multiple media (audio, video and data) in a connection, which may be the aggregate of a number of physical channels. The provision of these services is not, however, limited to the ISDN, and a range of other network scenarios is identified. For instance, CSDN may provide a similar, though less flexible, service to that of ISDN, and PSTN may provide a service that, though limited in performance, is more readily available. Teleconferencing may also be extended over PSDN and B-ISDN. LANs may provide conferencing locally within an enterprise or a means of access to wide area networks.

1.1 Networks identified

Network-specific profiles are defined for ISDN, CSDN, PSDN and PSTN, as required by [ITU-T F.702]. The scope of this Recommendation also includes B-ISDN and LAN.

1.2 Audio and video signals

The handling of audio and video signals in a multimedia conference is not part of this Recommendation, other than the possibility of their multiplexed transport over the same connection in some cases.

1.3 ISDN call set-up

Examples of ISDN call set-up procedures for the audiographic teleconference are given in Appendix I. These procedures illustrate:

a) the use of ISDN information elements;

b) coordination of the D-channel and the B-channel;

c) the phases of connection establishment;

d) interworking with telephone services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.702] ITU-T Recommendation F.702 (1996), *Multimedia conference services.*

[ITU-T H.221] ITU-T Recommendation H.221 (2004), *Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices.*

[ITU-T H.222.0] ITU-T Recommendation H.222.0 (2006) | ISO/IEC 13818-1:2006, *Information technology – Generic coding of moving pictures and associated audio information: Systems.*

[ITU-T H.223] ITU-T Recommendation H.223 (2001), *Multiplexing protocol for low bit rate multimedia communication.*

[ITU-T H.230] ITU-T Recommendation H.230 (2004), *Frame-synchronous control and indication signals for audiovisual systems.*

[ITU-T H.231] ITU-T Recommendation H.231 (1997), *Multipoint control units for audiovisual systems using digital channels up to 1920 kbit/s.*

[ITU-T H.233] ITU-T Recommendation H.233 (2002), *Confidentiality system for audiovisual services.*

[ITU-T H.242] ITU-T Recommendation H.242 (2004), *System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s.*

[ITU-T H.243] ITU-T Recommendation H.243 (2005), *Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 1920 kbit/s.*

[ITU-T H.310] ITU-T Recommendation H.310 (1998), *Broadband audiovisual communication systems and terminals.*

[ITU-T H.320] ITU-T Recommendation H.320 (2004), *Narrow-band visual telephone systems and terminal equipment.*

[ITU-T H.324] ITU-T Recommendation H.324 (2005), *Terminal for low bit-rate multimedia communication.*

[ITU-T I.320] ITU-T Recommendation I.320 (1993), *ISDN protocol reference model.*

[ITU-T I.321] ITU-T ~~CCITT~~ Recommendation I.321 (1991), *B-ISDN protocol reference model and its application.*

[ITU-T I.361] ITU-T Recommendation I.361 (1999), *B-ISDN ATM layer specification.*

[ITU-T I.363.1] ITU-T Recommendation I.363.1 (1996), *B-ISDN ATM Adaptation Layer specification: Type 1 AAL.*

[ITU-T I.363.3] ITU-T Recommendation I.363.3 (1996), *B-ISDN ATM Adaptation Layer specification: Types 3/4 AAL.*

[ITU-T I.363.5] ITU-T Recommendation I.363.5 (1996), *B-ISDN ATM Adaptation Layer specification: Type 5 AAL.*

[ITU-T I.365.1] ITU-T Recommendation I.365.1 (1993), *B-ISDN ATM adaptation layer sublayers: Frame relaying service specific convergence sublayer (FR-SSCS).*

[ITU-T I.365.3] ITU-T Recommendation I.365.3 (1995), *B-ISDN ATM adaptation layer sublayers: Service-specific coordination function to provide the connection-oriented transport service.*

[ITU-T I.430] ITU-T Recommendation I.430 (1995), *Basic user-network interface – Layer 1 specification.*

[ITU-T I.431] ITU-T Recommendation I.431 (1993), *Primary rate user-network interface – Layer 1 specification*.

[ITU-T I.432.1] ITU-T Recommendation I.432.1 (1999), *B-ISDN user-network interface – Physical layer specification: General characteristics*.

[ITU-T I.432.2] ITU-T Recommendation I.432.2 (1999), *B-ISDN user-network interface – Physical layer specification: 155 520 kbit/s and 622 080 kbit/s operation*.

[ITU-T I.432.3] ITU-T Recommendation I.432.3 (1999), *B-ISDN user-network interface – Physical layer specification: 1544 kbit/s and 2048 kbit/s operation*.

[ITU-T I.432.4] ITU-T Recommendation I.432.4 (1999), *B-ISDN user-network interface – Physical layer specification: 51 840 kbit/s operation*.

[ITU-T Q.920] ITU-T Recommendation Q.920 (1993), *ISDN user-network interface data link layer – General aspects*.

[ITU-T Q.921] ITU-T Recommendation Q.921 (1997), *ISDN user-network interface – Data link layer specification*.

[ITU-T Q.921 *bis*] ITU-T Recommendation Q.921 *bis* (1993), *Abstract test suite for LAPD conformance testing*.

[ITU-T Q.922] ITU-T ~~CCITT~~ Recommendation Q.922 (1992), *ISDN data link layer specification for frame mode bearer services*.

[ITU-T Q.931] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

[ITU-T Q.933] ITU-T Recommendation Q.933 (2003), *ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

[ITU-T Q.2110] ITU-T Recommendation Q.2110 (1994), *B-ISDN ATM adaptation layer – Service specific connection oriented protocol (SSCOP)*.

[ITU-T Q.2130] ITU-T Recommendation Q.2130 (1994), *B-ISDN signalling ATM adaptation layer – Service specific coordination function for support of signalling at the user-network interface (SSFC at UNI)*.

[ITU-T Q.2931] ITU-T Recommendation Q.2931 (1995), *Digital Subscriber Signalling System No. 2 – User-Network interface (UNI) layer 3 specification for basic call/connection control*.

[ITU-T T.90] ITU-T ~~CCITT~~ Recommendation T.90 (1992), *Characteristics and protocols for terminals for telematic services in ISDN*.

[ITU-T T.120] ITU-T Recommendation T.120 (2007), *Data protocols for multimedia conferencing*.

[ITU-T T.122] ITU-T Recommendation T.122 (1998), *Multipoint communication service – Service definition.*

[ITU-T T.124] ITU-T Recommendation T.124 (2007), *Generic Conference Control*.

[ITU-T T.125] ITU-T Recommendation T.125 (1998), *Multipoint communication service protocol specification*.

[ITU-T T.126] ITU-T Recommendation T.126 (1997), *Multipoint still image and annotation protocol*.

[ITU-T T.127] ITU-T Recommendation T.127 (1995), *Multipoint binary file transfer protocol*.

[ITU-T V.7] ITU-T ~~CCITT~~ Recommendation V.7 (1988), *Definitions of terms concerning data communication over the telephone network.*

[ITU-T V.8] ITU-T Recommendation V.8 (2000), *Procedures for starting sessions of data transmission over the public switched telephone network.*

[ITU-T V.8 *bis*] ITU-T Recommendation V.8 *bis* (2000), *Procedures for the identification and selection of common modes of operation between data circuit-terminating equipments (DCEs) and between data terminal equipments (DTEs) over the public switched telephone network and on leased point-to-point telephone-type circuits.*

[ITU-T V.14] ITU-T Recommendation V.14 (1993), *Transmission of start-stop characters over synchronous bearer channels.*

[ITU-T V.34] ITU-T Recommendation V.34 (1998), *A modem operating at data signalling rates of up to 33 600 bit/s for use on the general switched telephone network and on leased point-to-point 2-wire telephone-type circuits.*

[ITU-T V.42] ITU-T Recommendation V.42 (2002), *Error-correcting procedures for DCEs using asynchronous-to-synchronous conversion*.

[ITU-T V.42 *bis*] ITU-T ~~CCITT~~ Recommendation V.42 *bis* (1990), *Data compression procedures for data circuit-terminating equipment (DCE) using error correction procedures.*

[ITU-T V.61] ITU-T Recommendation V.61 (1996), *A simultaneous voice plus data modem, operating at a voice plus data signalling rate of 4800 bit/s, with optional automatic switching to data-only signalling rates of up to 14 400 bit/s, for use on the General Switched Telephone Network and on leased point-to-point 2-wire telephone type circuits.*

[ITU-T V.70] ITU-T Recommendation V.70 (1996), *Procedures for the simultaneous transmission of data and digitally encoded voice signals over the GSTN, or over 2-wire leased point-to-point telephone type circuits*.

[ITU-T V.120] ITU-T Recommendation V.120 (1996), *Support by an ISDN of data terminal equipment with V-series type interfaces with provision for statistical multiplexing.*

[ITU-T X.21] ITU-T ~~CCITT~~ Recommendation X.21 (1992), *Interface between Data Terminal Equipment and Data Circuit-Terminating equipment for synchronous operation on public data networks.*

[ITU-T X.21 *bis*] ITU-T ~~CCITT~~ Recommendation X.21 *bis* (1988), *Use on public data networks of Data Terminal Equipment (DTE) which is designed for interfacing to synchronous V-series modems*.

[ITU-T X.25] ITU-T Recommendation X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*

[ITU-T X.200] ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[ITU-T X.213] ITU-T Recommendation X.213 (2001) | ISO/IEC 8348:2002, *Information technology – Open Systems Interconnection – Network service definition.*

[ITU-T X.214] ITU-T Recommendation X.214 (1995) | ISO/IEC 8072:1996, *Information technology – Open Systems Interconnection – Transport service definition*.

[ITU-T X.224] ITU-T Recommendation X.224 (1995) | ISO/IEC 8073:1997, *Information technology – Open Systems Interconnection – Protocol for providing the connection-mode transport service*.

[ISO/IEC 3309] ISO/IEC 3309:1993, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure*.

[ISO/IEC 7776] ISO/IEC 7776:1995, *Information technology – Telecommunications and information exchange between systems – High-level data link control procedures – Description of the X.25 LAPB-compatible DTE data link procedures*.

[ISO/IEC 8208] ISO/IEC 8208:2000, *Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment*.

[ISO/IEC 8802] ISO/IEC TR 8802-1:2001, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks specific requirements – Part 1: Overview of Local Area Network Standards*.

3 Definitions

This Recommendation uses the following terms defined in [ITU-T F.700]:

– Audiographic conference service;

– Multipoint control unit.

This Recommendation uses the following terms defined in [ITU-T I.320]:

– Control plane;

– User plane.

This Recommendation uses the following term defined in [ITU-T Q.920]:

– Data link connection identifier.

This Recommendation uses the following term defined in [ITU-T Q.922]:

– Synchronization and convergence function.

This Recommendation uses the following term defined in [ITU-T V.7]:

– Start-stop transmission.

This Recommendation uses the following term defined in [ITU-T X.213] and [ITU-T X.214]:

– Quality of Service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAL ATM Adaptation Layer

AL Adaptation Layer

ATM Asynchronous Transfer Mode

B-ISDN Broadband Integrated Services Digital Network

CPCS Common Part Convergence Sublayer

CSDN	Circuit Switched Data Network
DCE	Data Circuit-terminating Equipment
DLCI	Data Link Connection Identifier
DLSAP	Data Link Service Access Point
DTE	Data Terminal Equipment
FCS	Frame Check Sequence
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MCS	Multipoint Communication Service
MCSAP	Multipoint Communication Service Access Point
MCU	Multipoint Control Unit
MLP	Multi-Layer Protocol
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PES	Packetized Elementary Stream
PhSAP	Physical Service Access Point
PSDN	Packet Switched Data Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SCF	Synchronization and Convergence Function
SDU	Service Data Unit
TPDU	Transport Protocol Data Unit
TSAP	Transport Service Access Point
UNERM	Unacknowledged Non-Error Recovery Mode
VC	Virtual Channel

5 Multipoint configuration

A multipoint configuration is created from point-to-point connections between three or more terminals and MCUs. Figure 1 shows a typical configuration where terminals are connected in a multipoint star around each MCU. It also shows how MCUs may be interconnected to form a larger conference.

Figure 2 shows the framework of the T.120 protocol suite. This Recommendation defines the network-specific protocols in any direct connection between terminal and MCU, between two terminals, or between two MCUs.

The point-to-point connections to a single MCU need not have identical communication profiles. Operation of the MCS protocol layer supports communication across different networks.

If two terminals lack a common profile, they cannot be connected directly to one another. In that case, an MCU may serve as an intermediary making communication possible. This is a special example of multipoint configuration.

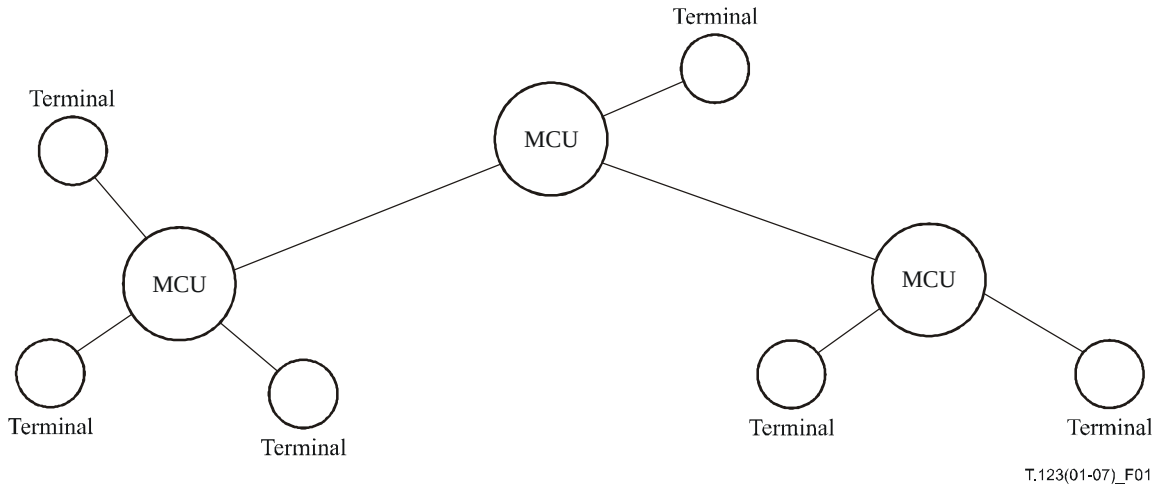


Figure 1 – Typical multipoint configuration

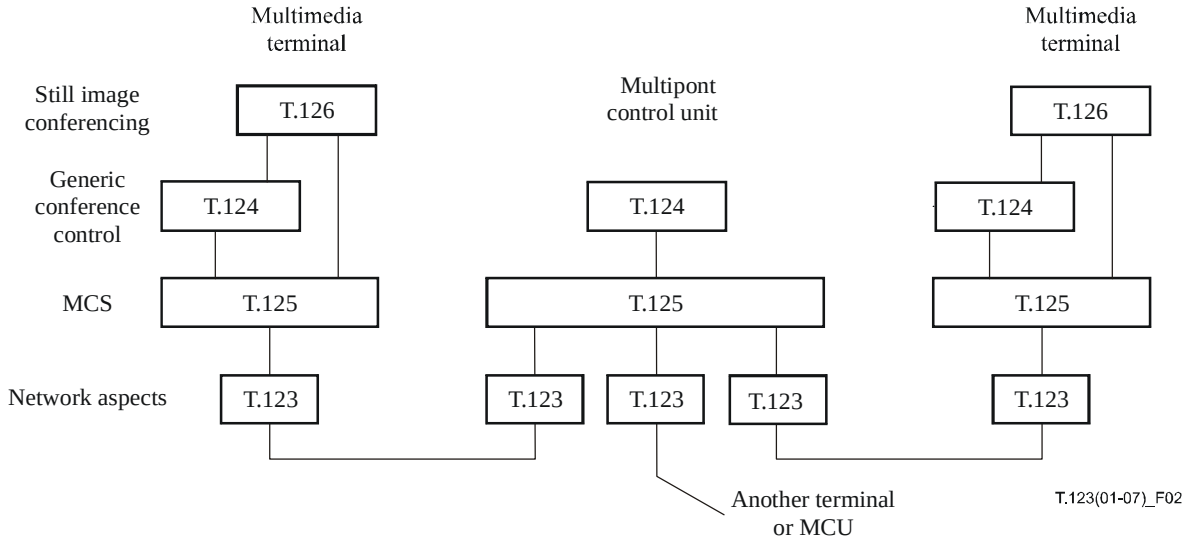


Figure 2 – Framework of the T.120 protocol suite

6 Profile overview

The general structure of the network-specific profiles is shown in Figure 3. Profiles are defined in detail in the following clauses.

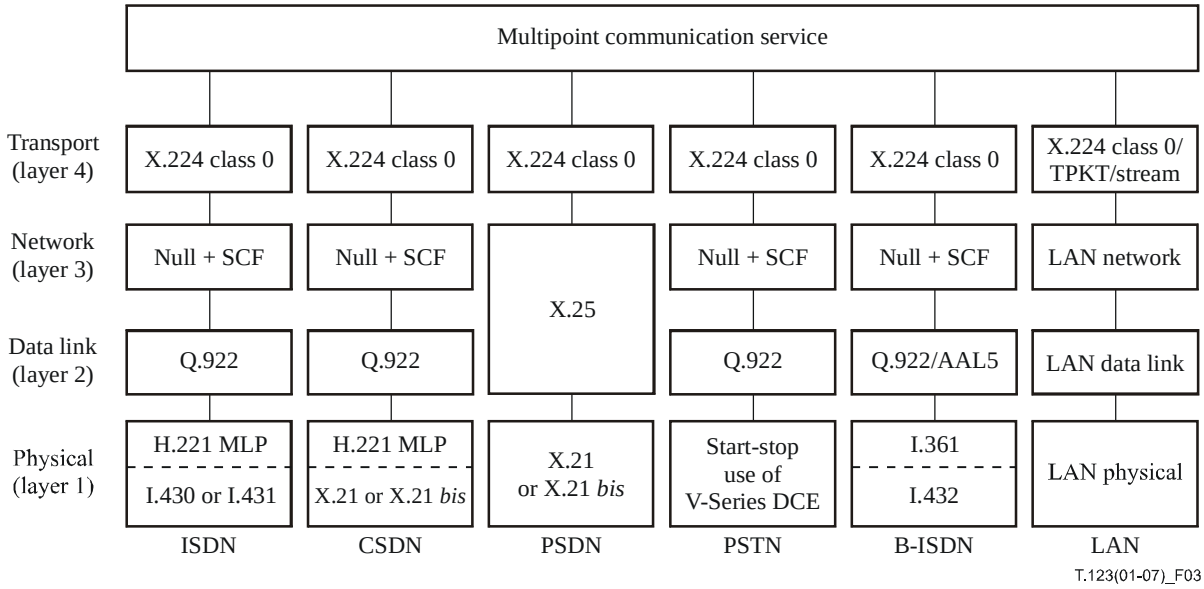


Figure 3 – Basic profiles general structure

NOTE 1 – The use of [ITU-T Q.922] over ISDN does not imply the use of a frame relay bearer service. [ITU-T Q.922] is used to enhance the quality of service provided by the physical layer of an ISDN, CSDN, PSTN, or B-ISDN. This Recommendation exploits the error recovery mechanisms of Q.922 multiframe acknowledged mode for operation of one or more data links over a point-to-point connection provided by the corresponding network.

The service that MCS requires from lower layers is the reliable, sequential, flow-controlled transfer of data units of unlimited size. One MCS connection consists of between one and four transport connections. The number depends on how many MCS data transfer priorities are implemented distinctly.

Multiple transport connections are derived from a point-to-point connection over a specific network by multiplexing in some lower protocol layer. This occurs at layer 2 for those cases where [ITU-T Q.922] is used and at layer 3 where [ITU-T X.25] or a LAN protocol is used.

Figure 4 shows the location of an MCS provider in the OSI reference model. An MCS provider exchanges MCS protocol data units with remote MCS providers. For this purpose, it uses transport-layer services. An MCS provider communicates with MCS users through an MCSAP by means of the MCS primitives defined in [ITU-T T.122].

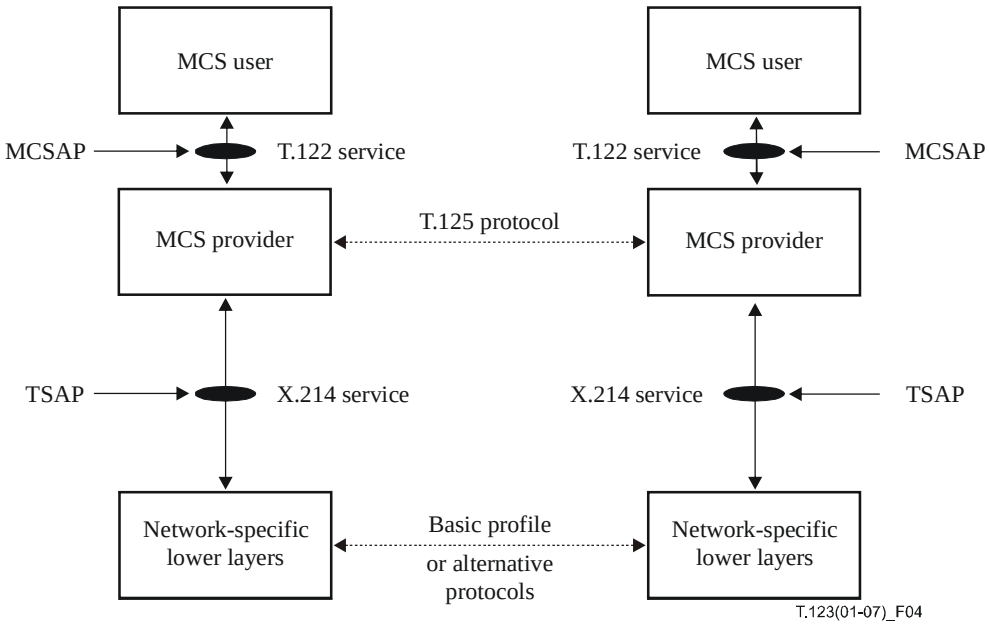


Figure 4 – Location of an MCS provider in the OSI reference model

To simplify the address information that must be supplied when establishing an MCS connection, it is recommended that terminals and MCUs be administered so that null NSAP and TSAP selectors will resolve to a default MCS provider at the destination system.

This does not preclude the possibility that a specific selector may be required to reach an MCS provider in a particular context. This may be the case, for example, if the data connection is to be associated with an audio or video connection that is established independently. It may also be the case if the MCS connection is to join a conference hosted in one partition of a large MCU. Ideally, the specific selector to be used will be communicated dynamically through some prior exchange.

NOTE 2 – An NSAP selector may occur in the domain-specific part of an NSAP address. The format for this is not standardized.

NOTE 3 – In each of the profiles specified here, the transport layer protocol is [ITU-T X.224]. It conveys TSAP selectors as TSAP-ID parameters of connection establishment TPDUs.

NOTE 4 – Annex B specifies the profiles that shall be used when establishing T.120 extended transport connections.

7 Basic profiles

When call set-up protocols or audio and video are shown in the profiles that follow, it is only to aid understanding. They are not a normative part of this Recommendation.

7.1 ISDN basic profile

Figure 5 defines the ISDN basic profile.

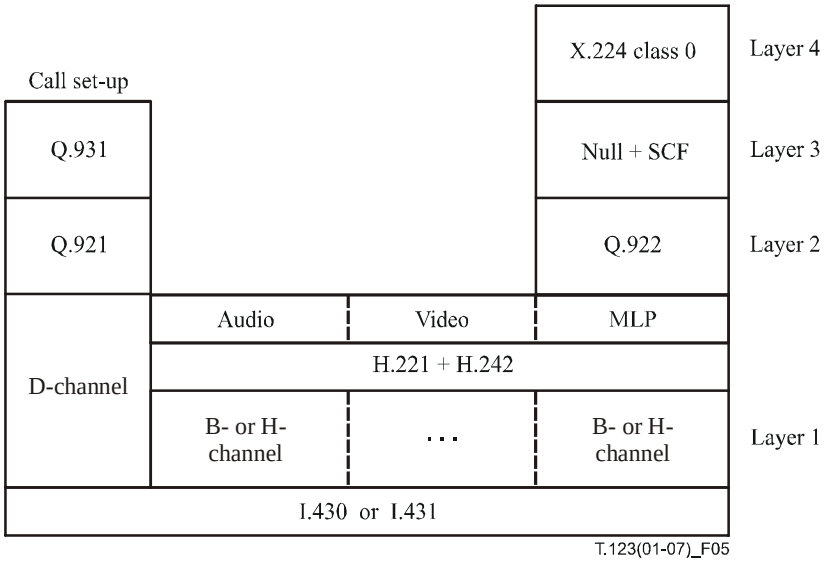


Figure 5 – ISDN basic profile

Layer 4

– X.224.

– Class 0 preferred, no alternative class.

– Maximum TPDU size shall not exceed layer 2 parameter N201.

Layer 3

– User plane: null (no extra protocol during data transfer).

– Control plane: SCF as specified in clause 9.

Layer 2

– Q.922.

– Protocol parameters and options as specified in clause 10, Q.922 protocol parameters and options.

Layer 1

Sublayer formed by H.221 MLP channels:

– As specified in clause 12, Physical sublayer formed by H.221 MLP channels.

Sublayer formed by ISDN:

– 1-6 B-channels, or 1-5 H0-channels, or 1 H1-channel.

– Unrestricted digital information, optionally with tones and announcements.

– B-channels may be rate-adapted to 56 kbit/s for restricted networks.

– D-channel is used for network signalling only, not for user data.

NOTE – This Recommendation does not specify call set-up in the ISDN (although possible scenarios are illustrated in Appendix I). The SCF shown here operates only in the MLP channel, after ISDN call set-up and H.242 mode switching have occurred.

7.2 CSDN basic profile

Figure 6 defines the CSDN basic profile. Layers above H.221 are identical to the ISDN basic profile.

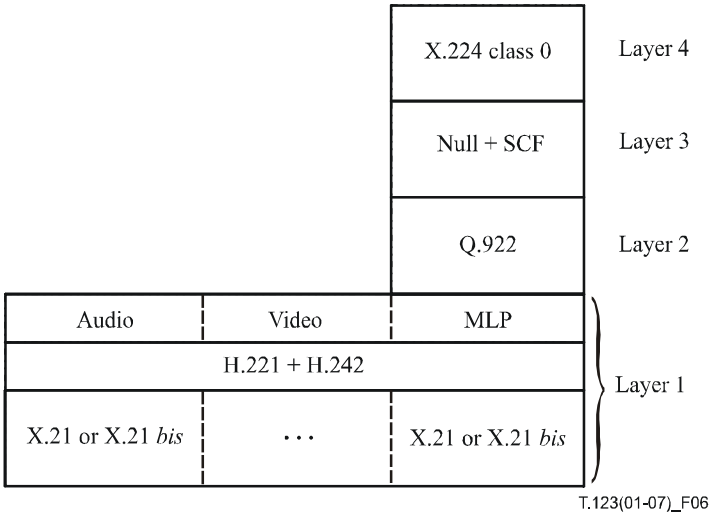


Figure 6 – CSDN basic profile

Layer 4

– As specified in clause 7.1, ISDN basic profile.

Layer 3

– As specified in clause 7.1, ISDN basic profile.

Layer 2

– As specified in clause 7.1, ISDN basic profile.

Layer 1

Sublayer formed by H.221 MLP channels:

– As specified in clause 12, physical sublayer formed by H.221 MLP channels.

Sublayer formed by CSDN:

– X.21 or X.21 *bis* for each circuit switched connection.

– Bit rates shall be a uniform multiple of 64 kbit/s or 56 kbit/s.

7.3 PSDN basic profile

Figure 7 defines the PSDN basic profile.

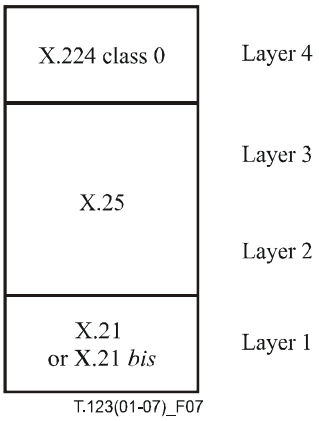


Figure 7 – PSDN basic profile

Layer 4

– X.224.

– Class 0 preferred, no alternative class.

Layer 3

– X.25 virtual call service.

Layer 2

– X.25 LAPB single link procedure.

Layer 1

– X.21 or X.21 *bis*.

7.4 PSTN basic profile

Figure 8 defines the PSTN basic profile. Layers above Q.922 are identical to the ISDN basic profile.

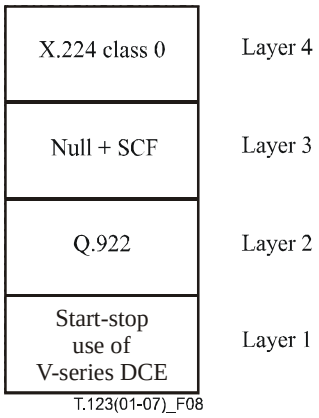


Figure 8 – PSTN basic profile

Layer 4

– As specified in 7.1, ISDN basic profile.

Layer 3

– As specified in 7.1, ISDN basic profile.

Layer 2

– Q.922.

– Protocol parameters and options as specified in clause 10, Q.922 protocol parameters and options.

– Modified frame transparency based on [ISO/IEC 3309] as specified in clause 11, Data link frame structure transparency for start-stop transmission.

Layer 1

– Start-stop transmission by DTE.

– When using V.14: one start bit, one stop bit, eight data bits, no parity.

– Any compatible V-series DCE operating over PSTN may be employed.

– The DTE and DCE may be logical functions that are not physically separated if integrated equipment can produce the same transmitted signals.

– The choice of V-series DCE is unrestricted and includes, for example, V.34, V.61 and V.70 modems, with optional use of V.42 and V.42 *bis*. Selection of a compatible operating mode may be assisted by V.8 or V.8 *bis*.

NOTE 1 – If the error control function of V.42 is activated, system parameters should be set to avoid adverse interaction with the error-correcting operation of Q.922. Important elements are the acknowledgement timer, the maximum number of octets in an information field, and the data forwarding conditions.

NOTE 2 – The effectiveness of V.42 *bis* data compression will vary depending on how much of the application data exchanged in a conference has already been compressed by other means.

NOTE 3 – V.70 DCE, if made aware that this profile is being employed, may negotiate between themselves the use of enhanced techniques, such as UNERM tunnelling for T.120, as long as the service provided at the DTE interface remains start-stop transmission.

7.5 B-ISDN basic profile

Figure 9 defines the B-ISDN basic profile. Layers above Q.922 are identical to the ISDN basic profile.

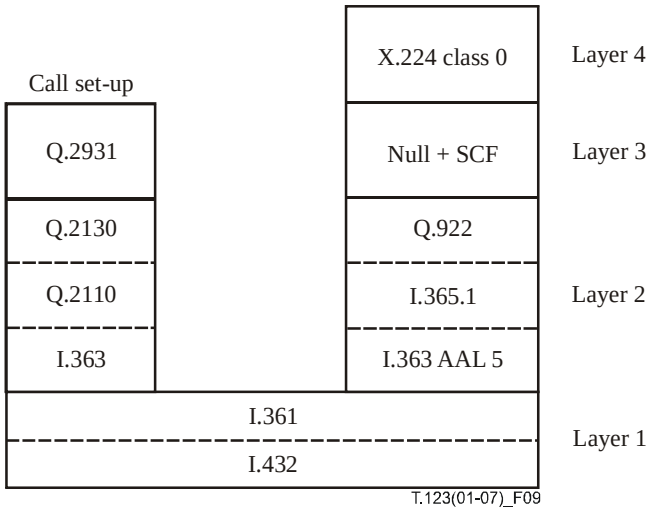


Figure 9 – B-ISDN basic profile

Layer 4

– As specified in 7.1, ISDN basic profile.

Layer 3

– As specified in 7.1, ISDN basic profile.

Layer 2

– Q.922.

– Protocol parameters and options as specified in clause 10, Q.922 protocol parameters and options.

– PDU structure defined in Figure 3 of [ITU-T I.365.1] (no use of flags, transparency or FCS).

– PDU octets conveyed as one CPCS-SDU using AAL type 5.

Layer 1

– ATM virtual channel.

7.6 LAN basic profile

Figure 10 defines the LAN basic profile.

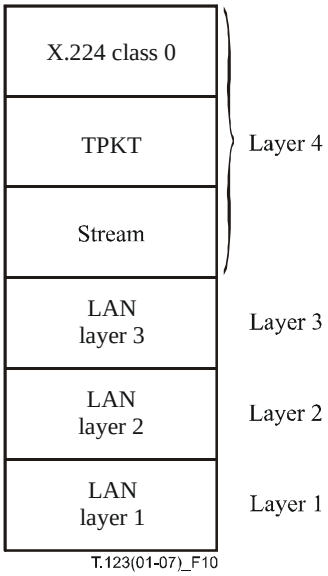


Figure 10 – LAN basic profile

Layer 4

– X.224 class 0 preferred, no alternative class.

– Default TPDU size 65531, but smaller values may be negotiated.

– TPKT packet header to delimit TPDUs, as specified in clause 8, Packet header to delimit data units in an octet stream.

NOTE 1 – TPKT is required because an octet-stream service does not mark where data unit boundaries occur.

– Octet-stream transfer with the following characteristics:

a) Connection-oriented service preserving octet sequence.

b) Boundary between data units *not* retained as part of the transfer.

c) Residual error rate low enough to use as a type A network service.

d) Flow control mechanism to exert back-pressure on a transmitter.

NOTE 2 – The following specifies a protocol for octet-stream transfer that is a common example of the above:

a) RFC 793, Transmission control protocol.

b) By default, destination port number 1503 per RFC 1700, Assigned numbers, but others may be used.

Layer 3

– Commonly, RFC 791, 792, 919, 922, 950, 1112, Internet protocol.

Layer 2

– Commonly, [ISO/IEC 8802] logical link control and medium access sublayers.

Layer 1

– Commonly, [ISO/IEC 8802] physical medium.

8 Packet header to delimit data units in an octet stream

[ITU-T X.224] expects information to be transmitted and received in discrete units termed network service data units (NSDUs), which can be an arbitrary sequence of octets. Although other classes of the transport protocol may combine more than one TPDU inside a single NSDU, X.224 class 0 does not use this facility. Hence, in the context of T.123 protocol stacks, a TPDU may be identified with its underlying NSDU.

A fundamental difference between the network service expected by [ITU-T X.224] and an octet-stream transfer service, as characterized in clause 7.6, is that the latter conveys a continuous sequence of octets with no explicit boundaries between related groups of octets.

This clause specifies a distinct protocol layer to repair the discrepancy and meet the needs of [ITU-T X.224]. It defines a simple packet format whose purpose is to delimit TPDUs. Each packet, termed a TPKT, is a unit composed of a whole integral number of octets, of variable length.

A TPKT consists of two parts: a packet header, followed by a TPDU. The format of the packet header is constant, independent of the type of TPDU. The packet header consists of four octets as shown in Figure 11.

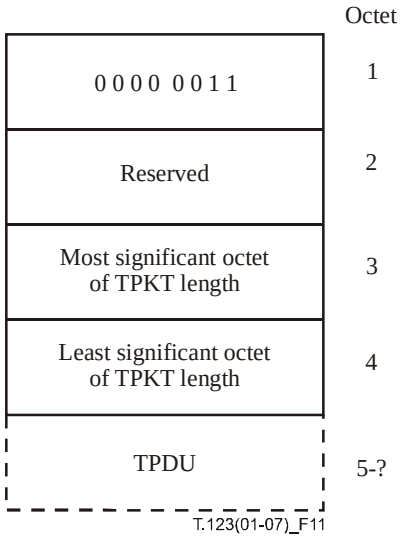


Figure 11 – Format of the TPKT packet header

Octet 1 is a version number, with binary value 0000 0011. Octet 2 is reserved for further study. Octets 3 and 4 are the unsigned 16-bit binary encoding of the TPKT length. This is the length of the entire packet in octets, including both the packet header and the TPDU.

Since an X.224 TPDU occupies at least 3 octets, the minimum value of TPKT length is 7. The maximum value is 65535. This permits a maximum TPDU size of 65531 octets.

NOTE – This description of the TPKT protocol layer agrees with RFC 1006, *ISO transport services on top of the TCP*.

9 Synchronization and convergence function

9.1 SCF overview

The SCF resides in the network layer of each communication profile whose data link layer is specified to be Q.922. It coordinates network connection establishment and release between the control plane and the user plane as described in clause 4 of [ITU-T Q.922]. The purpose of the SCF is to provide network services to the transport layer. Figure 12 is the architectural model of the SCF.

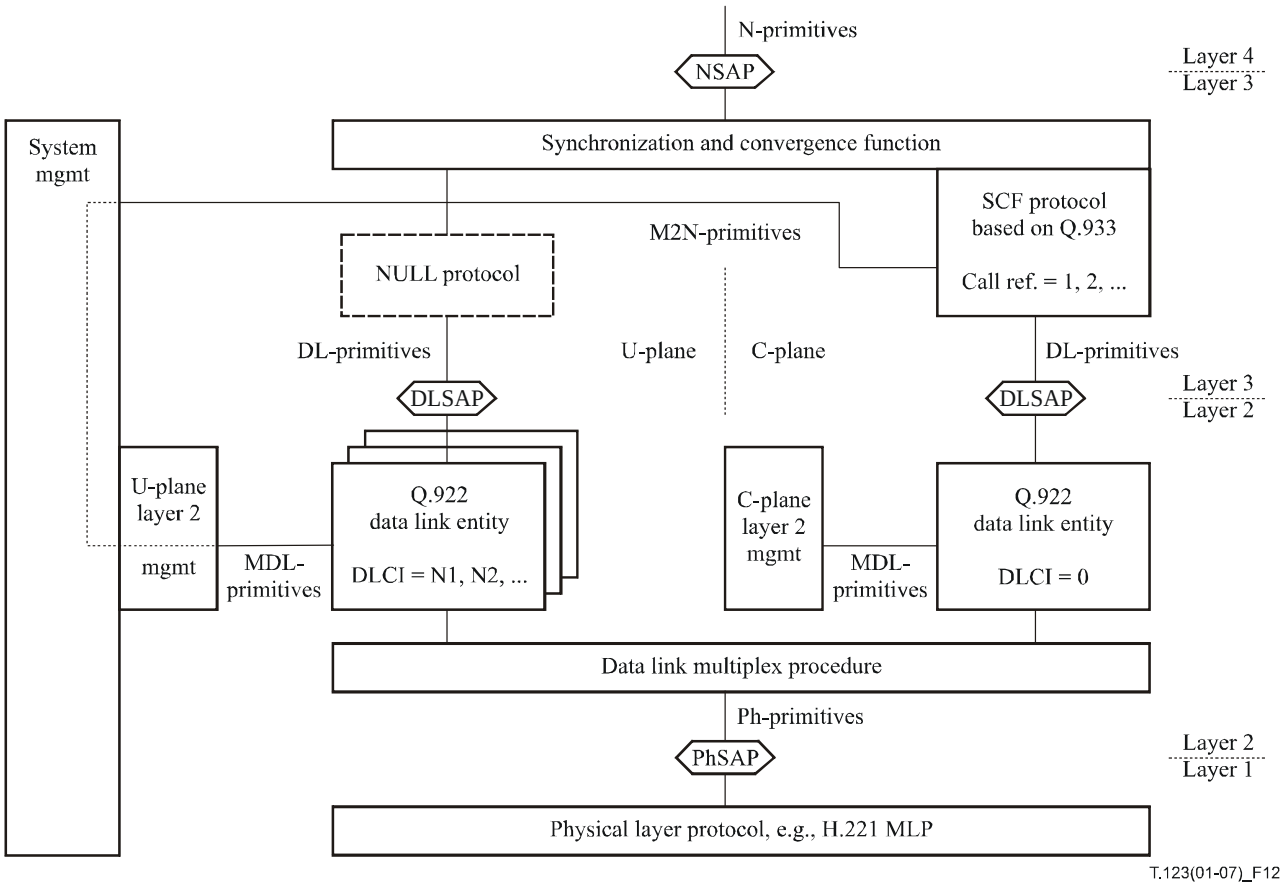


Figure 12 – Architectural model of the SCF

Network services required by the X.224 transport protocol are listed in Table 1. This table is derived from Table 2 of [ITU-T X.224] by excluding optional features and N-RESET (because N-RESET is never requested, according to Table A.3 of [ITU-T X.224], and any indication of it can be escalated to N-DISCONNECT).

Table 1 – Network services required by X.224

Primitives	Parameters
N-CONNECT request N-CONNECT indication	Called address Calling address QoS parameter set
N-CONNECT response N-CONNECT confirm	Responding address QoS parameter set
N-DATA request N-DATA indication	NS user data
N-DISCONNECT request N-DISCONNECT indication	

The SCF implements the N-CONNECT and N-DISCONNECT primitives. During data transfer it is inactive, and N-DATA maps directly to DL-DATA with no extra protocol. This requires that the transport layer limit the size of its TPDUs to one Q.922 I-frame.

[ITU-T Q.922] supports multiple data link connections distinguished by DLCI. Acting through layer 2 management, the SCF controls DLCI assignments. It communicates with a peer SCF by

sending and receiving Q.933 messages over DLCI 0, which is reserved for in-channel signalling. DLCI 0 serves the control plane, supporting SCF control. Other DLCIs serve the user plane, supporting data transfer.

SCF procedures are based on those specified in [ITU-T Q.933], in which are defined case A covering circuit switched access to a remote frame handler, and case B covering integrated access to a local frame handler. The SCF use of Q.933 messages may be considered a new case C, covering circuit switched access directly to another network user. This new case C does not use DLCIs to distinguish connections to different destinations. It uses DLCIs to distinguish multiple connections between the same two end points. Each such connection may have a different quality of service.

The sequence of actions to obtain a physical circuit between two users can vary with the communication profile and other circumstances. A circuit may be established without the aid of SCF prior to the first N-CONNECT request and indication. When these primitives are finally invoked, called and calling addresses may be omitted or ignored. Alternatively, N-CONNECT request may initiate events, and network addresses may be required for circuit routing.

9.2 SCF procedures

The SCF shall act as a network user required to act for Q.933 case A of frame relaying. It shall behave as though connected semi-permanently to a remote frame handler, even though the bit rate allotted to the physical circuit may not be exactly the same as an ISDN information transfer rate.

The sole exception is clause 5.6 of ITU-T Rec. Q.933 (1995) concerning DLCI collisions. To maintain a symmetric relationship between two network users, the SCF shall give neither direction preference as incoming. Instead, it shall resolve collisions by forcing new DLCI selections on both sides, as specified in detail below.

The SCF shall obey the additional requirements stated in the remainder of this clause.

As soon as a duplex physical circuit is activated, the SCF shall assign and establish DLCI 0 to serve the control plane. DLCI 0 shall carry Q.933 messages in Q.922 I-frames. If DLCI 0 is ever re-established, which indicates a protocol error, the SCF shall cause it to be released. If DLCI 0 is ever released, the SCF shall remove all other DLCIs assigned to the physical circuit and shall indicate that their data links are disconnected. The SCF may then attempt to establish DLCI 0 again and reinitialize Q.933 signalling.

As a positive response to SETUP, the SCF shall transmit CONNECT, and this shall be answered by CONNECT ACKNOWLEDGE. In this situation, there is no advantage in transmitting ALERTING, CALL PROCEEDING, or PROGRESS. If received, these messages may be ignored.

The negative response to SETUP shall be RELEASE COMPLETE. This is also the simplest means of clearing an active call. In this situation there is no advantage in transmitting DISCONNECT, STATUS, or STATUS ENQUIRY. If received, these messages may stimulate the transmission of RELEASE COMPLETE. If RELEASE is received during most call states specified in [ITU-T Q.933], e.g., while the call is active but not while awaiting a response to SETUP or RELEASE, it shall cause the transmission of RELEASE COMPLETE. Although an unexpected RELEASE COMPLETE is considered a message sequence error, it achieves the intended effect of forcing the receiver to clear a call.

Figure 13 shows the messages exchanged and primitives invoked during a successful N-CONNECT. This figure assumes that DLCI 0 is already established, as the result of exchanging SABME and UA when the physical circuit was activated.

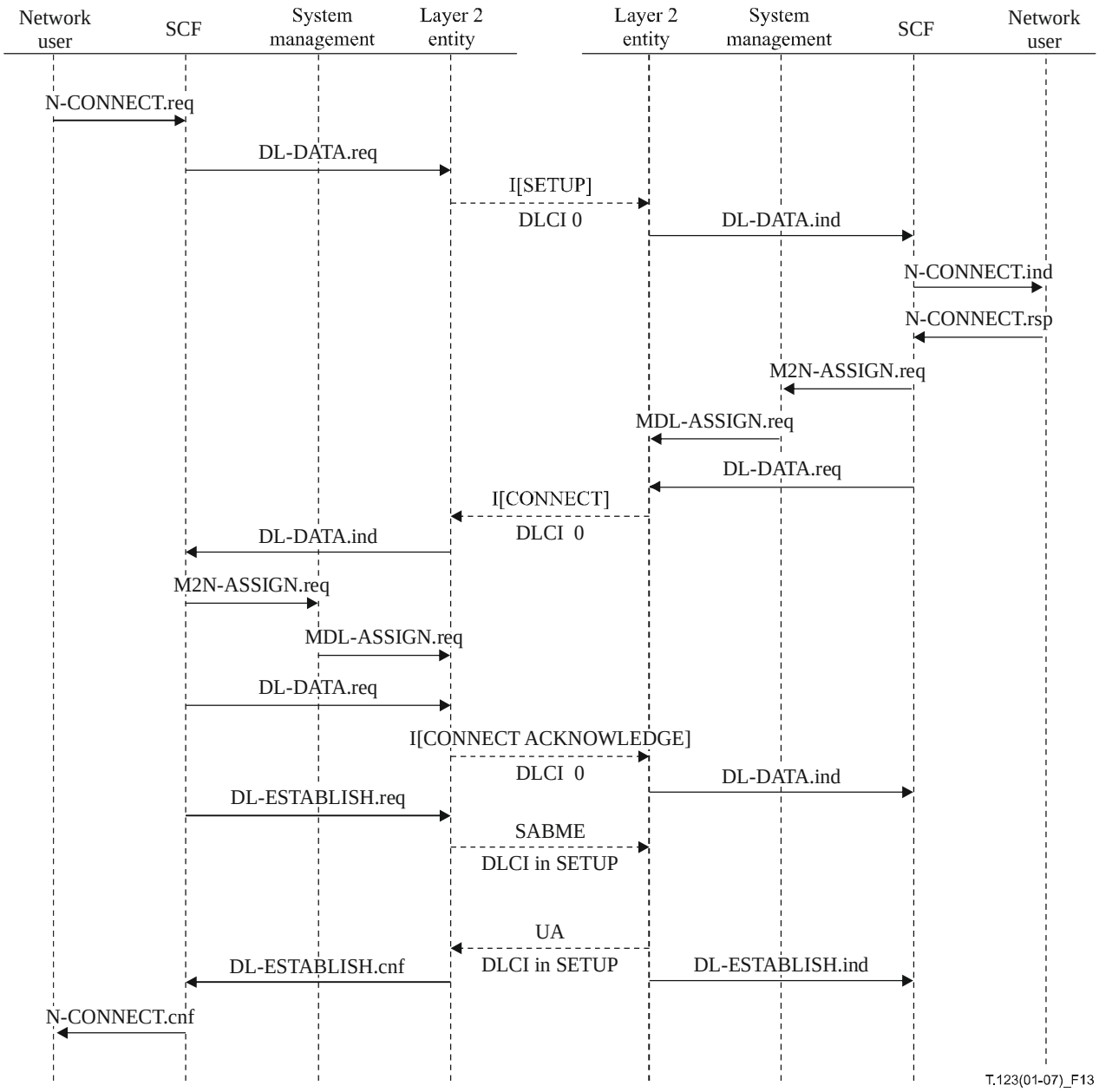


Figure 13 – Sequence of actions for N-CONNECT

The SCF shall employ one-octet call reference values (ranging from 1 to 127 on each side) and two-octet DLCI values (comprising 10 bits). DLCIs shall be selected randomly within the range allotted by [ITU-T Q.922] for support of user information, namely, from 16 to 991 inclusive.

An SCF processing N-CONNECT request shall propose a preferred DLCI value in SETUP. An SCF receiving SETUP shall consider the DLCI value it contains. It is an error if the DLCI value is already assigned. If the receiving SCF has proposed the same DLCI value in an unanswered SETUP, it shall respond RELEASE COMPLETE with a cause number 44 *requested circuit/channel not available*. Otherwise, it shall accept the received DLCI value. Its response to SETUP shall then depend on a consideration of other parameters and the will of the network user. If the response is positive, the same DLCI value shall be returned in CONNECT; if negative, a cause number other than 44 shall be returned in RELEASE COMPLETE. An SCF receiving a response of RELEASE COMPLETE with cause 44 shall retry its failed SETUP with a new randomly selected DLCI value. If the number of retries seems excessive, the SCF may choose to reseed its random number

generator. An SCF receiving a response of RELEASE COMPLETE with a cause number other than 44 shall indicate through N-DISCONNECT that the N-CONNECT request failed.

Figure 14 shows the messages exchanged and the primitives invoked following a user-requested N-DISCONNECT. Note that DL-RELEASE request and the transmission of DISCONNECT are not required, because MDL-REMOVE on each side properly resets the state of the affected DLCI.

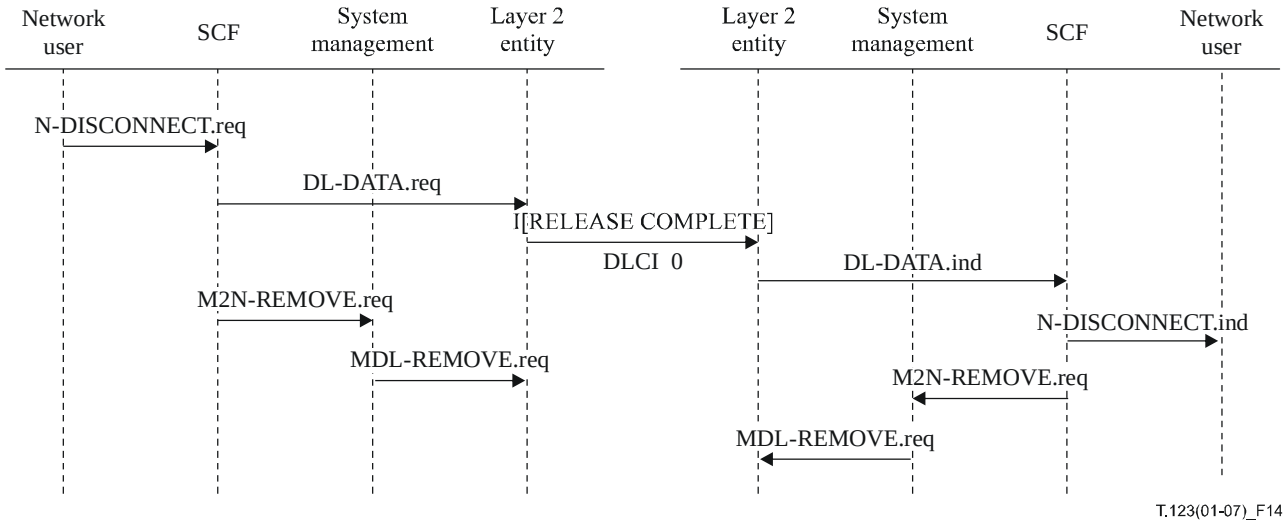


Figure 14 – Sequence of actions for N-DISCONNECT

To avoid a race condition, the SCF should delay re-using its released call reference for a new call if it initiated N-DISCONNECT. The reason for this is that if both sides disconnect and the caller reconnects using the same call reference value, a RELEASE COMPLETE in transit for the old call may be misinterpreted as a failure of the new call. The probability of this occurring is minimized if the SCF chooses next its least recently used call reference value. In practice, a serial assignment of values (incrementing by one each time) may suffice. Alternatively, the SCF may choose to employ a more complicated disconnect procedure, transmitting RELEASE and awaiting RELEASE or RELEASE COMPLETE.

An unrecovered error in data transfer over a DLCI is indicated by DL-ESTABLISH or by DL-RELEASE, depending on the success of resetting the data link. Either of these shall cause N-DISCONNECT to begin with an indication instead of a request, followed by the remaining actions of Figure 14. The exception is if DLCI 0 is affected; this has the more severe consequences specified earlier.

9.3 SCF messages

Information elements appear in a fixed order, as shown in Tables 2 through 5. Those of type M are either mandatory in [ITU-T Q.933] or required as part of the specification of this SCF. Those of type O are optional. Information elements that are not listed here should not be transmitted and may be ignored if received.

NOTE 1 – If NSAP selectors for a default MCS provider are administered to be null as recommended in clause 6, there may be no advantage in carrying subaddress information elements as part of SETUP and CONNECT. However, specific selectors may be required to reach an MCS provider in a particular context. Their possible use to support protocols other than T.125 sharing the same physical circuit is for further study.

NOTE 2 – The preferred binary encoding of an NSAP address is specified in clause A.5.3 of [ITU-T X.213].

Table 2 – SETUP message content

Information element	Type	Notes
Protocol discriminator	M	
Call reference	M	
Message type	M	
Bearer capability	M	ITU-T Rec. Q.922
DLCI	M	Preferred
End-to-end transit delay	O	Cumulative, requested, maximum
Link layer core parameters	O	N201, throughput(s), minimum(s)
Link layer protocol parameters	O	k, T200
X.213 priority	O	Data priority, lowest acceptable
Calling party subaddress	O	NSAP address
Called party subaddress	O	NSAP address

Table 3 – CONNECT message content

Information element	Type	Notes
Protocol discriminator	M	
Call reference	M	
Message type	M	
DLCI	M	Exclusive
End-to-end transit delay	O	Cumulative
Link layer core parameters	O	N201, throughput(s)
Link layer protocol parameters	O	k, T200
Connected subaddress	O	NSAP address
X.213 priority	O	Data priority

Table 4 – CONNECT ACKNOWLEDGE message content

Information element	Type
Protocol discriminator	M
Call reference	M
Message type	M

Table 5 – RELEASE COMPLETE message content

Information element	Type
Protocol discriminator	M
Call reference	M
Message type	M
Cause	M

9.4 Quality of service parameters

Important characteristics of data transfer performance are throughput, transit delay and priority. These are part of the QoS parameter set of N-CONNECT. QoS parameters are separate from, but may influence, the choice of protocol parameters. Parameters of both kinds may be conveyed by the SCF using optional information elements in SETUP and CONNECT.

Parameter negotiations shall obey the rules of clauses 5.1.3.3 and 5.2.3.3 of ITU-T Rec. Q.933 (1995).

Q.922 system parameters that may be negotiated are: k, N201 and T200. Their value shall be the same for both directions of transfer. If these parameters are not explicitly signalled, they shall take the default values of clause 10 below.

If QoS parameters are not explicitly signalled, the corresponding qualities are indeterminate and may take any values that are convenient for the service providers.

The QoS and protocol parameters in CONNECT, supplemented by any defaults, shall be final values for the assigned DLCI. The SCF shall pass these to the underlying layer 2 entity by M2N-ASSIGN, which emerges from the management plane as MDL-ASSIGN. This accords with clauses 4.1.1.5 and 4.1.1.10 of [ITU-T Q.922], which note that additional optional parameters may be included in these primitives.

The QoS and protocol parameters of DLCI 0 are not explicitly signalled. The QoS shall implicitly equal or exceed that of any other DLCI. The protocol parameters k, N201 and T200 for DLCI 0 shall take the default values.

A layer 2 entity may or may not implement data priority as a QoS parameter. If it does, the relative priority of DLCIs should determine the order of servicing user data requests queued for transmission, assuming that their respective protocol states are equally ready. DLCIs of the same priority should be treated impartially.

The SCF shall express data priorities using the value encoding of the information element *X.213 priority* (which agrees with the encoding of the X.25 packet layer). The lowest priority shall be 0 and the highest shall be, at most, 14. Requested priorities shall be negotiated downward into the range of values, beginning with 0, that the underlying layer 2 entity can implement distinctly.

10 Q.922 protocol parameters and options

The address field format shall be two octets (10-bit DLCIs).

Three bits of the address field are reserved for use with frame relaying service: forward explicit congestion notification (FECN), backward explicit congestion notification (BECN) and discard eligibility (DE). These bits shall be set to 0 by the transmitter and shall be ignored by the receiver.

Information transfer shall be in I-frames using the procedures of multiple frame acknowledged operation.

Frame types UI and XID shall not be transmitted.

System parameters are associated with each individual data link connection. Their values should be set taking into account characteristics of the underlying physical circuit. Default values are specified in Table 6.

Table 6 – Data link default system parameter values

System parameter	Default value	Parameter description
k	40	Maximum number of outstanding I-frames
N200	10	Maximum number of retransmissions
N201	260	Maximum number of octets in an information field
T200	1.5 s	Retransmission timer
T203	30 s	Idle timer

Values of k, N201 and T200 can be negotiated by the SCF specified in clause 9. The values of N200 and T203 need not be communicated from transmitter to receiver and may be set locally on each side.

The default value of k is the maximum value cited in clause 5.9.4 of [ITU-T Q.922] (for a link speed of 1536-1920 Mbit/s). This is also the value cited in Appendix VI of [ITU-T T.90], independent of the link speed, for optimum throughput with a packet size of 256 octets.

A value of k that is too large is better than a value that is too small. A Q.922 receiver need not accept a full window of I-frames if buffers are scarce; it can set the *own receiver busy* condition at some intermediate point. Moreover, a Q.922 transmitter can voluntarily limit itself to a smaller number of outstanding I-frames; it is not obliged to fill the window to maximum capacity. On the other hand, if k is set small and the window fills too quickly, a transmitter is required to cease. Throughput and response may suffer.

Appendix I of [ITU-T Q.933] suggests a procedure to negotiate the value of k using a formula that involves the data frame size in octets.

Implementers should consider the possibility of limiting frame size dynamically to a smaller value than system parameter N201 allows. This may require coordination with the transport layer that is forming TPDUs. It may be prudent to restrict the worst-case serial transmission time of lower priority data, so that newly queued data of higher priority can be serviced promptly. A maximum latency of 60 ms has been suggested.

The alternative option of aborting a low priority transmission already in progress may also be considered.

11 Data link frame structure transparency for start-stop transmission

Since start-stop transmission is organized as a sequence of octets, it is convenient to use an octet-stuffing scheme for data link frame structure transparency. This is a recognized alternative to the bit-stuffing scheme (insert a 0 bit after all sequences of five contiguous 1 bits) that is suitable for synchronous transmission. It makes the implementation of Q.922 for the PSTN profile easier and more efficient, especially when using the serial port of a typical personal computer.

For the PSTN case, clause 2.6 of [ITU-T Q.922], which defines frame structure transparency by reference to [ITU-T Q.921], shall not be implemented. In its place shall be implemented the following procedures taken from clause 4.5.2 of [ISO/IEC 3309]:

The control escape octet is a transparency identifier that identifies an octet occurring within a frame to which the following transparency procedure is applied. The encoding of the escape octet is given in Figure 15.

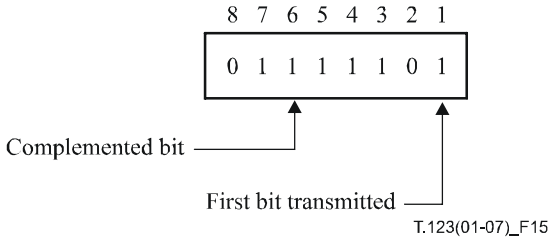


Figure 15 – Control escape octet for start-stop transparency

The transmitter shall examine the frame content between the opening and closing flag sequences including the address, control and FCS fields and, following completion of the FCS calculation, shall:

a) upon the occurrence of the flag or a control escape octet, complement the 6th bit of the octet; and

b) insert a control escape octet immediately preceding the octet resulting from the above prior to transmission.

Other octet values may optionally be included in the transparency procedure by the transmitter.

The receiver shall examine the frame content between the two flag octets and shall, upon receipt of a control escape octet and prior to FCS calculation:

a) discard the control escape octet; and

b) restore the immediately following octet by complementing its 6th bit.

A frame that ends with a control escape octet followed by a closing flag is invalid and shall be ignored by the receiver (frame abort).

NOTE – This procedure does not preclude any particular character occurring within the transmitted data stream. In the case of separate DTE and DCE, flow control between them via command characters (XON/XOFF) must be disabled because it cannot be distinguished from the DTE-to-DTE transmission of the same characters. For this Recommendation, in this case, flow control is a function of the Q.922 protocol.

12 Physical sublayer formed by H.221 MLP channels

Use of the H.221 MLP and H-MLP channels shall conform to the specifications of [ITU-T H.221], [ITU-T H.230], [ITU-T H.233], [ITU-T H.242] and [ITU-T H.243] for the integration of multimedia signals:

– To determine a compatible mode of operation, H.242 capability exchange sequence A applies.

– All systems capable of MLP shall declare at least the common capability MLP-6.4k.

– Other MLP and H-MLP bit rates defined by [ITU-T H.221] may also be declared.

– To establish or change mode, H.242 mode switching sequence B applies.

– Upon receipt of an H.221 command opening MLP or H-MLP, a system shall act to ensure that at least one of these is open in the opposite direction, so that full duplex communication may occur.

– The bit rates of MLP and H-MLP need not be the same in both directions of transmission unless symmetry is explicitly commanded.

– H.230 command MCS (multipoint command symmetrical data transmission) applies to MLP and H-MLP, requiring that the outgoing bit rates be set equal to the incoming bit rates.

As suggested in clause 9.2 of [ITU-T H.242], if both MLP and H-MLP are in force, their bit rates shall be combined to form a single serial stream. Bit positions shall be numbered horizontally across the synchronized H.221 framing of initial and additional channels, as illustrated in Tables 7 through 9.

H.221 commands to set the rate of MLP or H-MLP shall not disrupt the logical continuity of the combined serial stream. The input or output of bits shall simply continue in the next sub-multiframe at a modified rate. The operation of higher layer protocols will not be impacted unless the bit rate is reduced too low for a long period of time.

In particular, MLP, H-MLP, or both may be turned off temporarily in the process of re-arranging the bit rates of a multimedia multiplex. This by itself is not sufficient cause to disconnect Q.922 data links involuntarily. That step shall only be taken, in the absence of protocol-detected errors, upon receipt of the H.221 command T.120-off.

Table 7 – Bit positions for MLP-6.4k, restricted, encryption active

Initial channel							
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
						FAS	1
							1
							1
						BAS	1
							1
							1
						ECS	1
							1
							1
						M1	1
						M2	1
						•	1
						•	1
						M55	1
						M56	1

FAS Frame alignment signal
BAS Bit-rate allocation signal
ECS Encryption control signal

Table 8 – Bit positions for MLP-6.4k plus H-MLP-62.4k

Initial channel								Additional channel							
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
								M1	M2	M3	M4	M5	M6	M7	
							FAS	M8	•	•	•	•	•	M14	FAS
								•	•	•	•	•	•	•	
								•	•	•	•	•	•	•	
							BAS	•	•	•	•	•	•	•	BAS
								M106	•	•	•	•	•	M112	
							M113	M114	•	•	•	•	•	M120	M121
							•	•	•	•	•	•	•	•	•
							•	•	•	•	•	•	•	•	•
							M680	•	•	•	•	•	•	•	M688

Table 9 – Bit positions for H-MLP-128k in an H0 channel

Time-slot 1	Time-slot 2			Time-slot 3			Time-slot 4	Time-slot 5	Time-slot 6
	M1	• • •	M8	M9	• • •	M16			
	M17	• • •	•	•	• • •	M32			
	•	• • •	•	•	• • •	•			
	•	• • •	•	•	• • •	•			
	M1265	• • •	•	•	• • •	M1280			

13 Alternative profiles

These alternatives are designed to allow point-to-point connections between terminals or MCUs in special circumstances. Their use may be specified in the system recommendation for a particular service or may be agreed bilaterally.

The set of alternative profiles is not complete and is not intended to be an exhaustive list of all possibilities.

No procedures are offered here by which terminals may discover the fact that they share a common profile, nor is any provision made for negotiation in the event that they share more than one. The coding of Q.931 or Q.2931 call control information elements can restrict the set of profiles that may be considered, but it cannot guarantee a successful outcome. Such concerns are part of a larger design, which may choose to reference this Recommendation.

13.1 Alternative: ISDN based on [ITU-T Q.922]

Figure 16 defines an alternative profile for ISDN based on [ITU-T Q.922]. When video is not required and audio can be assigned its own channel, this is a less expensive protocol stack to implement than H.221. Layers above the B- or H-channel are identical to the ISDN basic profile.

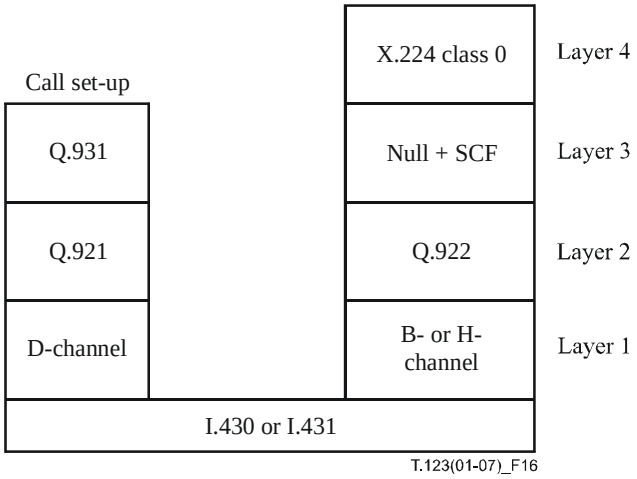


Figure 16 – Alternative profile for ISDN based on [ITU-T Q.922]

Layer 4

– As specified in clause 7.1, ISDN basic profile.

Layer 3

– As specified in clause 7.1, ISDN basic profile.

Layer 2

– As specified in clause 7.1, ISDN basic profile.

Layer 1

– One B-channel, one H0-channel, or one H1-channel.

– Some networks may also offer channels of intermediate bit rate.

13.2 Alternative: ISDN based on [ITU-T T.90]

Figure 17 defines an alternative profile for ISDN based on [ITU-T T.90]. Though less efficient than Q.922, the X.25 protocol stack is more familiar as a component of telematic terminals.

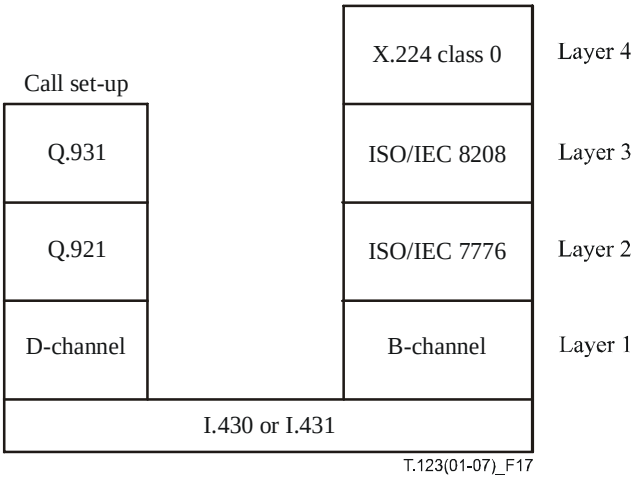


Figure 17 – Alternative profile for ISDN based on [ITU-T T.90]

Layer 4

– X.224.

– Class 0 preferred, no alternative class.

Layer 3

– DTE-DTE communication as specified in clause 2 of [ITU-T T.90].

Layer 2

– DTE-DTE communication as specified in clause 2 [ITU-T T.90].

Layer 1

– DTE-DTE communication as specified in clause 2 of [ITU-T T.90].

13.3 Alternative: ISDN based on [ITU-T V.120]

Figure 18 defines an alternative profile for ISDN based on [ITU-T V.120]. This protocol stack gives a typical personal computer access to ISDN speeds through a common terminal adapter. Layers above the terminal adaptation are identical to the PSTN basic profile.

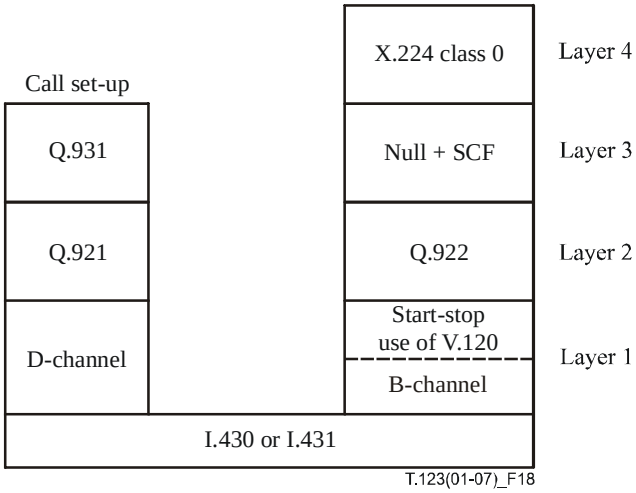


Figure 18 – Alternative profile for ISDN based on [ITU-T V.120]

Layer 4

– As specified in clause 7.1, ISDN basic profile.

Layer 3

– As specified in clause 7.1, ISDN basic profile.

Layer 2

– As specified in clause 7.1, ISDN basic profile.

Layer 1

– Start-stop transmission by DTE.

– DCE as specified in V.120 asynchronous mode operation.

– The DTE and DCE may be logical functions that are not physically separated if integrated equipment can produce the same transmitted signals.

13.4 Alternative: PSTN based on [ITU-T H.324]

Figure 19 defines an alternative profile for PSTN based on [ITU-T H.324]. This permits data conferencing to be widely deployed in conjunction with the PSTN videophone. Mapping Q.922 frames to AL-SDUs is a better use of scarce bandwidth than other possible framings. Layers above the adaptation are identical to the PSTN basic profile.

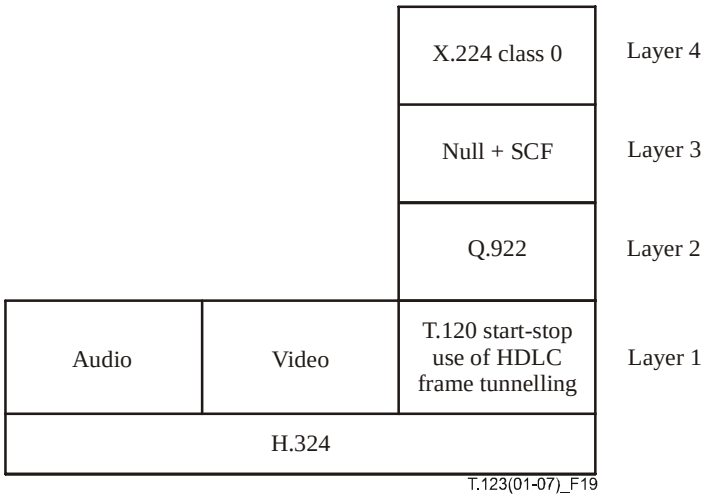


Figure 19 – Alternative profile for PSTN based on [ITU-T H.324]

Layer 4

– As specified in clause 7.1, ISDN basic profile.

Layer 3

– As specified in clause 7.1, ISDN basic profile.

Layer 2

– As specified in clause 7.4, PSTN basic profile.

Layer 1

– Start-stop transmission by DTE.

– DCE as specified in H.324 HDLC frame tunnelling for [ITU-T T.120].

– The DTE and DCE may be logical functions that are not physically separated if integrated equipment can produce the same transmitted signals.

NOTE – The net effect is that the content of a Q.922 frame – including FCS but without flags or transparency – is conveyed as one AL-SDU using framed AL1 over an H.223 logical channel opened for the T.120 data application.

13.5 Alternative: B-ISDN based on [ITU-T H.222]

Figure 20 defines an alternative profile for B-ISDN based on [ITU-T H.222]. This protocol stack multiplexes audio, video and data together over a single ATM virtual channel. Layers above Q.922 are identical to the ISDN basic profile.

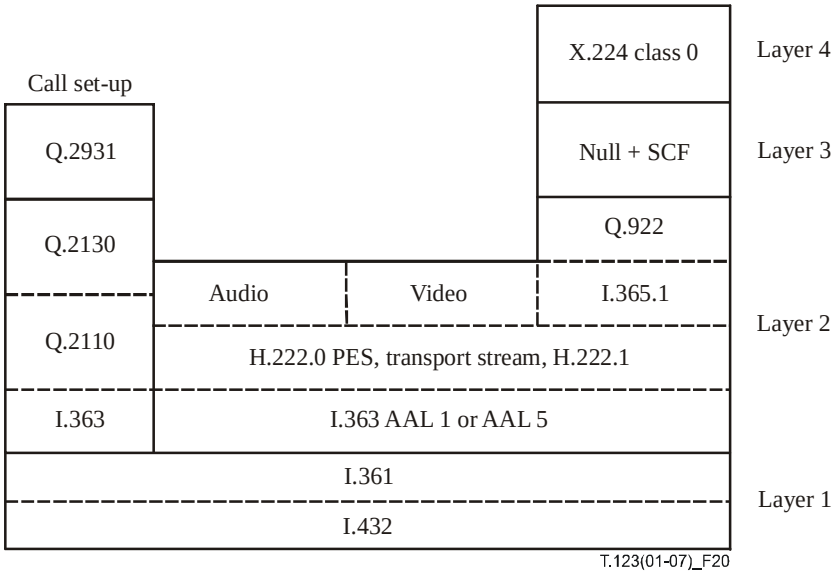


Figure 20 – Alternative profile for B-ISDN based on [ITU-T H.222]

Layer 4

– As specified in clause 7.1, ISDN basic profile.

Layer 3

– As specified in clause 7.1, ISDN basic profile.

Layer 2

– Q.922.

– Protocol parameters and options as specified in clause 10, Q.922 protocol parameters and options.

– Modified frame structure: no use of flags or transparency.

– Each frame (address octets through FCS) conveyed as the data bytes of one PES packet in the H.222.1-defined data elementary stream for protocol type T.120 subchannel.

– Transport stream transmission as specified in ITU-T Rec. H.222.1.

NOTE – The payload_unit_start_indicator classifies each transport stream packet as containing either the first segment or a continuation segment of a PES packet. If a segment is less than the maximum size, the difference is absorbed by stuffing bytes before the PES packet header to a total of 188 bytes.

Layer 1

– ATM virtual channel.

13.6 Alternative: LAN based on data unit transfer

Figure 21 defines an alternative profile for LAN based on data unit transfer. By aligning TPDUs with data units of the underlying LAN, such a protocol stack can eliminate some buffer management. Though its segmentation feature may add nothing to what the LAN already offers, X.224 is recommended for uniformity and as a basis for future enhancements.

NOTE 1 – No LAN protocol is named here, because the commercially important services are better known through their application programming interfaces. The protocols that support a service may be undisclosed or undocumented.

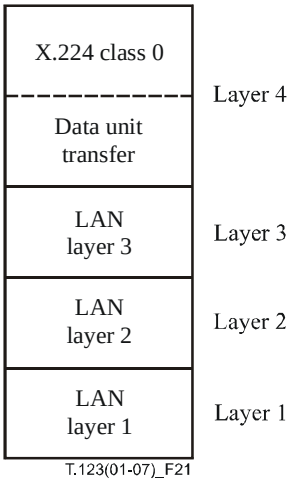


Figure 21 – Alternative profile for LAN based on data unit transfer

Layer 4

– X.224 class 0 preferred, no alternative class.

– Maximum TPDU size shall not exceed maximum LAN data unit.

– Data unit transfer with the following characteristics:

a) Connection-oriented service preserving octet sequence.

b) Boundary between data units retained as part of the transfer.

c) Residual error rate low enough to use as a type A network service.

d) Flow control mechanism to exert back-pressure on a transmitter.

NOTE 2 – NetBIOS extended user interface (NetBEUI), NetWare sequenced packet exchange (SPX), and AppleTalk data stream protocol (ADSP) are examples of the above.

NOTE 3 – In the case of SPX and ADSP, data unit boundaries are marked by setting an end-of-message bit.

Layer 3

– Common examples include NetWare internetwork packet exchange (IPX) and Apple datagram delivery protocol (DDP).

Layer 2

– Commonly, [ISO/IEC 8802] logical link control and medium access sublayers.

Layer 1

– Commonly, [ISO/IEC 8802] physical medium.

Annex A

Integration of multimedia signals framed according to [ITU-T H.221]

(This annex forms an integral part of this Recommendation)

Figure A.1 illustrates how [ITU-T H.221] aggregates the throughput of one or more digital channels and then partitions the total transfer rate into bit rate allocations for the individual media.

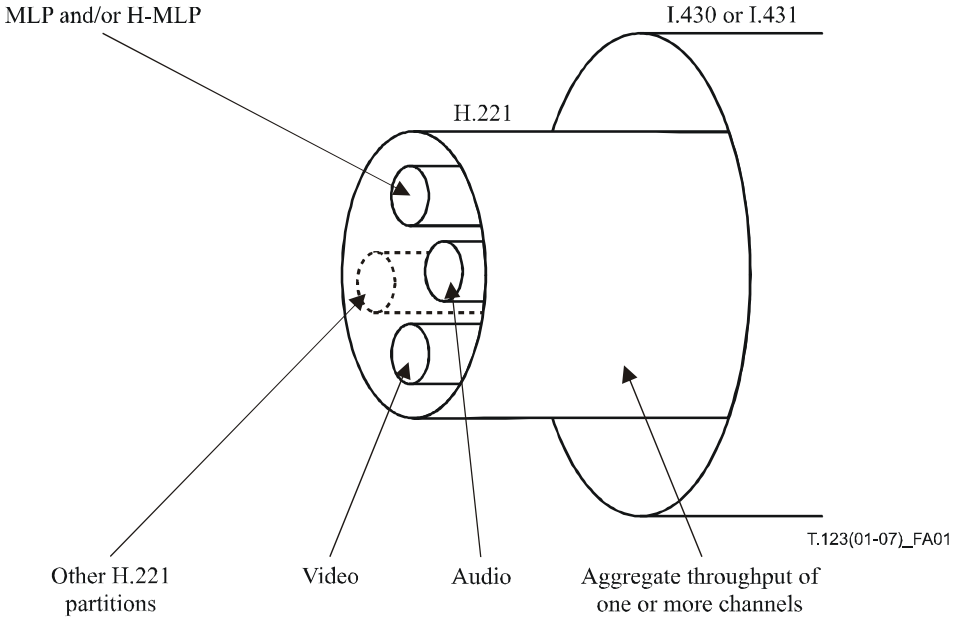


Figure A.1 – Integration of multimedia signals framed according to [ITU-T H.221]

Annex B

Extended transport connections

(This annex forms an integral part of this Recommendation)

B.1 Scope

This annex defines the procedures and protocol that will allow transport connections for a T.120 conference to negotiate the availability of extended transport services. These services may include use of security protocols, transport protocols, levels of reliability for data transfer and support for address aliases. This negotiation is designed to provide backward compatibility with T.123 transport stacks that only support baseline transport connections.

B.2 References

[ITU-T H.225.0] ITU-T Recommendation H.225.0 (2006), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T X.234] ITU-T Recommendation X.234 (1994) | ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless-mode transport service*.

[ITU-T X.274] ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Telecommunication and information exchange between systems – Transport layer security protocol*.

[ITU-T X.680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.681] ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2:2002, *Information Technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

[ITU-T X.691] ITU-T Recommendation X.691 (2002) | ISO/IEC 8825-2:2002, *Information technology – ASN.1 encoding rules – Specification of Packed Encoding Rules (PER)*.

B.3 Definitions

This annex defines the following terms:

B.3.1 baseline transport stack: A transport stack that does not support the procedures and protocol defined in this annex, but is otherwise compliant with T.123.

B.3.2 extended transport stack: A T.123 transport stack that supports the procedures and protocol defined in this annex.

B.3.3 network connection: A connection between two T.120 nodes using a specific set of protocols.

B.3.4 reliable protocol: A protocol that guarantees that data will reach its destination complete, uncorrupted and in the order that it was transmitted. TCP is an example of a reliable protocol.

B.3.5 transport connection: A logical connection between two T.120 nodes using one or more network connections.

B.3.6 unreliable protocol: A protocol that does not guarantee that data will reach its destination complete, uncorrupted and in the order that it was transmitted. UDP is an example of an unreliable protocol.

B.4 Abbreviations and acronyms

This annex uses the following abbreviations and acronyms:

CNP	Connection Negotiation Protocol
CNPPDU	Connection Negotiation Protocol – Protocol Data Unit
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
MAP	Multicast Adaptation Protocol (defined in Annex A of [ITU-T T.125])
MCS	Multipoint Communication Service
NSDU	Network Service Data Unit
PDU	Protocol Data Unit
SA ID	Security Association Identification
SAR	Segmentation And Reassembly
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security (protocol, defined by IETF RFC 4346~~Internet draft~~)
TLSP	Transport Layer Security Protocol (defined in [ITU-T X.274])
TPDU	Transport Protocol Data Unit
TSDU	Transport Service Data Unit
UDP	User Datagram Protocol

B.5 Conventions

– In this annex, "shall" refers to a mandatory requirement, while "should" refers to a suggested but optional feature or procedure. The term "may" refers to an optional course of action without expressing a preference.

– Unless otherwise specified, the aligned variant PER encoding of ASN.1 shall be used for all ASN.1 specified in this annex.

– Bits in an octet are numbered from 1 to 8, where bit 1 is the lowest order bit.

– Octets in a TPDU are numbered starting from 1 and increasing in the order they are put into an NSDU.

– All X.224 messages and message fields are in *ITALICIZED CAPS*.

– All ASN.1 and octet structure elements for CNP are in **Bold**.

B.6 Overview

T.123 baseline transport service is limited to the fully reliable transfer of data between nodes. A need for transport services not supported in baseline transport stacks has been identified. These services include security, unreliable data transfer and addressing by aliases.

Because the X.224 protocol cannot be arbitrarily extended, these services cannot simply be added to T.123's definition of a baseline transport connection while retaining backward compatibility. In response to this problem, the procedures and protocol in this annex define an extended transport connection with services that can be negotiated and extended.

B.6.1 Extended transport connection model

The model for a T.123 baseline transport connection is shown in Figure B.1. Connections of this type provide communication service between T.120 nodes using a single, reliable network connection. The specific network address of the called node must be known for a connection of this type to be established. In addition, neither security services nor unreliable data transfer services can be provided with this type of connection.

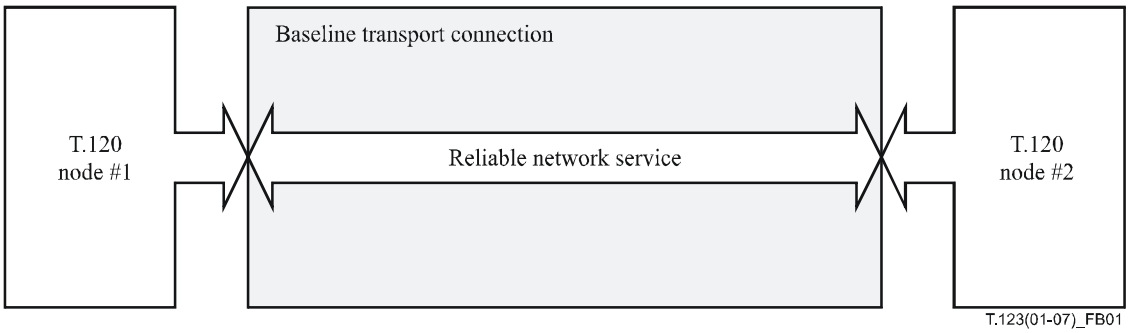


Figure B.1 – Baseline transport connection model

To add extended services to T.123 transports, a new connection model is being defined. This model is shown in Figure B.2. In this model, a transport connection consists of one or more network services, logically bound. These services may include reliable and unreliable data transfer as well as security services for transmitted data. This model is functionally equivalent to the baseline model when all optional services are omitted.

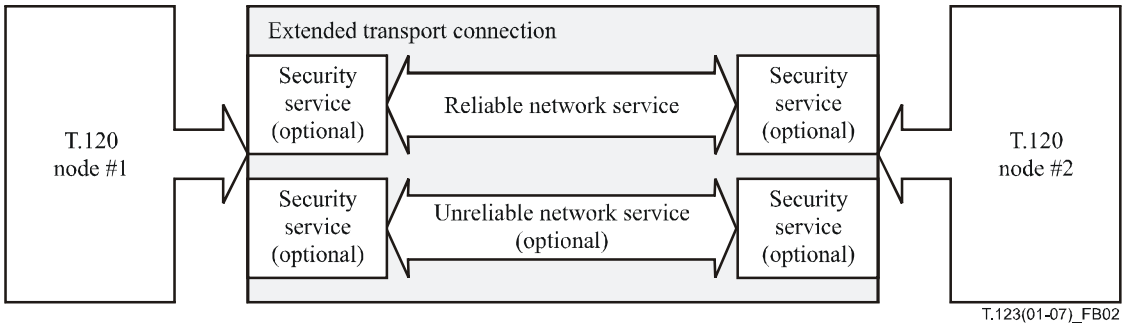


Figure B.2 – Extended transport connection model

In addition to security and reliability services, this annex specifies a method for using an alias address list to establish extended transport connections. These aliases can be used for a variety of purposes, including proxy, gateway and call redirection services for T.120 communications. An example of this type of extended transport connection is shown in Figure B.3.

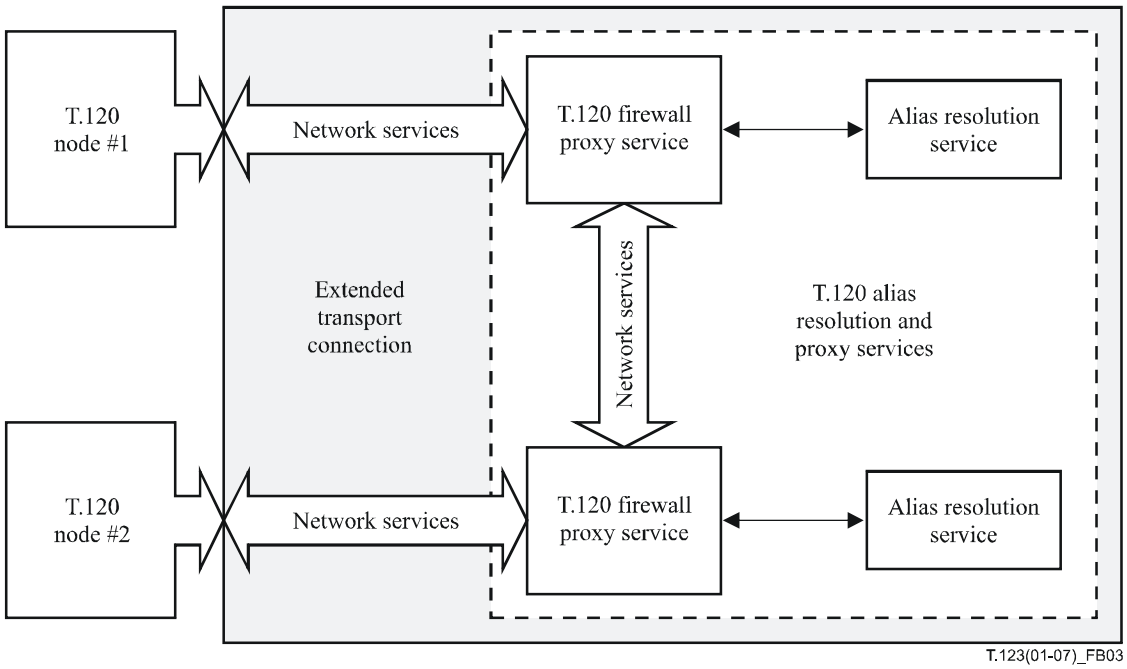


Figure B.3 – Example of extended transport connection via T.120 proxy

B.6.2 Transport services

While a variety of transport services may be negotiated using the procedures and protocol in this annex, the exact specification of many of these services is beyond the scope of this Recommendation. In particular, service definitions for T.120 gateways and proxies are topics for future study.

It should also be noted that many security services are implicitly defined in this annex. Where not otherwise specified, the mechanisms used to provide and control these services (e.g., obtaining certificates and out of band key exchange) are left to implementers.

B.6.3 Modified use of X.224

[ITU-T T.123] mandates the use of the X.224 class 0 protocol for baseline connections. It is desirable that extended connection establishment remain compatible with baseline connection establishment. To achieve this goal, the information for extended connection negotiations will be encapsulated within the X.224 *CONNECTION REQUEST (CR)***,** *CONNECTION CONFIRM (CC)* and *DISCONNECT REQUEST (DR)* TPDUs. The details for this procedure are given in clause B.7, Extended transport connections.

B.6.4 Connection negotiation protocol

This annex defines the protocol that will be used to establish extended transport connections. The connection negotiation protocol (CNP) is designed for encapsulation within X.224 or for use as a stand-alone protocol over a reliable network connection. To allow the protocol to be extended, CNP is defined using ASN.1 for its control PDUs. The details of CNP are given in clause B.9, Connection negotiation protocol (CNP).

B.7 Extended transport connections

The purpose of this clause is to define the procedure for establishing extended transport connections. This extended connection procedure is designed to allow a T.120 node to establish a transport connection to another T.120 node without prior knowledge about the called node's ability to support extended transport connections.

B.7.1 Initial connection establishment

[ITU-T X.224] defines the *TRANSPORT-SELECTOR* field as an optional, variable length field in the variable part of its PDU headers. As defined in clause 6.5.5 of [ITU-T X.224], it "indicates the calling and called transport service access points". This optional field is not used by X.224, or by baseline T.123. This clause defines its use for T.120 nodes to support extended transport connections.

Nodes supporting extended transport connections shall support the use of the *TRANSPORT-SELECTOR* field in the X.224 *CONNECTION REQUEST (CR)* TPDU and the *CONNECTION CONFIRM (CC)* TPDU. The variable part of the *DISCONNECT REQUEST (DR)* TPDU shall also be supported. The *TRANSPORT-SELECTOR* field of the *CR-TPDU, CC-TPDU* and the variable part of *DR-TPDU* shall contain CNP PDUs as specified in clause B.9. In all cases, the 128-octet limit set by X.224 for the *CR-TPDU* and the *DR-TPDU* shall be respected.

T.120 nodes supporting extended transport connections shall support the following call models.

B.7.1.1 Call establishment from a baseline transport

This call model is used when a T.120 node that supports only baseline connections attempts to connect to a node that supports extended connections. See Figure B.4.

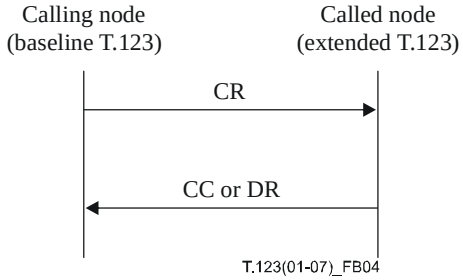


Figure B.4 – Call from baseline T.123 to extended T.123

This model is signalled at the called node when a *CR-TPDU* is received which does not contain a *TRANSPORT-SELECTOR* field. In this case, the called node shall respond according to the connection establishment defined for baseline T.123 connections. A response of *CC-TPDU* shall not contain a *TRANSPORT-SELECTOR* field. A response of *DR-TPDU* shall not contain the variable part of the PDU header. If the connection is accepted, the called node shall treat the connection as a baseline connection.

B.7.1.2 Call establishment to a baseline transport

This call model is used when a T.120 node that supports extended connections attempts to connect to a node supporting only baseline connections. See Figure B.5.

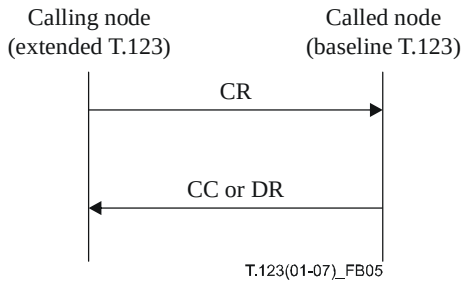


Figure B.5 – Call from extended T.123 to baseline T.123

In this model, the calling node shall place a *TRANSPORT-SELECTOR* field in the *CR-TPDU*. The baseline node will ignore the field and respond with a *CC-TPDU* without a *TRANSPORT-SELECTOR* field or a *DR-TPDU* without a variable part. This call model is signalled to the calling node when the response TPDU is received and it does not contain the appropriate optional field. If the connection is accepted, the calling node shall treat the connection as a baseline connection.

B.7.1.3 Call establishment using the initial network connection

This call model is used when a T.120 node supporting extended connections attempts to connect to a node that also supports extended connections. For this case, the called node determines that the services available with the existing network connection are sufficient and the T.120 connection is accepted. See Figure B.6.

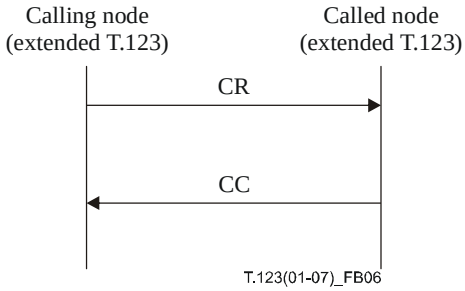


Figure B.6 – Call between extended T.123 nodes – Existing network connection selected

In this model, the calling node shall place a *TRANSPORT-SELECTOR* field in the *CR-TPDU*. The called node shall examine this field to determine if the existing network connection is to be maintained. If so, it shall respond with a *CC-TPDU* containing a *TRANSPORT-SELECTOR* field. This call model is signalled at the calling node when it receives the *CC-TPDU* containing the optional field.

Note that negotiated transport protocol changes may occur after the initial PDU exchange is complete, providing the existing network connection is maintained. Changes in transport protocol shall occur as if the network connection was newly created. Full connection procedures for the negotiated transport protocol shall occur over the existing network connection.

B.7.1.4 Call establishment by network reconnection

This call model is used when a T.120 node supporting extended connections attempts to connect to a node that also supports extended connections. For this case, the called node determines that the services available with the existing network connection are insufficient for the T.120 connection.

The connection attempt is rejected, but sufficient information is returned to the caller to allow a successful reconnection. See Figure B.7.

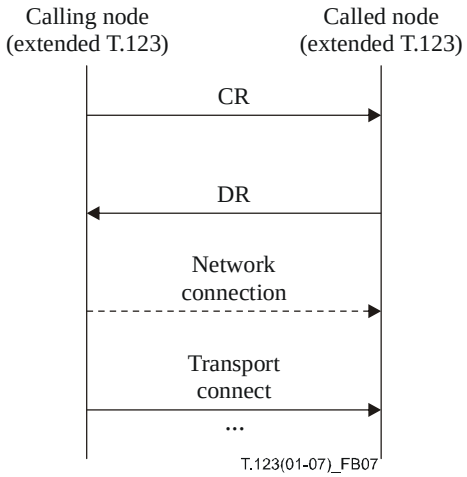


Figure B.7 – Call between extended T.123 nodes – Reconnection selected

In this model, the calling node shall place a *TRANSPORT-SELECTOR* field in the *CR-TPDU*. The called node will examine the field. If the called node determines that the existing network connection services are not sufficient, a new network connection may be required. In this case, the called node shall respond with a *DR-TPDU* containing a variable part.

This call model is signalled at the calling node when it receives the *DR-TPDU* containing the optional field.

After receiving the *DR-TPDU* containing the optional field, the calling node shall close the existing network connection. The caller shall then create a new network connection using the protocols, services and addresses returned in the variable part of *DR-TPDU*. Details of the reconnection procedure are given in clause B.9.5.2, Reconnection procedures.

Note that this reconnection procedure may occur more than once in the establishment of a single transport connection, if it is deemed necessary to establish the required transport services.

B.7.1.5 Connection refusal

This call model is used when a T.120 node supporting extended connections attempts to connect to any node that does not wish to accept the connection. See Figure B.8.

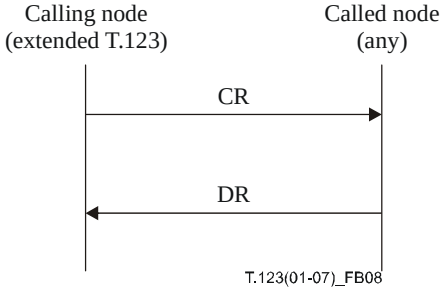


Figure B.8 – Call refusal

In this model, the calling node shall place a *TRANSPORT-SELECTOR* field in the *CR-TPDU*. The called node may examine the field. If the called node determines that the transport connection is to be refused, the caller shall respond with a *DR-TPDU* that does not contain a variable part. This call model is signalled at the calling node when it receives the *DR-TPDU* without the optional field.

Reasons for refusing a connection are a matter left to implementers. These may include security incompatibility, exceeded connection limits, or other local policy violations.

B.7.1.6 Abandoned connection attempt

This call model is used when a T.120 node supporting extended connections attempts to connect to any node and the calling node decides to abandon the call attempt before the connection is completed. See Figure B.9.

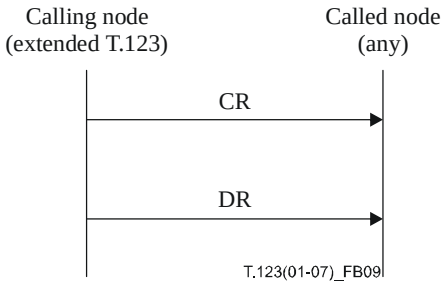


Figure B.9 – Abandoned call attempt

In this model, the calling node shall place a *TRANSPORT-SELECTOR* field in the *CR-TPDU*. If the calling node decided to abandon the call attempt before it receives a *CC-TPDU* or *DR-TPDU*, then it shall send a *DR-TPDU* that contains a variable part. This call model is signalled at the called node when it receives the *DR-TPDU* containing the optional field.

Reasons for abandoning a connection attempt are a matter left to implementers. These may include an expired time-out on a connection attempt or other local policy violations.

B.7.2 Connection re-establishment

When a calling node, in response to a *CR-TPDU*, receives a *DR-TPDU* containing the variable part of the PDU, it indicates that the existing network services are not adequate for the set of transport services selected by the calling node. In this case, the calling node shall immediately close the network connection associated with the attempted call.

After the network connection is closed, the calling node will create a network connection that provides the services (e.g., security) indicated in the variable part of the *DR-TPDU*. Once the new network connection has been established, the full connection procedure for the selected transport protocols will be followed normally.

One case where reconnection may occur is if the desired parameter lists were too large to send within the 128-octet limit on PDU sizes imposed by X.224. In this case, the calling node should negotiate the use of CNP as the transport protocol to be used. In the subsequent **ConnectRequestPDU**, the 128-octet limit does not apply and desired parameter lists may be included.

Note that it may be necessary to re-establish the network connection multiple times in order to establish the final transport connection.

B.7.3 Unreliable network service

If an unreliable data transmission service is to be provided by a transport connection, it shall be negotiated by the same CNP exchange that establishes the final reliable data transmission service.

The unreliable data service for the T.120 connection shall be considered established only after the reliable data transmission service has been established.

B.8 Extended profiles

B.8.1 Reliable transports

B.8.1.1 CNP extended profile

Figure B.10 defines the CNP extended profile for reliable transport service. This profile is identical to any of the basic or alternative profiles defined in this Recommendation, except that the CNP layer replaces the X.224 class 0 layer.

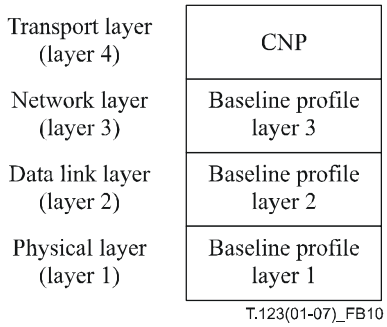


Figure B.10 – Extended profile using CNP for reliable transport service

Layer 4

– CNP.

Layer 3

– As specified in T.123 basic or alternative profiles.

Layer 2

– As specified in T.123 basic or alternative profiles.

Layer 1

– As specified in T.123 basic or alternative profiles.

B.8.1.2 SSL/TLS extended profiles

Figure B.11 defines the extended profiles for adding security services to T.123 using SSL or TLS. These profiles are identical to the basic, alternative or extended LAN profiles, except that SSL or TLS is added to the transport layer between the TPKT layer and the stream layer.

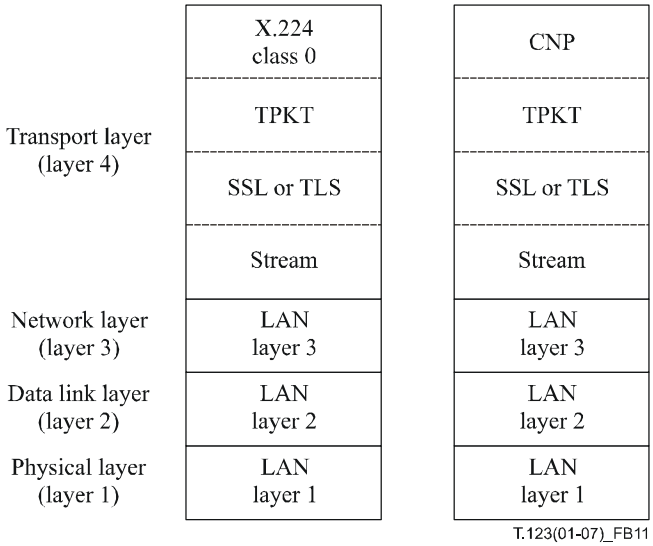


Figure B.11 – Extended profiles using SSL or TLS for security services

Layer 4

– X.224 class 0 or CNP for reliable transport service.

– TPKT packet header to delimit TPDUs, as specified in clause 8, Packet header to delimit data units in an octet stream.

NOTE 1 – TPKT is required because an octet-stream service does not mark where data unit boundaries occur.

– SSL or TLS.

– Octet-stream transfer with the following characteristics:

a) Connection-oriented service preserving octet sequence.

b) Residual error rate low enough to use as a type A network service.

c) Flow control mechanism to exert back-pressure on a transmitter.

NOTE 2 – The following specifies a protocol for octet-stream transfer that is a common example of the above:

a) RFC 793, Transmission control protocol.

b) By default, destination port number 1503 per RFC 1700, Assigned numbers, but others may be used.

Layer 3

– Commonly, RFCs 791, 792, 919, 922, 950, 1112, Internet protocol.

Layer 2

– Commonly, [ISO/IEC 8802] logical link control and medium access sublayers.

Layer 1

– Commonly, [ISO/IEC 8802] physical medium.

B.8.1.3 IPSec extended profiles

Figure B.12 defines the extended profiles for adding security services to T.123 using IPSec. These profiles are identical to the basic, alternative or extended LAN profiles, except that IPSec is added to the network layer.

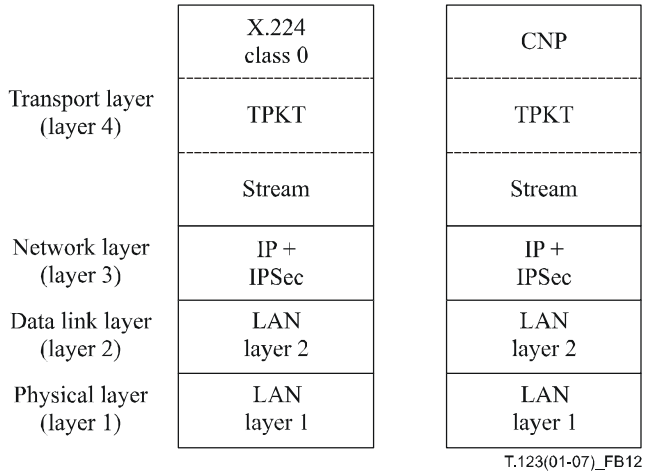


Figure B.12 – Extended profiles using IPSec for security services

Layer 4

– X.224 class 0 or CNP for reliable transport service.

– TPKT packet header to delimit TPDUs, as specified in clause 8, Packet header to delimit data units in an octet stream.

NOTE 1 – TPKT is required because an octet-stream service does not mark where data unit boundaries occur.

– Octet-stream transfer with the following characteristics:

a) Connection-oriented service preserving octet sequence.

b) Residual error rate low enough to use as a type A network service.

c) Flow control mechanism to exert back-pressure on a transmitter.

NOTE 2 – The following specify a layered protocol for octet-stream transfer that is an example of the above:

a) RFC 793, Transmission control protocol.

b) By default, destination port number 1503 per RFC 1700, Assigned numbers, but others may be used.

Layer 3

– Commonly, RFCs 791, 792, 919, 922, 950, 1112, Internet protocol.

– IPSec.

Layer 2

– Commonly, [ISO/IEC 8802] logical link control and medium access sublayers.

Layer 1

– Commonly, [ISO/IEC 8802] physical medium.

B.8.1.4 X.274 extended profiles

Figure B.13 defines the extended profiles for adding security services to T.123 using X.274. These profiles are identical to any of the basic or alternative profiles, or to the extended profile of B.8.1.1, CNP extended profile, except that X.274 is added to the transport layer immediately below the CNP or X.224 class 0 layers.

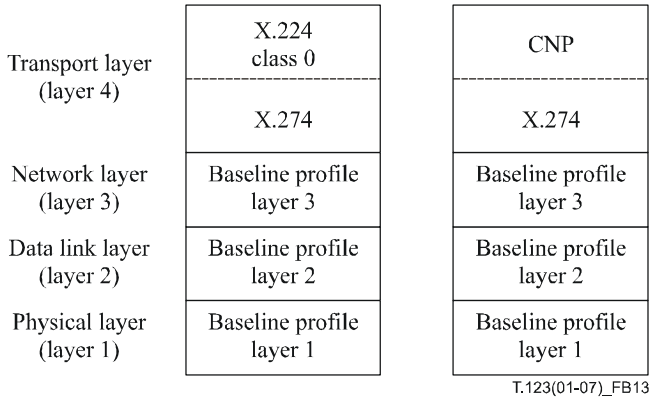


Figure B.13 – Extended profiles using X.274 for security services

Layer 4

– X.224 class 0 or CNP for reliable transport service.

– X.274 for security service.

Layer 3

– As specified in T.123 basic or alternative profiles.

Layer 2

– As specified in T.123 basic or alternative profiles.

Layer 1

– As specified in T.123 basic or alternative profiles.

B.8.1.5 GSS-API extended profiles

Figure B.14 defines the extended profiles for adding security services to T.123 using the IETF GSS-API security framework. Appendix II provides background on the security framework defined by IETF GSS-API. These profiles are identical to the basic, alternative or extended LAN profiles, except that GSS-API token passing is added to the transport layer above the X.224 class 0 or CNP layers.

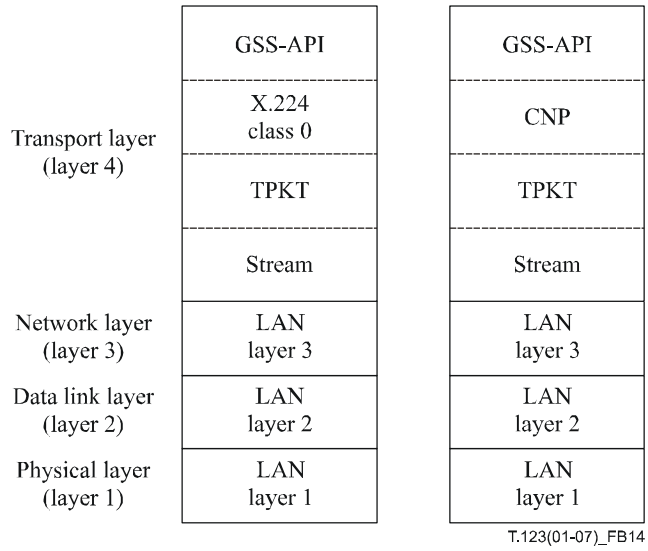


Figure B.14 – Extended profiles using GSS-API for security services

Layer 4

– GSS-API token exchange.

– X.224 class 0 or CNP for reliable transport service.

– TPKT packet header to delimit TPDUs, as specified in clause 8, Packet header to delimit data units in an octet stream.

NOTE 1 – TPKT is required because an octet-stream service does not mark where data unit boundaries occur.

– Octet-stream transfer with the following characteristics:

a) Connection-oriented service preserving octet sequence.

b) Boundary between data units *not* retained as part of the transfer.

c) Residual error rate low enough to use as a type A network service.

d) Flow control mechanism to exert back-pressure on a transmitter.

NOTE 2 – The following specifies a protocol for octet-stream transfer that is a common example of the above:

a) RFC 793, Transmission control protocol.

b) By default, destination port number 1503 per RFC 1700, Assigned numbers, but others may be used.

Layer 3

– Commonly, RFCs 791, 792, 919, 922, 950, 1112, Internet protocol.

Layer 2

– Commonly, [ISO/IEC 8802] logical link control and medium access sublayers.

Layer 1

– Commonly, [ISO/IEC 8802] physical medium.

B.8.2 Unreliable transports

B.8.2.1 Unreliable LAN profile

Figure B.15 defines the extended profile for adding unreliable transport services to T.123 over LAN connections. Layers 1, 2 and 3 are identical to any of the basic or alternative LAN profiles.

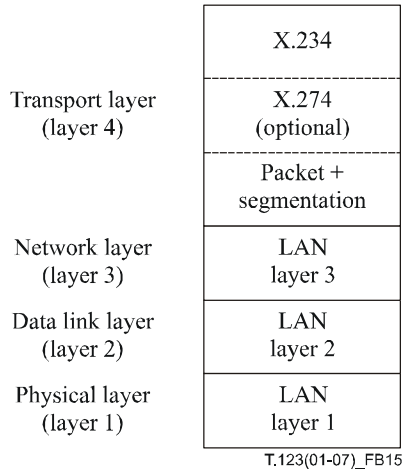


Figure B.15 – Unreliable LAN profile

Layer 4

– X.234, connectionless mode.

– X.274 (optionally negotiated by CNP).

– Unreliable packetized data transfer with segmentation.

NOTE – User datagram protocol (UDP) is a common example of the above.

Layer 3

– As specified in T.123 baseline LAN profiles.

Layer 2

– As specified in T.123 baseline LAN profiles.

Layer 1

– As specified in T.123 baseline LAN profiles.

B.8.2.2 Unreliable PSTN profile

See Figure B.16.

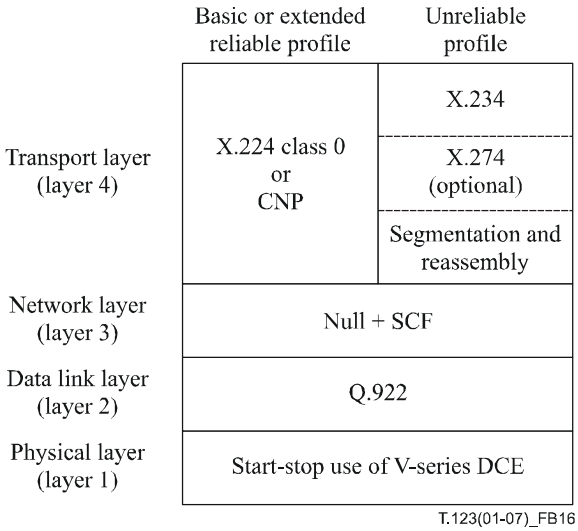


Figure B.16 – Unreliable PSTN profile

Layer 4

– X.234, connectionless mode.

– X.274 (optional, negotiated via CNP).

– Unreliable segmentation and reassembly protocol as defined in clause B.10, Unreliable segmentation and reassembly protocol.

Layer 3

– As specified in T.123 basic PSTN profile.

Layer 2

– Q.922, using unnumbered information (UI)

Layer 1

– As specified in T.123 basic PSTN profile.

B.9 Connection negotiation protocol (CNP)

B.9.1 Overview

The PDUs defined in this protocol are based on their X.224 class 0 counterparts. Both X.224 and CNP provide connect request, connect confirm, disconnect request, data, and error TPDUs. In addition, CNP provides a **NonStandardPDU** for protocol extensibility.

The CNP TPDUs defined in this annex shall not be used outside the context of T.120 communications.

B.9.2 Structure of CNP TPDUs

All CNP transport protocol data units (TPDUs) shall contain a whole number of octets. When consecutive octets are used to represent a binary number, the lower octet number shall have the most significant value. CNP transport entities shall respect bit and octet ordering conventions, thus allowing communication to take place.

Figure B.17 illustrates the structure of CNP TPDUs.

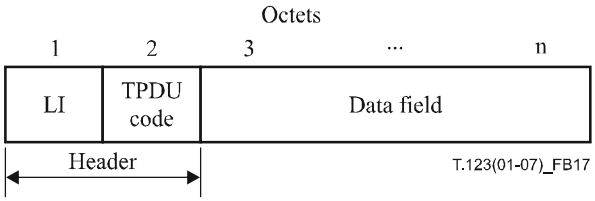


Figure B.17 – CNP general TPDU structure

CNP TPDUs shall contain, in the following order:

– The header, comprising:
  a) the length indicator (LI) field;
  b) the TPDU code.
– The data field.

CNP TPDUs are divided into two categories: control and data. The values of the header fields for each of these TPDU types are given in Table B.1. The data field of control TPDUs shall contain an ASN.1 structure as defined in clause B.9.3, Control TPDUs. The data field of data TPDUs shall contain octet structures as defined in clause B.9.4, Data TPDUs.

Table B.1 – CNP TPDU field values

TPDU	Type	LI	TPDU code	Data field
Connect request	Control	0000 0001	0100 0111	ASN.1
Connect confirm	Control	0000 0001	0100 0111	ASN.1
Disconnect request	Control	0000 0001	0100 0111	ASN.1
Error	Control	0000 0001	0100 0111	ASN.1
Nonstandard	Control	0000 0001	0100 0111	ASN.1
Data	Data	0000 0001	0100 0110	Octet structures

B.9.3 Control TPDUs

The structure of a CNP control TPDU is illustrated in Figure B.18.

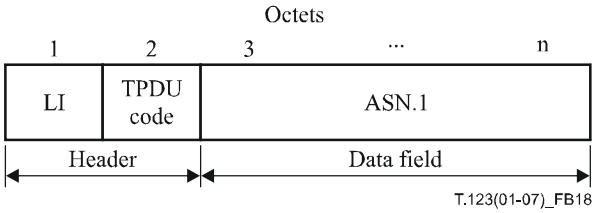


Figure B.18 – CNP control TPDU structure

All CNP control TPDUs shall use the following octet values for header fields:

– LI 0000 0001

– TPDU code 0100 0111

The data field for these TPDUs shall consist of a single ASN.1 encoded **CNPControlPDU** structure, as defined in clause B.9.6, ASN.1 definition. Descriptions of this structure's components are given below.

B.9.3.1 Common information elements

Portions of the ASN.1 for CNP were derived from other sources, as described below:

1) **Priority** was derived from Annex A of [ITU-T T.125].

2) **H221NonStandard, NonStandardIdentifier, NonStandardParameter** and **AliasAddress** (as well as its required sub-types such as **TransportAddress** and **PartyNumber**) were derived from [ITU-T H.225.0].

ReliableTransportProtocol: specifies a single, reliable transport protocol and the conditions under which it may be used. This structure contains the following elements:

– **type**: specifies CNP, X.224, MAP or a non-standard protocol.

– **maxTPDUSize**: the maximum supported size (in octets) of a single TPDU, including the header.

– **nonStandardParameters**: information not defined in this Recommendation. (e.g., proprietary data).

ReliableSecurityProtocol: specifies a single security protocol for use with reliable data transfer. This value will specify one of the following:

– None.

– TLS.

– SSL.

– IPSec (with IKE or manual key management).

– X.274 (with or without SA ID support).

– GSS-API.

– Physical[1].

– A non-standard protocol.

---

[1] Indicates that a physically secure connection exists between the connecting nodes for reliable communications. Determining whether or not this condition exists is outside the scope of this Recommendation and is a matter for implementers. Note that this condition must be both proposed and accepted during connection establishment to be considered in effect.

UnreliableTransportProtocol: specifies a single, unreliable transport protocol and the conditions under which it may be used. This structure contains the following elements:

– **type**: Specifies either X.234 or a non-standard protocol.

– **maxTPDUSize**: The maximum supported size of a single TPDU, including the header.

– **sourceAddress**: Network address to be used in conjunction with this protocol. This is the address that the sender of the **UnreliableTransportProtocol** structure will use to receive unreliable data for the connection being negotiated.

– **sourceTSAP**: TSAP to be used in conjunction with this protocol. The sender of the **UnreliableTransportProtocol** structure may use this identifier to distinguish between data for this connection and data from other connections when both are received at the same network address.

– **nonStandardParameters**: Information not defined in this Recommendation (e.g., proprietary data).

UnreliableSecurityProtocol: specifies a single security protocol for use with unreliable data transfer. This value will specify one of the following:

– None.

– IPSec (with IKE or manual key management).

– X.274 (with or without SA ID support).

– Physical[2].

– A non-standard protocol.

B.9.3.2 Connect request

protocolIdentifier: The version of the CNP protocol supported by the caller.

reconnectRequested: When a called node receives a connect request with this field set to *true*, it shall respond with a disconnect request. This field should be set *true* by the calling node in an X.224 encapsulated connect request when the full connection information will not fit within the size constraints of a *CR-TPDU*. In this case, CNP should be negotiated for reconnection so that the complete set of connection information may be exchanged.

Priority: The priority of the data to be sent over this transport connection. If omitted, this connection shall be used to transfer all data priorities.

reliableTransportProtocols: A list of the reliable transport protocols supported by the calling node, in order of preference. If omitted, the existing protocol shall continue to be used.

reliableSecurityProtocols: A list of the reliable security protocols supported by the calling node, in order of preference. Omitting this field indicates that the caller does not support reliable security protocols.

unreliableTransportProtocols: A list of the unreliable transport protocols supported by the calling node, in order of preference. Omitting this field indicates that the caller does not support unreliable data transfer.

unreliableSecurityProtocols: A list of the unreliable security protocols supported by the calling node, in order of preference. Omitting this field indicates that the caller does not support unreliable security protocols.

destinationAddress: A sequential list of transport aliases for establishing the connection.

nonStandardParameters: Information not defined in this Recommendation (e.g., proprietary data).

---

[2] See Footnote 1.

B.9.3.3 Connect confirm

protocolIdentifier: The version of the CNP protocol to be used by this transport connection.

reliableTransportProtocol: The reliable transport protocol to be used by this transport connection. If omitted, the current protocol (i.e., X.224 or CNP) shall continue to be used.

reliableSecurityProtocol: The reliable security protocol to be used by this transport connection. Omitting this field indicates that a reliable security protocol will not be used by this connection.

unreliableTransportProtocol: The unreliable security protocol to be used by this transport connection. Omitting this field indicates that an unreliable data transfer will not be supported by this connection.

unreliableSecurityProtocol: The unreliable security protocol to be used by this transport connection. Omitting this field indicates that an unreliable security protocol will not be used by this connection.

nonStandardParameters: Information not defined in this Recommendation (e.g., proprietary data).

B.9.3.4 Disconnect request

disconnectReason: Reason for the disconnection. This field may have the following values:

– **unacceptableVersion**: In response to a connect request, indicates that the version of CNP used in the connect request is not acceptable.

– **incompatibleParameters**: In response to a connect request, indicates that no acceptable common set of valid connection parameters was found.

– **securityDenied**: Indicates that local security policies do not permit the connection to be established[3] or to continue operation if already established.

– **destinationUnreachable**: In response to a connect request, indicates that the called node cannot complete the connection as specified by the caller.

– **userRejected**: In response to a connect request, indicates that the connection attempt was rejected at a level above the transport.

– **userInitiated**: After a connection has been established, indicates that the disconnection was requested at a level above the transport.

– **protocolError**: Indicates that a fatal error occurred while processing a TPDU.

– **unspecifiedFailure**: A non-specific error occurred.

– **routeToAlternate**: In response to a connect request, indicates that the connection is desired, but that the caller should attempt to reconnect using the information in the remaining fields.

– **nonStandardDisconnectReason**: A reason not defined in this Recommendation (e.g., a proprietary reason).

reliableTransportProtocol: The reliable transport protocol to be used after reconnection. If omitted, X.224 shall continue to be used. This field is valid only if **disconnectReason** was **routeToAlternate**.

reliableSecurityProtocol: The reliable security protocol to be used after reconnection. Omitting this field indicates that a reliable security protocol will not be used after reconnection. This field is valid only if **disconnectReason** was **routeToAlternate**.

---

[3] It is acceptable to issue a *DR-TPDU* without the optional field (as described in clause B.7.1.5, Connection refusal) if the called node does not wish to disclose the reason for rejecting a connection attempt.

unreliableTransportProtocol: The unreliable transport protocol to be used after reconnection. Omitting this field indicates that an unreliable data transfer will not be supported after reconnection. This field is valid only if **disconnectReason** was **routeToAlternate**.

unreliableSecurityProtocol: The unreliable security protocol to be used after reconnection. Omitting this field indicates that an unreliable security protocol will not be used after reconnection. This field is valid only if **disconnectReason** was **routeToAlternate**.

destinationAddress: A sequential list of transport aliases to be used by the caller for establishing the new connection. This field is valid only if **disconnectReason** was **routeToAlternate**.

nonStandardParameters: Information not defined in this Recommendation (e.g., proprietary data).

B.9.3.5 Error

rejectCause: reason the PDU was rejected. This field may have the following values:

– **unrecognizedPDU**: Indicates that the PDU did not decode into a recognizable form.

– **invalidParameter**: Indicates that the PDU contained one or more invalid parameter values.

– **causeUnspecified**: A non-specific cause.

– **nonStandardRejectCause**: A cause not defined in this Recommendation (e.g., a proprietary cause).

rejectedPDU: The rejected PDU.

nonStandardParameters: Information not defined in this Recommendation (e.g., proprietary data).

B.9.3.6 Nonstandard PDU

nonStandardParameters: Information not defined in this Recommendation (e.g., proprietary data).

B.9.4 Data TPDUs

B.9.4.1 Structure

The structure of a CNP data TPDU is illustrated in Figure B.19.

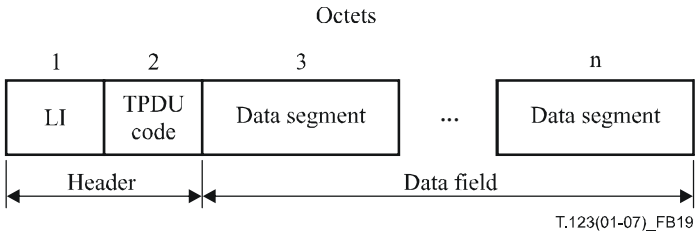


Figure B.19 – CNP data TPDU structure

All CNP data TPDUs shall use the following octet values for header fields:

– LI 0000 0001

– TPDU Code 0100 0110

The data field for a data TPDU shall consist of one or more data segments, as described below.

B.9.4.2 Data segments

The structure of a data segment is shown in Figure B.20.

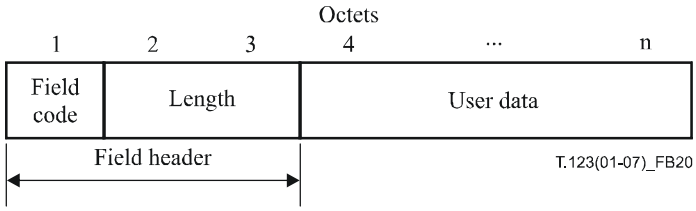


Figure B.20 – Data segment structure

A data segment is an octet structure composed of a fixed length field header and variable number of user data octets.

The following parameters are required in a data segment:

a) **Field code** **(octet 1)**

Parameter length: one octet

Parameter value: 000y zzzz

y indicates whether this is the final segment of a user data packet. Setting y to a value of 1 indicates a final segment.

zzzz is a binary value equal to the MCS priority of the data.

b) **Length** **(octets 2 and 3)**

Parameter length: two octets

Parameter value: a binary value indicating the number of user data octets, with a maximum value of 65530.

c) **User data** **(octets 4 through length + 3)**

Parameter length: **Length** octets

Parameter value: user data octets

B.9.5 Using CNP within X.224

B.9.5.1 Encapsulating TPDUs

During the connection procedures described in clause B.7.1, Initial connection establishment, X.224 TPDUs shall be used to encapsulate CNP TPDUs as follows:

– The *TRANSPORT-SELECTOR* field in a *CR-TPDU* shall contain a **Connect Request TPDU**.

– The *TRANSPORT-SELECTOR* field in a *CC-TPDU* shall contain a **Connect Confirm TPDU**.

– The variable part of a *DR-TPDU* shall contain either a **Disconnect Request TPDU** or an **Error TPDU**.

B.9.5.2 Reconnection procedures

– If the reliable transport protocol indicated in a **Connect Confirm TPDU** is X.224, either side may immediately send a *DATA (DT) TPDU*, or any other valid X.224 PDU.

– If the reliable transport protocol indicated in a **Connect Confirm TPDU** is CNP, either side may immediately send a **Data TPDU**, or any other valid CNP PDU.

– If the reliable transport protocol indicated in a **Connect Confirm TPDU** is not X.224 or CNP, both the calling and called nodes shall follow the complete connection establishment procedure for the selected protocol (i.e., the caller will issue the appropriate connect request PDU).

B.9.6 ASN.1 definition

```
--*****************************************************************************
--*     ASN.1 Definition for CNP Control PDUs
--*****************************************************************************

CNP-PROTOCOL {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

--
--  Imported Definitions
--

IMPORTS
        NonStandardParameter,
        TransportAddress,
        AliasAddress
    FROM H323-MESSAGES
            -- H.225.0 Version 2
            -- {itu-t (0) recommendation (0) h (8) 2250 version (0) 2}

        Priority
    FROM MAP-PROTOCOL;
            -- T.125 Annex A Version 1

ProtocolIdentifier ::= OBJECT IDENTIFIER
    -- shall be set to
    -- {itu-t (0) recommendation (0) t (20) 123 annexb (2) 1}

--
--  Service Negotiation Types
--

TPDUSize ::= INTEGER (128..65535)

ReliableTransportProtocolType ::= CHOICE
{
    cnp                          NULL,
    x224                         NULL,
    map                          NULL,
    nonStandardTransportProtocol NonStandardParameter,
    ...
}

ReliableTransportProtocol ::= SEQUENCE
{
    type                         ReliableTransportProtocolType,
    maxTPDUSize                  TPDUSize,
    nonStandardParameters        SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}
ReliableSecurityProtocol ::= CHOICE
{
    none                         NULL,
    tls                          NULL,
    ssl                          NULL,
    ipsecIKEKeyManagement        NULL,
    ipsecManualKeyManagement     NULL,
    x274WithoutSAID              NULL,
    x274WithSAID                 X274WithSAIDInfo,
    gssApi                       NULL,
    physical                     NULL,
```

```
    nonStandardSecurityProtocol  NonStandardParameter,
    ...
}

UnreliableTransportProtocolType ::= CHOICE
{
    x234                         NULL,
    nonStandardTransportProtocol NonStandardParameter,
    ...
}

UnreliableTransportProtocol ::= SEQUENCE
{
    type                              UnreliableTransportProtocolType,
    maxTPDUSize                       TPDUSize,
    sourceAddress                     TransportAddress,
    sourceTSAP                        OCTET STRING OPTIONAL,
    nonStandardParameters             SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

UnreliableSecurityProtocol ::= CHOICE
{
    none                              NULL,
    ipsecIKEKeyManagement             NULL,
    ipsecManualKeyManagement          NULL,
    x274WithoutSAID                   NULL,
    x274WithSAID                      X274WithSAIDInfo,
    physical                          NULL,
    nonStandardSecurityProtocol       NonStandardParameter,
    ...
}

X274WithSAIDInfo ::= SEQUENCE
{
    localSAID                         OCTET STRING,
    peerSAID                          OCTET STRING,
    ...
}

--
--  CNP Control PDU Types
--

ConnectRequestPDU ::= SEQUENCE
{
    protocolIdentifier                ProtocolIdentifier,
    reconnectRequested                BOOLEAN,
    priority                          Priority OPTIONAL,
    reliableTransportProtocols        SEQUENCE OF ReliableTransportProtocol
                                      OPTIONAL,
    reliableSecurityProtocols         SEQUENCE OF ReliableSecurityProtocol
                                      OPTIONAL,
    unreliableTransportProtocols      SEQUENCE OF UnreliableTransportProtocol
                                      OPTIONAL,
    unreliableSecurityProtocols       SEQUENCE OF UnreliableSecurityProtocol
                                      OPTIONAL,
    destinationAddress                SEQUENCE OF AliasAddress OPTIONAL,
    nonStandardParameters             SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

ConnectConfirmPDU ::= SEQUENCE
{
```

```
    protocolIdentifier              ProtocolIdentifier,
    reliableTransportProtocol       ReliableTransportProtocol OPTIONAL,
    reliableSecurityProtocol        ReliableSecurityProtocol OPTIONAL,
    unreliableTransportProtocol     UnreliableTransportProtocol OPTIONAL,
    unreliableSecurityProtocol      UnreliableSecurityProtocol OPTIONAL,
    nonStandardParameters           SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

DisconnectReason ::= CHOICE
{
    unacceptableVersion             NULL,
    incompatibleParameters          NULL,
    securityDenied                  NULL,
    destinationUnreachable          NULL,
    userRejected                    NULL,
    userInitiated                   NULL,
    protocolError                   NULL,
    unspecifiedFailure              NULL,
    routeToAlternate                NULL,
    nonStandardDisconnectReason     NonStandardParameter,
    ...
}

DisconnectRequestPDU ::= SEQUENCE
{
    disconnectReason                DisconnectReason,
    reliableTransportProtocol       ReliableTransportProtocol OPTIONAL,
    reliableSecurityProtocol        ReliableSecurityProtocol OPTIONAL,
    unreliableTransportProtocol     UnreliableTransportProtocol OPTIONAL,
    unreliableSecurityProtocol      UnreliableSecurityProtocol OPTIONAL,
    destinationAddress              SEQUENCE OF AliasAddress OPTIONAL,
    nonStandardParameters           SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

RejectCause ::= CHOICE
{
    unrecognizedPDU                 NULL,
    invalidParameter                NULL,
    causeUnspecified                NULL,
    nonStandardRejectCause          NonStandardParameter,
    ...
}

ErrorPDU ::= SEQUENCE
{
    rejectCause                     RejectCause,
    rejectedPDU                     OCTET STRING,
    nonStandardParameters           SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}
NonStandardPDU ::= SEQUENCE
{
    nonStandardParameters           SEQUENCE OF NonStandardParameter OPTIONAL,
    ...
}

CNPControlPDU ::= CHOICE
{
    connectRequest                  ConnectRequestPDU,
    connectConfirm                  ConnectConfirmPDU,
    disconnectRequest               DisconnectRequestPDU,
    error                           ErrorPDU,
```

```
    nonStandardCNPPDU                   NonStandardPDU,
    ...
}

END
```

B.10 Unreliable segmentation and reassembly protocol

B.10.1 Overview

This protocol was designed for use over unreliable, packet-based connections and is based on the SAR functions described in RFC 791, Internet protocol. The protocol defines a single PDU that will allow a sender to segment a TSDU into one or more TPDUs small enough to be transmitted by a size-limited lower network layer. At the receiver, the TPDU segments can be reassembled to provide the complete, original TSDU to a higher network layer. Although this protocol does not assume ordered or guaranteed delivery of packets, it does assume that received packets are uncorrupted.

B.10.2 Structure of unreliable SAR TPDUs

All unreliable SAR transport protocol data units (TPDUs) shall contain a whole number of octets. When consecutive octets are used to represent a binary number, the lower octet number shall have the most significant value. Unreliable SAR transport entities shall respect bit and octet ordering conventions, thus allowing communication to take place.

Note that the issues involved in re-ordering out-of-order fragments by the receiver are a matter left for implementers.

The structure of an unreliable SAR TPDU is shown in Figure B.21.

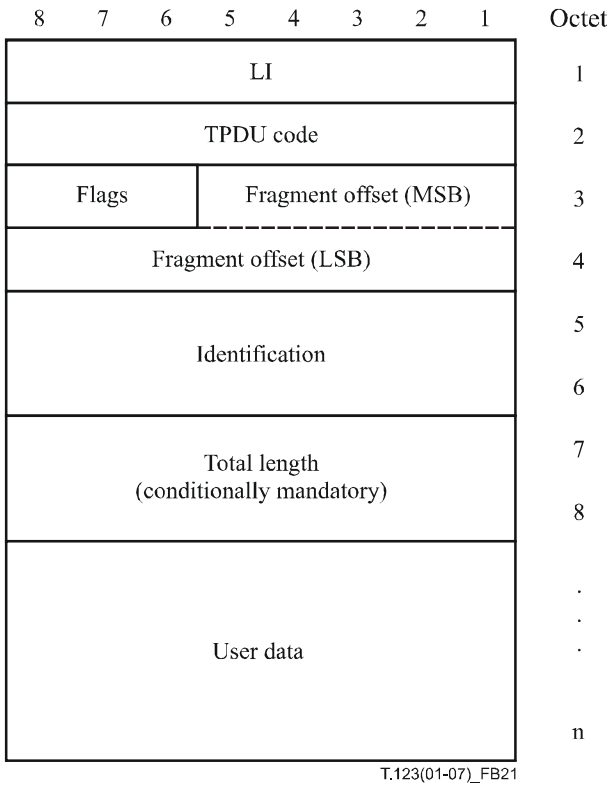


Figure B.21 – Unreliable SAR TPDU structure

Unreliable SAR TPDUs shall contain, in the following order:

– The header, comprising:
  a) The length indicator (LI) field;
  b) The TPDU code;
  c) The flags field;
  d) The fragment offset field;
  e) The identification field;
  f) Conditionally, a total length field.
– The user data field.

B.10.2.1 Length indicator field

Field length: one octet

Field value: a binary value indicating the header length in octets, including optional fields, but excluding the length indicator field and user data.

B.10.2.2 TPDU code

Field length: one octet

Field value: the binary value: 0100 0110

B.10.2.3 Flags field

Field length: 3 bits

Field value: Bit 8: reserved, must be set to zero

Bit 7: reserved, must be set to zero

Bit 6: more fragments (MF) flag

0 = last fragment in TSDU

1 = more TSDU fragments to follow

B.10.2.4 Fragment Offset field

Field length: 13 bits

Field value: a binary value indicating where in the reassembled TSDU this fragment belongs. The fragment offset is measured in units of 8 octets. The offset of the first fragment is zero. Bit 5 of octet 3 represents the most significant bit of this value.

B.10.2.5 Identification field

Field length: two octets

Field value: a binary value identifying common fragments of a datagram. This unsigned value shall be zero for the first TSDU sent over a connection and incremented by 1 for each succeeding TSDU.

B.10.2.6 Total Length field (conditionally mandatory)

Field length: two octets

Field value: a binary value indicating the total length of the TSDU, measured in octets. This value shall be included with the first fragment of any TSDU segmented into multiple fragments. The value may be included with any or all other fragments.

B.10.2.7 User Data field

Field length: variable

Field value: user data octets

~~Bibliography~~

~~– IETF RFC 2078 (January 1997), *Generic Security Service Application Program Interface*.~~

Appendix I

Multimedia conference call set-up in the ISDN

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

I.1 Introduction

Multimedia conference (MMC) terminals, currently under standardization in ITU-T, are intended to operate within the ISDN. However, various terminals of different types such as telephone, facsimile group 4, videophones and teleconference systems are also connected to the ISDN.

The following scenarios are derived from [ITU-T Q.931], which provides more information and describes other possibilities. Attention should be paid to the coding of information elements for BC, LLC and HLC, because they are important for interworking.

Table I.1 suggests values that may be used in a SETUP message. The called side terminal should also accept other values of the information elements for BC, LLC and HLC. Alternative settings include unrestricted digital information with tones and announcements (UDI-TA), rate adaptation to 56 kbit/s for restricted networks, double BC/HLC and absence of LLC. When HLC is used, call acceptance should be configured by the user to allow either telephony 7 kHz, video telephony, or telephony 3.1 kHz.

Table I.1 – Parameter settings originated in SETUP message

Information element	BC	LLC	HLC
Information transfer capability	Unrestricted digital information	Unrestricted digital information	
Transfer mode	Circuit	Circuit	
Information transfer rate	64 kbit/s	64 kbit/s	
User information layer 1 protocol		H.221	
High layer characteristics identification			AC[a)]

[a)] AC audiographic teleconference.

VC (videoconferencing), VP (videophone) and AV (audiovisual) are acceptable in the case of the called side.

I.2 Basic requirements

The following conditions are basic requirements:

1) An MMC terminal has the ISDN I/F function inside it and directly connects to the ISDN at a S(T) point.

2) An MMC terminal desires to intercommunicate with the following terminals:

   a) MMC terminal;

   b) Videophone, teleconference with H.221 frame structure supported.

   Items a) and b) mentioned above will together be called AV (audiovisual) terminals in the following.

   Intercommunication between MMC terminals and telephones is the fundamental demand. However, each side uses different ISDN services (e.g., MMC: unrestricted digital

information, telephone: speech); therefore, this type of intercommunication would be difficult, without using special sequences, as shown in Figures I.2 and I.3.

3) This description is for the point-to-point connection only. The outline of the sequence is shown in Figure I.1.

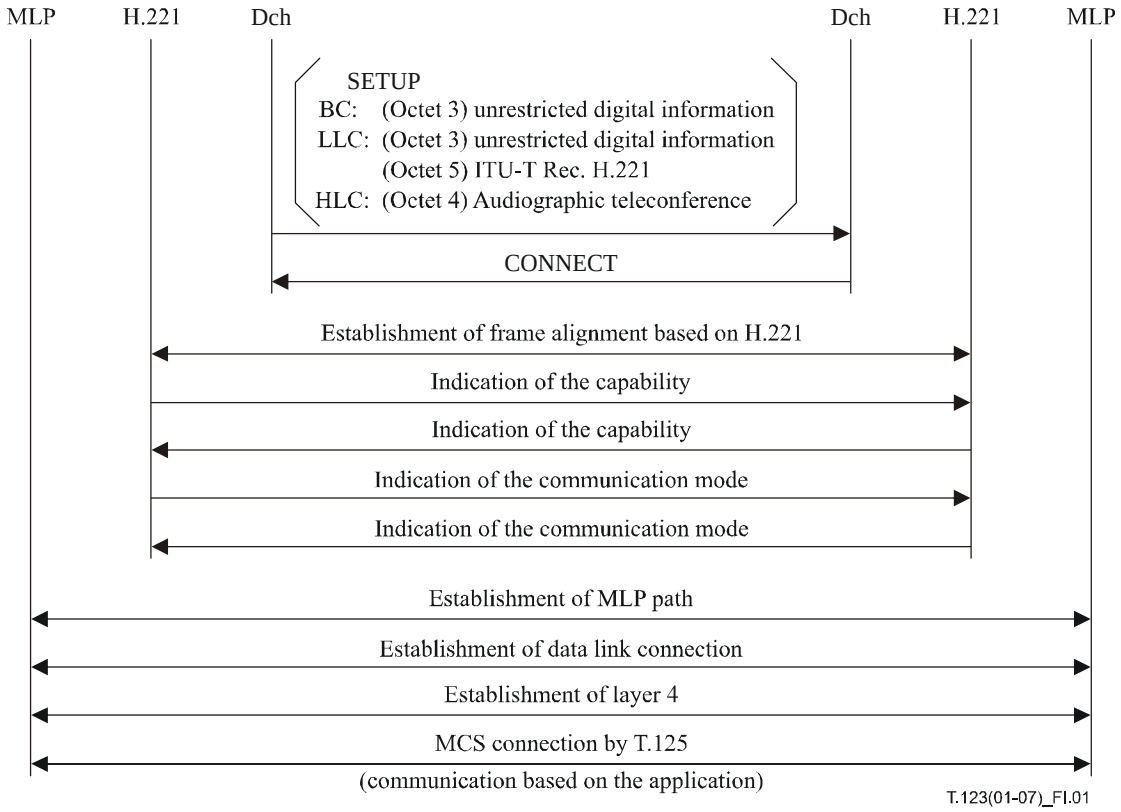
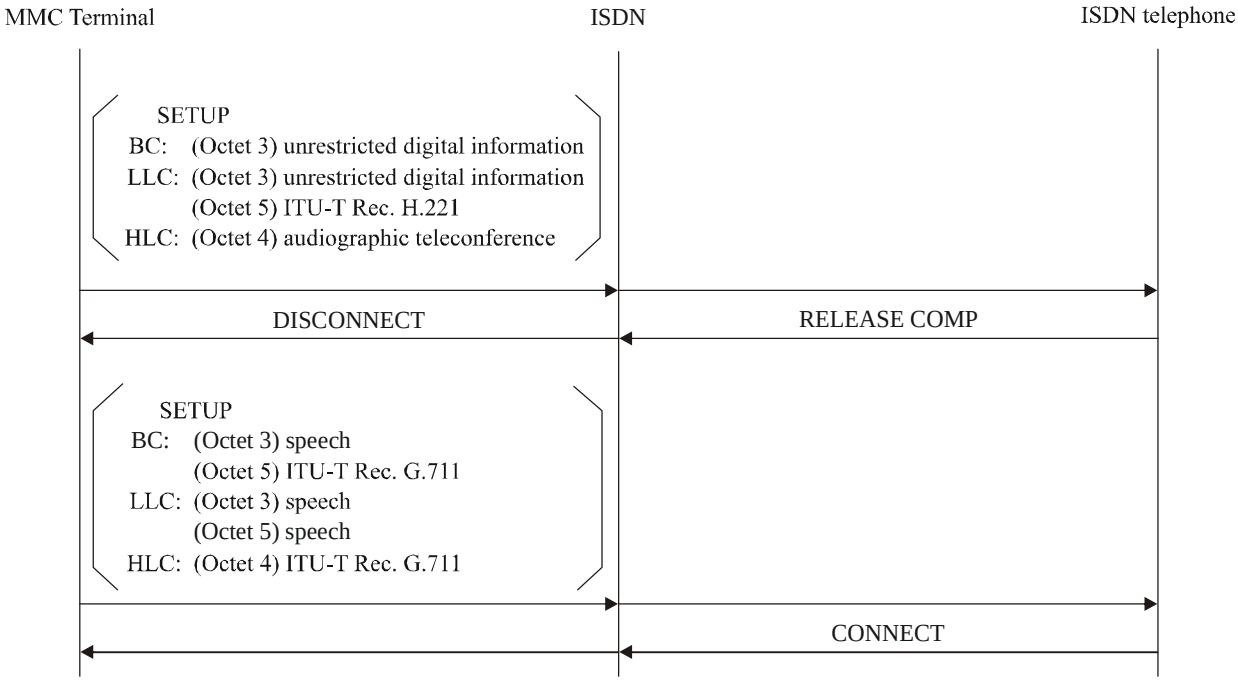
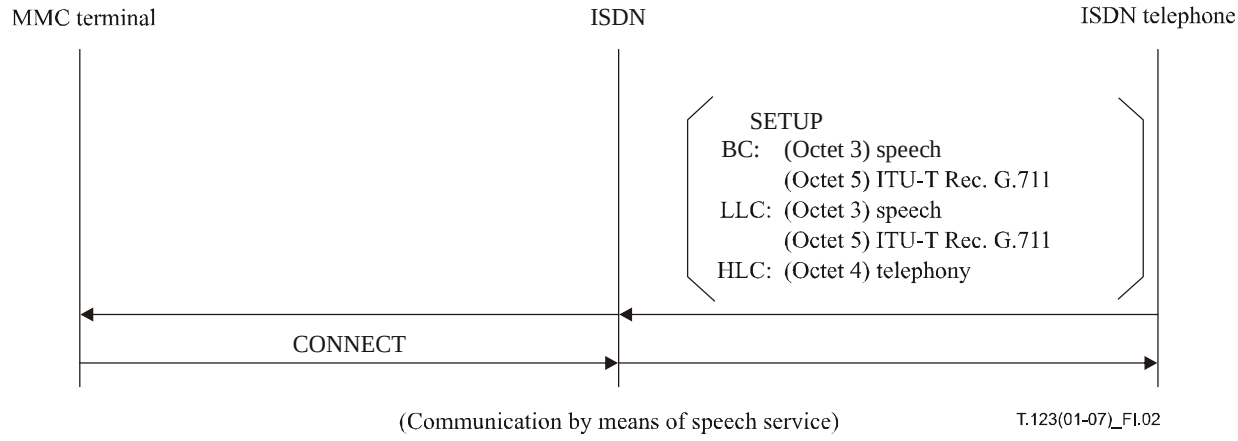


Figure I.1 – Communication establishment sequence for MMC terminals

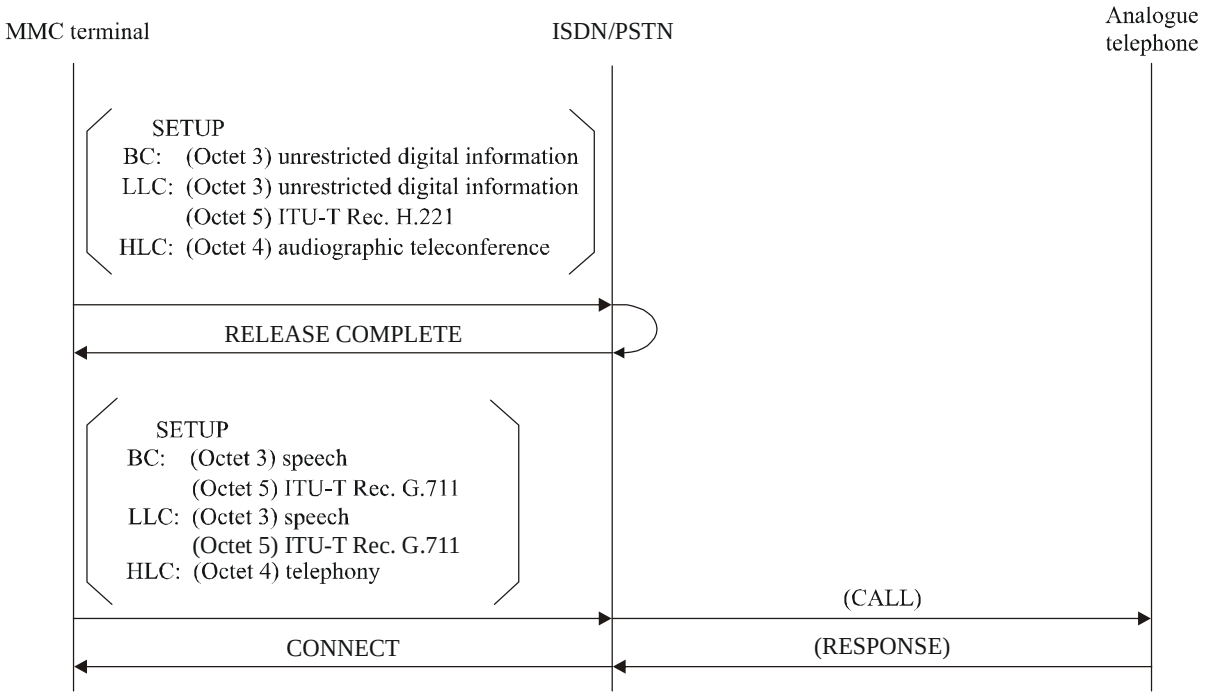


1) Call from MMC terminal to ISDN telephone



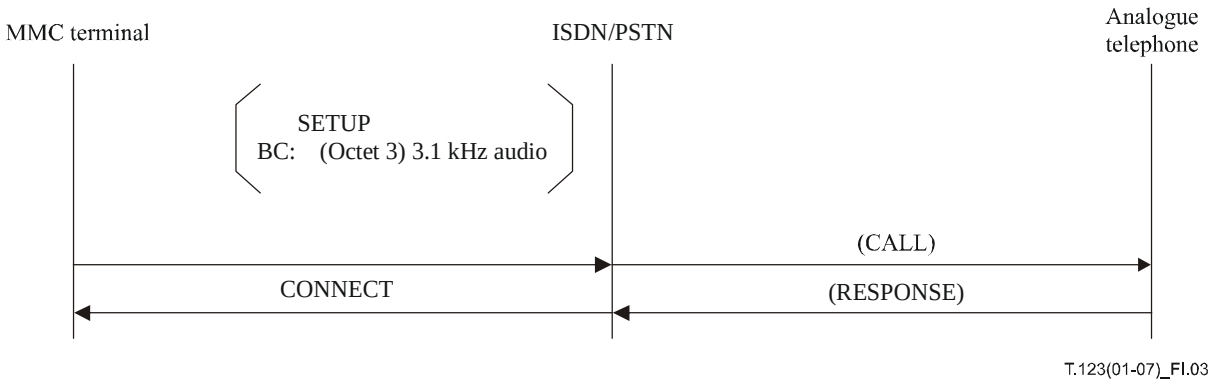
2) Call from ISDN telephone to MMC terminal

Figure I.2 – Intercommunication sequences for MMC terminal and ISDN telephone



(Communication by means of speech service)

3) Call from MMC terminal to analogue telephone



(Communication by means of speech service)

4) Call from analogue telephone to MMC terminal

Figure I.3 – Intercommunication sequences for MMC terminal and analogue telephone

I.3 Connection phase

The connection procedure can be divided into the following three phases:

1) Phase A (ISDN D-channel protocol) – By using the D-channel signalling protocol (see [ITU-T Q.931]), an MMC terminal makes the call control so as to establish an ISDN B-channel for communicating with an AV terminal.

2) Phase B (H.242 protocol) – An MMC terminal based on [ITU-T H.221] establishes frame alignment and decides communication mode based on the H.242 sequence (MMC mode/speech mode), and establishes the MLP path.

3) Phase C (T.120-series protocol) – In the case that both terminals have MMC functionality and decide to communicate by MMC mode, the T.120 protocol is started and the final communication function is decided in detail, leading to the start of actual communication.

I.4 Phase A (ISDN D-channel protocol)

In making call control based on [ITU-T Q.931] (D-channel signalling protocol), the parameters specified in Table I.1 are to be set in the SETUP message on the originating side. In this Recommendation, however, the table shows only information elements of:

1) Bearer capability (BC);

2) Low layer capability (LLC);

3) High layer capability (HLC);

all of which are needed to recognize the other terminal's communication capability.

An MMC terminal on the calling side should set the above parameters in the SETUP message for sending, whilst on the called side it should check the parameters so as to judge the possibility of communication. Finding it possible to communicate, it may accept the call and connect to a B-channel. Then an MMC terminal starts to intercommunicate with an audiovisual terminal which may be another MMC terminal, or another type of audiovisual terminal such as videophone.

I.5 Phase B (H.242 protocol)

After connecting to the B-channel, the following procedures should be carried out based on [ITU-T H.242]:

1) Frame alignment conforming to [ITU-T H.221] is the mode. Then, by using BAS, the capability exchange sequence is executed in 7-bit PCM mode (mode 0F).

2) After each side recognizes the other's capability, they decide their own communication mode including common mode. That is, when both are sure of having MLP capability, the MLP path is established and the T.120 protocol is started, leading to phase C.

3) In the case where one side has no MLP capability, their communication is limited to audio and possibly video (for example, if one side is an MMC and the other side is a videophone).

I.6 Phase C (T.120-series protocol)

1) To establish a data link connection on the MLP path.

2) To establish layer 4.

3) After channels are established, conforming with [ITU-T T.125], the negotiations, in order to recognize each other's function regarding MMC and the information necessary for the conference, are exchanged by generic conference control through the application roster.

Appendix II

GSS-API security framework

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

II.1 Introduction

This appendix provides background on the security framework defined by the IETF generic security service-application programming interface (GSS-API) within Annex B.

II.2 IETF common authentication technology (CAT)

This clause provides background references on various security efforts within the IETF that relate to GSS-API.

II.2.1 IETF and cat working group

The Internet Engineering Task Force (IETF) has centralized its security work within one framework that is now commonly used across all IETF protocols. RFC 1511, entitled "Common Authentication Technology Overview", outlines this work and its purpose.

II.2.2 GSS-API security framework

The security framework of the CAT working group is manifested by GSS-API in RFC 1508. GSS-API is an API that produces a well-defined set of data structures for communication over a reliable channel between two negotiating entities. [b-RFC 2078] explains the mechanics of the security framework.

II.2.3 SPNEGO

The GSS-API security context negotiation can be problematical. It is possible to support multiple security mechanisms within GSS-API. However, there is no means to identify which security mechanism an opaque token is intended for. Effectively, upon receiving the first token, a calling application of GSS-API must attempt validation of the token for each installed security mechanism, until success (or ultimate failure). This approach will unambiguously arrive at the correct conclusion, but it is inefficient. To optimize the use of GSS-API, a security mechanism that enables simple negotiation is being defined by the CAT working group. The simple and protected GSS-API negotiation mechanism, or SPNEGO, is standards-track RFC 2478.

II.3 T.123 Annex B security framework

Annex B implicitly defines a security framework for T.120. Assuming the reliable transmission case, the framework has the following characteristics.

A list of well-known reliable security protocols. This list is extensible, allowing the inclusion of non-standard protocols (i.e., protocols not included in the list).

Nodes that support extended transport connections can select and make use of a particular security protocol they may both support, through a simple capability negotiation mechanism using the call models specified in clause B.7.

The caller transmits a set of reliable security protocols it can support in the CNP ConnectRequestPDU.

The called party may signal that the services available with the current network connection are sufficient or insufficient for the security protocol desired (using either a CNP DisconnectRequestPDU or CNP ConnectConfirmPDU, respectively). In either case, the called party transmits its choice of the single reliable security protocol to use (that must be an element of the set advertised by the caller).

In the case of sufficient services, the T.120 connection proceeds using the existing network connection (this may include negotiated transport protocol changes).

In the case of insufficient services, the caller closes the existing network connection and creates a new network connection that provides the services indicated by the called party in the CNP DisconnectRequestPDU.

In all of the extended profiles defined in Annex B, security is implicitly a service that exists below the X.224 class 0 or CNP layer. However, nothing prohibits a non-standard profile that may be negotiated from providing services (including security) above the X.224 class 0 or CNP layers.

II.3.1 GSS-API: Carrying GSS-API tokens via X.224 class 0 or CNP

The GSS-API security framework implements a process whereby a security mechanism creates opaque tokens for communication via a reliable mechanism (i.e., transport) between two negotiating entities. This process is ongoing for all communication between the entities, and therefore spans an entire session. It includes not only the set-up phase of a security context where security mechanisms may be chosen and credentials exchanged, but also any subsequent exchange of encrypted data.

A common use of the GSS-API security framework is for the invoking application to manage the security of a session with regard to the security policy that may be locally scoped to the application. For example, the application may decide which security protocols to advertise and which credentials to select.

Other uses of the GSS-API are of course possible. For example, an operating system network service may establish its own security context between two endpoints. Because the existence of this security context may or may not be known to a higher-level invoking application, the application may not know whether or not it needs to manage the security of its session (e.g., IP security may be invoked by the networking service, but its invocation is likely to be transparent to a higher-level application using TCP/IP). Even if it does know about another security context, the application may want to manage its own security for the session anyway.

Consequently, the most likely use of the GSS-API security framework in the T.120 series of Recommendations is where a T.120 application desires to directly manage the security of a session. There is naturally then the question of where the T.120 application should decide to layer the GSS-API token stream within the T.120 session.

Considering that GSS-API does not care about the communication mechanism for its token stream, Annex B specifies a scheme that signals the GSS-API security framework as a reliable security protocol within CNP and, in an extended profile, layers the GSS-API token stream above the X.224 class 0 component of layer 4 (or layers the stream above CNP in the case where CNP replaces X.224 class 0).

Bibliography

[b-RFC 2078] IETF RFC 2078 (1997), *Generic Security Service Application Program Interface*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	**Terminals for telematic services**
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007