INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 1997 - 2000

COM 16-R 35-E
November 1998
Original: English

Questions: 1-23/16

Texte disponible seulement en
Text available only in
Texto disponible solamente en **E**

STUDY GROUP 16 – REPORT R 35

SOURCE*: STUDY GROUP 16 (GENEVA, 14-25 SEPTEMBER 1998)

TITLE: IMPLEMENTOR'S GUIDE FOR RECOMMENDATIONS OF STUDY GROUP 16

CONTENTS

*** Contact:** TSB

Tel: +41 22 730 5860
Fax: +41 22 730 5853
Email: bigi@itu.int

1 Implementor's Guide for the ITU-T Recommendation V.18 - Operational and interworking requirements for DCEs operating in the text telephone mode

1 Introduction

The amendments described in this document are essential for implementations of V.18.

The modifications correct minor errors and add important information.

Revised Appendix 3/V.18 contains informative material on how to apply V.18, V.8 and V.8bis procedures successfully in different situations and environments. Since these procedures are regarded as important for successful operation, they are planned to be made normative at the 1999 meeting of Study Group 16. The V.8bis procedures are planned to be strongly recommended but still optional. The way to perform them, when used, is to be described in a normative way.

2 Contact information

Alistair Farquharson	Tel: +44 1473 645089
V.18 editor	Fax: +44 1473 644140
BT Labs	Email: alistair.farquharson@bt.com

3 Document history

Version	Date	Description
1	25 September 1998	Initial version – completed at the ITU-T Study Group meeting, Geneva, September 1998

4 References

– ITU-T Recommendation V.18 (1998), Operational and interworking requirements for DCEs operating in the text telephone mode.

5 Modifications to the main body including the annexes of V.18 - Operational and interworking requirements for DCEs operating in the text telephone mode

[Begin Correction V.18]

5.1 Modification to Section 5 of Recommendation V.18

Since V.8 procedures are added in Appendix 3, this addition should be mentioned in the main body of the Recommendation. The next to last paragraph in Section 5 is changed from "This section specifies ...... and Appendix 3." to read:

"This section specifies the automoding procedures for the cases when all the following statements are true:

- V.8 procedures are not supported;
- V.8bis procedures are not supported;
- it is evident that the DCE is either the calling or the answering party (i.e. it is activated from the beginning of a call).

Appendix 3 gives guidance on the procedures, specifically for cases when at least one of the following statements is true.

- V.8 procedures are supported;
- V.8bis procedures are supported;
- it is not evident if the DCE shall use procedures for originating or answering mode. (e.g. activated from voice mode).

The possibility to use V.8bis procedures is also described in Section 6.

5.2 Modification to V.18 Annex E

In V.18 Annex E Section E.2. In last sentence, change "Prestel" to "Minitel". It should read: " .. it should be assumed that the answering terminal is a Minitel terminal."

5.3 Modification to V.18 Annex F

In V.18 Annex F, Section F.5. In second sentence, change "BS(0/7)" to "BS(0/8)".

5.4 Modification to V.18 Annex F

In V.18 Annex F Section F.4. Add new sentence at end of Section F.4: "Received parity should be ignored".

5.5 Modification to V.18 Annex B

Add new Section B.3.

B.3 Timing

The DCE shall detect DTMF characters at least 40 ms in length with silent intervals of at least 40 ms.

The DCE shall transmit DTMF characters at least 70 ms in length with silent intervals of at least 50 ms.

2 Implementor's Guide for the ITU-T H.223 Recommendation series - Multiplexing protocol for low bit-rate multimedia communication

Contact information

ITU-T Study Group 16/ Question 11 Rapporteur

Tom Geary
Rockwell Semiconductor Systems
4311 Jamboree Road, MC 510-350
Newport Beach, CA 92660-3095
United States

Tel: +1.714.221.4092
Fax: +1.714.221.6511
Email: tom.geary@rss.rockwell.com

Implementor's Guide Co-Editor

Toshiro Kawahara
NTT Mobile Communications Network, Inc.
3-5 Hikarinooka, Yokosuka
Kanagawa 239-8536
Japan

Tel: +81.468.40.3518
Fax: +81.468.40.3788
Email: kawahara@spg.yrp.nttdocomo.co.jp

Implementor's Guide Co-Editor

Bernhard G. Wimmer
SIEMENS AG
ZT IK 2
Otto-Hahn-Ring 6
81730 Munchen
Germany

Tel: +49.89.636.50417
Fax: +49.89.636.52393
Email: Bernhard.Wimmer@ties.itu.int

Document history

Revision	Date	Description
1	22 September 1998	Initial version and approved

CONTENTS

2 Introduction

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T H.223 series Recommendations. It is intended to be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementors. The changes, clarifications and corrections defined herein are expected to be included in future versions of affected H.223 series Recommendations.

The first version of the guide was produced following the September 1998 ITU-T Study Group 16 meeting. Wide distribution of this document is expected and encouraged.

3 Scope

This guide resolves defects in the following categories:

- editorial errors;
- technical errors such as omissions or inconsistencies;
- ambiguities.

In addition the Guide may include explanatory text found necessary as a result of interpretation difficulties apparent from the defect reports.

This Guide will not address proposed additions, deletions or modifications to the Recommendations that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in the normal way through contributions to the ITU-T.

4 Policies for updating this document

This document is managed by the ITU-T Study Group 16 Question 11 Rapporteur's Group. It can be revised at any recognized Q.11/16 Rapporteur's Group meeting provided the proposed revisions are unanimously accepted by the members of the group. A revision history cataloguing the evolution of this document is included.

5 Defect resolution procedure

Upon discovering technical defects with any components of the H.223 Recommendations series, please provide a written description directly to the editors of the affected Recommendations with a copy to the Q.11/16 Rapporteur. The template for a defect report is enclosed. Contact information for these parties is included in this document. Return contact information should also be supplied so a dialogue can be established to resolve the matter and an appropriate reply to the defect report can be conveyed. This defect resolution process is open to anyone interested in H.223 series Recommendations. Formal membership in the ITU is not required to participate in this process.

6 References

This document refers to the following H.223 series Recommendations:

– ITU-T Recommendation H.223 (1996), *Multiplexing Protocol for low bit-rate Multimedia Communication.*

– ITU-T Recommendation H.223/Annex A (1998), *Multiplexing Protocol for low bit-rate Multimedia Communication over low error-prone Channels.*

– ITU-T Recommendation H.223/Annex B (1998), *Multiplexing Protocol for low bit-rate Multimedia Communication over moderate error-prone Channels.*

– ITU-T Recommendation H.223/Annex C (1998), *Multiplexing Protocol for low bit-rate Multimedia Communication over highly error-prone channels.*

7 Nomenclature

In addition to traditional revision marks, the following marks and symbols are used to indicate to the reader how changes to the text of a Recommendation should be applied:

Symbol	Description
[Begin Correction]	Identifies the start of revision marked text based on extractions from the published Recommendations affected by the correction being described.
[End Correction]	Identifies the end of revision marked text based on extractions from the published Recommendations affected by the correction being described.
...	Indicates that the portion of the Recommendation between the text appearing before and after this symbol has remained unaffected by the correction being described and has been omitted for brevity.
--- *SPECIAL INSTRUCTIONS* --- *{instructions}*	Indicates a set of special editing instructions to be followed.

8 Technical and editorial corrections

8.1 Replacement in Section C.4.1.4

Description:	Clarify that tail bits are also required in FEC_ONLY mode.

[Begin Correction]

FEC_ONLY In this mode a AL-SDU* with ~~an~~mandatory tails bits (TB)[1] and CRC is RCPC encoded with a code rate r ≤ 1.0. The resulting AL-PDU only consists of an AL-PDU payload field. Splitting mode is not supported.

[End Correction]

8.2 Replacement in Section C.4.1.7.2

Description:	The CRC is appended to AL-SDU* not to AL-PDU, as seen in Figure C.2/H.223.

[Begin Correction]

C.4.1.7.2 Cyclic redundancy check (CRC)

The CRC provides error detection capability~~ across the entire AL-SDU*~~. The CRC is appended to the AL- ~~PDU~~SDU* before the error correction coding procedure is done. The CRC is used by the AL1M receiver to verify whether the decoding procedure of the error correction algorithm is error-free. CRC lengths of 4, 12, 20 and 28 bits are supported. The length of the CRC field shall be specified during the H.245 OpenLogicalChannel procedure. The evaluation of the CRC shall be performed by the same procedure as described as in 7.3.3.2.3 of Recommendation H.223.

[End Correction]

8.3 Replacement in Section C.4.1.8

Description:	The wording interleaver may be misleading. Therefore a more particular definition is required. In this chapter the wording is corrected, in chapter 8.2 an enhanced description is provided. In addition to that, the information about the range of the value *b* is not correct. So it is deleted.

[Begin Correction]

C.4.1.8 Interleaving

For some channels block interleaving may be used.

If interleaving is used, it shall be a applied to the entire AL-PDU including the control field. As the length of the AL-PDU varies, the dimension of the block interleaver matrix has to be recalculated for each length. Given a AL-PDU of length l_v, the dimensions, the width *a* and the height *b* of the block interleaver can be calculated:

$$a = \max_{\alpha \in \Im,\, l_v \bmod \alpha = 0} \left\{ \alpha \le \sqrt{l_v} \right\}, \quad \text{with } \Im \text{ all integers}$$

$$b = l_v / a$$

b describes the distance between two before interleaving consecutive bits after interleaving. ~~As the AL-PDU is an integer number of octets, the minimum *b* is *8*.~~

The receiver shall calculate the dimensions of the interleaver with the upper equation and the length of the received AL-PDU l_v. Deinterleaving shall also be applied to the entire AL-PDU.

[End Correction]

8.4 Replacement in Section C.4.1.9 Item 1

Description:	The parameter *lp* is not defined. Therefore it shall be replaced by a defined parameters.

[Begin Correction]

1) Calculate the length of the AL-PDU ~~payload~~ l_v~~l_p~~ according to Section C.4.1.7.1 and the first rate required in the H.245 OpenLogicalChannel message.

[End Correction]

8.5 Replacement in Section C.4.1.9 Item 6

Description:	The parameter *lp* is not defined. Therefore it shall be replaced by a defined parameters.

[Begin Correction]

6) For the first transmission read $l_v - l_h$~~l_p~~ (AL-PDU payload length) bits from the buffer, starting from the beginning of the buffer and~~,~~ fill these bits into the AL-PDU payload field. The first octet of the buffer is the first octet of the AL-PDU payload field.

[End Correction]

8.6 Replacement to Section C.4.1.9 Item 7

Description:	Clarification of the appropriate H.245 message.

[Begin Correction]

7) ~~If required in the H.245 OpenLogicalChannel message, the Control Field (CF) shall be added at the beginning of the AL-PDU.~~The Control Field (CF) shall not be used if the ARQ mode, signalled by the H.245 message, is set to "noArq".

[End Correction]

8.7 Replacement to Section C.4.1.9

Description:	The old description is not precise enough for an implementation. Therefore this replacement is done for a sufficient description.

[Begin Correction]

ARQII ~~The transmitting entity shall first transmit the first code rate according to the H.245 OpenLogicalChannel message and may choose any AL-PDU payload length. for following incremental retransmissions.~~If $V^j(S) = 0$, the encoding procedure step 6 of this chapter shall be performed. Otherwise, the transmitter may choose any AL-PDU payload length, whereby the AL-PDU payload length shall be integral number of octets. This AL-PDU payload shall be read in the consecutive order from the linear buffer.

However if the mother code rate is reached, the transmitter begins transmitting at the beginning of the linear buffer and is still free to choose the code rate, if the maximum number of retransmissions is not reached.

Figure C.6/H.223C illustrates the encoding procedures of the AL1M at the transmit side.

[End Correction]

8.8 Correction of error in Figure C.6/H.223

Description:	Replace Figure C.6/H.223 due to errors of two of the indexes. Also the caption refers to the wrong AL layer.

[Begin Correction]

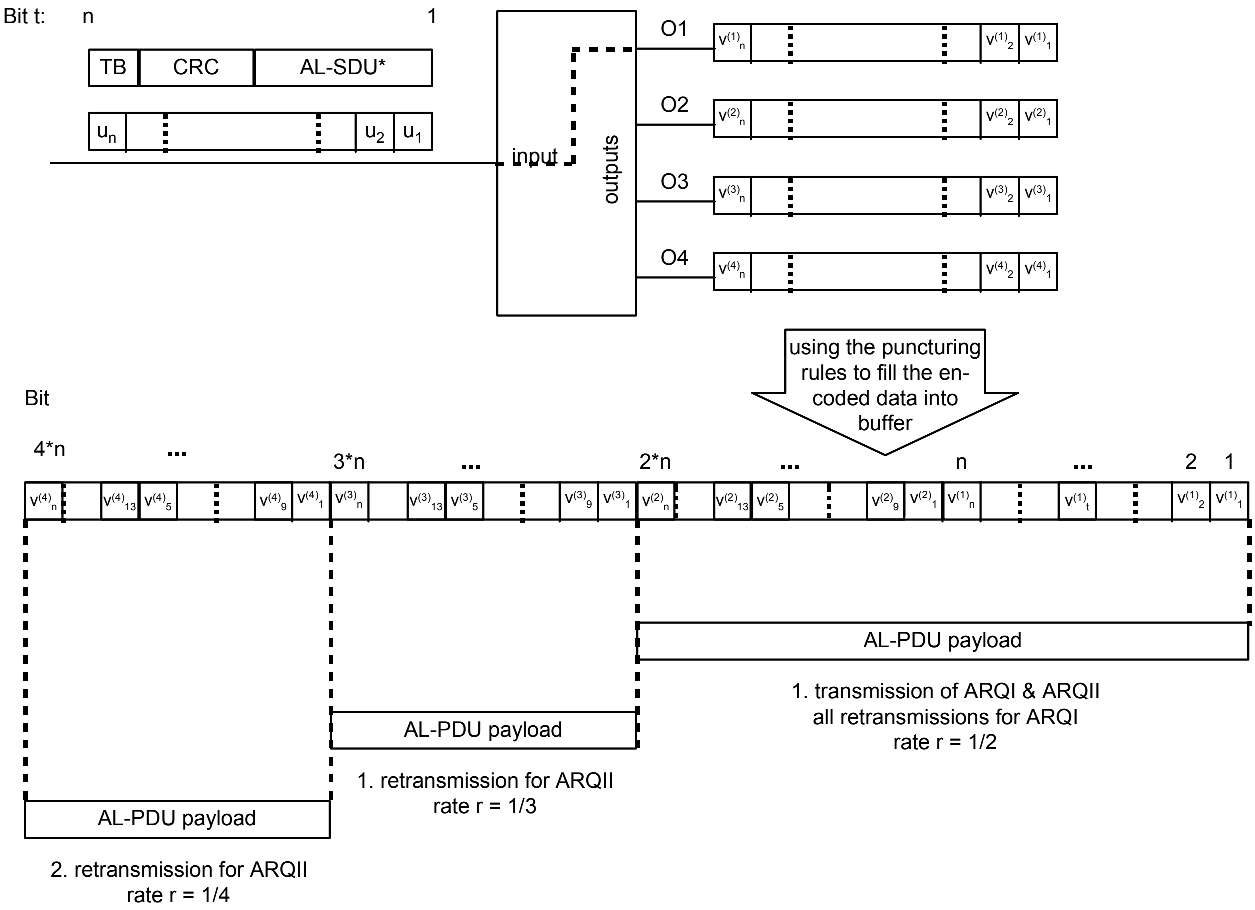


FIGURE C.6/H.223

Encoding procedure of the AL~~3~~1M at the transmitter side

[End Correction]

8.9 Correction of error in Section C.4.1.13

Description:	In Section C.4.1.13.1, there is a description on the range of sequence number field, but the maximum value is not correct. The maximum value is 2^5-1 or 2^{10}-1 for 5-bit or 10-bit field, respectively.

[Begin Correction]

C.4.1.13.1. Definitions

a) Modulo

Each AL-PDU Payload is sequentially numbered modulo 2^5 or 2^{10} and may have the value 0 through 2^5-1 or 2^{10}-1. The length of the sequence number field (SN) is set with the OpenLogicalChannel message of Recommendation H.245.

NOTE - All arithmetic operations on state variables and sequence numbers contained in this section are modulo 2^5 or 2^{10}.

…

[End Correction]

8.10 Correction of error in Section C.4.1.13.6

Description:	The 1-bit receive retransmission number in the CF is RN, as described in Section C.4.1.5.2.

[Begin Correction]

C.4.1.13.6 Receiving SREJ-PDUs

On receipt of a valid SREJ-PDU, the AL1M entity shall act as follows:

a) If the I-PDU, whose N(S) is equal to the N(R) of the SREJ message is still in the send buffer, the AL1M entity shall pass a corresponding AL-PDU to the MUX layer as soon as possible.

When ARQI error protection is used the same AL-PDU payload shall be used for re-transmission.

When ARQII is used, the parity of the send retransmission variable $V^j(S)$ is checked against the 1-bit receive retransmission number ~~N(R)~~RN. If the parity differs, $V^j(S)$ will be decremented by 1. Then the next I-PDU payload, according to the procedure described in C.4.1.9, shall be re-transmitted to the receiver.

No other previously transmitted I-PDUs shall be retransmitted as a result of receiving the SREJ-PDU.

…

[End Correction]

8.11 Correction of error in Section C.4.1.13.8

Description:	In the original text, it is not explicitly stated whether the exception conditions are cleared or not, in case the retransmission I-PDU with N(S) doesn't equal to V(R), while it implicitly says that they are cleared. This change is in order to clarify that.

[Begin Correction]

C.4.1.13.8 Exception condition reporting and recovery

Exception conditions may occur as a result of errors on the physical connection or procedural errors by an AL1M entity.

The error-recovery procedures that are available following the detection of an exception condition by an AL1M entity are defined in this subsection.

a) Receiving invalid AL-PDUs

When a received AL-PDU is invalid, it is either discarded or saved for possible delivery later to the AL1 user.

b) N(S) sequence error

When there are no other outstanding exception conditions, an N(S) sequence error exception condition occurs in the receiving AL1M entity when a valid I-PDU is received containing an N(S) value that is not equal to the V(R) at the receiver. In this case, V(R) shall not be incremented, and one or more SREJ-PDUs, each containing a different N(R), may be transmitted by the AL1M receiving entity to initiate an exception condition recovery for each SREJ-PDU. After passing each SREJ-PDU to the MUX layer, the AL1M entity shall start a local timer. Several factors that affect the length of the timer are given in Appendix IV/V.42. A different timer is maintained for each outstanding SREJ-PDU. Successive SREJ-PDUs are transmitted in the order indicated by their N(R) field.

For each SREJ-PDU that it transmits, the AL1M receiver may pass an empty AL-SDU or an invalid received AL-SDU (previously saved), with an appropriate EI parameter, to the AL1 user via the AL-DATA.indication primitive.

When the retransmitted I-PDU with $N(S) = V(R)$ is received, the exception condition for that I-PDU shall be cleared. The AL1M receiver should pass the associated AL-SDU, together with an appropriate EI parameter, to the AL1 user via the AL-DATA.indication primitive. When the exception condition is cleared, the associated timer shall be stopped and V(R) shall be incremented as many times as necessary so that V(R) represents the send sequence number of the next expected in-sequence I-PDU.

When a retransmitted I-PDU with $N(S) \neq V(R)$ is received, the AL1M receiving unit shall ~~stop the timers associated with~~clear all exception conditions related to previously sent SREJ-PDUs for which retransmission is received, by stopping the associated timers. For each exception condition cleared, the AL1M receiver shall increment V(R) by 1, and may deliver an empty AL-SDU, together with an appropriate EI parameter, to the AL1 user via the AL-DATA.indication primitive, prior to delivering the AL-SDU associated with the received I-PDU.

The information in all other received valid I-PDUs should be delivered to the AL1 user in AL-SDUs, together with an appropriate EI parameter.

…

[End Correction]

8.12 Corrections in Appendix I

Description:	The calculation in the example is wrong.

[Begin Correction]

APPENDIX I

(to Annex C to H.223)

Generator matrixes of the systematic extended BCH

This appendix describes Systematic Extended Bose-Chaudhuri-Hocquenghem (SEBCH) codes and includes the generator matrixes, which are used by the Recommendation H.223/Annex C.

I.1 BCH codes

BCH codes are linear cyclic block codes, hence they can be described using a generator polynomial. However, the easiest way to describe short block codes is using a generator matrix which describes all characteristics of the code. With a generator matrix $\underline{\boldsymbol{G}}$ and a information sequence $\underline{\boldsymbol{i}}$ of length $\boldsymbol{k}$ the code vector $\underline{\boldsymbol{c}}$ of length $\boldsymbol{n}$ can be obtained by:

$$\underline{\mathbf{c}} = \underline{\mathbf{i}} \cdot \underline{\mathbf{G}} = [\, \underline{\mathbf{i}}^{\mathbf{T}} \mid \underline{\mathbf{c}}_{\mathbf{o}}^{\mathbf{T}} \,]^{\mathbf{T}}$$

with $\underline{\boldsymbol{G}} = [\ \underline{\boldsymbol{1}} \mid \underline{\boldsymbol{A}}\ ]$ a ($\boldsymbol{k}\times\boldsymbol{n}$) matrix containing a ($\boldsymbol{k}\times\boldsymbol{k}$) identity matrix in the first $\boldsymbol{k}$ columns/rows to obtain a systematic code. For a primitive BCH code the length of the code $\boldsymbol{n}$ is always $\boldsymbol{n = 2^{h}-1}$. For $\boldsymbol{k}$ there are some constraints, not all values are possible.

The third parameter describing a block code besides code length $\boldsymbol{n}$ and information length $\boldsymbol{k}$ is the minimum distance between two code words $\boldsymbol{d}$. If a code has minimal distance $\boldsymbol{d}$, it can correct at most $\lfloor(d-1)/2\rfloor$errors or detect $(d-1)$ errors.

I.2 Systematic extended BCH codes

As all linear cyclic block codes can be made systematic, there always exits a systematic BCH code.

As we evaluated earlier, primitive BCH codes always have the length $\boldsymbol{n=2^{h}-1}$. To make these codes octet aligned, extension has to be applied. The extension of a BCH($\boldsymbol{n, k, d}$) has the length $\boldsymbol{n+1}$. One digit is appended, so that each code word has even weight. The extended BCH code then always has minimal distance $\boldsymbol{d+1}$. Hence we derived from BCH($\boldsymbol{n, k, d}$) a code EXBCH($\boldsymbol{n+1, k, d+1}$). Extended codes are still linear, but no more cyclic. Hence the description using generator polynomials is impossible.

The generator matrix of the extended code from $\underline{\boldsymbol{G}}$ of the mother code can be derived by adding one column which contains the parity check bit of each row. The examples of the generator matrices ~~of the codes used in this proposal~~ are given in Table I.1 and I.2.

I.3 Decoder overview

For decoding BCH codes, usually Berleykamp-Massey algorithm is used. This is an efficient method to determine error locations in the received vector. There are also some approaches to use reliability information for decoding block codes. However, these algorithms yield in high complexity.

One main feature of BCH codes is the possibility to use these codes for error correction and detection at the same time. For example a code with ***d*=5** could correct up to 1 error and detect up to 3 errors in parallel. With the usage of BCH codes only, the decoder has the flexibility to decide how many errors to correct and use the rest of redundancy for error detection. Berleykamp-Massey algorithm can also be used for this.

I.4 Example

In this example we use the SEBCH(16,5,8). The information vector ***~~c~~ i*** is given as:

~~c~~ i* = *[1 0 0 1 1]

By using the generator matrix ***G*** the code word ***c*** can be evaluated by:

c* = *i*·*G* = *[1 0 0 1 1 0 1 0 1 1 1 1 ~~1~~ 0 0 0 0]

For transmission these bits are filled into octet-aligned fields. The LSB-bit of the vector ***c*** is at its left side, the MSB at its right. The LSB of ***c*** is filled to the lowest numbered bit of the last octet (octet 2) and the MSB of ***c*** to the highest-numbered bit of the first octet (octet 1), see Figure I.1.

Bit:	8	7	6	5	4	3	2	1	Octet
	0	0	0	~~1~~0	1	1	1	1	1
	0	1	0	1	1	0	0	1	2

FIGURE I.1/H223

Field mapping convention of SEBCH-codes

…

[End Correction]

9 Implementation clarifications

9.1 Clarification of the mapping procedure of Figure C.7/H.223 of H.223/Annex C

General

The mapping from the temporary matrix to the linear buffer is done by the rules of the puncturing table C.4/H.223 that describes the exact reading order from the temporary matrix. Table 1 reflects that reading order for the output 2, 3 and 4.

TABLE 1

Reading order for the output 2, 3 and 4 of the temporary matrix of Figure C.7/H.223

column number	1	2	3	4	5	6	7	8
reading order	1	5	3	7	2	6	4	8

Mapping Procedure

The linear buffer is filled in the following way:

1) The first output line of the convolutional encoder is directly written to the linear buffer.

2) The columns of output 2 of the temporary matrix are written to the linear buffer by the use of the Table 1. Thus first all the bits in column 1 are read from the top to down and filled to the linear buffer, followed by column 5 and so on. After all columns are read the mapping procedure continues with output 3.

3) The columns of output 3 of the temporary matrix are written to the linear buffer by the use of the Table 1. Therefore first all the bits in column 1 are read from the top to down and filled to the linear buffer, followed by column 5 and so on. After all columns are read the mapping procedure continues with output 4.

4) The columns of output 4 of the temporary matrix are written to the linear buffer by the use of the Table 1. Therefore first all the bits in column 1 are read from the top to down and filled to the linear buffer, followed by column 5 and so on. After all columns are read the mapping procedure is finished.

9.2 Clarification of the interleaving procedure of chapter C.4.1.8 of H.223/Annex C

The process of block interleaving with the width a and the height b is as follows:

1) Prepare a rectangular buffer with a columns and b rows.

2) The input data is written in to the buffer from the top left to the bottom right, row by row, bit by bit.

3) The output data is read out from the buffer from the top left to the bottom right, column by column, bit by bit.

This is represented with a formula as follows:

x_i: i-th input bit to the interleaver. i=0..N-1,

y_j: j-th output bit from the interleaver. j=0..N-1,

$y_j = x_i$,where $i = (j \bmod b) \cdot a + \lceil j/b \rceil$

N is the number of bits input to the interleaver, and $\lceil x \rceil$ is the maximum integer value which is smaller than or equal to x.

H.223 RECOMMENDATION SERIES DEFECT REPORT FORM

DATE:	
CONTACT INFORMATION **NAME:** **COMPANY:** **ADDRESS:** **TEL:** **FAX:** **EMAIL:**	
AFFECTED RECOMMENDATIONS:	
DESCRIPTION OF PROBLEM:	
SUGGESTIONS FOR RESOLUTION:	

NOTE - Attach additional pages if more space is required than is provided above.

3 Implementor's Guide for the ITU-T H.324 Recommendation series Version 2 - Terminal for low bit-rate multimedia communication

Abstract

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T H.324 series Recommendations. It is intended to be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementors. The changes, clarifications and corrections defined herein are expected to be included in future versions of affected H.324 series Recommendations.

Contact information

ITU-T Study Group 16/Question 11 Rapporteur	Tom Geary Rockwell Semiconductor Systems 4311 Jamboree Road, MC 510-350 Newport Beach, CA 92660-3095 United States	Tel: Fax: Email:	+1.714.221.4092 +1.714.221.6511 tom.geary@rss.rockwell.com
Implementor's Guide Editor	Cor Quist KPN Research P.O. Box 421 2260 AK Leidschendam Netherlands	Tel: Fax: Email:	+31.70.332.4005 +31.70.332.6477 C.P.Quist@research.kpn.com
ITU-T Recommendation H.324 Editor	Mickey Nasiri Ericsson Telecom S-125 25 Stockholm Sweden	Tel: Fax: Email:	+46.8.726.2125 +46.8.18.7620 mickey@clab.ericsson.se

Document history

Revision	Date	Description
1	8-11 June 1998	Initial version - Reviewed at the Q.11/SG 16 meeting.
2	22 September 1998	Final version - Completed at the ITU-T Study Group 16 Rapporteurs meeting.

CONTENTS

Page

Introduction

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T H.324 series Recommendations. It is intended to be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementors. The changes, clarifications and corrections defined herein are expected to be included in future versions of affected H.324 series Recommendations.

The first version of the guide was produced following the September 1998 ITU-T Study Group 16 meeting. Wide distribution of this document is expected and encouraged.

Scope

This guide resolves defects in the following categories:

- editorial errors;
- technical errors such as omissions or inconsistencies;
- ambiguities.

In addition the Guide may include explanatory text found necessary as a result of interpretation difficulties apparent from the defect reports.

This Guide will not address proposed additions, deletions or modifications to the Recommendations that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in the normal way through contributions to the ITU-T.

Policies for updating this document

This document is managed by the ITU-T Study Group 16 Question 11 Rapporteur's Group. It can be revised at any recognized Q.11/16 Rapporteur's Group meeting provided the proposed revisions are unanimously accepted by the members of the group. A revision history cataloguing the evolution of this document is included.

Defect resolution procedure

Upon discovering technical defects with any components of the H.324 Recommendations series, please provide a written description directly to the editors of the affected Recommendations with a copy to the Q.11/16 Rapporteur. The template for a defect report is enclosed. Contact information for these parties is included in this document. Return contact information should also be supplied so a dialogue can be established to resolve the matter and an appropriate reply to the defect report can be conveyed. This defect resolution process is open to anyone interested in H.324 series Recommendations. Formal membership in the ITU is not required to participate in this process.

References

This document refers to the following H.324 series Recommendations:

– ITU-T Recommendation H.324 (1998), *Terminal for low bit-rate Multimedia Communication.*

Nomenclature

In addition to traditional revision marks, the following marks and symbols are used to indicate to the reader how changes to the text of a Recommendation should be applied:

Symbol	Description
[Begin Correction]	Identifies the start of revision marked text based on extractions from the published Recommendations affected by the correction being described.
[End Correction]	Identifies the end of revision marked text based on extractions from the published Recommendations affected by the correction being described.
...	Indicates that the portion of the Recommendation between the text appearing before and after this symbol has remained unaffected by the correction being described and has been omitted for brevity.
--- *SPECIAL INSTRUCTIONS* --- *{instructions}*	Indicates a set of special editing instructions to be followed.

Technical and editorial corrections

There are no technical nor editorial corrections.

Implementation clarifications

This section describes the procedures for using the supplementary services Call Hold and Explicit Call Transfer in H.324/ISDN. Implementation of these procedures is optional.

Procedures for Call Hold (CH)

The two procedures as described below should be used if a terminal supports the Call Hold supplementary service.

1 Invocation procedure for CH

Initial situation: Terminal A is connected to terminal B. Either Terminal A or terminal B has established the call.

Objective: Terminal A wishes to put terminal B on hold.

1) In case Multilink is used, terminal A should remove all but one B-channel connections from the H.Multilink Channel Set according to the Multilink procedures.

2) Terminal A should proceed with phase F of Annex D/H.324. The **EndSessionCommand** message should indicate to the far end that the terminal will be put on hold by signalling **terminalOnHold** in **isdnOptions**.

3) Terminal A should invoke the CH supplementary service by D-channel signalling, requesting the network to put all B-channel connections with terminal B on hold.

2 Retrieval after invocation of CH

Initial situation: Terminal A has terminal B on hold.

Objective: Terminal A wishes to retrieve the call with terminal B.

1) Terminal A should apply D-channel signalling to retrieve all the B-channel connections with terminal B.

2) Terminal A should initiate phase A of Annex D/H.324 starting with the execution of H.Dispatch, because the channel is already established.

3) Terminal A should add the additional B-channel connections to the H.Multilink Channel Set using the Multilink procedures.

NOTE - The CH procedures should only be used if both terminals A and B are H.324/I terminals.

Procedures for Explicit Call Transfer (ECT)

The procedure as described below should be used if a terminal supports the invocation of ECT.

Initial situation: Terminal A is connected to terminal B. Either terminal A or terminal B has established the call.

Objective: Terminal A wishes to put terminal B on HOLD, make a call to terminal C and then connect terminal B to terminal C.

1 Invocation procedure for ECT

1) In case Multilink is used, terminal A should disconnect all but one B-channel connections with terminal B according to the Multilink procedures defined in Annex F/H.324.

2) Terminal A should put terminal B on hold according to the procedures of the CH supplementary service.

3) Terminal A should establish a call with terminal C.

4) ECT should not be activated when terminal A does not succeed in establishing a call with terminal C or when terminal C is not a H.324/I terminal; Appropriate indications should be given to the user(s).

5) In case Multilink is used, terminal A should disconnect all but one B-channel connections with terminal C according to the Multilink procedures defined in Annex F/H.324.

6) Terminal A should put terminal C on hold according to the procedures of the CH supplementary service.

7) Terminal A should invoke the ECT supplementary service by D-channel signalling, requesting the network to connect terminal B to C.

NOTE 1 - The procedure for ECT should only be used if all terminals A, B and C are H.324/I terminals. The implementation of ECT in case not all the terminals A, B and C are H.324/I terminals is left for further study.

NOTE 2 - The method used for addressing phone numbers in H.Multilink in case calls are transferred is left for further study.

NOTE 3 - The network provider may restrict the invocation of the ECT supplementary service to either the calling or the called terminal.

H.324 RECOMMENDATION SERIES DEFECT REPORT FORM

DATE:	
CONTACT INFORMATION **NAME:** **COMPANY:** **ADDRESS:** **TEL:** **FAX:** **E-MAIL:**	
AFFECTED RECOMMENDATIONS:	
DESCRIPTION OF PROBLEM:	
SUGGESTIONS FOR RESOLUTION:	

NOTE - Attach additional pages if more space is required than is provided above.

4 Implementor's Guide for the ITU-T H.323, H.225.0, H.245, H.246, H.235, and H.450 series Recommendations - Packet-based multimedia communication systems

Contact information

ITU-T Study Group 16/ Question 13 Rapporteur	Dale Skran Ascend Communications 620 Tinton Avenue Building A, Second Floor Tinton Falls, NJ. 07724 United States	Tel: +1 (908) 578-3101 Fax: +1 (908) 578-3131 Email: dale.skran@ascend.com
ITU-T Study Group 16/Question 14 Rapporteur ITU-T Recommendation H.323 Editor	Gary Thom Delta Information Systems 300 Welsh Road, Bldg 3 Horsham, PA. 19044-2273 United States	Tel: +1.215.657.5270 Fax: +1.215.657.5273 Email: gthom@delta-info.com
Implementor's Guide Editor ITU-T Recommendation H.235 Editor	James Toga Intel Corporation 2111 NE 25th Avenue JF3-212 Hillsboro, OR. 97124-5961 United States	Tel: +1.503.264.8816 Fax: +1.503.264.3485 Email: jim.toga@intel.com
ITU-T Recommendation H.225.0 Editor	Glen Freundlich Lucent Technologies 11900 N. Pecos St. Westminster, CO 80234 United States	Tel: +1.303.538.2899 Fax: +1.303.538.5478 Email: ggf@dr.lucent.com
ITU-T Recommendation H.245 Editor	Mark Reid Video Server Incorporated	Tel: +1 (781) 505-2368 Fax: +1 (781) 505-2101 Email: mreid@videoserver.com

1 Introduction

The first version of the guide was produced following the April 1998 ITU-T Study Group 16 meeting. Wide distribution of this document is expected and encouraged.

2 Scope

This guide resolves defects in the following categories:

- editorial errors;
- technical errors such as omissions or inconsistencies;
- ambiguities.

In addition the Guide may include explanatory text found necessary as a result of interpretation difficulties apparent from the defect reports.

This Guide will not address proposed additions, deletions or modifications to the Recommendations that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in the normal way through contributions to the ITU-T.

3 Policies for updating this document

This document is managed by the ITU-T Study Group 16. It can be revised at any recognized Q.13/16 and Q.14/16 Rapporteur's Group meeting provided the proposed revisions are reached through consensus by the members of the group. A revision history cataloguing the evolution of this document is included.

4 Defect resolution procedure

Upon discovering technical defects with any components of the H.323 Recommendations series, please provide a written description directly to the editors of the affected Recommendations with a copy to the Q.13/16 or Q.14/16 Rapporteur. The template for a defect report is enclosed. Contact information for these parties is included in this document. Return contact information should also be supplied so a dialogue can be established to resolve the matter and an appropriate reply to the defect report can be conveyed. This defect resolution process is open to anyone interested in H.323 series Recommendations. Formal membership in the ITU is not required to participate in this process.

5 References

This document refers to the following H.323 series Recommendations:

– ITU-T Recommendation H.323 (1998), *Packet-Based Multimedia Communications Systems.*

– ITU-T Recommendation H.225.0 (1998), *Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems.*

– ITU-T Recommendation H.245 (1998), *Control Protocol for Multimedia Communication.*

– ITU-T Recommendation H.235 (1998), *Security and Encryption for H series (H.323 and other H.245 based) multimedia terminals.*

6 Nomenclature

In addition to traditional revision marks, the following marks and symbols are used to indicate to the reader how changes to the text of a Recommendation should be applied:

Symbol	Description
[Begin Correction]	Identifies the start of revision marked text based on extractions from the published Recommendations affected by the correction being described.
[End Correction]	Identifies the end of revision marked text based on extractions from the published Recommendations affected by the correction being described.
...	Indicates that the portion of the Recommendation between the text appearing before and after this symbol has remained unaffected by the correction being described and has been omitted for brevity.
--- SPECIAL INSTRUCTIONS --- {instructions}	Indicates a set of special editing instructions to be followed.

7 Technical and editorial corrections

7.1 Technical and editorial corrections to ITU-T Recommendation H.323

7.1.1 Early call signalling channel closure

Description: An incomplete description concerning closing of the call signalling channel is contained within Section 7.3.1 of H.323.

This information will be contained in the revision 3 of H.323 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.323 document that was submitted for approval in 1998.

In general this change should not effect implementations, it is intended to clarify consistency issues should they occur. The corrected text is shown below.

[Begin Correction]

7.3.1 Call signalling channel routing

...

For the Gatekeeper Routed method, the Gatekeeper may choose to close the Call Signalling Channel after the call set-up is completed, or it may choose to keep it open for the duration of the call to support supplementary services. Only the Gatekeeper shall close the Call Signalling Channel and it should not be closed when a Gateway is involved in the call. If the Gatekeeper closes the Call Signalling Channel then the present state of the call shall be retained by the entities involved. The Gatekeeper may re-open the Call Signalling Channel at any time during the call.

[End Correction]

7.1.2 FastConnect clarifications

Description: In Section 8.1.7 of H.323, Fast Connect Procedures, the text regarding the refusal of the fast connect is not clear and may be confusing to the reader.

The clarified text will be contained in the revision 3 of H.323 Recommendation to be published by the ITU-T. However, the current text in revision 2 of H.323 should be amended with the clarifying paragraph shown below.

This change should not affect the functionality or local operation of an Gatekeeper or endpoint.

[Begin Correction]

8.1.7 Fast connect procedure

...

The called endpoint may refuse to use the Fast Connect procedure, either because it does not implement it or because it intends to invoke features that require use of the procedures defined in Recommendation H.245. Refusal of the Fast Connect procedure is accomplished by not returning **fastStart** element in any of the messages up to and including CONNECT message. Note that an endpoint may not return fastStart element in a message prior to CONNECT, but then later return fastStart element in the CONNECT message thereby accepting the fast connect procedure. Refusing the Fast Connect procedure (or not initiating it) requires that H.245 procedures be used for capabilities exchange and opening of media channels.

[End Correction]

Description: An inconsistency in the use of channel addressing within the FastStart procedure has been discovered.

This information will be contained in the revision 3 of H.323 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.323 document that was submitted for approval in 1998.

As a part of the "Fast Connect Procedure", it is the responsibility of the called endpoint to decide about the coupling of proposed incoming and outgoing media streams for each SessionId. According to RTP/RTCP specifications, media streams in the same session, must use a common RTCP channel. Additionally, many RTP/RTCP implementations mandate adjacent odd/even port pairs to be allocated.

This requirement mandates that for any and all fastStart structures that are proposed in a SETUP message, those with common sessionID values shall also have common mediaChannelControl values.

This change may affect the functionality or local operation of an implementation.

[Begin Correction]

8.1.7.1 Proposal, selection and opening of media channels

...

In an **OpenLogicalChannel** which proposes a channel for transmission from the called endpoint to the calling endpoint, the **reverseLogicalChannelParameters** element shall be included and contain parameters specifying the characteristics of the proposed channel. The **forwardLogicalChannelParameters** element must also be included (because it is not optional), with the **dataType** element set to **nullData**, **multiplexParameters** set to **none**, and all optional elements omitted. Alternative proposals for the same receive channel shall contain the same **sessionID** value in **H2250LogicalChannelParameters**. All alternative OpenLogicalChannel structures, that propose a channel for transmission from the called endpoint to the calling endpoint, shall contain the same sessionID and the same mediaChannel value~~The **mediaChannel** element shall be set appropriately according to the calling endpoint requirements; different values may be used in alternative proposals if desired~~. The other **H2250LogicalChannelParameters** and **dataType** within **reverseLogicalChannelParameters** shall be set to correctly describe the receive capabilities of the calling endpoint associated with this proposed channel. The calling endpoint may choose to not propose any channels for transmission from the called endpoint to the calling endpoint, such as if it desires to use H.245 procedures later to establish such channels.

All alternative OpenLogicalChannel structures, that propose a channel for transmission from the called endpoint to the calling endpoint, shall contain the same sessionID and the same mediaChannel value.

In the SETUP message, each **OpenLogicalChannel** which proposes a channel for transmission from the called endpoint to the calling endpoint, shall contain **mediaControlChannel** element (indicating the RTCP channel going in the same direction) into the **H2250LogicalChannelParameters** element of the **reverseLogicalChannelParameters** structure. All **mediaControlChannel** elements inserted by the calling endpoint for the same **sessionID** for both directions shall have the same value.

Upon receipt of a **SETUP** message containing **fastStart**, determining that it is willing to proceed with the Fast Connect procedure, and reaching the point in the connection at which is ready to begin media transmission, the called endpoint shall choose from amongst the proposed **OpenLogicalChannel** structures containing **reverseLogicalChannelParameters** elements for each media type it wants to transmit, and from amongst the proposed **OpenLogicalChannel** structures specifying **forwardLogicalChannelParameters** (and omitting **reverseLogicalChannelParameters**) for each media type it wants to receive. If alternative proposals are presented, only one **OpenLogicalChannel** structure shall be selected from amongst each alternative set; alternatives within a set have the same **sessionID**. The called endpoint accepts a proposed channel by returning the corresponding **OpenLogicalChannel** structure in any Q.931 message sent in response to **SETUP**, up to and including **CONNECT**. The called endpoint may choose to not open media flow in a particular direction or of a particular media type by not including a corresponding **OpenLogicalChannel** structure in the **fastStart** element of the Q.931 response.

When accepting a proposed channel for transmission from called endpoint to calling endpoint, the called endpoint shall return the corresponding **OpenLogicalChannel** structure to the calling endpoint, inserting a unique **forwardLogicalChannelNumber** into the **forwardLogicalChannelParameters** structure and a valid mediaControlChannel element (indicating the reverse RTCP channel) into the H2250LogicalChannelParameters element of the reverseLogicalChannelParameters structure. All mediaControlChannel elements inserted by the called endpoint for the same sessionID for both directions shall have the same value.~~unique~~ ~~**forwardLogicalChannelNumber** into the **forwardLogicalChannelParameters** structure.~~ The called endpoint may begin transmitting media on the accepted channel according to the parameters specified in **reverseLogicalChannelParameters** immediately after sending the Q.931 response containing **fastStart**, unless **mediaWaitForConnect** was set to TRUE in which case it must wait until after sending the **CONNECT** message.

When accepting a proposed channel for transmission from the calling endpoint to the called endpoint, the called endpoint shall return the corresponding **OpenLogicalChannel** structure to the calling endpoint~~,~~. The called endpoint shall ~~inserting a~~insert valid mediaChannel and **mediaControlChannel**~~element~~ fields (indicating the RTCP channel going in the same direction) into the **H2250LogicalChannelParameters** element of the **forwardLogicalChannelParameters** structure. The called endpoint shall then prepare to immediately receive media flow according to the parameters specified in **forwardLogicalChannelParameters**. The calling endpoint may begin transmitting media on the accepted and opened channels upon receipt of the Q.931 response containing **fastStart**, and may release any resources allocated to reception on proposed channels that were not accepted.

[End Correction]

7.1.3 Gateway inbound calling

Description: An omission in the operation of gateways during inbound calls between the SCN and the IP network.

This information will be contained in the revision 3 of H.323 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.323 document that was submitted for approval in 1998.

The TCS-4/IIS option of requesting a remote LAN extension was omitted. We should add this description to H.323 Section 8.1.8.1 or include it in the H.323 Implementor's Guide.

This change may affect the functionality or local operation of an gateway depending on options implemented.

[Begin Correction]

8.1.8.1 Gateway inbound call set-up

...

A Gateway which cannot directly route an incoming SCN call to an H.323 endpoint shall be able to accept two-stage dialling. For Gateways to H.320 networks (also H.321, H.322 and H.310 in H.321 mode), the Gateway shall accept SBE numbers from the H.320 terminal. Optionally, Gateways to H.320 networks may support the TCS-4 and IIS BAS codes to retrieve the H.323 dialing information after a H.320 call has been established. For Gateways to H.310 native mode and H.324 networks, the Gateway shall accept H.245 **userInputIndication** messages from the H.324 terminal. In these two cases, support of DTMF is optional. For Gateways to speech only terminals, the Gateway shall accept DTMF numbers from the speech only terminal. These numbers will indicate a second stage dialling number to access the individual endpoint on the network.

[End Correction]

7.1.4 Facility redirection

Description: A clarification in the operation of MC(U)s which host multiple conferences has been added.

This information will be contained in the revision 3 of H.323 Recommendation to be published by the ITU-T. However, this information appears missing in the final H.323 document that was submitted for approval in 1998.

The clarifying paragraph is shown below.

This change may affect the functionality or local operation of an MC(U) or endpoints depending on options implemented.

[Begin Correction]

8.4.3.1 Direct endpoint call signalling - Conference create

...

A2d) If the MC(U) hosts multiple conferences and wishes to provide endpoint 1 with a choice of conferences to join, it can send a Facility message indicating conferenceListChoice and a list of conferences that endpoint 1 may choose from. The list of conferences is sent as part of the Facility-UUIE. For backward compatibility, with version 1 endpoints, conference lists are only provided if the ProtocolIdentifier in endpoint 1's Setup message indicates that it is version 2 or above.

The recipient of this "routeCallToMC" Facility message should consider the previous exchange completed and send a new SETUP message to the MC(U) address with the chosen conference it wishes to join.

[End Correction]

7.1.5 Annex C - H.323 on ATM

Description: An error in the use of the B-HLI field concerning mapping between ATM virtual circuits and logical channel numbers has been discovered.

B-HLI is used by the receiving endpoint to associate the ATM VC with the proper RTP logical channel. The endpoint that initiates the OpenLogicalChannel command is the endpoint that opens the ATM VC. It is possible for the initiating endpoint to select a B-HLI that is already in use by the receiving endpoint. This would cause a failure in the OLC procedure.

Additionally the receiving RTCP port is also specified by the initiating endpoint by implication. H.323 states that the corresponding RTCP data shall flow on a UDP port number equal to the VC Association port number plus 1. It is possible that the resulting port number for RTCP, VC Association port number plus 1, will be in use on the receiving endpoint since the VC Association port number is selected by the initiating endpoint.

Due to the above problems the receiving endpoint should have the choice of selecting the B-HLI.

This change will affect the functionality or local operation of an implementation. Note that there is an associated ASN.1 change within H.245.

[Begin Correction]

C.4.1.1 Broadband high layer information

IE Parameter	Value	Notes
Length of B-HLI contents (octets 3-4)	3	One octet type plus two octets VC association port number
High layer information type (octet 5)	"000 0001"	User-specific
High layer information (octets 6-7)	VC association port number	In basic mode, the UDP port number to be used for RTP

It should be noted that the~~portID~~ **portNumber** field in H.245 is only 16 bits in length. For this reason, only 16 bits are used in the B-HLI High Layer Information parameter.

The portNumber field of the OpenLogicalChannel message is used to select the B-HLI. The receiving endpoint uses this B-HLI to associate the ATM VC with the proper RTP logical channel. If the receiving endpoint finds that the given B-HLI is inappropriate it can select a new B-HLI and use the portNumber field of the OpenLogicalChannelAck message to indicate the new value to the initiating endpoint. The selected portNumber field is conveyed in the B-HLI information element. The format of the B-HLI is specified in the protocol section below. This enables the receiving side to associate the ATM VC with the proper RTP logical channel.

The VC association port number is represented in network byte order in octets 6 and 7 of the B-HLI (i.e. octet 6 holds the MSB and octet 7 holds the LSB).

~~The VC Association port number is used to identify the ATM VC for the RTP media stream. The corresponding RTCP data shall flow on a UDP port number equal to the VC Association port number plus 1.~~

[End Correction]

7.2 Technical and editorial corrections to ITU-T Recommendation H.225.0

7.2.1 Use of connect acknowledge

Description: In Section 7.3.4 Connect Acknowledge states "This message shall not be sent." However, additional text states "Follow Table 3-5/Q.931 as modified below", and includes Table 8/H.225.0 showing the contents of the Connect Acknowledge message. This message is not allowed in H.225.0

An error in the description of the Connect Acknowledge message has been detected. The included table should be deleted.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998. The Connect Acknowledge message is not permitted, the corrected text is shown below.

[Begin Correction]

7.3.4 Connect acknowledge

~~Follow Table 3-5/Q.931 as modified below.~~

This message shall not be sent.

~~Information element~~	~~H.225.0 status(M/F/O)~~	~~Length in H.225.0~~
~~Protocol discriminator~~	~~M~~	~~1~~
~~Call reference~~	~~M~~	~~3~~
~~Message type~~	~~M~~	~~1~~
~~Display~~	~~O~~	~~2-82~~
~~Signal~~	~~O~~	~~2-3~~
~~User-to-User~~	~~M~~	~~2-131~~

~~Table 8/H.225.0~~

[End Correction]

7.2.2 Information element labelling

Description: An error in the labelling of the Information element as described in H.225.0.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

This change does not affect the functionality or operation of the protocol.

[Begin Correction]

7.3.6 Information

This message may be sent to provide~~supplementary~~ additional information. It may be used to provide information for call establishment (e.g. overlap sending) or miscellaneous call-related information. It may be used to deliver proprietary features.

This message may be sent by an H.323 entity; its processing on receipt is optional.

This message follows Table 3-7/Q.931 with the following modifications:

TABLE 9/H.225.0

Information message content

Information element	**H.225.0 status(M/F/O)**	**Length in H.225.0**
Protocol discriminator	M	1
Call reference	M	3
Message type	M	1
Sending complete	O	1
Display	O	2-82
Keypad facility	O	2-34
Signal	O	2-3
Called party number	O	2-35
User-to-User	M	2-131

The user-to-user information element contains the ~~UI~~Information-UUIE defined in the H.225.0 Message Syntax. The ~~U~~Information-UUIE includes the following:

protocolIdentifier - set to the version of H.225 supported.

CallIdentifier - a globally unique call identifier set by the originating endpoint which can be used to associate RAS signalling with the modified Q.931 signalling used in H.225.0.

[End Correction]

7.2.3 Progress message

Description: An error has been detected concerning the required Information Elements in a Progress message.

This correction will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

In general this change should not effect implementations, the corrected text is shown below. Table A/H.225.0 indicates the progress indicator IE is optional in the Progress message, but this IE should be marked as mandatory.

[Begin Correction]

7.3.7 Progress

...

TABLE A/H.225.0

Progress

Information element	H.225.0 status(M/F/O)	Length in H.225.0
Protocol discriminator	M	1
Call reference	M	3
Message type	M	1
Bearer capability	O(Note 1)	5-6
Cause	O	2-32
Extended facility	O	8-*
Channel identification	FFS	NA
Facility	O	8-*
Progress indicator	~~O~~M	2-4
Notification Indicator	O	2-*
Display	O	2-82
High layer compatibility	FFS	NA
User-to-User	M	2-131

[End Correction]

7.2.4 Missing field descriptions

Description: Omitted descriptions of the indicated ASN.1 elements as described in H.225.0 have been detected.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

This change does not affect the functionality or operation of the protocol.

[Begin Correction]

7.8.1 GatekeeperRequest (GRQ)

...

algorithmOIDs - indicates the entire set of encryption algorithms supported by the endpoint.

7.8.2 GatekeeperConfirm (GCF)

...

algorithmOID - indicates the encryption algorithm required by the Gatekeeper.

[End Correction]

7.2.5 Use of CallIdentifier in IRQ

Description: An unclear description of the callReferenceValue in the IRQ message of H.225.0 has been detected.

These clarifications will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

This change should not affect the functionality or operation of the protocol, it may affect the response of an endpoint to this message.

[Begin Correction]

...

7.15 InfoRequest (IRQ)

callReferenceValue - CRV of the call that the query is about. If zero, this message is interpreted as a request for an IRR for each call the terminal is active on. If the terminal is not active on any calls, an IRR shall be sent in response to a CallReferenceValue of 0 with all appropriate fields provided. If callReferenceValue is 0, the endpoint shall ignore callIdentifier – in this case the gatekeeper shall fill callIdentifier with 0.

[End Correction]

7.2.6 H.225.0 Non-standard message

Description: An error in the description of the requestSeqNum contained within the non-standard message has been detected.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

The non-standard message has no well defined or corresponding response message and therefore there can be no correlation between sequence numbers on incoming and outgoing messages from a particular endpoint.

If H.323 applications are to utilize this message and need to be able to detect lost or duplicated messages, the implementation must supply its own sequencing information within the body of the message. The corrected text is shown below.

[Begin Correction]

7.16 Non-standard message

The **NonStandardMessage** structure is as follows:

requestSeqNum - this is a monotonically increasing number unique to the sender.~~It shall be returned by the receiver in any response associated with this specific message.~~

...

[End Correction]

7.2.7 Retries and timeouts for RAC/RAI

Description: Missing timeout values or retry counters were discovered for RAI/RAC in H.225.0 Section 7.19.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

In general this change should not effect implementations, it is intended to clarify interworking issues should they occur. The corrected text is shown below.

[Begin Correction]

7.19 RAS timers and request in progress (RIP)

...

RAS Message	timeout value (sec)	retry count
GRQ	5	2
RRQ	3	2
URQ	3	1
ARQ	3	2
BRQ	3	2
IRQ	3	1
IRR NOTE 1	5	2
DRQ	3	2
LRQ	5	2
RAI	3	2

[End Correction]

7.2.8 G.723.1 audio packetization

Description: A misleading statement in the description of the G.723.1 packetization is contained within Section 13.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

In general this change should not effect implementations, it is intended to clarify interworking issues should they occur. The corrected text is shown below.

[Begin Correction]

ANNEX F

Audio packetization

This annex describes RTP packetization details for audio codecs standardized by the ITU.

This Recommendation specifies a coded representation that can be used for compressing the speech signal component of multi-media services at a very low bit rate. A G.723.1 frame can be one of three sizes: 24 bytes (6.3 kb/s frame), 20 bytes (5.3 kb/s frame), or 4 bytes. These 4-byte frames are called SID frames (Silence Insertion Descriptor) and are used to specify comfort noise parameters. There is no restriction on how 4, 20, and 24 byte frames are intermixed. The least significant two bits of the first octet in the frame determine the frame size and codec type (refer to Table 5/G.723.1 and Table 6/G.723.1 for more information on bit order). It is possible to switch between the two rates at any 30 ms frame boundary. Both (5.3 kb/s and 6.4 kb/s) rates are a mandatory part of the encoder and decoder. This coder was optimized to represent speech with near-toll quality at the above rates using a limited amount of complexity.

All the bits of the encoded bit stream are transmitted always from the least significant bit towards the most significant bit. NOTE - This refers to the order of bits presented to the transport layer and not the order of bits on the wire.

[End Correction]

7.2.9 ANNEX H - H.225.0 message syntax (ASN.1)

Description: A number of errors have been detected in the ASN.1 syntax of H.225.0 and are shown in the corrected text below.

This information will be contained in the revision 3 of H.225.0 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.225.0 document that was submitted for approval in 1998.

The syntax has been changed to appropriately label the information elements as described in the following correcting section.

The Facility message has had a fastStart field added to it. When utilizing the gatekeeper routed model, the gatekeeper will respond to a Setup with a Call Proceeding. When the gatekeeper sends the Setup to an endpoint, the endpoint can respond with Call Proceeding, but the gatekeeper cannot forward the Call Proceeding to the originating endpoint. If the endpoint included fast start information in the Call Proceeding, the gatekeeper can pass this information to the originating endpoint in a Facility message. The Progress message has inappropriate extension markers. These should have been placed at the end of the currently defined message.

The FastStart token as previously defined, did not include the ASN.1 syntax to enforce the presence of required fields within this token. This correction does not change any protocol that is transmitted.

An error in the syntax for security tokens is present in H.225.0 version 2. The typographical error provides a circular reference, which although is not detrimental to implementations, does not provide the intended option.

In order to allow H.323 implementations to utilize the generic H.235 token format in an application specific manner, the ASN.1 is changed to account for the typographical error. Note that this is a required change whether the functionality is used or not.

[Begin Correction]

...

```
H323-UU-PDU ::= SEQUENCE
{
    h323-message-body  CHOICE
    {
        setup              Setup-UUIE,
        callProceeding          CallProceeding-UUIE,
        connect            Connect-UUIE,
        alerting      Alerting-UUIE,
        ~~userInformationinformation    UIInformation-UUIE,~~information      Information-UUIE,
        releaseComplete    ReleaseComplete-UUIE,
        facility      Facility-UUIE,
        ...,
        progress      Progress-UUIE,
        empty              NULL        -- used when a FACILITY message is sent,
                                            -- but the Facility-UUIE is not to be invoked
                                            -- (possible when transporting supplementary
                                            -- services messages)
    },
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    h4501SupplementaryService     SEQUENCE OF OCTET STRING OPTIONAL,
                            -- each sequence of octet string is defined as one
                            -- H4501SupplementaryService APDU as defined in
                            -- Table 3/H.450.1
    h245Tunneling                 BOOLEAN,
                            -- if TRUE, tunneling of H.245 messages is enabled
    h245Control             SEQUENCE OF OCTET STRING OPTIONAL,
                            -- each octet string may contain exactly
                            -- one H.245 PDU
    nonStandardControl            SEQUENCE OF NonStandardParameter OPTIONAL
}


~~UI~~Information-UUIE    ::=SEQUENCE
{
    protocolIdentifier  ProtocolIdentifier,
    ...,
    callIdentifier      CallIdentifier
}
ReleaseCompleteReason ::= CHOICE
{
    noBandwidth        NULL,        -- bandwidth taken away or ARQ denied
    gatekeeperResources         NULL,        -- exhausted
    unreachableDestination           NULL,        -- no transport path to the destination
    destinationRejection        NULL,        -- rejected at destination
    invalidRevision             NULL,
    noPermission       NULL,        -- called party's gatekeeper rejects
    unreachableGatekeeper  NULL,        -- terminal cannot reach gatekeeper for ARQ
    gatewayResources       NULL,
    badFormatAddress       NULL,
    adaptiveBusy    NULL,    -- call is dropping due to LAN crowding
    inConf          NULL,    -- no address in AlternativeAddress
    undefinedReason        NULL,
    ...,
    facilityCallDeflection          NULL,       -- call was deflected using a Facility message
securityDenied          NULL,  -- incompatible security settings
calledPartyNotRegistered        NULL,  -- used by gatekeeper when endpoint has
                        -- preGrantedARQ to bypass ARQ/ACF
~~callerNotregistered~~callerNotRegistered              NULL   -- used by gatekeeper when endpoint has
                        -- preGrantedArq to bypass ARQ/ACF
}

Facility-UUIE ::= SEQUENCE
{
    protocolIdentifier              ProtocolIdentifier,
    alternativeAddress              TransportAddress OPTIONAL,
    alternativeAliasAddress         SEQUENCE OF AliasAddress OPTIONAL,
    conferenceID                ConferenceIdentifier OPTIONAL,
    reason                      FacilityReason,
    ...,
    callIdentifier                  CallIdentifier,
    destExtraCallInfo               SEQUENCE OF AliasAddress OPTIONAL,
    remoteExtensionAddress              AliasAddress OPTIONAL,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                    SEQUENCE OF CryptoH323Token OPTIONAL,
    conferences                 SEQUENCE OF ConferenceList OPTIONAL,
    h245Address                 TransportAddress OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL
}

Progress-UUIE ::= SEQUENCE
{
    protocolIdentifier          ProtocolIdentifier,
    destinationInfo             EndpointType,
    h245Address         TransportAddress OPTIONAL,
    callIdentifier              CallIdentifier,
    h245SecurityMode            H245Security OPTIONAL,
    ...,
    tokens                      SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens                SEQUENCE OF CryptoH323Token OPTIONAL,
    fastStart                   SEQUENCE OF OCTET STRING OPTIONAL,
    ...
}


FastStartToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, dhkey PRESENT,
generalID PRESENT -- set to 'alias' -- })
EncodedFastStartToken ::= TYPE-IDENTIFIER.&Type (FastStartToken)
CryptoH323Token::= CHOICE
{
    cryptoEPPwdHash SEQUENCE
        {
    alias           AliasAddress, -- alias of entity generating hash
    timeStamp   TimeStamp, -- timestamp used in hash
                token           HASHED     { EncodedPwdCertToken -- generalID set to 'alias' -- }
    },
    cryptoGKPwdHash  SEQUENCE
        {
                gatekeeperId  GatekeeperIdentifier, -- GatekeeperID of GK generating hash
            timeStamp   TimeStamp, -- timestamp used in hash
                token           HASHED     { EncodedPwdCertToken  -- generalID set to Gatekeeperid
        -- }
    },
    cryptoEPPwdEncr          ENCRYPTED
                             { EncodedPwdCertToken -- generalID set to Gatekeeperid --},
    cryptoGKPwdEncr          ENCRYPTED
                             { EncodedPwdCertToken -- generalID set to Gatekeeperid --},
    cryptoEPCert       SIGNED { EncodedPwdCertToken — generalID set to Gatekeeperid -- },
    cryptoGKCert             SIGNED { EncodedPwdCertToken — generalID set to alias -- },
    cryptoFastStart          SIGNED { EncodedFastStartToken },
    nestedcryptoToken        Crypto~~H323~~Token,
    ...
}
```

```
UUIEsRequested ::= SEQUENCE
{
        setup              BOOLEAN,
        callProceeding           BOOLEAN,
        connect            BOOLEAN,
        alerting     BOOLEAN,
        ~~userInformation~~information      BOOLEAN,
        releaseComplete    BOOLEAN,
        facility     BOOLEAN,
        progress     BOOLEAN,
        empty              BOOLEAN,
        ...
}
```

[End Correction]

7.3 Technical and editorial corrections to ITU-T Recommendation H.245

7.3.1 H.2250LogicalChannelAckParameters

Description: A missing field in the LogicalChannelAck corresponding the ATM virtual circuit issues raised in Annex A of this document.

The corrected ASN.1 is shown below.

[Begin Correction]

...

```
H2250LogicalChannelAckParameters      ::=SEQUENCE
{
        nonStandard SEQUENCE OF NonStandardParameter OPTIONAL,
        sessionID       INTEGER(1..255) OPTIONAL,
        mediaChannel  TransportAddress OPTIONAL,
        mediaControlChannel   TransportAddress OPTIONAL, -- forward RTCP channel
        dynamicRTPPayloadType          INTEGER(96..127) OPTIONAL, -- used only by the master or MC
        ...,
        flowControlToZero       BOOLEAN,
        portNumber  INTEGER (0..65535) OPTIONAL
}
```

...

[End Correction]

7.3.2 H.320/H.323 continuous presence

Description: A minor inconsistency has been discovered in the Recommendation H.245 concerning H.320 continuous presence operation.

The H.245 equivalent continuous presence BAS codes were not included in H.245v3 so continuous presence processing cannot be translated through an H.320-H.323 gateway. To correct this, the following ASN.1 should be included with H.245v3.

This information will be contained in the revision 4 of H.245 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.245v3 document that was submitted for approval in 1998.

[Begin Correction]

...

```
    TerminalYouAreSeeingInSubPictureNumber  SEQUENCE
        {
        terminalNumber              TerminalNumber,
        subPictureNumber INTEGER (0..255),
        ...
    }

    VideoIndicateCompose            SEQUENCE
    {
        compositionNumber           INTEGER (0..255),
        ...
    }

ConferenceIndication        ::=CHOICE
{
    sbeNumber   INTEGER (0..9),     -- same as H.230 SBE Number

    terminalNumberAssign            TerminalLabel,-- same as H.230 TIA

    terminalJoinedConference        TerminalLabel,-- same as H.230 TIN

    terminalLeftConference          TerminalLabel,-- same as H.230 TID

    seenByAtLeastOneOther           NULL,       -- same as H.230 MIV
    cancelSeenByAtLeastOneOther     NULL,       -- same as H.230 cancel MIV

    seenByAll                       NULL,       -- like H.230 MIV
    cancelSeenByAll                 NULL,       -- like H.230 MIV

    terminalYouAreSeeing            TerminalLabel,-- same as H.230 VIN
```

```
        requestForFloor             NULL,       -- same as H.230 TIF

        ...,
        withdrawChairToken      NULL,       -- same as H.230 CCR        --      MC-> chair
        floorRequested      TerminalLabel       NULL,-- same as H.230 TIF               -- MC-> chair
        terminalYouAreSeeingInSubPictureNumber TerminalYouAreSeeingInSubPictureNumber,
        videoIndicateCompose      VideoIndicateCompose
}
...
ConferenceCapability        ::=SEQUENCE
{
        nonStandardData   SEQUENCE OF NonStandardParameter OPTIONAL,
        chairControlCapability    BOOLEAN,
        ...
        VideoIndicateMixingCapability  BOOLEAN

}
```

...

[End Correction]

7.3.3 Conference definitions

Description: Minor omissions concerning conference related definitions have been discovered.

This information will be contained in the revision 4 of H.245 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.245v3 document that was submitted for approval in 1998.

These changes should not affect implementations.

[Begin Correction]

B.13.7 Conference indications

– terminalYouAreSeeingInSubPictureNumber shall be defined as H.230 VIN2. subPictureNumber is defined as N as indicated in Figures 2-4/H.243;

– videoIndicateCompose shall be defined as H.230 VIC. compositionNumber is defined as M in Table 4/H.243.

[End Correction]

[Begin Correction]

B.2.2.9 Conference capabilities

videoIndicateMixingCapability shall be defined as H.230 VIM

[End Correction]

7.4 Technical and editorial corrections to ITU-T Recommendation H.246

7.4.1 Annex A corrections

Description: A minor inconsistency has been discovered in the Recommendation H.246 Annex A Section A.5.2.4.1.

The commands MCV and Cancel-MCV are listed with a H.245 equivalent of broadcastMe and cancelBroadcastMe. The H.245 equivalent of these messages should have been listed as the ConferenceCommands broadcastMyLogicalChannelNumber and cancelBroadcastMyLogicalChannel. (NOTE - There is also a H.245 ConferenceRequest to broadcastMyLogicalChannelNumber that provides for a response.)

This information will be contained in the revision 2 of H.246 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.246 document that was submitted for approval in 1998.

This change should not affect behavior in any way.

[Begin Correction]

A.5.2.4.1 Multipoint control C&I

H.230 command/indication	H.245 equivalent
MCV	Send **broadcast**~~**Me**~~MyLogicalChannel
Cancel-MCV	Send **cancelBroadcast**~~**Me**~~MyLogicalChannel

[End Correction]

Description: A minor inconsistency has been discovered in the Recommendation H.246 Annex A Section A.5.2.4.4.

The H.245 equivalent continuous presence BAS codes were not included in H.245v3 so continuous presence processing cannot be translated through a H.320-H.323 gateway. To correct this, commands are added to H.245 and the following corrected translations amend H.246.

This information will be contained in the revision 2 of H.246 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.246 document that was submitted for approval in 1998.

This change should may affect behavior of gateways.

[Begin Correction]

A.5.2.4.4 Video selection and notification C&I

H.230 command/indication	**H.245 equivalent**
VIN	Send **terminalYouAreSeeing**
VCB/Cancel-VCB	Send **makeTerminalBroadcaster/** **CancelMakeTerminalBroadcaster**
VCS/Cancel-VCS	Send **sendThisSource/** **CancelSendThisSource**
VCR	Send **videoCommandReject**
~~VIN2~~	~~FFSSend **terminalYouAreSeeingInSubPictureNumber**~~
VIN2	~~FFS~~Send **terminalYouAreSeeingInSubPictureNumber**
VIC	~~FFS~~send **videoIndicateCompose**
VIM	~~FFS~~send **videoIndicateMixingCapability**

[End Correction]

7.5 Technical and editorial corrections to ITU-T Recommendation H.235

7.5.1 Key escrow usage

Description: A minor inconsistency has been discovered in the Recommendation H.235 Section 6.6.1.

This information will be contained in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

This change does not affect behavior or implementations in any way.

[Begin Correction]

6.6.1 Key escrow

Although not specifically required for operation, this recommendation contains provision for entities utilizing the H.235 protocol to support ~~key recovery~~ the facility known as trusted third party (TTP) within the signalling elements.

[End Correction]

7.5.2 H.235 control channel references

Description: A typographical error has been discovered in Section 8 of the Recommendation H.235.

This information will be contained in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

This change does not affect intended behavior or implementations in any way, the uncorrected text is misleading and in error.

[Begin Correction]

8.2 Unsecured H.245 channel operation

Alternatively, the H.245 channel may operate in an unsecured manner and the two entities open a secure logical channel with which to perform authentication and/or shared-secret derivation. For example TLS or IPSEC may be utilized by opening a logical channel with the datatype containing a value for **~~encryptionData~~h235Control**. This channel could then be used to derive a shared secret which protects any media session keys or to transport the **EncryptionSync**.

[End Correction]

7.5.3 Multipoint procedure section reference

Description: A minor section reference has been discovered in the Recommendation H.235 Section 9.

This information will be contained in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

[Begin Correction]

9 Multipoint procedures

9.1 Authentication

Authentication shall occur between an endpoint and the MC(U) in the same manner that it would in a point to point conference. The MC(U) shall set the policy concerning level and stringency of authentication. As stated in Section~~0~~ 6.6 the MC(U) is trusted; existing endpoints in a conference may be limited by the authentication level employed by the MC(U). New **ConferenceRequest**/**ConferenceResponse** commands, allow endpoints to obtain the certificates of other participants in the conference from the MC(U). As outlined in H.245 procedures, endpoints in a multipoint conference may request other endpoint certificates via the MC, but may not be able perform direct cryptographic authentication within the H.245 channel.

...

[End Correction]

7.5.4 Introduction to authentication

Description: The introductory text (paragraph 1) to Section 10 of revision 1 of H.235 Recommendation has been determined to be unclear and potentially misleading.

This text will be corrected in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this text appears in the final H.235 document that was submitted for approval in 1998.

This change should not effect implementations or operations, but readers are encouraged to utilize the following text.

[Begin Correction]

10.1 Introduction

Authentication is in general based either on using a shared secret (you are authenticated properly if you know the secret) or on public key based methods with certifications (you prove your identity by possessing the correct private key). A shared secret and the subsequent use of symmetric cryptography requires a prior contact between the communicating entities. A prior face-to-face or secure contact can be replaced by generating or exchanging the shared secret key with methods based on public key cryptography, e.g. by Diffie-Hellman key exchange. The communication parties in the key generation and exchange have to be authenticated for example by using digitally signed messages; otherwise the communication parties cannot be sure with whom they share the secret.

This Recommendation presents authentication methods based on subscription, i.e. there must be a prior contact for sharing a secret, and authentication methods where public key cryptography is directly used in authentication or it is used for generating the shared secret.

~~There are two types of authentication that may be utilized. The first type is symmetric encryption based that requires no prior contact between the communicating entities. The second type is based on the ability to have some prior shared secret (further referenced as 'subscription' based). Two forms of subscription-based authentication are provided; password and certificate.~~

[End Correction]

7.5.5 Diffie-Hellman exchange with optional authentication

Description: Two errors have been discovered in the labelling of parameters of arguments in the Diffie-Hellman exchange described in the Recommendation H.235 Section 10.2. Additionally, the note concerning authentication is to be clarified.

This information will be contained in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

Phase 1: As this correction affects implementations, which utilize this mechanism to provide authentication during the Diffie-Hellman exchange. Note that if these optional parameters are not utilized (denoted by italics below and in the original recommendation) no implementation changes are needed.

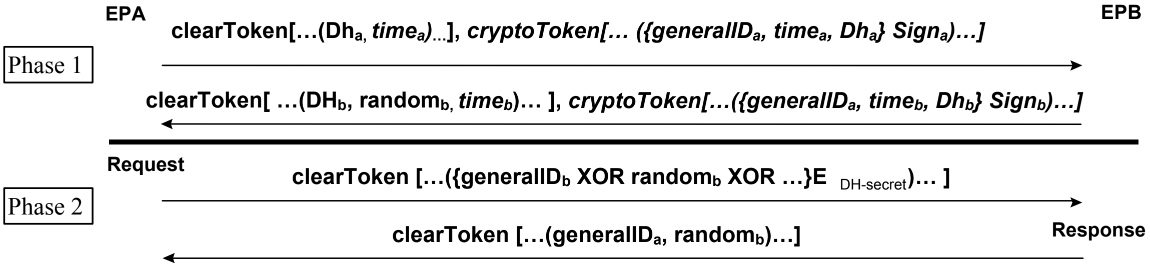
Phase 2: The identifier (generalID) passed from in the second exchange (e.g. Response) should be that of the recipient of the Response message (e.g. EPA).

[Begin Correction]

10.2 Diffie-Hellman with optional authentication

...

NOTE - If the messages are exchanged over an insecure channel, then digital signatures (or other message origin authentication method) must be used in order to authenticate the parties between whom the secret will be shared. An optional signature element may also be provided these are illustrated in ***italics*** below.


EPA
EPB
clearToken[…(Dh$_a$, *time$_a$)…*], *cryptoToken[… ({generalID$_a$, time$_a$, Dh$_a$} Sign$_a$)…]*
Phase 1
clearToken[…(DH$_b$, random$_b$, *time$_b$*)…], *cryptoToken[…({generalID$_a$, time$_b$, Dh$_b$} Sign$_b$)…]*
Request
clearToken […({generalID$_b$ XOR random$_b$ XOR …}E $_{\text{DH-secret}}$)…]
Phase 2
clearToken […(generalID$_a$, random$_b$)…]
Response

...

[End Correction]

7.5.6 Introduction to subscription based authentication

Description: The introductory text (paragraph 1) to Section 10.3 of revision 1 of H.235 Recommendation has been determined to be unclear and potentially misleading. The included text should be added as a new, final paragraph.

This text will be corrected in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this text appears in the final H.235 document that was submitted for approval in 1998.

This change should not effect implementations or operations, but readers are encouraged to utilize the following text.

[Begin Correction]

10.3.1 Introduction

...

NOTE - In all cases where timestamps are generated and passed as part of a security exchange, implementors should take the following precautions. The time stamp granularity should be fine enough that it is guaranteed to increment with each message. If this is not guaranteed, replay attacks are possible. (e.g. if the timestamp only increments by the minute, then an endpoint "C" can spoof endpoint "A" within duration of one minute after endpoint "A" has sent a message to endpoint "B").

...

[End Correction]

7.5.7 Password with Hashing

Description: The text to Section 10.3.3 of revision 1 of H.235 Recommendation has been determined to be unclear with respect to parameters that are passed in the exchange of messages. The included text should be added as a new, final paragraph.

This text will be corrected in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this text appears in the final H.235 document that was submitted for approval in 1998.

This change should not effect implementations or operations, but readers are cautioned to take into account the following text.

[Begin Correction]

10.3.3 Password with Hashing

...

NOTE 3 - The **cryptoHashedToken** structure is used to pass the parameters used in this exchange. Included in this structure are the "clear" versions of parameters needed to compute the hashed value. Implementors should include the timestamp in the **hashedVals** and should ***not*** include the password. (E.g. both the password and the "generalID" should be known a priori by the recipient).

...

[End Correction]

7.5.8 Corrections to Annex A

Description: An omission in the ASN.1 syntax for H.235 has been discovered. Specifically, an identifier is missing from the ClearToken structure.

This information will be contained in the revision 2 of Recommendation H.235 to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

The absence of this identifier will not allow multiple ClearTokens included in a single RAS message to be associated with individual uses. Additionally, ClearTokens may be defined for different uses that have the same format and these need to be differentiated by the **tokenOID**.

[Begin Correction]

```
ClearToken          ::= SEQUENCE  -- a `token' may contain multiple value types.
{
        tokenOID    OBJECT IDENTIFIER,
        timeStamp           TimeStamp OPTIONAL,
        password            Password OPTIONAL,
        dhkey               DHset OPTIONAL,
        challenge           ChallengeString OPTIONAL,
        random              RandomVal OPTIONAL,
        certificate         TypedCertificate OPTIONAL,
        generalID           Identifier OPTIONAL,
        nonStandard         NonStandardParameter OPTIONAL,
        ...
}
```

[End Correction]

7.5.9 Corrections to Annex B

Description: A number of typographical errors have been discovered in Annex B. Their corrected values are shown below.

This information will be contained in the revision 2 of Recommendation H.235 to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

[Begin Correction]

2 Signalling and procedures

...

One purpose of H.225.0 exchanges as they relate to H.323 security, is to provide a mechanism to set up the secure H.245 channel. Optionally, authentication may occur during the exchange of H.225.0 messages. This authentication may be certificate or password based, utilizing encryption and/or hashing (i.e. signing). The specifics of these modes of operation are described in Sections ~~(0-04.2-4.3)~~(4.2-4.3)

...

[End Correction]

[Begin Correction]

4.1 Introduction

This annex will not explicitly provide any form of message privacy between gatekeepers and endpoints. There are two types of authentication that may be utilized. The first type is symmetric encryption based that requires no prior contact between the endpoint and Gatekeeper. The second type is subscription based and will have two forms, password or certificate. All of these forms are derived from the procedures shown in Sections ***[change these to document cross-references]*** 10.2, 10.3.2, 10.3.3 and 10.3.4. In this annex, the generic labels (EPA and EPB) showed in the aforementioned sections will represent the Endpoint and Gatekeeper respectively.

...

[End Correction]

[Begin Correction]

4.2 Endpoint-Gatekeeper authentication (non-subscription based)

This mechanism may provide the Gatekeeper with a cryptographic link that a particular endpoint, which previously registered, is the same one that issues subsequent RAS messages. It should be noted that this might not provide any authentication of the Gatekeeper to the endpoint, unless the optional signature element is included. The establishment of the identity relationship occurs when the terminal issues the **GRQ** as outlined in H.323 Section ***[change to cross-reference]*** **7.2.1**. The Diffie-Hellman exchange shall occur in conjunction with the **GRQ** and **GCF** messages as shown in the first phase of Section 0. This shared secret key shall now be used on any subsequent **RRQ**/**URQ** from the terminal to the gatekeeper. If a Gatekeeper operates in this mode and receives a **GRQ** without a token containing the *DHset* or an acceptable algorithm value, it shall return a **securityDenial** reason code in the **DRJ**.

Terminal (**xRQ**):

1) The terminal shall provide all of the information in the message as described in the appropriate H.225.0 sections.

2) The terminal shall encrypt the **GatekeeperIdentifier** (as returned in the **GCF**) using the shared secret key that was negotiated. This shall be passed in a~~**cryptoToken**~~ **clearToken (see Section 10.2)** as the **generalID**.

   The 16 bits of the **random** and then the **requestSeqNum** shall be XOR'd with each 16 bits of the **GatekeeperIdentifier**. If the **GatekeeperIdentifier** does not end on an even 16 boundary, the last 8 bits of the **GatekeeperIdentifier** shall be XOR'd with the least significant octet of the random value and then **requestSeqNum.** The **GatekeeperIdentifier** shall be encrypted using the selected algorithm in the **GCF** (~~integrity~~algorithmOID) and utilizing the entire shared secret.

   The following example illustrates this procedure:

   RND16: 16 bit value of the Random Value

   SQN16: 16 bit value of requestSeqNum

   BMPX: the Xth BMP character of GatekeeperIdentifier

   BMP1' = (BMP1) XOR (RND16) XOR (SQN16)

   BMP2' = (BMP2) XOR (RND16) XOR (SQN16)

   BMP3' = (BMP3) XOR (RND16) XOR (SQN16)

   BMP4' = (BMP4) XOR (RND16) XOR (SQN16)

   BMP5' = (BMP5) XOR (RND16) XOR (SQN16)

   :

   :

   BMPn' = (BMPn) XOR (RND16) XOR (SQN16)

...

[End Correction]

[Begin Correction]

5.1 Gateway

As stated in Section***[change to cross reference]*** **6.6**, an H.323 Gateway should be considered a trusted element. This includes protocol gateways (H.323-H.320 etc.) and security gateways (proxy/firewalls). The media privacy can be assured between the communicating endpoint and the gateway device; but what occurs on the far side of the gateway should be considered insecure by default.

[End Correction]

7.5.10 Corrections to Appendix I

Description: A typographical error has been discovered with respect to a section reference of encryption key generation.

This information will be contained in the revision 2 of H.235 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.235 document that was submitted for approval in 1998.

The referenced section was incorrectly labelled to a non-existent section heading.

[Begin Correction]

4.2 Password

...

The encryption key is constructed from the user's password using the procedure described in Section ~~3.3.3.341~~10.3.2 of H.235**.** The resulting octet "string" is then used as the DES key to encrypt the **challenge**.

...

[End Correction]

7.6 Technical and editorial corrections to ITU-T H.450 series Recommendations

7.6.1 H.450.1 corrections

Description: Typographical errors have been discovered by Delayed Contribution "D.214 (WP 2/16) – reprint" of the September 1998 SG 16 Meeting in clause 6.6 of H.450.1.

This information will be contained in the revision 2 of H.450.1 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.450.1 document that was submitted for approval in 1998. These changes do not affect behavior or implementations in any way.

1) Editorial, Clause 6.6, line 6

Change:

"rejectUnrecognizedInvokePdu"

to

"rejectAnyUnrecognizedInvokePdu"

2) Editorial, Clause 6.6, line 12

Change:

"discardAnyUnrecognizedInvokePDU"

to

"discardAnyUnrecognizedInvokePdu"

7.6.2 H.450.2 corrections

Description: Typographical errors have been discovered by Delayed Contribution "D.214 (WP 2/16) – reprint" of the September 1998 SG 16 Meeting in H.450.2 clauses 11.4.2, 11.5.2, 11.6.2 and 13.4.

This information will be contained in the revision 2 of H.450.2 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.450.2 document that was submitted for approval in 1998. These changes do not affect behaviour or implementations in any way.

1) Editorial - Clause 11.4.2, line 4 c)

Change:

"The CTSetup.request primitive is used to request call establishment from TRTSE."

to

"The CTSetup.request primitive is used to request call establishment to TRTSE"

2) Editorial - Clause 11.4.2, line 5 d)

Change:

"The CTSetup.confirm primitive is used to indicate success of call establishment to TRTSE."

to

"The CTSetup.confirm primitive is used to indicate success of call establishment from TRTSE."

3) Editorial - Clause 11.5.2, line 6 e)

Change:

"The CTIdentify.indication primitive is used to request a call identification."

to

"The CTIdentify.indication primitive is used to indicate a call identification."

4) Editorial - Clause 11.5.2, line 11,12 j)

Change:

"The CTComplete.request primitive may be used by GKs to request sending of call transfer information to the transferred-to user."

to

"The CTComplete.request primitive may be used by GKs to request sending of call transfer information to the transferred-to endpoint."

5) Editorial - Clause 11.5.2, line 13,14 k)

Change:

"The CTComplete.indication primitive is used to indicate call transfer information to the transferred-to endpoint."

to

"The CTComplete.indication primitive is used to indicate call transfer information to the transferred-to user."

6) Editorial - Clause 11.6.2, line 2

Change:

"CT-T1 - Timer CT-T1 shall operate at the TRGSE during state CT-Await-Identify-Response. Its purpose is to protect against the absence of response to the CTIdentify.request""

to

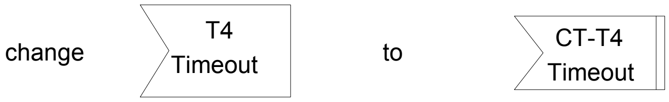
"CT-T1 - Timer CT-T1 shall operate at the TRGSE during state CT-Await-Identify-Response. Its purpose is to protect against the absence of response to the CTIdentify.invoke."

7) Editorial – Clause 13.4, FIGURE 25 (sheet 2 of 3, 4th branch) of H.450.2

(i.e. FIGURE 22/H.450.2 (sheet 2 of 3, 4th branch) of H.450.2 (2/98) publication)

Change "T4 Timeout" to "CT-T4 Timeout".

In addition, the type of symbol was mistake. Time-Out event is an internal event.



7.6.3 H.450.3 Corrections

Description: Typographical errors have been discovered by Delayed Contribution "D.214 (WP 2/16) – reprint" of the September 1998 SG 16 Meeting in H.450.3 clause 12 SDLs.

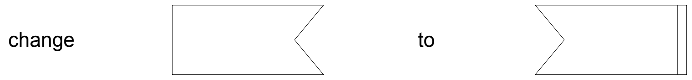
This information will be contained in the revision 2 of H.450.3 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.450.3 document that was submitted for approval in 1998. These changes do not affect behaviour or implementations in any way.

1) Editorial – Clause 12 SDL FIGURES 21 (most right branch), 22 (most right branch), 23 (most right branch), 28 (sheet 1 of 4, second right branch) of H.450.3

(i.e. FIGURES 19, 20, 21 and 24 (sheet 1 of 4) of H.450.3 of H.450.3 (2/98) published).

The type of symbol was mistake. Time-Out event is an internal event

NOTE - The text within the referred symbols remains unchanged.



7.6.4 H.450.3 ASN.1 correction

Description: A typographical error has been discovered in the ASN.1 definitions presented in H.450.3, Chapter 11.

This information will be contained in the revision 2 of H.450.3 Recommendation to be published by the ITU-T. However, this information appears incorrectly in the final H.450.3 document that was submitted for approval in 1998.

The corrected, included element is shown below.

[Begin Correction]

H225InformationElement FROM H225-~~Generic~~generic-parameters-definition

...

[End Correction]

8 Implementation clarifications

8.1 Token usage in H.323 systems

There has been some confusion on the usage of individual **CryptoH323Tokens** as passed in RAS messages. There are two main categories of CryptoH323Tokens; those used for H.235 procedures and those used in an application specific manner. The use of these tokens should be according to the following rules:

- All H.235 defined (e.g. cryptoEPPwdHash, cryptoGKPwdHash, cryptoEPPwdEncr, cryptoGKPwdEncr, cryptoGKCert, and cryptoFastStart). shall be utilized with the procedures and algorithms as described in H.235.
- Application specific or proprietary use of tokens shall utilize the nestedcryptoToken for their exchanges.
- Any nestedcryptoToken used should have an tokenOID (object identifier) which unambiguously identifies it.

8.2 H.235 random value usage in H.323 systems

The random value that is passed in xRQ/xCF sequence between endpoints and Gatekeepers may be updated by the Gatekeeper. As described in Section 4.2 of H.235 this random value may be refreshed in any xCF message to be utilized by a subsequent xRQ messages from the endpoint. Due to the fact that RAS messages may be lost (including xCF/xRJ) the updated random value may also be lost. The recovery from this situation may be the reinitializing of the security context but is left to local implementation.

Implementations that require the use of multiple outstanding RAS requests will be limited by the updating of the random values used in any authentication. If the updating of this value occurs on every response to a request, parallel requests are not possible. One possible solution, is to have a logical "window" during which a random value remains constant. This issue is a local implementation matter.

8.3 Gateway resource availability messages

The Resources Available Indication (RAI) is a notification from a gateway to a gatekeeper of its current call capacity for each H-series protocol and data rate for that protocol. The gatekeeper responds with a Resources Available Confirmation (RAC) upon receiving a RAI to acknowledge its reception. A Gatekeeper should ignore any RAI notifications (e.g. send no RAC) upon receiving a RAI which contains bogus information (i.e. a bad endpointIdentifier).

8.4 OpenLogicalChannel in fastStart

In the H.225.0 ASN.1, fastStart is defined as SEQUENCE OF OCTET STRING OPTIONAL. The text definition states "This uses the OpenLogicalChannel structure defined in H.245…" Each OCTET STRING in fastStart is to contain the OpenLogicalChannel structure, not an entire request message.

8.5 Clarification in Q.931

Table 4-3/Q.931 (Information Element Identifier Coding) shows that the Progress Indicator IE identifier (like an opcode) shows 0x1e, but Figure 4-29/Q.931 (octet layout of Progress Indicator IE) shows the identifier as 0x1f. Note that the identifier should be 0x1e.

8.6 Graceful closure of TCP connection

When a TCP connection is closed, the graceful closure procedure documented in Section 3.5 of RFC 793 should always be used.

8.7 Race condition on simultaneous close of channel

In Section 8.5 step 6 of Phase E cleardown procedure it is possible for both ends to simultaneously issue a Release Complete. The endpoint must therefore be prepared to receive and ignore the redundant Release Complete message.

H.323 RECOMMENDATION SERIES DEFECT REPORT FORM

DATE:	
CONTACT INFORMATION **NAME:** **COMPANY:** **ADDRESS:** **TEL:** **FAX:** **E-MAIL:**	
AFFECTED RECOMMENDATIONS:	
DESCRIPTION OF PROBLEM:	
SUGGESTIONS FOR RESOLUTION:	

NOTE - Attach additional pages if more space is required than is provided above.