INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 1997 - 2000

COM 16-63-E
March 2000
Original: English only

Question(s): 1-24/16

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

STUDY GROUP 16 – REPORT R 63

SOURCE*: Study Group 16 (Geneva, 7 – 18 February 2000)

TITLE: Implementor's Guide for ITU-T Recommendations

CONTENTS

* **Contact:** TSB

Tel: 730 5860
Fax: 730 5853

1. Implementor's Guide for the ITU-T V.140 Recommendation – Procedures for establishing communication between two multiprotocol audiovisual terminals using digital channels at a multiple of 64 or 56 kbit/s

Abstract

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T V.140 Recommendation. It is intended to be read in conjunction with the Recommendation 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 the affected V.140 Recommendation.

Contact information

ITU-T Study Group 16/Question 5 Rapporteur

Mr. John Magill
Consultant, Probe Communications
Meadow View
Braydonside
Chippenham
Wilts SN15 5AR
UK

Tel/Fax: +441 666 510270
E-mail: hjm@probecom.demon.co.uk

Implementor's Guide Editor

Patrick Luthi
PictureTel Corp.
100 Minuteman Road
Andover, MA 01810
USA

Tel: +1 978 292 5000
Fax: +1 978 292 3328
Email: luthip@pictel.com

ITU-T Recommendation V.140 Editor

Document history

Revision	Date	Description
1	7-18 February 2000	Initial version - Reviewed at ITU-T Study Group 16 Rapporteurs meeting.

1. Introduction

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T V.140 Recommendation. It is intended to be read in conjunction with the Recommendation 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 the affected V.140 Recommendation.

The first version of the guide was produced following the February 2000 ITU-T Study Group 16/Question 5 & 11 Rapporteur 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 Question 5 Rapporteur's Group. It can be revised at any recognized Q.5/16 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.

4. Defect resolution procedure

Upon discovering technical defects with any components of the V.140 Recommendation, please provide a written description directly to the editors of the affected Recommendations with a copy to the Q.5/16 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 V.140 Recommendation. Formal membership in the ITU is not required to participate in this process.

5. References

This document refers to the following V.140 Recommendation:

– ITU-T Recommendation V.140 (1998), *Procedures for establishing communication between two multiprotocol audiovisual terminals using digital channels at a multiple of 64 or 56 kbit/s*

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 V.140

7.1.1 Figure 11/V.140 – FCS mapping convention

The description in the 3rd paragraph of Section 8.5.1 is not aligned with Figure11 to which it refers. Therefore, Figure 11 should be replaced with the following corrected figure:

[Begin Correction]

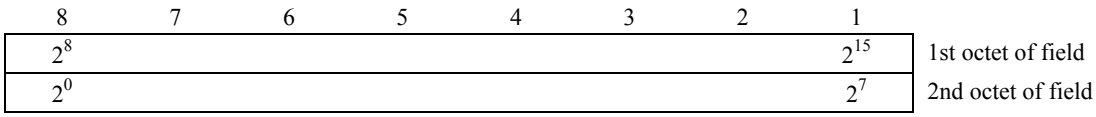


Figure 11/V.140 – FCS mapping convention

[End Correction]

7.1.2 Figure 12/V.140 – "Ladder" diagram of the sequence of signals and phases of V.140

In the top left section of figure 12, the text "H.247 signature" is being replaced by "V.140 signature".

7.1.3 Annex A – ASN.1 definition of Phase 3 PDU values

7.1.3.1 Changes to roleAndCapability and modeSelect PDUs

In the structure of IsdnCapability and IsdnMode, an element "h324Multilink" (Annex F/H.324) is defined, but was omitted from the text found in the last part of Annex A. Therefore, the text is being updated as follows:

[Begin Correction]

The following refers to fields and structures used within the **roleAndCapability** PDU:

- **g711aLaw**, **g711uLaw**, **h320**, **h324AnnexD**, **h324Multilink, group4Fax**, **t120**, **t140**, **v110**, or **v120** assigned to an **IsdnCapability** field shall indicate that the terminal can support operation according to Recommendations G.711 (A-law encoding), G.711 (μ-law encoding), H.320, Annex D/H.324, Annex F/H.324, T.6, T.120. T.140, V.110, or V.120, respectively.

[End Correction]

…

[Begin Correction]

The following refers to fields and structures used within the **modeSelect** PDU:

- **g711aLaw**, **g711uLaw**, **h320**, **h324AnnexD**, **h324Multilink, group4Fax**, **t120**, **t140**, **v110**, or **v120** assigned to the **plainIsdnMode** field (an **IsdnMode** structure) shall indicate that the terminal has selected operation according to Recommendations G.711 (a-law encoding), G.711 (μ-law encoding), H.320, Annex D/H.324, Annex F/H.324, T.6, T.120. T.140, V.110, or V.120, respectively.

[End Correction]

7.1.3.2 Changes to ASN.1 syntax

The definition of Mode in ASN.1 structure is missing and a text description is being added after the end of the IsdnCapability structure before the "{" as follows:

[Begin Correction]

```
Mode                                ::= CHOICE
{
        nonStandard                         NonStandardParameter,
        plainIsdnMode                           IsdnMode,
        h244                                    IsdnMode,
        is13871                                 IsdnMode,           -- BONDING protocol
        multilinkAdditionalConnection       SEQUENCE
        {
                callAssociationNumber   INTEGER (0..4294967295),
                …
        },
        …
}
```

[End Correction]

V.140 RECOMMENDATION SERIES DEFECT REPORT FORM

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

2 Implementer's Guide for H.323, H.225.0, H.245, H.246, H.235, H.450 Series and H.341 Recommendations

Contact Information

ITU-T Study Group 16 / Question 13 Rapporteur	Dale Skran Sonus Networks USA	Tel: Fax: E-mail:
ITU-T Study Group 16 / Question 14 Rapporteur ITU-T Recommendation H.450.8 Editor	Glen Freundlich Lucent Technologies 11900 N. Pecos St. Westminster, CO 80234 USA	Tel: +1 303 538 2899 Fax: +1 303 538 5478 E-mail: ggf@lucent.com
ITU-T Recommendation H.225.0 Editor	Rich Bowen Cisco Systems, Inc. 7025 Kit Creek Road Research Triangle Park, NC 27709 USA	Tel: +1 919 392 3890 Fax: +1 919 392 6801 E-mail: rkbowen@cisco.com
ITU-T Recommendation H.225.0 Annex G Editor	Michael Fortinsky VocalTec Communications, Ltd. 2 Maskit St. Herzeliya 46733 Israel	Tel: +972 9 970 7768 Fax: +972 9 956 1867 E-mail: mike@vocaltec.com
ITU-T Recommendation H.235 Editor	Martin Euchner Siemens AG ZT IK 3 Otto-Hahn-Ring 6 81730 Munich Germany	Tel: +49 89 636 46201 Fax: +49 89 636 48000 E-mail: Martin.Euchner@mchp.siemens.de
ITU-T Recommendation H.245 Editor	Mike Nilsson BT Labs Ipswitch United Kingdom	Tel: +44 1 473 645413 Fax: +44 1 473 643791 E-mail: mike.nilsson@bt-sys.bt.co.uk
ITU-T Recommendation H.323 Editor H.323 Series Implementers Guide Editor	Paul E. Jones Cisco Systems, Inc. 7025 Kit Creek Road Research Triangle Park, NC 27709 USA	Tel: +1 919 392 6948 Fax: +1 919 392 6801 E-mail: paul.jones@ties.itu.int
ITU-T Recommendation H.341 Editor	Irina Suconick Ennovate Networks USA	Tel: Fax: E-mail: irina@ennovatenetworks.com
ITU-T Recommendation H.450.1, H.450.2, and H.450.3, H.450.4, H.450.5, H.450.6 Editor	Markku Korpi Siemens AG Munich Germany	Tel: +49 89 722 34570 Fax: +49 89 722 23977 E-mail: korpim@sbs.de
ITU-T Recommendation H.450.7 Editor	Dave Walker SS8 Networks 135 Michael Cowpland Drive, Suite 200 Kanata, Ontario, K2M 2E9 Canada	Tel: +1 613 592 8450 Fax: +1 613 592 9634 E-mail: dwalker@ss8networks.com

1 Introduction

This document is a compilation of reported defects identified with the 1998 and 1999 decided editions of the ITU-T H.323 series Recommendations. It must be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementers. The changes, clarifications and corrections defined herein are expected to be included in future versions of affected H.323 series Recommendations.

2 Scope

This guide resolves defects in the following categories:

- editorial errors
- technical errors, such as omissions and inconsistencies
- anbiguities

In addition, the Implementers 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 through contributions to the ITU-T.

3 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 Q13/16 or Q14/16 Rapporteur. The template for a defect report is located at the end of the Guide. Contact information for these parties is included at the front of the 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.

4 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.323 (1999), *Packet-Based multimedia communications systems*
- ITU-T Recommendation H.225.0 (1998), *Call signaling protocols and media stream packetization for packet based multimedia communications Systems*
- ITU-T Recommendation H.225.0 (1999), *Call signaling 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.245 (1999), *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
- ITU-T Recommendation H.450.1 (1998), *Generic functional protocol for the support of supplementary services in H.323*
- ITU-T Recommendation H.450.2 (1998), *Call transfer supplementary service for H.323*
- ITU-T Recommendation H.450.3 (1998), *Call diversion supplementary service for H.323*
- ITU-T Recommendation H.450.4 (1999), *Call Hold Supplementary Service for H.323*
- ITU-T Recommendation H.450.5 (1999), *Call Park and Call Pickup Supplementary Services for H.323*
- ITU-T Recommendation H.450.6 (1999), *Call Waiting Supplementary Service for H.323*
- ITU-T Recommendation H.450.7 (1999), *Message Waiting Indication Supplementary Service for H.323*
- ITU-T Recommendation H.450.8 (2000), *Name Identification Supplementary Service For H.323*
- ISO/IEC 11571 (1998), Information technology – Telecommunications and information exchange between systems – Private Integrated Services Networks – Addressing
- ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*

5 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.

6 Technical and Editorial Corrections

6.1 Technical and Editorial Corrections to ITU-T Recommendation H.323 (1998)

In addition to the corrections noted in the Implementers Guide approved in May 1999, this section contains corrections to errors that were discovered and corrected in H.323 (1998) after the previously approved Implementers Guide. In addition, there may be additional changes in section 6.2 applicable to H.323 (1998)—such changes will be explicitly stated in the "Description" areas.

6.1.1 Facility Redirection

DESCRIPTION:	An editorial error was discovered in the Implementers Guide approved in May 1999. Section 6.1.4 of that document proposed textual changes to sections 8.4.3.1 of H.323 (1998) that were incorrect. In addition, changes should have been made to section 8.4.3.4. The correct text was introduced into H.323 (1999) and is shown below.

[Begin Correction]

8.4.3.1 Direct Endpoint Call Signalling – Conference Create

...

A2d) If Endpoint 2 is an MC(U) that 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.

Upon receipt of this **conferenceListChoice** Facility message, Endpoint 1 may join a conference from the list of conferences by sending a new Setup message to the MC(U) on the Call Signaling Channel which contains the selected CID and which has **conferenceGoal = join**. If Endpoint 1 chooses not to join any of the listed conferences, it shall send a Release Complete message to the MC(U).

...

[End Correction]

[Begin Correction]

8.4.3.4 Gatekeeper Routed Call Signalling – Conference Create

...

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.

Upon receipt of this **conferenceListChoice** Facility message, Endpoint 1 may join a conference from the list of conferences by sending a new Setup message to the MC(U) on the Call Signaling Channel which contains the selected CID and which has **conferenceGoal = join**. If Endpoint 1 chooses not to join any of the listed conferences, it shall send a Release Complete message to the MC(U).

...

[End Correction]

6.1.2 Third Party Initiated Pause and Re-routing

DESCRIPTION:	A technical error was discovered in the definition of the Empty Capability Set in H.323 (1998). According to the text, the empty capability set was one that did not contain receive capabilities. However, this was a source of problems for announcement servers and other "transmit-only" devices. H.323 (1999) has corrected this definition. In addition to re-defining what an empty capability set is, H.323 (1999) also clarifies that a "pause" is a "transmitter-side" pause. When a terminal receives an empty capability set, it shall stop transmitting and close any logical channels it has opened. Below is the full text of 8.4.6/H.323 (1999) and should replace the text found in H.323 (1998).

[Begin Correction]

8.4.6 Third party initiated pause and re-routing

For the purpose of this section, an empty capability set is defined as a **terminalCapabilitySet** message that contains only a sequence number and a protocol identifier.

To allow Gatekeepers to re-route connections from endpoints that do not support supplementary services, endpoints shall respond to the reception of an empty capability set as defined in this section. This feature allows "network" elements such as PBXs, call centers, and IVR systems to re-route connections independently of supplementary services and facilitates pre-connect announcements. It can also be used to delay H.245 media establishment when features such as Gatekeeper based user location are being used. It is also highly recommended that Version 1 endpoints support this feature.

On reception of an empty capability set, an endpoint shall enter a "transmitter side paused" state. On entering this state, the endpoint shall stop transmitting on established logical channels, and shall close all logical channels that it previously opened, including bi-directional logical channels. It shall close these channels in the usual way, that is, by sending the **closeLogicalChannel** message. The endpoint shall not request the remote endpoint to close logical channels, either uni-directional or bi-directional, that the remote endpoint opened. The endpoint shall send the **terminalCapabilitySetAck** message in the usual way: the message may be sent before stopping transmission, and so shall not be interpreted as an indication that transmission has stopped.

While in the "transmitter side paused" state, an endpoint shall not initiate the opening of any logical channels, but shall accept the opening and closing of logical channels from the remote end based on the usual rules and shall continue to receive media on open logical

channels opened by the remote endpoint. This allows endpoints to receive announcements (e.g. pre-connect call progress) where the announcing entity does not wish to receive media from the endpoint. A **terminalCapabilitySet** message may be sent whenever an endpoint's capabilities change, including when the endpoint is in the "transmitter side paused" state. This allows communication to be established between two endpoints that initially do not declare any capabilities.

An endpoint shall leave the "transmitter side paused" state on reception of any **terminalCapabilitySet** message, other than an empty capability set. On leaving this state, an endpoint shall reset its H.245 state to that which it was in just after the H.245 transport connection was made at call establishment time (i.e. the beginning of phase B), but shall preserve state information relating to any logical channels that are open. This puts the endpoint in a known H.245 state after the pause. This allows an endpoint to be connected to a different endpoint when it is released from the paused state.

After leaving the "transmitter side paused" state, an endpoint shall proceed with normal H.245 procedures: it shall take part in master/slave determination signalling, and may proceed with normal open logical channel signalling procedures. When an MC leaves the "transmitter side paused" state, it shall act as if a new endpoint has entered the conference.

Unless its capabilities have changed, an endpoint need not resend a capability set as the gatekeeper will have supplied this to the remote endpoint to remove any paused state in the remote endpoint. This option of not sending a capability set enables faster reconnection. If the first **terminalCapabilitySet** message sent by an endpoint after leaving the "transmitter side paused" state differs from the capability set that the gatekeeper provided to the remote endpoint, the gatekeeper shall signal the remote endpoint to remove capabilities which were not indicated by the initiating endpoint.

NOTE – An endpoint should take care with the capabilities it sends at this time. In particular, an endpoint shall send all capabilities it wants to advertise and not a small addition to previously signalled capabilities. In addition, if the endpoint has so many capabilities that it requires more than one **terminalCapabilitySet** to signal them, there may be a window of time when the gatekeeper has removed the capabilities described in second and subsequent **terminalCapabilitySet** messages.

NOTE – A non-empty capability set shall not be sent to an endpoint until all of its transmit and receive logical channels have been closed. A switching entity should also send an H.450 redirection indication Facility message if the endpoint is being re-routed.

[End Correction]

6.2 Technical and Editorial Corrections to ITU-T Recommendation H.323 (1999)

6.2.1 Termination of Fast Connect when using H.245 Tunneling

DESCRIPTION:	An ambiguity exists regarding the termination of Fast Connect when using H.245 tunneling. The text below attempts to correct this ambiguity.

[Begin Correction]

8.1.7.2 Switching to H.245 procedures

After establishment of a call using the Fast Connect procedure, either endpoint may determine that it is necessary to invoke call features that require the use of H.245 procedures. Either endpoint may initiate the use of H.245 procedures at any point during the

call, using tunneling as described in 8.2.1 (if **h245Tunneling** remains enabled) or a separate H.245 connection. The process for switching to a separate H.245 connection is described in 8.2.3.

It is possible to switch to H.245 procedures before the Fast Connect procedure completes. If **h245Tunneling** is enabled, the terminating party may start using tunneling as described in 8.2.1. If H.245 transport address is included in the Setup message, then the terminating party may start the switch to H.245 as described in 8.2.3.

When a call is established using the Fast Connect procedure, both endpoints shall keep the Q.931 Call Signalling Channel open until either the call is terminated or a separate H.245 connection is established.

...

[End Correction]

6.2.2 Tones and Announcements

DESCRIPTION:	H.323 does not explicitly describe how tones and announcements should be provided, although implicit procedures may be derived from the Q.931 heritage of H.225.0. The Fast Connect procedures allow "early cut through" of the media stream for providing ringback tones, but no mention is made of how the originating is supposed to decide if locally generated ringback shall be applied or not. The text below shall be added to H.323 to clarify this issue.

[Begin Addition]

8.1.7.4 Tones and announcements

Tones and announcements can be locally generated or passed in-band from the terminating endpoint.

On completing call setup, the endpoint on the terminating side shall decide if it will provide in-band tones or if locally generated tones at the originating side shall be used. Note that other type of indication can replace locally generated tones and announcement in some systems (visual indications on a screen for example: for the purpose of this section, they will be referred-to as locally generated tones and announcements). Locally generated tones, provided at the originating side, is the default. The terminating side may wish to provide in-band-generated tones and announcements, for example when the terminating endpoint is a gateway to an analogue network. To instruct the originating side not to generate locally generated tones such as ringback or busy, the terminating side shall open the media channel by responding to the Fast Connect request and send a Progress indicator information element with progress descriptor #1, *Call is not end-to-end ISDN; further call progress information may be available in-band*, or #8, *In-band information or an appropriate pattern is now available* in a Call Proceeding, Progress or Alerting message, or in a Connect message if an Alerting message was not sent. The response to the Fast Connect message shall be done before or at the same time the Progress indicator is sent (i.e., up to and including the same message the Progress indicator is sent). The terminating side can provide in-band tones or announcements (such as ringback or busy) as soon as the progress descriptor has been sent and the media channel has been opened. Note that the Progress

indicator should be in an Alerting message only if the endpoint is being alerted. If another in-band tone, such as busy or re-order tone is provided, the Progress indicator should not be in an Alerting. When no appropriate call setup message is available, a Progress message can be used to carry the Progress indicator.

Note – When an endpoint or a Gatekeeper intervening in call signalling receives a Progress indicator information element in a Call Proceeding message, it will not be able to relay the Call Proceeding if the Call Proceeding message has already been sent to the originating side. In that case, the Progress indicator information element in the Call Proceeding message shall be mapped to a Progress indicator information element in a Progress message.

If the terminating side does not wish to provide far-end tones and announcements, it shall not send a Progress indicator information element with progress descriptor #1 or #8. To instruct the originating side that locally generated alerting shall be applied, the Alerting message shall be sent.

Upon receipt of an Alerting message, the originating side shall provide locally generated tones and announcement unless both the following conditions are true:

1) A media channel is available for "listening". The fastStart element could have been received in any message up to and including Alerting message.

2) A Progress indicator information element with progress descriptor #1, *Call is not end-to-end ISDN; further call progress information may be available in-band*, or #8, *In-band information or an appropriate pattern is now available*, was received in any message up to and including the Alerting message.

Upon receipt of a Release Complete message including a Cause information element, the originating side shall generate a tone or provide an indication appropriate to the received cause value. For example, if cause value #17, *User busy*, is received, the originating shall generate busy tone or provide an indication of user busy.

When locally generated tones and announcements are used, the Signal information element can optionally also be present to include more information about the type of signal to be provided.

[End Addition]

6.2.3 Correct H.245 Version for H.323 Version 1 Devices

DESCRIPTION:	An editorial error was discovered in the H.323 (1998) and H.323 (1999) publications. It specifies that for H.323 (1996) equipment, H.245 (1996) is required. The correct version of H.245 that should be specified in those Recommendations is H.245 (1997). The corrected text, taken from H.323 (1999), is shown below.

[Begin Correction]

Summary

...

Products claiming compliance with Version 1 of H.323 shall comply with all of the mandatory requirements of H.323 (1996) which references Recommendations H.225.0 (1996) and H.245 (1997). Version 1 products can be identified by H.225.0 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 1} and

H.245 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) 2}. Products claiming compliance with Version 2 of H.323 shall comply with all of the mandatory requirements of this Recommendation, H.323 (1998), which references Recommendations H.225.0 (1998) and H.245 (1998). Version 2 products can be identified by H.225.0 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 2} and H.245 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) 3}. Products claiming compliance with Version 3 of H.323 shall comply with all of the mandatory requirements of this Recommendation, H.323 (1999), which references Recommendation H.225.0 (1999) and H.245 (1999). Version 3 products can be identified by H.225.0 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 3} and H.245 messages containing a **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) 5}.

...

[End Correction]

6.2.4 Clarification of Call Identification Fields

DESCRIPTION:	H.225.0 Version 3 introduced new fields for caller identification without procedural text describing the usage of those fields. To prevent interoperability issues, that procedural text is presented here and will be introduced into the next revision of H.323.

[Begin Addition]

7.8 Caller identification services

7.8.1 Description of services

This section describes the caller identification services, which includes:

- Calling party number presentation and restriction
- Connected party number presentation and restriction
- Called (Alerting) party number presentation and restriction
- Busy party number presentation and restriction

7.8.1.1 Calling party address presentation

Calling party address presentation is a feature which provides the alias address of the calling party to the called party. The calling party address may be provided by the calling endpoint or by the gatekeeper for Gatekeeper routed calls that originate in the packet network. When the call is routed through the gatekeeper with which the calling endpoint is registered, the Gatekeeper may provide a screening service that assures the address provided is actually that of the calling party. The Gatekeeper may also provide the calling party address when no address is provided by the calling party or when the calling party provides an address other than an address with which the calling party registered.

When a call originates in the switched circuit network and enters the packet network through a Gateway, the Gateway shall pass to the packet network the calling party number information provided from the switched circuit network.

7.8.1.2 Calling party address restriction

Calling party address restriction is a feature which allows the calling endpoint or the calling endpoint's Gatekeeper to restrict presentation of the calling party alias address to the called party. This feature may reside in the endpoint or in the Gatekeeper for Gatekeeper routed calls.

In some cases where calling party address restriction has been indicated, there may exist certain situations where the restriction is overridden (for example, if the called party provides some emergency service).

7.8.1.3 Connected party address presentation

Connected party address presentation is a feature which provides the alias address of the connected or answering party to the calling party. The connected party address may be provided by the connected endpoint or by the Gatekeeper for Gatekeeper routed calls. When the call is routed through the Gatekeeper with which the connected endpoint is registered, the Gatekeeper may provide a screening service that assures the address provided is actually that of the connected party. The Gatekeeper may also provide the connected party address when no address is provided by the connected party or when the connected party provides an address other than an address with which the connected party registered.

A Gateway shall pass connected party information received from the switched circuit network to the packet network.

7.8.1.4 Connected party address restriction

Connected party address restriction is a feature which allows the connected endpoint or the connected endpoint's Gatekeeper to restrict presentation of the connected party alias address to the calling party. This feature may reside in the endpoint or in the Gatekeeper for Gatekeeper routed calls.

In some cases where connected party address restriction has been indicated, there may exist certain situations where the restriction is overridden (for example, if the calling party provides some emergency service).

7.8.1.5 Called (alerting) party address presentation

Alerting party address presentation is a feature which provides the alias address of the alerting party to the calling party. The alerting party address may be provided by the alerting endpoint or by the Gatekeeper for Gatekeeper routed calls. When the call is routed through the gatekeeper with which the alerting endpoint is registered, the Gatekeeper may provide a screening service that assures the address provided is actually that of the alerting party. The Gatekeeper may also provide the alerting party address when no address is provided by the alerting party or when the alerting party provides an address other than an address with which the alerting party registered.

7.8.1.6 Called (alerting) party address restriction

Alerting party address restriction is a feature which allows the alerting endpoint or the alerting endpoint's Gatekeeper to restrict presentation of the alerting party alias address to the calling party. This feature may reside in the endpoint or in the Gatekeeper for Gatekeeper routed calls.

7.8.1.7 Busy party address presentation

Busy party address presentation is a feature which provides the alias address of the busy party to the calling party. The busy party address may be provided by the busy endpoint or by the Gatekeeper for Gatekeeper routed calls. When the call is routed through the

gatekeeper with which the busy endpoint is registered, the Gatekeeper may provide a screening service that assures the address provided is actually that of the busy party. The Gatekeeper may also provide the busy party address when no address is provided by the busy party or when the busy party provides an address other than an address with which the busy party registered.

7.8.1.8 Busy party address restriction

Busy party address restriction is a feature which allows the busy endpoint or the busy endpoint's Gatekeeper to restrict presentation of the busy party alias address to the calling party. This feature may reside in the endpoint or in the Gatekeeper for Gatekeeper routed calls.

7.8.2 Messages and information elements

This section describes the various messages and information elements that allow H.323 devices to provide address presentation and restriction services.

7.8.2.1 Calling party address information

Calling party address information appears in the Setup message.

When address information represents a telephone number, the relevant information may appear in the Calling Party Number IE. This IE contains the caller's number, information about the number, and presentation and screening indicators found in octet 3a. This is the recommended mode of operation for the case where a PSTN Gateway sends a Setup message on the packet network.

Alternatively, calling party information may appear in the sourceAddress, presentationIndicator, and screeningIndicator fields of the Setup message. This mode of operation is required when the sourceAddress is not in any form of telephone number (i.e., sourceAddress is not type a dialedDigits or partyNumber).

The presentationIndicator field in the Setup message carries information identical to the presentation indicator found in the Calling Party Number IE. The meaning and use of the presentation indicator is defined in Q.951.

The screeningIndicator field in the Setup message carries information identical to the screening indicator found in the Calling Party Number IE. The meaning and use of the screening indicator is defined in Q.951.

7.8.2.2 Connected party address information

Connected party address information appears in the Connect message.

When address information represents a telephone number, the relevant information may appear in the Connected Number IE, including the presentation indicator and screening indicator. This is the recommended mode of operation for the case where a PSTN Gateway sends a Connect message on the packet network.

Alternatively, connected party information may appear in the connectedAddress, presentationIndicator, and screeningIndicator fields of the Connect message. This mode of operation is required when connectedAddress is not in any form of telephone number (i.e., connectedAddress is not type dialedDigits or partyNumber).

The presentationIndicator field in the Connect message carries information identical to the presentation indicator found in the Connected Number IE. The meaning and use of the presentation indicator is defined in Q.951.

The screeningIndicator field in the Connect message carries information identical to the screening indicator found in the Connected Number IE. The meaning and use of the screening indicator is defined in Q.951.

7.8.2.3 Called (alerting) party address information

Alerting party address information appears in the Alerting message.

Alerting party information may appear in the alertingAddress, presentationIndicator, and screeningIndicator fields of the Alerting message.

The presentationIndicator field in the Alerting message carries information identical to the presentation indicator found in the Connected Number IE. The meaning and use of the presentation indicator is defined in Q.951.

The screeningIndicator field in the Alerting message carries information identical to the screening indicator found in the Connected Number IE. The meaning and use of the screening indicator is defined in Q.951.

7.8.2.4 Busy party address information

Busy party address information appears in the Release Complete message.

Busy party information may appear in the alertingAddress, presentationIndicator, and screeningIndicator fields of the Release Complete message.

The presentationIndicator field in the Release Complete message carries information identical to the presentation indicator found in the Connected Number IE. The meaning and use of the presentation indicator is defined in Q.951.

The screeningIndicator field in the Release Complete message carries information identical to the screening indicator found in the Connected Number IE. The meaning and use of the screening indicator is defined in Q.951.

7.8.3 Actions at the originating endpoint

This section describes the procedural aspects required to provide caller identification services at the originating endpoint.

7.8.3.1 Gateway as originating endpoint

In the case of a Setup message received by a Gateway from the ISDN, the caller's number and presentation information reside in the Calling Party Number IE. The Gateway shall send a Setup message on the packet network with the Calling Party Number IE containing the same information as was found in the Setup message from the SCN.

A Gateway in receipt of a Connect message shall copy the Connected Number IE from the Connect message from the packet network to the Connect message to be sent to the ISDN. If the Connected Number IE is not present in the Connect message, the Gateway shall convert connectedAddress, presentationIndicator, and screeningIndicator into a Connected Number IE, if that connectedAddress represents some form of telephone number. If connectedAddress does not represent some form of telephone number or if the Connected Number IE is not present in the Connect message, the Gateway shall omit the Connected Number IE from the Connect message sent to the ISDN.

A Gateway in receipt of an Alerting message with alerting party information or a Release Complete message with busy party information shall convert the party information to the signaling format of the Gateway's circuit side if the signaling format supports this party information.

7.8.3.2 Terminal or MCU as originating endpoint

For calls originated on the packet network, the originating terminal or MCU may send a Setup message with either the Calling Party Number IE with presentation and screening indicators or with sourceAddress, presentationIndicator, and screeningIndicator fields. In either case, the screening indicator shall indicate "user provided not screened". As an example, if the caller wants to block identification to the called party, the presentation indicator would be set to "presentation restricted", but the caller's number would still appear in the Calling Party Number IE. In Gatekeeper routed cases, the calling party's Gatekeeper may add this information if it is missing or incorrect and the called party's Gatekeeper may remove the caller's identification information if appropriate. The calling party's Gatekeeper or the called party's Gatekeeper may also add or remove address information based on local policy.

A terminal or MCU in receipt of a Connect, Alerting, or Release Complete message should honor the presentation indicator when presenting address information to the user.

7.8.4 Actions at the terminating endpoint

This section describes the procedural aspects required to provide caller identification services at the terminating endpoint.

7.8.4.1 Gateway as terminating endpoint

A PSTN Gateway in receipt of a Setup message from the packet network shall copy the information found in the Calling Party Number IE from the Setup message to the signaling format supported in the PSTN. For example, this information would be copied to the Calling Party Number IE of the Q.931 Setup message for ISDN. If the Calling Party Number IE is not present in the Setup message, the Gateway shall form the Calling Party Number IE using the sourceAddress (assuming it is one of the telephone number alias types), presentationIndicator, and screeningIndicator from the Setup message.

The Gateway shall send a Connect message on the packet network with the Connected Number IE containing the same information as was found in the signaling format supported in the telephone network. In the case of a Q.931 Connect message received by a Gateway from the ISDN, connected party information resides in the Connected Number IE.

7.8.4.2 Terminal or MCU as terminating endpoint

A terminal or MCU in receipt of the Setup message should honor the presentation indicator when presenting caller information to the user.

For calls answered on the packet network, the answering terminal or MCU may include in the Connect message either the Connected Number IE or connectedAddress, presentationIndicator, and screeningIndicator fields. In either case, the terminal or MCU shall set the screeningIndicator to indicate "user provided not screened". In Gatekeeper routed cases, the answering party's Gatekeeper may add this information if it is missing or incorrect and the calling party's Gatekeeper may remove the answering party's address information if appropriate.

A terminal or MCU may provide address information in the Alerting message, using the alertingAddress, presentationIndicator, and screeningIndicator found in the Alerting message. If the address is provided, the terminal or MCU shall set the screeningIndicator to indicate "user provided not screened". In Gatekeeper routed cases, the answering party's Gatekeeper may add this information if it is missing or incorrect and the calling party's Gatekeeper may remove the answering party's address information if appropriate. The

answering party's Gatekeeper or the calling party's Gatekeeper may also add or remove address information based on local policy.

A busy terminal or MCU may provide address information in the Release Complete message, using the busyAddress, presentationIndicator, and screeningIndicator found in the Release Complete message. If the address is provided, the terminal or MCU shall set the screeningIndicator to indicate "user provided not screened". In Gatekeeper routed cases, the answering party's Gatekeeper may add this information if it is missing or incorrect and the calling party's Gatekeeper may remove the answering party's address information if appropriate.

7.8.5 Actions at a gatekeeper

In Gatekeeper routed scenarios, the Gatekeeper may provide identification information or may provide a screening service. Services that may be provided by a Gatekeeper depend on the type of endpoint served. This section describes the procedural aspects required to provide caller identification services when the Gatekeeper routes the call signalling.

7.8.5.1 Gateway as originating endpoint

In Gatekeeper routed cases, a Gatekeeper should not modify the information found in the Setup message sent from a Gateway. This assumes that the telephone network has provided correct information.

7.8.5.2 Terminal or MCU as originating endpoint

In Gatekeeper routed cases, a Gatekeeper may provide calling party information when the calling party is not a Gateway. The Gatekeeper may provide a calling party address if the calling party did not provide one or if the Gatekeeper determines the address is not correct. If the Gatekeeper provides an address other than that sent in the Setup message, the Gatekeeper shall set the screening indicator to indicate "network provided". If the Gatekeeper verifies the address information sent in the Setup message, but does not modify the address information, the Gatekeeper shall set the screening indicator to indicate "user provided, verified, and passed". If the Gatekeeper determines that the address information sent in the Setup message is incorrect, but does not modify the address information, the Gatekeeper shall set the screening indicator to indicate "user provided, verified, and failed". The Gatekeeper may set the presentation indicator to provide service to the endpoint. The Gatekeeper may allow the endpoint to override the endpoint's service by specifying a different presentation (for example, restricting presentation for the current call when the endpoint's service is to allow presentation).

7.8.5.3 Gateway as terminating endpoint

In Gatekeeper routed cases, a Gatekeeper should not modify the information found in the Connect message sent from a Gateway. This assumes that the telephone network has provided correct information.

7.8.5.4 Terminal or MCU as terminating endpoint

In Gatekeeper routed cases, a Gatekeeper may provide connected, alerting, or busy party information when the connected, alerting, or busy party is not from a Gateway. The Gatekeeper may provide a connected party (or alerting party, or busy party) address if none was provided by the connected party (or alerting party, or busy party), or if the Gatekeeper determines the address is not correct. If the Gatekeeper provides an address other than that sent in the Connect, Alerting, or Release Complete message, the Gatekeeper shall set the screening indicator to indicate "network provided". If the Gatekeeper verifies the address

information sent in the Connect, Alerting, or Release Complete message, but does not modify the address information, the Gatekeeper shall set the screening indicator to indicate "user provided, verified, and passed". If the Gatekeeper determines that the address information sent in the Connect, Alerting, or Release Complete message is incorrect, but does not modify the address information, the Gatekeeper shall set the screening indicator to indicate "user provided, verified, and failed". The Gatekeeper may set the presentation indicator to provide service to the endpoint. The Gatekeeper may allow the endpoint to override the endpoint's service by specifying a different presentation (for example, restricting presentation for the current call when the endpoint's service is to allow presentation).

[End Addition]

6.2.5 Clarification of the Fast Connect Procedure

DESCRIPTION:	It was noted that some text within the Fast Connect procedure was ambiguous. This section attempts to clarify some issues within section 8.1.7.1 of H.323 (1999).

[Begin Correction]

8.1.7.1 Proposal, selection and opening of media channels

...

In an **openLogicalChannel** which proposes a channel for transmission from the calling endpoint to the called endpoint, the **forwardLogicalChannelParameters** element shall contain parameters specifying the characteristics of the proposed channel, and the **reverseLogicalChannelParameters** element shall be omitted. Each such **OpenLogicalChannel** structure shall have a unique **forwardLogicalChannelNumber** value. Alternative proposals for the same transmit channel shall contain the same **sessionID** value in **H2250LogicalChannelParameters**. The **mediaChannel** element shall be omitted in the proposal; it will be provided by the called endpoint should the proposal be accepted. The other **H2250LogicalChannelParameters** and **dataType** shall be set to correctly describe the transmit capabilities of the calling endpoint associated with this proposed channel. The calling endpoint may choose not to propose any channels for transmission from the calling endpoint to the called endpoint, such as if it desires to use H.245 procedures later to establish such channels.

In the Setup message, each **openLogicalChannel** that proposes a channel for transmission from the calling endpoint to the called endpoint shall contain the **mediaControlChannel** element (indicating the reverse RTCP channel) in the **H2250LogicalChannelParameters** element of the **forwardLogicalChannelParameters** structure.

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 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 not to 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.

...

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. 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 insert valid **mediaChannel** and **mediaControlChannel** fields (indicating the RTCP channel going in the same direction) into the **h2250LogicalChannelParameters** element of the **forwardLogicalChannelParameters** structure. All **mediaControlChannel** elements inserted by the called endpoint for the same **sessionID** for both directions shall have the same value. 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 Addition]

6.2.6 Call Linkage

DESCRIPTION:	It has become apparent that for certain applications, such as Automatic Call Distribution and Billing, there is a need to "link" calls together when certain supplementary services are performed. Some implementers have attempted to use the Call Identifier for this purpose, but it is not well suited for the task. The section is introduced to overcome this shortcoming and to provide implementers with the necessary tools.

[Begin Correction]

10.3 Call Linkage in H.323

10.3.1 Description

Call Linkage in H.323 is an optional feature. A term "shall" within this section 10.3 shall be interpreted as a mandatory requirement provided the Call Linkage feature is supported.

10.3.1.1 General description

The Thread Identification feature allows different calls or call independent signalling connections – those that logically belong together from a service's or application's point of view in terms of their progression – to be linked together.

The Global Call Identification feature allows a call or a call independent signalling connection to be identified by one unique identifier that is applicable to the call or call independent signalling connection end-to-end without regards to its route or its history.

NOTE – The Call Identifier is defined in section 7.5 as a globally unique identifier for a call. A new basic call from the same endpoint/entity or a new call as part of a service scenario would use a new Call Identifier value.

10.3.1.2 Service definitions

10.3.1.2.1 Thread identification, thread ID, TID

A value assigned to calls that are logically linked together for the purpose of correlating them. If two or more calls are logically linked together (e.g. due to service interactions), the current Thread ID of one of these calls is assigned to all of the other linked calls.

10.3.1.2.2 Global call identification, global call ID, GID

A value assigned to an end-to-end call to uniquely identify that call from end-to-end. If different calls are being transformed into a new call (i.e. due to service interactions), the GIDs of the old calls are updated (if already assigned previously) or assigned by a new GID value for the new end-to-end call.

NOTE – A call that is being transformed out of different call legs due to certain services may end up having call legs with different Call Identifiers. The Call Identifier is therefore not suitable to uniquely identify a call end-to-end.

10.3.2 Invocation and operation

A Call ID shall be assigned to each new call that is set up (see Section 7.5). Due to service interactions, different Call IDs may be assigned to different parts (call legs) of a call.

A Global Call ID may be assigned either at call establishment time, while in the active state or while call establishment/call clearing is in progress when two or more calls are being transformed into a new call due to certain services being invoked or due to an application request.

A Global Call ID may be changed during the lifetime of the call due to the call being transformed.

A Thread ID may be assigned either at call establishment time, while in the active state or while call establishment/call clearing is in progress when two or more calls are logically linked together due to certain services being invoked or due to an application request.

The Thread ID may be changed during the lifetime of a call (e.g. due to service interactions).

10.3.3 Interaction with H.450 supplementary services

Interactions with H.450 supplementary services for which standards were available at the time of publication of this Recommendation are specified below.

For the Call ID, no interactions with other supplementary services apply, as it shall be unique for each new call. All interactions described in this section apply only to the Global Call ID and/or the Thread ID.

A Global Call ID and a Thread ID may be assigned, regardless of a supplementary service invocation, as part of the basic call establishment. Specific feature interactions are described below for specific supplementary service invocations.

10.3.3.1 Call transfer

This section describes the usage of the Call Linkage fields when using H.450.2.

10.3.3.1.1 Transfer without consultation

The Thread ID of the transferred call shall be inherited from the Thread ID of the primary call. The Thread ID of the primary call shall therefore be provided by the transferring endpoint to the transferred endpoint along with the call transfer request. If the primary call does not have an assigned Thread ID, the transferring endpoint shall generate one. If the transferred entity does not receive a Thread ID along with the call transfer request, it shall inherit the Thread ID that was assigned to the primary call at call establishment time. If no Thread ID is available to inherit from at all, the transferred endpoint shall generate a Thread ID and assign it to both the transferred call (in call establishment message) and the primary call (in call clearing message).

A new Global Call ID shall be assigned to a transferred call. If a Gatekeeper establishes the transferred call on behalf of a transferred endpoint, the Gatekeeper shall assign the same Global Call ID to the remaining call leg of the primary call. This ensures that the resulting call after successful transfer has one unique GID end-to-end.

10.3.3.1.1 Transfer with consultation

At the time of transfer, the transferred call shall be assigned the same Thread ID as the former primary call if:

a) the primary call is an incoming call and the secondary call is an outgoing call, or

b) both calls are incoming calls and the primary call has been established before the secondary call, or

c) both calls are outgoing calls and the primary call has been established before the secondary call.

At the time of transfer, the transferred call shall be assigned the same Thread ID as the former secondary call if:

a) the secondary call is an incoming call and the primary call is an outgoing call, or

b) both calls are incoming calls and the secondary call has been established before the primary call, or

c) both calls are outgoing calls and the secondary call has been established before the primary call.

The Thread ID appropriate for the transferred call (either based on primary or secondary call depending on the situation) shall be provided by the transferring endpoint to the transferred endpoint along with the call transfer request. If the call from which the Thread ID shall be inherited (either primary or secondary call) does not have assigned a Thread ID, the transferring endpoint shall generate one. If the transferred endpoint does not receive a Thread ID along with the call transfer request (e.g. transferring endpoint does not support call linkage), it shall generate a Thread ID that shall be inherited from the primary call if possible.

At the time of transfer, the transferred entity shall assign a new GID value to the transferred call. If a Gatekeeper established the transferred call on behalf of a transferred endpoint, the

Gatekeeper shall assign the same GID to the remaining call leg of the primary call. A Gatekeeper acting on behalf of the transferred-to endpoint shall assign the same GID to the remaining part of the secondary call. This ensures that the resulting call after successful transfer has one unique GID end-to-end.

A transferring entity may, as an option, choose to "join" the primary call and the secondary call together. The call linkage rules for the resulting call ("joined" call) shall be the same as specified for a transferred call above.

10.3.3.2 Call diversion

This section describes the usage of the Call Linkage fields when using H.450.3.

The originating call, the forwarding and the forwarded call shall use the same Thread ID.

The Thread ID of the forwarded call and the originating call shall be inherited from the Thread ID of the forwarding call. The served endpoint shall therefore assign a Thread ID to the forwarding call (if not already assigned as part of the basic call) and shall provide this Thread ID to the re-routing entity along with the call forwarding request. The re-routing entity shall use this Thread ID as the Thread ID for the establishment of the forwarded call. In addition, the originating call leg (if any) shall be assigned/updated with this Thread ID as well.

If the re-routing entity does not receive a Thread ID along with the call forwarding request, it shall inherit the Thread ID that was assigned to the forwarding call at call establishment time. If no Thread ID is available to inherit from at all, the re-routing endpoint shall generate a Thread ID and assign it to the forwarding call, the forwarded call, and to the originating call.

A new GID shall be assigned to the end-to-end call from the calling user (i.e., diverted user) to the diverted-to user by assigning a new GID in the forwarded call Setup and assigning (or updating) the same GID to the originating call leg (if any).

10.3.3.3 Call hold and consultation

This section describes the usage of the Call Linkage fields when using H.450.4.

A consultation call shall use the same Thread ID as the first call.

NOTE – Whether a call is considered being a consultation call rather than a further basic call is the decision of the endpoint.

A consultation call shall use a new Global Call ID.

10.3.3.4 Call park/call pickup

This section describes the usage of the Call Linkage fields when using H.450.5.

The parked call shall have the same Thread ID as the primary call; however, it shall use a different GID.

If available, the Thread ID shall be used for associating call independent signalling connections (indicating group notifications and pickup requests), the call from a calling/parked user to the picking-up user, and a previously alerting/parked call.

NOTE – Call Park/Pickup contains a specific call pickup id that is used by the picking-up user.

The call independent signalling connections used as part of Call Park / Call Pickup shall use new GIDs. The call from the calling user/parked user to the picking-up user shall have a new end-to-end global GID.

10.3.3.5 Call waiting

There is no interaction with Call Linkage and H.450.6.

10.3.3.6 Message waiting indication

There is no interaction with Call Linkage and H.450.7.

10.3.3.7 Name identification service

There is no interaction with Call Linkage and H.450.8.

[End Addition]

ASN.1 changes required to support Call Linkage appears in section 6.4.9.

6.2.7 Early Termination of Fast Connect

DESCRIPTION:	A race condition exists in the text of H.323 that states that opening a separate H.245 connection terminates the Fast Connect procedure. The problem is that, due to certain network conditions, an endpoint may receive an H.245 connection prior to receiving a Connect message. This should not result in an early termination of Fast Connect.

[Begin Correction]

8.2.1 Encapsulation of H.245 messages within Q.931 messages

...

The calling endpoint shall *not* include both a **fastStart** element and encapsulated H.245 messages in **h245Control** in the same **SETUP** message, since the presence of the encapsulated H.245 messages would override the Fast Connect procedure. A calling endpoint may, however, include both a **fastStart** element and set **h245Tunneling** to TRUE within the same **SETUP** message; likewise, a called endpoint may include **fastStart** and set **h245Tunneling** to TRUE within the same Q.931 response. In this case, the Fast Connect procedures are followed, and the H.245 connection remains "unestablished" until actual transmission of the first tunneled H.245 message or opening of the separate H.245 connection.

...

[End Addition]

6.2.8 Assignment of the maintainConnection Field

DESCRIPTION:	Implementers have noted that the text in H.323 is not clear on the subject of whether the maintainConnection field shall remain "constant" or may be changed during a call. This section attempts to clarify that issue.

[Begin Correction]

7.3 Call signalling channel

...

The Call Signalling Channel may be established prior to the actual need to signal a call, and the channel may remain connected between calls. An entity may indicate this capability by setting the **maintainConnection** flag to TRUE in messages that it sends on the Call Signalling Channel. In addition, an endpoint which has this capability should indicate this when it registers with a gatekeeper. This will allow a gatekeeper that utilizes gatekeeper routing to connect to the endpoint at any point after registration. If the connection drops while no call or signalling is active, neither end shall attempt to open the connection until signalling is needed.

The value of the **maintainConnection** flag sent by an entity over a given Call Signalling Channel shall be the same for every message containing this field for the duration of the Call Signalling Channel. This does not preclude an entity from setting this value to TRUE for one Call Signaling Channel and FALSE for another Call Signalling Channel.

[End Addition]

6.3 Technical and Editorial Corrections to ITU-T Recommendation H.225.0 (1998)

In addition to the corrections noted in the Implementers Guide approved in May 1999, this section contains corrections to errors that were discovered and corrected in H.225.0 (1998) after the previously approved Implementers Guide. In addition, there may be additional changes in section 6.4 applicable to H.225.0 (1998)—such changes will be explicitly stated in the "Description" areas.

6.3.1 ANNEX H – H.225.0 Message Syntax (ASN.1)

DESCRIPTION:	Security issues were identified relating to the ReleaseComplete message in H.225.0. Also, an error in the ARJ syntax has been discovered in the published version of H.225.0 (1998). These errors will be corrected in subsequent publications of the Recommendation.

[Begin Correction]

```
ReleaseComplete-UUIE ::= SEQUENCE
{
    protocolIdentifier      ProtocolIdentifier,
    reason                  ReleaseCompleteReason OPTIONAL,
    . . .,
    callIdentifier          CallIdentifier,
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL
}

AdmissionReject ::= SEQUENCE --(ARJ)
{
    requestSeqNum           RequestSeqNum,
    rejectReason            AdmissionRejectReason,
    nonStandardData         NonStandardParameter OPTIONAL,
    ...,
    altGKInfo               AltGKInfo OPTIONAL,
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    callSignalAddress       SEQUENCE OF TransportAddress OPTIONAL,
    integrityCheckValue     ICV OPTIONAL
}
```

[End Correction]

6.3.2 Octet 3a of CallingPartyNumber Information Element

DESCRIPTION:	It should be noted that as of H.225.0 (1999), the previously forbidden octet 3a of the CallingPartyNumber information element is now legal. Study Group 16 agreed that this should not be a problem, as the rules in Q.931 specify that if an information element is not understood, it should be discarded. Thus, this change should not prevent a connection from being established when a newer device transmits this previously forbidden octet. An H.323v1 or H.323v2 device shall not simply ignore octet 3a—it should either discard the CallingPartyNumber information element if it receives one containing octet 3a or it shall use it in accordance with H.225.0 (1999).

6.4 Technical and Editorial Corrections to ITU-T Recommendation H.225.0 (1999)

6.4.1 Usage of the XRS Message

DESCRIPTION:	A technical problem was discovered with the text in all versions of the H.225.0 document relating to the XRS message, including H.225.0 (1999). The following changes should be applied to H.225.0 (1998) and H.225.0 (1999). Likewise, the same semantics shall be applied to H.225.0 (1996).

[Begin Correction]

7.17 Message Not Understood

This message is sent whenever an H.323 endpoint receives a RAS message it can decode, but does not understand. If a RAS message cannot be decoded it should be ignored.

RequestSeqNum – Shall be the **requestSeqNum** of the unknown message.

...

[End Correction]

6.4.2 Packetization of the G.722.1 bit stream for use with the Real Time Protocol (RTP)

DESCRIPTION:	The following text has been added to describe the packetization of G.722.1 audio. The text will appear in a new section of Annex F of H.225.0.

[Begin Addition]

F.6 G.722.1

For information on the packetization of G.722.1 bit stream, refer to Annex A/G.722.1.

[End Addition]

6.4.3 Packetization of G.722.1

DESCRIPTION:	The following text has been added to describe the packetization of G.722.1 audio. The text will appear in Annex B of H.225.0.

[Begin Addition]

Table B.1/H.225.0 – Properties of audio encodings

Encoding	Sample/frame	Bits/sample	ms/frame
G722	Sample	8	
G722.1	Frame	N/A	20
G728	Frame	N/A	2.5
PCMA	Sample	8	
PCMU	Sample	8	
G723	Frame	N/A	30
G729	Frame	N/A	10
GSM	Frame	N/A	20

[End Addition]

[Begin Addition]

Table B.2/H.225.0 – Payload Types (PT) for standard audio and video encodings

PT	Encoding name	Audio/video (A/V)	Clock rate (Hz)	Channels (audio)
0	PCMU	A	8 000	1
8	PCMA	A	8 000	1
9	G722	A	8 000	1
Dynamic	G722.1	A	16 000	1
4	G723	A	8 000	1
15	G728	A	8 000	1
18	G729	A	8 000	1
31	H261	V	90 000	
34	H263	V	90 000	
3	GSM	A	8 000	1
96-127	Dynamic	?		
NOTE – Payload types 1-7, 10-14, 16-30, and 30-95 are reserved. See Appendix II for more information.				

[End Addition]

6.4.4 Correction to Values in Table 12/H.225.0

DESCRIPTION:	An error was pointed out in the length value for the cause IE in the Release Complete message. The following text shows the correct changes to Table 12/H.225.0.

[Begin Correction]

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
Cause	CM (Note)	2-32
Facility	O	8-*
Notification indicator	O	2-*
Display	O	2-82
Signal	O	2-3
User-to-User	M	2-131
NOTE – Either the Cause IE or the **ReleaseCompleteReason** shall be present.		

[End Correction]

6.4.5 Support for New Annexes in G.729

DESCRIPTION:	The following text shall be inserted into in Annex F/H.225.0 to support new annexes to G.729.

[Begin Correction]

F.3 G.729

...

A Voice Activity Detector (VAD) and Comfort Noise Generator (CNG) algorithm in Annex B/G.729 is recommended. This algorithm is applied to Annexes F/G.729 (6.4 Kbps with VAD/CNG) and G/G.729 (11.8 Kbps with VAD/CNG), and Annex B/G.729 (G.729 and Annex A/G.729 with VAD/CNG), Annex I/G.729. A G.729 or Annex A/G.729 frame contains 10 octets, Annex D/G.729 and Annex E/G.279 contain 8 and 15 octets, respectively, while the Annexes B/G.729, F/G.729, and G/G.729 comfort noise frame occupies 2 octets, as shown in Figure F.3:

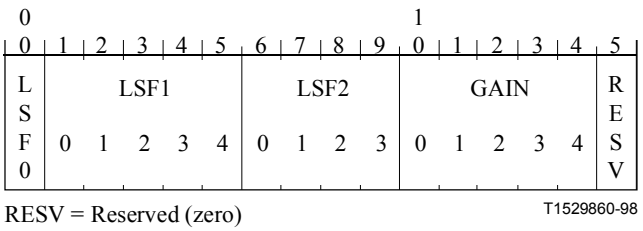


Figure F.3 – Annexes B/G.729, F/G.729, and G/G.729 CNG packetization format

...

[End Correction]

6.4.6 Clarification of Alternate Gatekeeper Procedures

DESCRIPTION:	Ambiguities have been identified in the procedures for "alternate gatekeepers". This section specifies changes to be applied to H.225.0 (1999) and H.225.0 (1998) to clarify the proper usage of this procedure. The change marks are against the 1999 revision.

[Begin Correction]

7.6 H.225.0 common message elements

...

A gatekeeper may send an endpoint a list of alternate gatekeepers in various messages. When communicating with its gatekeeper, an endpoint that implements the alternate gatekeeper mechanism shall replace any previously received list of alternate gatekeepers with the most recently received list of alternate gatekeepers. It is possible for an alternate gatekeeper to send a list of alternate gatekeepers. If an endpoint sends a request to an alternate gatekeeper that will potentially become its permanent gatekeeper, it shall accept the new list of alternate gatekeepers. Otherwise, if the alternate gatekeeper will not potentially become its permanent gatekeeper, any list of alternate gatekeepers received shall be ignored. A gatekeeper may potentially become an endpoint's permanent gatekeeper if either the current gatekeeper becomes unresponsive or if the "altGKisPermanent" flag is set to TRUE in the "AltGKInfo" structure.

When an endpoint is redirected to a new permanent alternate Gatekeeper, either as a result of the current gatekeeper becoming unresponsive or by receiving an explicit redirection message (xRJ), the endpoint shall not send a URQ to its current Gatekeeper. Additionally, all subsequent requests, including those for existing calls, shall be directed to the new permanent gatekeeper.

If the endpoint's gatekeeper becomes unresponsive and either no alternate gatekeeper list was provided or all alternate gatekeepers are also unresponsive, the endpoint shall attempt to discover a new gatekeeper and register with it according to the procedures defined in H.323. Note that procedures for handling existing calls in this scenario are for further study.

...

[End Correction]

The following correction shall be applied to sections 7.8.3, 7.9.3, 7.10.3, 7.11.3, 7.12.3, 7.13.3, 7.14.3, and 7.15.4.

[Begin Correction]

altGKInfo – Optional information about alternative gatekeepers. If this information is supplied, an endpoint should retransmit the request to one of the alternate gatekeepers listed. If an alternate gatekeeper rejects the request without supplying alternate gatekeeper information, the endpoint shall accept the rejection. If an alternate gatekeeper does not respond or returns a rejection with alternate gatekeeper information, the endpoint may send

the request to another alternate. (Refer to section 7.6 for the specific procedures on handling multiple lists of alternate gatekeepers.)

[End Correction]

In addition to the changes specified above, the following sections shall also contain these additional amendments.

[Begin Correction]

7.8.3 GatekeeperReject (GRJ)

...

altGKInfo – Optional information about alternative gatekeepers. If this information is supplied, an endpoint should retransmit the request to one of the alternate gatekeepers listed. If an alternate gatekeeper rejects the request, the endpoint shall accept the rejection. If an alternate gatekeeper does not respond, the endpoint may send the request to another alternate in the list. For this message, endpoints shall ignore the actual **altGKisPermanent** flag and the **needToRegister** flags in the **AlternateGK** sequence and assume the values are TRUE.

...

[End Correction]

[Begin Correction]

7.9.3 RegistrationReject (RRJ)

...

altGKInfo – Optional information about alternative gatekeepers. If this information is supplied, an endpoint should retransmit the request to one of the alternate gatekeepers listed. If an alternate gatekeeper rejects the request, the endpoint shall accept the rejection. If an alternate gatekeeper does not respond, the endpoint may send the request to another alternate in the list. If an endpoint has not yet successfully registered with a gatekeeper, the endpoint shall ignore the actual **needToRegister** flags in the **AlternateGK** sequence and assume the values are TRUE.

...

[End Correction]

A comment has been added to the **AltGKInfo** sequence to explain the usage of the **altGKisPermanent** field. Refer to the ASN.1 revisions in section 6.4.9 for this text.

6.4.7 Usage of Keypad Facility IE

DESCRIPTION:	SET devices (Annex F/H.323) shall support transmission of DTMF as Keypad Information Elements in the H.225.0 call signaling connection (e.g. using Information messages). However, there is no established method for carrying a hookflash indication in this information element.

	H.225.0 shall be modified as described below to allow the hookflash indication to be transmitted.

[Begin Correction]

7.2.2.16 Keypad facility

Encoded following Figure 4-24/Q.931. The use of the exclamation point character "!" shall represent a hookflash indication. Endpoints not supporting reception of the hookflash indication shall ignore the "!" if received.

[End Correction]

6.4.8 Order of Information Elements in H.225.0 Call Signalling Messages

DESCRIPTION:	Ambiguities have been identified with respect to the ordering of Information Elements in H.225.0 Call Signaling Messages. Table 8/H.225.0 of H.323 (1999) suggests an ordering of information elements that is inconsistent with Q.931. That was not intended as the ordering of information elements is specified in Q.931. The table and text below will appear in the next revision of H.225.0.

[Begin Correction]

Table 8/H.225.0 – Connect

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)	5-6
Extended facility	O	8-*
Channel identification	FFS	NA
Facility	O	8-*
Progress indicator	O	2-4
Notification indicator	O	2-*
Display	O	2-82
Date/Time	O	8
Connected Number	O	2-*
Connected Sub-Address	O	2-23
Low layer compatibility	FFS	NA
High layer compatibility	FFS	NA
User-to-User	M	2-131

NOTE – Bearer capability is mandatory if the message is between a terminal and a gateway.		

[End Correction]

[Begin Correction]

7.1 Use of Q.931 messages

...

Each H.225.0 endpoint shall be able to interpret and generate the information elements mandated in the following for the respective Q.931 and H.450 messages. It may interpret and generate the optional information elements as defined below as well. It also may interpret other information elements of Q.931, or other Q series or H.450 protocols. The endpoints shall be able to ignore unknown information elements contained in a Q.931 or H.450 message without disturbing operation. Procedures for receiving unrecognized "comprehension required" information elements shall apply according to 5.8.7.1/Q.931.

Information Elements shall be encoded according to Q.931, except where modified in this Recommendation. However, Q.931 shall always dictate the proper ordering of Information Elements within a message, regardless of the order of elements listed within this Recommendation.

...

[End Correction]

6.4.9 Changes to the H.225.0 (1999) ASN.1

DESCRIPTION:	This section details the changes to the published ASN.1 for H.225.0 (1999).

[Begin Correction]

```
H323-UU-PDU ::= SEQUENCE
{
        h323-message-body   CHOICE
        {
                setup               Setup-UUIE,
                callProceeding      CallProceeding-UUIE,
                connect             Connect-UUIE,
                alerting            Alerting-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,
        callLinkage                    CallLinkage OPTIONAL
}

Alerting-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,
        multipleCalls                  BOOLEAN,
        maintainConnection             BOOLEAN,
        alertingAddress                SEQUENCE OF AliasAddress OPTIONAL,
        presentationIndicator          PresentationIndicator,
        screeningIndicator             ScreeningIndicator,
        fastConnectRefused             NULL OPTIONAL
}

CallProceeding-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,
        multipleCalls                  BOOLEAN,
        maintainConnection             BOOLEAN,
        fastConnectRefused             NULL OPTIONAL
}

Connect-UUIE ::= SEQUENCE
{
        protocolIdentifier             ProtocolIdentifier,
        h245Address                    TransportAddress OPTIONAL,
        destinationInfo                EndpointType,
        conferenceID                   ConferenceIdentifier,
        ...,
        callIdentifier                 CallIdentifier,
        h245SecurityMode               H245Security OPTIONAL,
```

```
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        fastStart               SEQUENCE OF OCTET STRING OPTIONAL,
        multipleCalls           BOOLEAN,
        maintainConnection      BOOLEAN,
        language                SEQUENCE OF IA5String(SIZE (1..32)) OPTIONAL,
                                                    -- RFC1766 language tag
        connectedAddress        SEQUENCE OF AliasAddress OPTIONAL,
        presentationIndicator   PresentationIndicator,
        screeningIndicator      ScreeningIndicator,
        fastConnectRefused      NULL OPTIONAL
}

Information-UUIE ::=SEQUENCE
{
        protocolIdentifier  ProtocolIdentifier,
        ...,
        callIdentifier          CallIdentifier,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        fastStart               SEQUENCE OF OCTET STRING OPTIONAL,
        fastConnectRefused      NULL OPTIONAL
}

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,
        multipleCalls           BOOLEAN,
        maintainConnection      BOOLEAN,
        fastConnectRefused      NULL OPTIONAL
}

CallLinkage ::= SEQUENCE
{
        globalCallId            GloballyUniqueID  OPTIONAL,
        threadId                GloballyUniqueID  OPTIONAL,
        ...
}

AltGKInfo ::=SEQUENCE
{
        alternateGatekeeper     SEQUENCE OF AlternateGK,
        altGKisPermanent        BOOLEAN,
                -- It is illegal to set this flag to FALSE and to set the
                -- "needToRegister" flag inside an AlternateGK structure to TRUE.
        ...
```

```
}

AdmissionRequest ::= SEQUENCE --(ARQ)
{
        requestSeqNum           RequestSeqNum,
        callType                CallType,
        callModel               CallModel OPTIONAL,
        endpointIdentifier      EndpointIdentifier,
        destinationInfo         SEQUENCE OF AliasAddress OPTIONAL,   -- Note 1
        destCallSignalAddress   TransportAddress OPTIONAL,           -- Note 1
        destExtraCallInfo       SEQUENCE OF AliasAddress OPTIONAL,
        srcInfo                 SEQUENCE OF AliasAddress,
        srcCallSignalAddress    TransportAddress OPTIONAL,
        bandWidth               BandWidth,
        callReferenceValue      CallReferenceValue,
        nonStandardData         NonStandardParameter OPTIONAL,
        callServices            QseriesOptions  OPTIONAL,
        conferenceID            ConferenceIdentifier,
        activeMC                BOOLEAN,
        answerCall              BOOLEAN,  -- answering a call
        ...,
        canMapAlias             BOOLEAN,  -- can handle alias address
        callIdentifier          CallIdentifier,
        srcAlternatives         SEQUENCE OF Endpoint OPTIONAL,
        destAlternatives        SEQUENCE OF Endpoint OPTIONAL,
        gatekeeperIdentifier    GatekeeperIdentifier OPTIONAL,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        integrityCheckValue     ICV OPTIONAL,
        transportQOS            TransportQOS OPTIONAL,
        willSupplyUUIEs         BOOLEAN,
        callLinkage             CallLinkage OPTIONAL
}

AdmissionReject ::= SEQUENCE --(ARJ)
{
        requestSeqNum           RequestSeqNum,
        rejectReason            AdmissionRejectReason,
        nonStandardData         NonStandardParameter OPTIONAL,
        ...,
        altGKInfo               AltGKInfo OPTIONAL,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        callSignalAddress       SEQUENCE OF TransportAddress OPTIONAL,
        integrityCheckValue     ICV OPTIONAL
}

BandwidthRequest ::= SEQUENCE --(BRQ)
{
        requestSeqNum           RequestSeqNum,
        endpointIdentifier      EndpointIdentifier,
        conferenceID            ConferenceIdentifier,
        callReferenceValue      CallReferenceValue,
        callType                CallType OPTIONAL,
        bandWidth               BandWidth,
        nonStandardData         NonStandardParameter OPTIONAL,
        ...,
        callIdentifier          CallIdentifier,
        gatekeeperIdentifier    GatekeeperIdentifier OPTIONAL,
```

```
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        integrityCheckValue     ICV OPTIONAL,
        answeredCall            BOOLEAN,
        callLinkage             CallLinkage OPTIONAL
}

DisengageRequest ::= SEQUENCE --(DRQ)
{
        requestSeqNum           RequestSeqNum,
        endpointIdentifier      EndpointIdentifier,
        conferenceID            ConferenceIdentifier,
        callReferenceValue      CallReferenceValue,
        disengageReason         DisengageReason,
        nonStandardData         NonStandardParameter OPTIONAL,
        ...,
        callIdentifier          CallIdentifier,
        gatekeeperIdentifier    GatekeeperIdentifier OPTIONAL,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        integrityCheckValue     ICV OPTIONAL,
        answeredCall            BOOLEAN,
        callLinkage             CallLinkage OPTIONAL
}

InfoRequest ::= SEQUENCE --(IRQ)
{
        requestSeqNum           RequestSeqNum,
        callReferenceValue      CallReferenceValue,
        nonStandardData         NonStandardParameter OPTIONAL,
        replyAddress            TransportAddress OPTIONAL,
        ...,
        callIdentifier          CallIdentifier,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        integrityCheckValue     ICV OPTIONAL,
        uuiesRequested          UUIEsRequested OPTIONAL,
        callLinkage             CallLinkage OPTIONAL
}

InfoRequestResponse ::= SEQUENCE --(IRR)
{
        nonStandardData         NonStandardParameter OPTIONAL,
        requestSeqNum           RequestSeqNum,
        endpointType            EndpointType,
        endpointIdentifier      EndpointIdentifier,
        rasAddress              TransportAddress,
        callSignalAddress       SEQUENCE OF TransportAddress,
        endpointAlias           SEQUENCE OF AliasAddress OPTIONAL,
        perCallInfo             SEQUENCE OF SEQUENCE
        {
                nonStandardData         NonStandardParameter OPTIONAL,
                callReferenceValue      CallReferenceValue,
                conferenceID            ConferenceIdentifier,
                originator              BOOLEAN OPTIONAL,
                audio                   SEQUENCE OF RTPSession OPTIONAL,
                video                   SEQUENCE OF RTPSession OPTIONAL,
                data                    SEQUENCE OF TransportChannelInfo OPTIONAL,
                h245                    TransportChannelInfo,
```

```
            callSignaling           TransportChannelInfo,
            callType                CallType,
            bandWidth               BandWidth,
            callModel               CallModel,
            ...,
            callIdentifier          CallIdentifier,
            tokens                  SEQUENCE OF ClearToken OPTIONAL,
            cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
            substituteConfIDs       SEQUENCE OF ConferenceIdentifier,
            pdu                     SEQUENCE OF SEQUENCE
            {
                h323pdu     H323-UU-PDU,
                sent        BOOLEAN         -- TRUE is sent, FALSE is received
            } OPTIONAL,
            callLinkage             CallLinkage
        } OPTIONAL,
        ...,
        tokens                  SEQUENCE OF ClearToken OPTIONAL,
        cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
        integrityCheckValue     ICV OPTIONAL,
        needResponse            BOOLEAN
}
```

[End Correction]

6.4.10 Call Linkage

DESCRIPTION:	A description for the new CallLinkage fields found ARQ, BRQ, DRQ, IRQ, and IRR messages is defined below. This definition will appear in H.323v4.

[Begin Correction]

CallLinkage – The contents of this field is typically controlled by a call linkage service. For the procedures and semantics of this field refer to H.323 section 10.3 "Call Linkage in H.323".

[End Correction]

6.4.11 Missing Field Descriptions

DESCRIPTION:	It was pointed out that there were some field descriptions missing for some of the H323-UU-PDU elements in H.225.0 (1998) and H.225.0 (1999). Below is the text for those descriptions.

[Begin Correction]

nonStandardData – This field carries information not defined in this Recommendation (for example, proprietary data).

h4501SupplementaryService – This field carries a sequence of H4501SupplementaryService APDUs as defined in Table 3/H.450.1.

h245Tunneling – This element is set to TRUE if tunneling of H.245 messages is enabled.

h245Control – This field carries a sequence of tunneled H.245 PDUs.

nonStandardControl – This field contains a sequence of non-standard data elements that may be used in addition to or instead of the single **nonStandardData** field.

[End Correction]

6.4.12 Early Indication of the Refusal of Fast Connect

DESCRIPTION:	It has become apparent that there is a need for a called party to indicate to the calling party its acceptance or refusal of the Fast Connect procedures. A new field has been added to various H.225.0 messages to allow explicit indication that Fast Connect is refused. This will be incorporated into the next H.225.0 Recommendation. This change shall apply to both H.225.0 (1998) and H.225.0 (1999).

For each message in the ASN.1 that contains the **fastConnectRefused**, the following definition shall apply.

[Begin Correction]

fastConnectRefused – A called endpoint should return this element in any message up to and including the Connect message when establishing a call to indicate that it refuses the Fast Connect procedure.

[End Correction]

6.5 Technical and Editorial Corrections to ITU-T Recommendation H.245 (1999)

There are currently no corrections for H.245 (1999).

6.6 Technical and Editorial Corrections to ITU-T Recommendation H.246 (1998)

6.6.1 Annex A Corrections

DESCRIPTION:	A minor inconsistency has been discovered in section A.5.2.4 of H.246 Annex A. The commands MCV and Cancel-MCV are listed with an 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 an H.245 ConferenceRequest to broadcastMyLogicalChannelNumber that provides for a response.)

[Begin Correction]

A.5.2.4.1 Multipoint Control C&I

H.230 COMMAND/INDICATION	**H.245 equivelent**
MCV	Send **broadcaseMyLogicalChannel**

Cancel-MCV	Send **cancelBroadcastMyLogicalChannel**

[End Correction]

DESCRIPTION:	A minor inconsistency has been discovered in section A.5.2.4.4 of H.246 Annex A. 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.

[Begin Correction]

A.5.2.4.4 Multipoint Control C&I

H.230 COMMAND/INDICATION	**H.245 equivelent**
VIN	Send **terminalYouAreSeeing**
VCB/Cancel-VCB	Send **makeTerminalBroadcaster / CancelMakeTerminalBroadcaster**
VCS/Cancel-VCS	Send **sendThisSource / CancelSendThisSource**
VCR	Send **videoCommandReject**
VIN2	Send **terminalYouAreSeeingInSubPictureNumber**
VIC	Send **videoIndicateCompose**
VIM	Send **videoIndicateMixingCapability**

[End Correction]

6.6.2 Reference to ATM Forum Document

DESCRIPTION:	To help clarify the usage of H.246 with respect to ATM, a reference to an ATM Forum document has been proposed. This reference shall appear in next H.246 publication from the ITU.

[Begin Correction]

1 Scope

...

Voice/Voiceband terminals on GSTN use the appropriate national standards for call control and G.711 or analogue signals for voice. Voice/Voiceband terminals on ISDN use the appropriate national variant of Q.931 for call control and G.711 for voice.

Interworking of H.323 over ATM with H.323 over non-ATM IP networks is possible through the use of an H.323-H.323 gateway. Transport of H.323 media streams over ATM is described in AF-SAA-0124.000.

[End Correction]

[Begin Correction]

2 Normative References

...

- ATM Forum Technical Committee, AF-SAA-0124.000, *Gateway for H.323 Media Transport Over ATM*, 1999

[End Correction]

6.7 Technical and Editorial Corrections to ITU-T Recommendation H.235 (1998)

6.7.1 Key Escrow Usage

DESCRIPTION:	A minor inconsistency has been discovered in the Recommendation H.235 Section 6.6.1. This change does not affect behavior or implementations in any way. This change will be applied to H.235v2 when published by the ITU.

[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 the facility known as trusted third party (TTP) within the signalling elements.

[End Correction]

6.7.2 H.235 Control Channel References

DESCRIPTION:	A typographical error has been discovered in section 8 of the Recommendation H.235. This change does not affect behavior or implementations in any way. This change will be applied to H.235v2 when published by the ITU.

[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**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]

6.7.3 Multipoint Procedure Section Reference

DESCRIPTION:	A minor error in a section reference has been discovered in Recommendation H.235 section 9.

[Begin Correction]

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 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 to perform direct cryptographic authentication within the H.245 channel.

[End Correction]

6.7.4 Introduction to Authentication

DESCRIPTION:	The introductory text (paragraph 1) to Section 10 of Recommendation H.235 in unclear and potentially misleading. The corrected text is shown below.

[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.

[End Correction]

6.7.5 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 Recommendation H.235 section

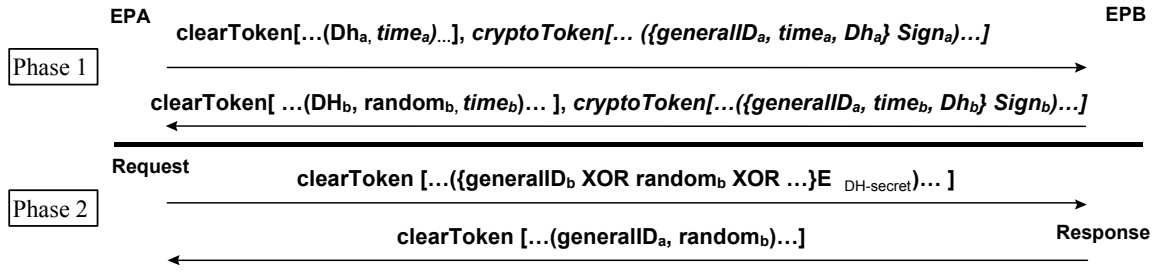
	10.2. Additionally, the note concerning authentication needs to be clarified. Phase 1: As this correction affects implementations, which utilize this mechanism to provide authentication during the Diffe-Hellman exchange. Note that if these optional parameters are not utilized (denoted by italics below 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.



...

[End Correction]

6.7.6 Introduction to Subscription Based Authentication

DESCRIPTION:	The introductory text (paragraph 1) to Section 10.3.1 of Recommendation H.235 in unclear and potentially misleading. The text shown below shall be added as the new final paragraph of that section.

[Begin Correction]

10.3.1 Introduction

...

Note - In all cases where timestamps are generated and passed as part of a security exchange, implementers 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]

6.7.7 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.

[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. Implementers 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).

Note 4: The hashing function shall be applied to the EncodedGeneralToken structure that includes at least the ID, timestamp and password fields. The password value should NOT be passed in the ClearToken.

[End Correction]

6.7.8 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 in the case where the **ClearToken** structure is placed directly into the message. 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,
    . . .
}

--  An object identifier should be placed in the tokenOID field when a
--  ClearToken is included directly in a message (as opposed to being
```

-- encrypted). In all other cases, an application should use the
-- object identifier { 0 0 } to indicate that the tokenOID value is not present.

[End Correction]

6.7.9 Corrections to Annex B

DESCRIPTION:	A number of typographical errors have been discovered in Annex B. The corrected text is shown below.

[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 (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 the **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 (**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]

6.7.10 Corrections to Appendix I

DESCRIPTION:	A typographical error has been discovered with respect to a section reference. The corrected text is shown below.

[Begin Correction]

4.2 Password

...

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

...

[End Correction]

6.8 Technical and Editorial Corrections to ITU-T Recommendation H.450 Series

6.8.1 Technical and Editorial Corrections to ITU-T Recommendation H.450.1 (1998)

6.8.1.1 Actions at a Destination Entity

DESCRIPTION:	Typographical errors have been discovered in section 6.6 of H.450.1 (1998). The text below outlines the necessary changes.

[Begin Correction]

1) Section 6.6, line 6

   Change:

   "**rejectUnrecognizedInvokePdu**"

   to

   "**rejectAnyUnrecognizedInvokePdu**"

2) Section 6.6, line 12

   Change:

   "**discardAnyUnrecognizedInvokePDU**"

   to

   "**discardAnyUnrecognizedInvokePdu**"

[End Correction]

6.8.1.2 Corrections to the ASN.1

DESCRIPTION:	H.225.0 (1999) introduces redundancy with H.450.1 in that both H.225.0 (1999) and H.450.1 have screening and presentation information. To

	remove the redundancy, it was decided that H.225.0 was the proper place for this information and the redundant elements shall be removed from H.450.1. Below shows the revision to the ASN.1 found in Table 6/H.450.1.

[Begin Correction]

```
Addressing-Data-Elements
        { itu-t recommendation h 450 1 version1(0) addressing-data-elements(9)}
    DEFINITIONS AUTOMATIC TAGS ::=
    BEGIN
    IMPORTS   AliasAddress, PartyNumber, PresentationIndicator, Screening Indicator FROM
H323-MESSAGES; -- see H.225.0

                                        ...
    -- PartyNumber defined in Recommendation H.225.0
    -- PublicPartyNumber defined in Recommendation H.225.0
    -- PrivatePartyNumber defined in Recommendation H.225.0
    -- NumberDigits defined in Recommendation H.225.0
    -- PublicTypeOfNumber defined in Recommendation H.225.0
    -- PrivateTypeOfNumber defined in Recommendation H.225.0
    -- PresentationIndicator defined in Recommendation H.225.0 (v3 and beyond)
    -- ScreeningIndicator defined in Recommendation H.225.0 (v3 and beyond)

    EndpointAddress              ::=   SEQUENCE{
        destinationAddress               SEQUENCE OF AliasAddress,
            -- multiple alias addresses may be used to address the same H.323 endpoint
        remoteExtensionAddress                AliasAddress OPTIONAL,
        ...,
        destinationAddressPresentationIndicator      PresentationIndicator OPTIONAL,
            -- Note 1, 2
        destinationAddressScreeningIndicator         ScreeningIndicator OPTIONAL,
        remoteExtensionAddressPresentationIndicator PresentationIndicator OPTIONAL,
            -- Note 1, 2
        remoteExtensionAddressScreeningIndicator     ScreeningIndicator OPTIONAL
                                        }
            -- Note 1: If this element is not available, presentation allowed shall be assumed.
            -- Note 2: If an H.450 APDU that carries this element EndpointAddress also
            -- contains an element PresentationAllowedIndicator, then the setting of the
            -- element PresentationAllowedIndicator shall take precedence in case of
            -- conflicting presentation information.

                                        ...
```

[End Correction]

6.8.2 Technical and Editorial Corrections to ITU-T Recommendation H.450.2 (1998)

6.8.2.1 Editorial Corrections

DESCRIPTION:	Typographical errors have been discovered in sections 11.4.2, 11.5.2, 11.6.2, and 13.4 of H.450.2. The text below outlines the necessary changes.

[Begin Correction]

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.

[End Correction]

6.8.2.2 Clarification of CallIdentifier and ConferenceIdentifier

DESCRIPTION:	A clarification of the setting of H.225.0 elements **CallIdentifier** and **ConferenceIdentifier** values in conjunction with H.450.2 transferred calls has been added within a new clause 10.7 "Interactions with H.225.0 parameters". ***Special Note: This section appeared in the May 1999 Implementers Guide, but stated that the CallIdentifier should be the same for transferred calls. That definition contradicted H.323v2's definition of the CallIdentifier, so this section has been changed to align with H.323v2 and higher.***

[Begin Addition]

10.7 Interactions with H.225.0 parameters

The H.225.0 CallIdentifier value of the transferred call shall use a new value, rather than the value that was used in the primary call.

The H.225.0 ConferenceIdentifier of a transferred call may use a new value. However, the ConferenceIdentifier of an existing conference (multipoint conference) shall not be altered.

[End Addition]

6.8.2.3 Transfer without Consultation

DESCRIPTION:	An exceptional procedure for a transferred endpoint B actions has been added in clause 8.2.1 to allow call transfer without consultation to take place successfully even if the transferred-to endpoint C does either not support H.450.2 or not support H.450 at all. Furthermore, clause 6 was enhanced to allow a different Interpretation APDU setting.

[Begin Correction]

6 Messages and Information elements

...

When conveying the invoke APDU of operation callTransferSetup, the Interpretation APDU shall contain value clearCallIfAnyInvokePduNotRecognized in case of Transfer with Consultation. In case of Call Transfer without Consultation, the Interpretation APDU shall be set to value discardAnyUnrecognizedInvokePdu.

[End Correction]

[Begin Addition]

8.2.1 Transfer without Consultation with transferred-to endpoint C not supporting H.450.2

a) When receiving a CONNECT message from endpoint C (that does not include a response to the callTransferSetup Invoke APDU) while being in state CT-Await-Setup-Response, the transferred endpoint B should continue as if a callTransferSetup Return Result APDU would have been received. This allows endpoint B to successfully continue with the Call Transfer procedures (including appropriate internal call transfer state handling and clearing of the primary call to the transferring endpoint A). This exceptional procedure enables successful Call Transfer even if the transferred-to endpoint C does not support H.450 at all.

b) When a RELEASE COMPLETE message as a response to a SETUP message containing callTransferSetup Invoke APDU is received in endpoint B on the transferred call attempt, possibly containing callTransferSetup Return Error or Reject APDU, then endpoint B may retry call establishment to endpoint C using a normal basic call. Upon receiving the CONNECT message from endpoint C, endpoint B may continue with the procedures as described in a) above.

Note that this procedure may apply if endpoint C supports H.450.1 but no H.450.2 and if endpoint B has not selected the recommended Interpretation APDU value discardAnyUnrecognizedInvokePdu but has set the value to clearCallIfAnyInvokePduNotRecognized.

[End Addition]

6.8.3 Technical and Editorial Corrections to ITU-T Recommendation H.450.3 (1998)

6.8.3.1 Editorial Correction in H.450.3

DESCRIPTION:	Typographical errors have been discovered in H.450.3 clause 12 SDLs.

[Begin Correction]

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.

change  to 

[End Correction]

6.8.3.2 Clarification of the CallIdentifier and ConferenceIdentifier

DESCRIPTION:	A clarification of the setting of H.225.0 elements **CallIdentifier** and **ConferenceIdentifier** values in conjunction with H.450.3 forwarded calls has been added within a new clause 9.9.3 "Interactions with H.225.0 parameters". ***Special Note: This section appeared in the May 1999 Implementers Guide, but stated that the CallIdentifier should be the same for diverted calls. That definition contradicted H.323v2's definition of the CallIdentifier, so this section has been changed to align with H.323v2 and higher.***

[Begin Addition]

9.9.3 Interactions with H.225.0 parameters

The H.225.0 **CallIdentifier** of a forwarded call shall use a new value, rather than the value that was used in the forwarding call.

The H.225.0 **ConferenceIdentifier** of a forwarded call may use a new value. However, the **ConferenceIdentifier** of an existing conference (multipoint conference) shall not be altered.

[End Addition]

6.8.3.3 Correction to the ASN.1

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

[Begin Correction]

H225InformationElement FROM H225-generic-parameters-definition

[End Correction]

6.8.4 Technical and Editorial Corrections to ITU-T Recommendation H.450.4 (1999)

There are no corrections for H.450.4.

6.8.5 Technical and Editorial Corrections to ITU-T Recommendation H.450.5 (1999)

6.8.5.1 Clarification of the CallIdentifier

DESCRIPTION:	A clarification of the setting of H.225.0 element CallIdentifier in conjunction with H.450.5 parked calls has been added within clause 8.3 "Interactions with H.225.0 parameters". This information will be contained in the revision 2 of H.450.5

	Recommendation to be published by the ITU-T. The modified text is shown below.

[Begin Correction]

8.3 Interaction with H.225.0 parameters

The H.225.0 **CallIdentifier** value within a parked call shall use a new value, rather the CallIdentifier value that was used in the primary call. For all other SETUP messages carrying SS-PARK or SS-PICKUP related APDUs as defined within this recommendation, new CallIdentifier values shall be used. Note that the CallIdentifier value of the parked/alerting call is preserved during the SS-PARK / SS-PICKUP procedure within the H.450 APDUs.

[End Correction]

6.8.6 Technical and Editorial Corrections to ITU-T Recommendation H.450.6 (1999)

There are no corrections for H.450.6.

6.8.7 Technical and Editorial Corrections to ITU-T Recommendation H.450.7 (1999)

There are no corrections for H.450.7.

6.8.8 Technical and Editorial Corrections to ITU-T Recommendation H.450.8 (2000)

There are no corrections for H.450.8.

6.9 Technical and Editorial Corrections to ITU-T Recommendation H.341 (1999)

6.9.1 Corrections to the RAS MIB in H.341

DESCRIPTION:	A few editorial errors have been identified in the RAS MIB in H.341. The following text describes the necessary corrections.

1) **RasAdmissionTableEntry** SEQUENCE, the field **RASAdmissionCallIdentifier** is inserted twice. The second entry shall be removed.

2) Each field in **CallSignalStatsEntry** SEQUENCE referred to the number of messages received ("In") and the number of messages transmitted ("Out"). These counters shall be combined. The new **CallSignalStatsEntry** SEQUENCE is shown below:

[Begin Correction]

```
CallSignalStatsEntry::= SEQUENCE {
        callSignalStatsCallConnections
           Counter32,

        callSignalStatsAlertingMsgs
           Counter32,

        callSignalStatsCallProceedings
           Counter32,

        callSignalStatsSetupMsgs
           Counter32,

        callSignalStatsSetupAckMsgs
```

Counter32,

callSignalStatsProgressMsgs
Counter32,

callSignalStatsReleaseCompleteMsgs
Counter32,

callSignalStatsStatusMsgs
Counter32,

callSignalStatsStatusInquiryMsgs
Counter32,

callSignalStatsFacilityMsgs
Counter32,

callSignalStatsInfoMsgs
Counter32,

callSignalStatsNotifyMsgs
Counter32,

callSignalStatsAverageCallDuration
Integer32
}

[End Correction]

3) In **RasRegistrationTableEntry** SEQUENCE, **rasRegistrationEndpointType** is defined to be type "**Integer32**" and should be defined as type "**MmH323EndpointType**".

6.10 Technical and Editorial Corrections to Annex G/H.225.0

6.10.1 Multiple Usage Indications for the Same Call

DESCRIPTION:	H.225 Annex G does not fully define the behavior when more than one **UsageIndication** message is received for the same **callIdentifier** and **senderRole**, although **usageCallStatus** of **callInProgress** implies that there will be another later **UsageIndication**. This text clarifies the text in Annex G/H.225.0 and will be inserted into the next version of Annex G published by the ITU.

[Begin Addition]

1.7.4.1 Multiple Usage Indications for the Same Call

Multiple Usage Indications for the same call provide increasingly more up to date information on the same media types, or usage information about new media types created in the same call. Also, since border elements may take over calls while being in progress, not all the Usage Indications necessarily originate from the same border element. The following rules define the semantics:

1. UsageIndication received with a usageCallStatus of callInProgress implies a subsequent UsageIndication with the same callIdentifier and senderRole should be received. If the recipient is configured for fault recovery it may choose to conclude after a configured

time interval with no further UsageIndication messages, that a fault has occurred and recover whatever data it can from the received UsageIndication messages.

2. Subsequent UsageIndication messages with the same usageField ids should report a startTime matching the endTime of the previous message (although this may be impossible for an alternate border element). Recipients shall assume each report is for a distinct period. Other information in the usageField overrides the information received in previous messages with the same usageField id.
3. A border element should send a new Usage Indication for each change in the media type during the call, e.g., audio stopped and fax started, or a codec has changed. If multiple media types are engaged at the same time (e.g. audio & video) they should be reported in the same UsageIndication message.

[End Addition]

[Begin Correction]

1.7.4 Usage Information Exchange

Administrative domains may request other domains to provide them information about the usage of resources in specific calls. UsageIndication messages may be provided at any stage of the call. Also, multiple usage indications may be sent for the same call, each one with possibly more up to date information, or reporting on consecutive call segments or different media type usage. See section 1.7.4.1 for detail.

...

[End Correction]

[Begin Correction]

1.8.2.28 Usage Indication

Report call details and usage information. This message is sent with respect to the last UsageSpecification element received by the BE concerning the call.

Field	Description
CallInfo	The call for which the indication applies.
AccessTokens	The access tokens for the call. These are the tokens that were received in the address template used for the call, and propagated in the AccessRequest / Setup message for the same call.
SenderRole	The role of the sender of the indication: • Originator – originating party. • Destination – terminating party.

	• NonStandard – other.
UsageCallStatus	The current status of the call: • preConnect • callInProgress • callEnded • RegistrationLost
SourceAddress	E.164 or e-mail address of the caller party. In case of E.164 this designates the ANI/CLI.
DestAddress	E.164 or e-mail address for the called party,
StartTime	The time the call started in UTC format. Relevant only for calls that passed the setup stage. For multiple media types used in the call, each media type should report a different StartTime, corresponding to the time at which that media stream started. For periodic messages StartTime should correspond with the EndTime of the previous message.
EndTime	The time the call ended in UTC format. Relevant only for ended calls. For multiple media types used in the call, each media type shall report a different EndTime corresponding to the time at which that media stream ended. For periodic messages, EndTime is the time which ends a reporting period.
TerminationCause	The reason for the end of the call. Relevant only for ended calls.
usageInformation	Set of fields of information. Each field is represented by a UsageField which can be a standard or non-standard. Standard UsageFields are for future study.

...

[End Correction]

6.10.2 Identifying the Terminated Service Relationship

DESCRIPTION:	In the **ServiceRelease** message, there is no information to identify the service relationship that is being terminated.

[Begin Correction]

1.8.2 Message Definitions

...

serviceID	This identifer identifies a particular service relationship session between two border elements. Whenever a border element receives a ServiceRequest message, it allocates a **globally** unique service ID and returns it to the sender of the ServiceReque st message in the ServiceConfirm message. Once a service relationship has been established, the service ID is included in all subsequent messages with the border element (e.g. usage indication, descriptorID request, descriptor request, access request). This is used by the recipient border element to check if it has a service relationship with the sender of the message.

...

[End Correction]

[Begin Correction]

1.8.2.6 Service Confirmation

A border element in receipt of a ServiceRequest message responds with a ServiceConfirmation message to indicate that it agrees to establish a service relationship. Every new service relationship is identified by a service identifier. Whenever a border element receives a new ServiceRequest message, it allocates a unique service ID and returns it to the sender of the service request message in the "service confirm" message. If the border element already has a service relationship with the border element that sent the ServiceRequest message, sending ServiceConfirmation indicates that the terms of the original relationship are terminated and replaced with the new terms.

...

[End Correction]

6.10.3 Need to Provide a replyAddress when using Bi-directional Connections

DESCRIPTION:	Currently a request message sent over bi-directional connection oriented transport like TCP is not expected to have the **replyAddress** element in the **AnnexGCommonInfo**.**replyAddress**. This implies that a receiver can send data to the sender only as long as the TCP connection is up. This results in a problem if a "response" needs to be sent to the sender after the original TCP connection has been released, because the receiver does not have the transport address of the sender. E.g.: this could happen when a **ServiceRelease** needs to be generated long after the establishment of a service relationship. The following corrections shall be applied to Annex G/H.225.0.

[Begin Correction]

1.8.2 Message Definitions

...

ReplyAddress	This is the address to which to send the reply to a request message. All request messages shall include a **replyAddress** except for cases where the address can be derived from the transport layer. On IP networks, if the sender of the request message is listening on the default port (2099), then the reply address need not be included. In such a case, the receiver obtains the transport address of the sender by appending default port (2099) to the IP address of the sender as received in the IP header of the request packet.

[End Correction]

A footnote shall also be added to the "ReplyAddress" definition that reads:

> BEs are assumed not to be hidden behind network address translation (NAT) devices, thus it is not required to prefer the transport address over the **replyAddress**, as is the case for RAS messages.

6.10.4 Sending UsageIndications without a Service Relationship

DESCRIPTION:	Currently Annex G specifications mandate that usage Indication message cannot be sent out unless there is a service relationship between two border elements. Since a border element is not mandated to have a service relationship in a secured environment (or in an environment where security issues are handled by non-Annex G procedures), it is limiting that such border elements cannot exchange usage indication messages. The following corrections shall be applied to Annex G/H.225.0.

[Begin Correction]

1.7.4 Usage Information Exchange

...

Usage Indications may be exchanged irrespective of whether the two border elements have a service relationship between them. However the policy of a border element may not allow such exchanges without a service relation. In such a case, the border element may reject the usage indication message, with an error code **noServiceRelationship**.

...

[End Correction]

[Begin Correction]

1.8.2.5 Service Request

...

The recipient of the ServiceRequest may indicate alternate border elements that the sender of ServiceRequest may try for backup service. Establishing a service relationship is an optional procedure, although a border element's policy may require such a relationship.

...

[End Correction]

6.10.5 Changes to the ASN.1 in Annex G/H.225.0

DESCRIPTION:	This section shows the changes to the ASN.1 required to support the changes and corrections to Annex G/H.225.0.

[Begin Correction]

2 Message Syntax

...

```
AnnexGCommonInfo ::= SEQUENCE
{
    sequenceNumber      INTEGER(0...65535),
    version             AnnexGVersion,
    hopCount            INTEGER (1...255),
    replyAddress        SEQUENCE OF TransportAddress OPTIONAL,
    integrityCheckValue ICV OPTIONAL,
    tokens              SEQUENCE OF ClearToken OPTIONAL
    cryptoTokens        SEQUENCE OF CryptoH323Token OPTIONAL
    nonStandard         SEQUENCE OF NonStandardParameter OPTIONAL,
    ...,
    serviceID           ServiceID   OPTIONAL
}

ServiceID               ::= GloballyUniqueID

UsageCallStatus ::= CHOICE
{
    preConnect          NULL,       -- Call has not started
    callInProgress      NULL,       -- Call is in progress
    callEnded           NULL,       -- Call ended
    ...,
    registrationLost    NULL   -- Uncertain if call ended or not
}

GlobalTimeStamp     ::=     IA5String (SIZE(14))
                            -- UTC in the form YYYYMMDDHHmmSS
                            -- where YYYY = year, MM = month, DD = day,
                            -- HH = hour, mm = minute, SS = second
                            -- (for example, 19981219120000 for noon
                            -- 19 December 1998)
```

...

[End Correction]

6.10.6 Clarification Relating to Service Relationships

DESCRIPTION:	The text in the section describing the fields for the Usage Specification suggests that an endpoint should have a service relationship with a border element, but this is entirely optional. The text altered to clarify the fact that this is, indeed, optional.

[Begin Correction]

6.8.2.4.5 USAGE SPECIFICATION

SendTo — Border element to send the UsageIndication messages to. If the sender has a service relationship with that border element, this is the element identifier returned in the ServiceConfirmation message.

[End Correction]

6.10.7 Corrections for the Usage Indication Rejection

DESCRIPTION:	The reasons for a Usage Indication Rejection in the field descriptions do not align with the ASN.1 and are also not fully defined. The corrected text is shown below.

[Begin Correction]

1.8.2.30 Usage Indication Rejection

Reason — This is the reason the border element rejected the UsageIndication message. Choices are:

- UnknownCall - The call specified in the UsageIndication is not a recognized call.
- Incomplete - The UsageIndication did not contain all the information required by the UsageSpecification that applies to this UsageIndication.
- Security – The UsageIndication did not meet the recipient's security requirements.
- NoServiceRelationship- The recipient will exchange this information only after establishment of a service relationship.
- Undefined – The reason for rejecting the UsageIndication does not match any of the other choices.

[End Correction]

6.10.8 Corrections to tables and Diagrams

DESCRIPTION:	It was pointed out that there are unintended ambiguous identifiers assigned as zone descriptor values in the tables and figures in sections 1.9.1, 1.9.1.1,

	1.9.2, and 1.9.2.1. The diagrams below replace the coresponding tables/figures those sections.

The table in 1.9.1 should be replaced with the below table.

[Begin Correction]

Administrative Domain	Template definition	Comment
A	Descriptor "d1": Pattern = 1732* Transport address = BE_A call signal address Message type = sendSetup	Signaling for any call into AD A will be through AD A's border element.
B	Descriptor "d2": Pattern = 1908* Transport address = BE_B annex g address Message type = sendAccessRequest Descriptor "d3": Pattern = 1908953* Transport address = GW_{B1} CALL SIGNALLING address Message type = sendSetup	For calls to 1908*, an AccessRequest message is needed to get the destination's (i.e., a gateway) call signaling address. For calls to 1908953*, the Setup can be sent directly to this particular gateway.
C	Descriptor "d4": Pattern = 1303538* Transport address = GK_{C1} call signal address Message type = sendSetup Descriptor "d5": Pattern = 1303* Transport address = BE_C annex g address Message type = sendAccessRequest	Calls to 1303538* will be routed through this particular gatekeeper. Calls to 1303* can be signalled directly to the destination gateway, but an AccessRequest must be sent to obtain the gateway's call signaling address.

[End Correction]

The figure in section 1.9.1.1 shall be replaced with the table below.

[Begin Correction]

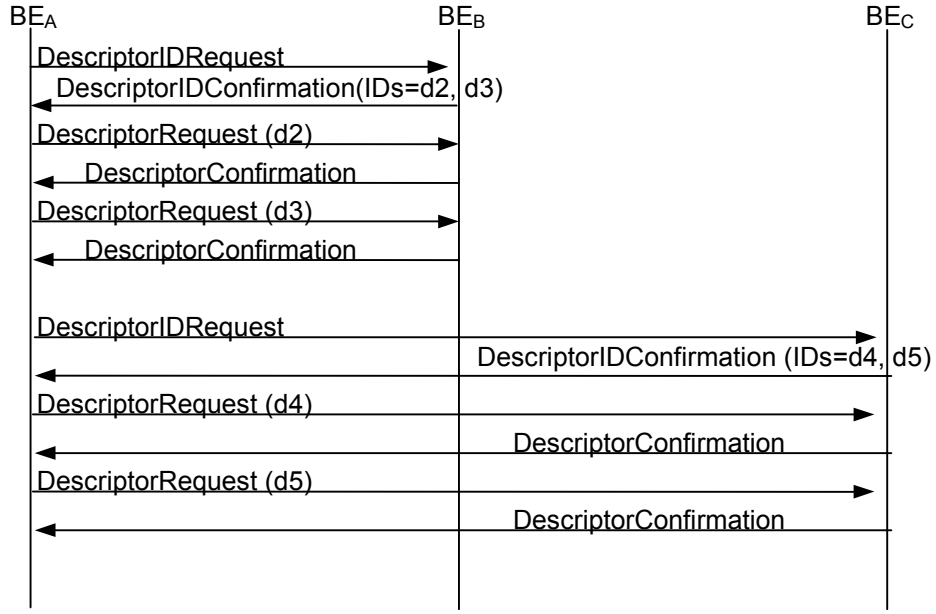


Figure 1 - Example of Descriptor Exchange

[End Correction]

The table in 1.9.2 should be replaced with the below table.

[Begin Correction]

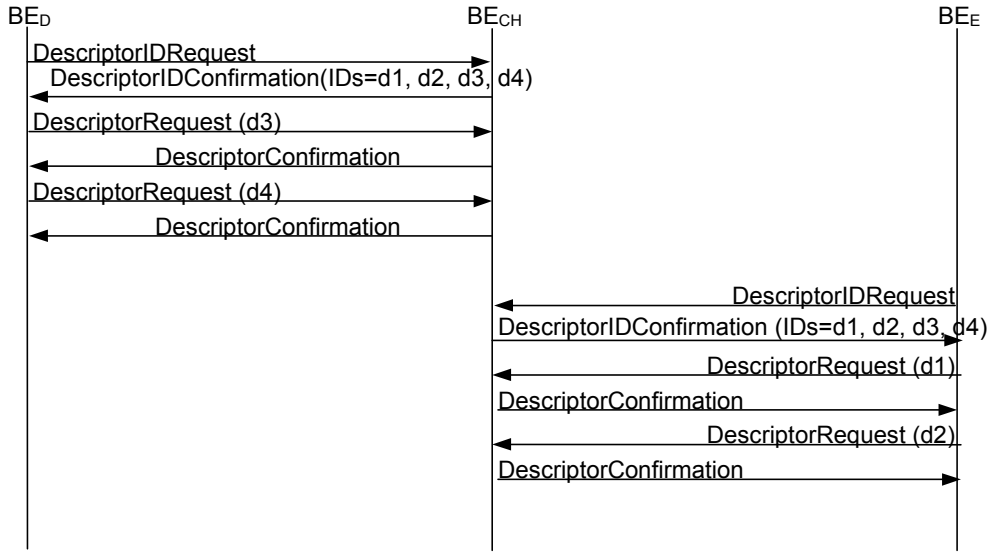
Administrative Domain	Template definition	Comment
D	Descriptor "d1": Pattern = 1908* Transport address = BE_D annex g address Message type = sendAccess Request Descriptor "d2": Pattern = 1908953* Transport address = GW_{D1} Call Signalling address Message type = sendSetup	For calls to 1908*, an Access Request message is needed to get the destination's (i.e., a gateway) call signaling address. For calls to 1908953*, the Setup can be sent directly to this particular gateway.
E	Descriptor "d3": Pattern = 1303538* Transport address = GK_{E1} call signal address Message type = sendSetup Descriptor "d4": Pattern = 1303*	Calls to 1303538* will be routed through this particular gatekeeper. Calls to 1303* can be signalled directly to the destination gateway, but an AccessRequest must be sent to obtain the gateway's call signaling address.

	Transport address = BE_E annex g address Message type = sendAccess Request	
CH	Descriptor "d1": Pattern = 1908* Transport address = BE_D annex g address Message type = sendAccess Request Descriptor "d2": Pattern = 1908953* Transport address = GW_{D1} call signalling address Message type = sendSetup Descriptor "d3": Pattern = 1303538* Transport address = GK_{E1} call signal address Message type = sendSetup Descriptor "d4": Pattern = 1303* Transport address = BE_E annex g address Message type = sendAccess Request	The clearing house obtains descriptors from other ADs and holds this information for distribution during descriptor exchange.

[End Correction]

The figure in section 1.9.2.1 shall be replaced with the figure below.

[Begin Correction]



[End Correction]

7 Implementation Clarifications

7.1 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 a **tokenOID** (object identifier) which unambiguously identifies it.

7.2 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.

7.3 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).

7.4 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.

7.5 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.

7.6 Graceful Closure of TCP Connections

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

7.7 Race Condition on Simultaneous Close of Channels

Section 8.5 of H.323 describes the procedures that an endpoint follows to terminate a call. It should be noted that as prescribed in Step 6, both endpoints shall issue a Release Complete simultaneously. Endpoints should be prepared for this potential race condition.

7.8 Acceptance of Fast Connect

When an endpoint accepts the Fast Connect procedure, it may select from the proposed channels as specified in section 8.1.7.1/H.323. The Recommendation clearly specifies what fields shall be modified by the endpoint to accept both the forward and the reverse channels. An endpoint shall not modify any fields other than those specified in 8.1.7.1/H.323 when returning the proposed channels.

Newer versions of H.245 may introduce new fields into the **OpenLogicalChannel** sequence or one of the structures contained therein, as well as new procedures. An older endpoint is obviously not required to decode such new fields or to return such new fields when accepting any proposal. Implementers should consider the consequences of transmitting a newer H.245 OLC to an older endpoint. For the purposes of Fast Connect, the calling endpoint shall assume that the called endpoint's version of H.245 is the minimum version of H.245 necessary to be complaint with an H.323 device that advertises the version of H.225.0 transmitted in the messages from the called endpoint (refer to the "Summary" section of H.323).

7.9 Semantic Differences between Lightweight RRQs and IRQ/IRR Messages

The lightweight RRQ and the IRR message serve two different functions with an H.323 system. While both are a means of allowing the Gatekeeper to discover that an endpoint is alive, they also each serve separate, unique functions.

The lightweight RRQ is intended to prevent a registration with a Gatekeeper from expiring. The message is generated by the endpoint and does not require the Gatekeeper to poll each endpoint on a regular interval. This message is also a means of allowing the Gatekeeper to provide updated registration information, such as a new list of Alternate Gatekeepers, after the initial registration.

Version 1 of H.323 did not have the concept of a lightweight RRQ, so the IRQ/IRR exchange is the only mechanism available to determine endpoint status of Version 1 devices. However, the lightweight RRQ may be a better choice for determining endpoint status for Version 2 and higher devices.

The IRQ/IRR exchange allows the Gatekeeper to poll the endpoint periodically to discover if the endpoint is still alive. However, an IRR is also intended to convey details about current active calls. This can be used by the Gatekeeper to discover calls that have terminated, which may happen if the endpoint fails to properly send a DRQ message for a call. The IRR message also provides specific details about active calls.

7.10 Specifying the Payload Format for a Channel

Implementers should be conscientious of the fact that there are possibly multiple payload formats defined for media formats. For example, two payload formats are defined for H.263—one is defined for the Recommendation H.263 (1996) and one for Recommendation H.263 (1998). Other payload formats may be defined for existing codecs or revisions of those codecs. For interoperability, it is strongly advised that implementers provide the **mediaPacketization** element of the **h2250LogicalChannelParameters** sequence in the **OpenLogicalChannel** message so that there is no ambiguity at to which payload format is being used.

8 Allocated Object Identifiers and Port Numbers

Information in this section is provided for informational purposes and convenience. This section does not supercede nor replace proper references in H.225.0, H.225, H.235, or other Recommendations.

8.1 Allocated Object Identifiers

The following object identifiers have been allocated for protocols associated with H.323. Any future object IDs that are allocated should be indexed here to prevent duplication.

Note that all object IDs below are allocated below the object ID { itu-t(0) recommendation(0) } which has been abbreviated as "0 0" below.

{ 0 0 h(8) 2250 version(0) *[v]* }	H225.0 version numbers
Assigned values of *v*: 1-3	
{ 0 0 h(8) 2250 annex(1) g(7) version(0) *[v]* }	H225.0 Annex G version numbers
Assigned values of *v*: 1	

{ 0 0 h(8) 2250 annex(1) g(7) usage(1) *[u]* }	H225.0 Annex G usage tags
Assigned values of *u*: none	
{ 0 0 h(8) 245 version(0) *[v]* }	H245 version numbers
Assigned values of *v*: 1-6	
{ 0 0 h(8) 245 generic-capabilities(1) video(0) *[c]* }	Generic video capabilities
Assigned values of *c*:	
Is14496-2(0)	
{ 0 0 h(8) 245 generic-capabilities(1) audio(1) *[c]* }	Generic audio capabilities
Assigned values of *c*: none	
{ 0 0 h(8) 245 generic-capabilities(1) data(2) *[c]* }	Generic data capabilities
Assigned values of *c*: none	
{ 0 0 h(8) 245 generic-capabilities(1) control(3) *[c]* }	Generic control capabilities
Assigned values of *c*:	
Logical-channel-bit-rate-management(0)	
{ 0 0 h(8) 245 generic-capabilities(1) multiplex(4) *[c]* }	Generic multiplex capabilities
Assigned values of *c*: none	
{ 0 0 h(8) 283 generic-capabilities(1) 0 }	H.283 Capability

8.2 Allocated Port Numbers

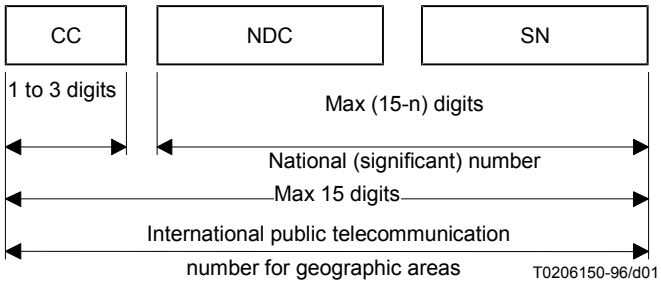
The following IP port numbers have been allocated:

1300	TLS secured call signalling
1718	Multicast RAS Signalling
1719	Unicast RAS Signalling
1720	TCP call signalling
2099	Annex G/H.225.0 Signalling
2517	Annex E/H.323 Signalling

9 Use of E.164 and ISO/IEC 11571 Numbering Plans

9.1 E.164 Numbering plan

ITU-T Recommendation defines E.164 numbers the following way for geographic areas:



CC Country Code for geographic areas
NDC National Destination Code (optional)
SN Subscriber Number
n Number of digits in the country code

NOTE – National and international prefixes are not part of the international public telecommunication number for geographic areas.

Figure – International public telecommunication number structure for geographic areas

Similar descriptions are also defined for non-geographic areas. Recommendation E.164 further defines country codes (CC) for all the countries and regions of the world.

An international E.164 number always starts with a country code and its total length is always 15 digits or less. More importantly, it does not include any prefixes that are part of a dialing plan (for example, "011" for an international call placed in North America, or "1" for a long-distance call), nor does it include "#" or "*". The number "49 30 345 67 00" is an E.164 number with CC=49 for Germany. A national number is the international number stripped of the country code, "30 345 67 00" in this case. The subscriber number is the national number stripped of the national destination code, "345 67 00" in this case.

An E.164 number has global significance: any E.164 number can be reached from any location in the world. A "dialed digit sequence", however, only has significance within a specific domain. Within a typical private numbering plan in an enterprise, for example, a prefix, such as "9", may indicate that a call goes "outside", at which point the local telephone company's dialing plan takes over. Each telephone company or private network is free to choose its own dialing plan. It is also free to change it as it pleases—and frequently does so (adding new area codes, for example).

In a typical geographically determined network where users input telephone numbers manually and where users do not travel too much, having different dialing plans everywhere is usually a problem. However, when a user travels, the user must determine the other network's numbering plan in order to place calls. When computer systems perform the dialing automatically, the user is usually required to customize the dialing software for every region or network.

Because of these issues with varying dialing plans and automated dialing, it is essential to be able to refer to an absolute "telephone number" instead of "what you have to dial to reach it from a specific location." Proper usage of E.164 numbers can resolve these issues. Many systems use E.164 numbers instead of dialed digits: for example, a PBX may gather the dialed digits from a user on a telephone and then initiate a call to the local phone company using an E.164 number in the Called Party Number information element in Q.931. When completing the Called Party Number IE, specifying the numbering plan as "ISDN/telephony numbering plan (Recommendation E.164)" indicates an E.164 number. Specifying the type of number as "unknown" and the specifying the numbering plan as "unknown" indicates dialed digits.

The following are a set of definitions from E.164:

number

A string of decimal digits that uniquely indicates the public network termination point. The number contains the information necessary to route the call to this termination point.

A number can be in a format determined nationally or in an international format. The international format is known as the International Public Telecommunication Number which includes the country code and subsequent digits, but not the international prefix.

numbering plan

A numbering plan specifies the format and structure of the numbers used within that plan. It typically consists of decimal digits segmented into groups in order to identify specific elements used for identification, routing and charging capabilities, e.g. within E.164 to identify countries, national destinations, and subscribers.

A numbering plan does not include prefixes, suffixes, and additional information required to complete a call.

The national numbering plan is the national implementation of the E.164 numbering plan.

dialing plan

A string or combination of decimal digits, symbols, and additional information that define the method by which the numbering plan is used. A dialing plan includes the use of prefixes, suffixes, and additional information, supplemental to the numbering plan, required to complete the call.

address

A string or combination of decimal digits, symbols, and additional information which identifies the specific termination point(s) of a connection in a public network(s) or, where applicable, in interconnected private network(s).

prefix

A prefix is an indicator consisting of one or more digits, that allows the selection of different types of number formats, networks and/or service.

international prefix

A digit or combination of digits used to indicate that the number following is an International Public Telecommunication Number.

country code (CC) for geographic areas

The combination of one, two or three digits identifying a specific country, countries in an integrated numbering plan, or a specific geographic area.

national (significant) number [N(S)N]

That portion of the number that follows the country code for geographic areas. The national (significant) number consists of the National Destination Code (NDC) followed by the Subscriber Number (SN). The function and format of the N(S)N is nationally determined.

national destination code (NDC)

A nationally optional code field, within the E.164 number plan, which combined with the Subscriber's Number (SN) will constitute the national (significant) number of the international public telecommunication number for geographic areas. The NDC will have a network and/or trunk code selection function.

The NDC can be a decimal digit or a combination of decimal digits (not including any prefix) identifying a numbering area within a country (or group of countries included in one integrated numbering plan or a specific geographic area) and/or network/services.

national (trunk) prefix

A digit or combination of digits used by a calling subscriber, making a call to a subscriber in his own country but outside his own numbering area. It provides access to the automatic outgoing trunk equipment.

subscriber number (SN)

The number identifying a subscriber in a network or numbering area.

9.2 Private Network Number

Private Network Numbers are used in private or virtual private telephony networks, e.g., a corporate network of PBXs and virtual private lines.

ISO/IEC 11571 defines Private Network Number (PNP) as having up to three regional levels.

A PNP Number shall comprise a sequence of x decimal digits (0,1,2,3,4,5,6,7,8,9) with the possibility that different PNP Numbers within the same PNP can have different values of x. The maximum value of x shall be the same as for the public ISDN numbering plan, see ITU-T Recommendation E.164.

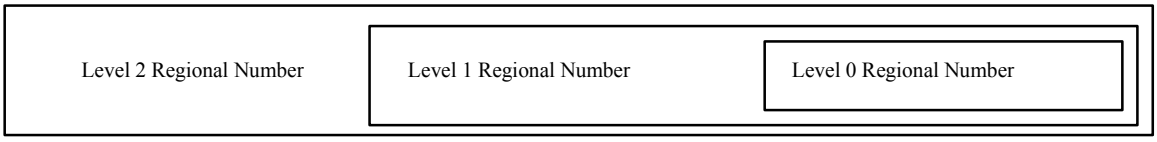


Figure – H.323 - Structure of a PNP Number with three levels of regions

A level n Regional Number (RN) shall have significance only within the level n region to which it applies. When that number is used outside that level n region, it shall be in the form of an RN of level greater than n. Only a Complete Number shall have significance throughout the entire PNP.

A typical example in North America would be a 4-digit "extension" as the Level 0 Regional Number: a 3-digit "location code" combined with the 4 digit "extension" would form the Level 1 Regional Number. The Level 2 Regional Number would be nil.

A prefix could also be used to signal which regional number is used, and would not be part of the regional number per se, but only part of the dialing plan. Again, a typical example would be the use of digit "6" to access a Level 1 Regional Number, and no digit for a Level 0 Regional Number.

The following are a set of definitions from ISO/IEC 11571:

Private Numbering Plan (PNP)

The numbering plan explicitly relating to a particular private numbering domain, defined by the PISN Administrator of that domain.

PNP Number

A number belonging to a PNP.

Region

The entire domain or a sub-domain of a PNP. A region does not necessarily correspond to a geographical area of a PISN.

Region Code (RC)

The leading digits of a PNP Number which identify a region. The RC may be omitted to yield a shortened form of a PNP Number for use internally to that region.

Regional Number (RN)

A particular form of a PNP Number which is unambiguous in the region concerned.

Complete Number

A number which is unambiguous in the entire PNP, i.e. which corresponds to the highest regional level employed in that PISN.

3 Implementor's Guide for the ITU-T H.320 Recommendation series (H.221, H.242)

Introduction

This document is a new draft Implementor's Guide for H.320 series recommendations. Changes are made against the 05/99 revision of H.221 and H.242. The changes will allow the use of G.722.1 in H.320 systems as they appeared and were agreed in Q11-K-06 (Red Bank 10/99).

Changes appear in the following sections:

7.1 Technical and editorial corrections to H.221

7.1.1 Table A1/H.221

7.1.2 Section A.1/H.221

7.1.3 Section A.5/H.221

7.1.4 Bit position for G.722.1

7.1.5 Clarifications to include revised T.35 country codes

7.2 Technical and editorial corrections to H.242

7.2.1 Table 5/H.242

7.2.2 Appendix 6

7.2.3 Clarifications to include revised T.35 country codes

Implementor's Guide for the ITU-T H.320 Recommendation series - Narrow-band visual telephone systems and terminal equipment

Abstract

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T H.320-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.320-series Recommendations.

Contact information

ITU-T Study Group 16/Question 11 Rapporteur
Tom Geary
Conexant Systems Inc.
4311 Jamboree Road
Newport Beach, CA 92660-3095
USA
Tel: +1 949 483 4092
Fax: +1 949 483 6511
Email: tom.geary@connexant.com

Implementor's Guide Editor
Patrick Luthi
PictureTel Corp.
100 Minuteman Road
Andover, MA 01810
USA
Tel: +1 978 292 5000
Fax: +1 978 292 3328
Email: luthip@pictel.com

ITU-T Recommendation H.320 Editor

Document history

Revision	Date	Description
1	7-18 February 2000	Initial version - Reviewed at the Q.11/16 Rapporteur meeting.

1. Introduction

This document is a compilation of reported defects identified with the 1997-2000 editions of the ITU-T H.320-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.320-series Recommendations.

The first version of the guide was produced following the October 1999 ITU-T Study Group 16/Question 11 Rapporteur 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 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.

4. Defect resolution procedure

Upon discovering technical defects with any components of the H.320 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.320-series Recommendations. Formal membership in the ITU is not required to participate in this process.

5. References

This document refers to the following H.320-series Recommendations:

– ITU-T Recommendation H.221 (1999), *Frame Structure for a 64 to 1920 kbit/s channel in audiovisual teleservices.*

– ITU-T Recommendation H.242 (1999), *System for establishing communication between audiovisual terminals using digital channel up to 2 Mbit/s.*

– ITU-T Recommendation H.320 (1999), *Narrow-band visual telephone systems and terminal equipment.*

– ITU-T Recommendation T.35 (2000), *Procedure for the allocation of ITU-T defined codes for non-standard facilities*

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.221

To support G.722.1 in H.320 systems, new BAS capability and command codes need to be added in Recommendation H.221.

In order to provide H.320/H.32x gateways the ability to constrain the bit rate allowed for use by the H.320 endpoint (for the purposes of enforcing bit rate symmetry, for example), capability codes for each bit rate are necessary. In the case of G.722.1, this means separate capability codes for 24 kbit/s and 32 kbit/s.

7.1.1 Table A.1/H.221 - BAS numerical values

The following new BAS code values are being added (to be updated in Table 1/H.221):

[Begin Correction]

G.722.1-32 (000)[27]

G.722.1-24 (000)[28]

G.722.1-32 (cap) (110)[5]

G.722.1-24 (cap) (110)[6]

[End Correction]

7.1.2 Section A.1/H.221 - Audio command values (000)

Section A.1/H.221 is being updated as follows:

[Begin Correction]

…

G.722.1-32 G.722.1 7 kHz audio at 32 kbit/s, in bits 1-4.

G.722.1-24 G.722.1 7 kHz audio at 24 kbit/s, in bits 1-3.

…

[End Correction]

7.1.3 Section A.5/H.221 - Audio capabilities (100)

Section A.5/H.221 is being updated as follows:

…

G.722-64 Capable of decoding audio to Recommendation G.722 (mode 1) and to Recommendation G.711.

G.722-48 Capable of decoding audio to Recommendation G.722 (modes 1, 2, 3) and to Recommendation G.711.

[Begin Correction]

G.722.1-32 (cap) Capable of decoding audio to Recommendation G.722.1 at 32 kbit/s and to Recommendation G.711.

G.722.1-24 (cap) Capable of decoding audio to Recommendation G.722.1 at 24 kbit/s and to Recommendation G.711.

…

[End Correction]

7.1.4 Bit Position for G.722.1 audio

This new section is being added at the end of section 4.2 (encoded audio streams) as follows:

4.2 Encoded audio streams

…

[Begin Correction]

G.722.1 audio

G.722.1 provides two bit rates, 24 kbit/s or 32 kbit/s, and uses a frame size of 20ms. This results in either 480 bits (60 octets) or 640 bits (80 octets) in any one frame respectively. The bitrate may be changed at any 20 ms audio frame boundary. Alignment of H.221 audio mode changes with a submultiframe boundary is required by section 3.2/H.221.

Figure 1 & 2 illustrate the bit allocation of the two G.722.1 frames for a bitrate of 32 kbit/s and 24 kbit/s respectively.

H.221 Frame	Sub-Channel Bit #	Sub-Channel							
		1	2	3	4	5	6	7	8
First H.221 Frame	1	1	2	3	4				FAS
	2	5	6	7	8				FAS
	3	9	10	11	12				FAS
	4	13	14	15	16				FAS
	5	...	...	...	...				FAS
	6								FAS
	7								FAS
	8								FAS
	9								
	...								
	80	317	318	319	320				
Second H.221 Frame	81	321	322	323	324				FAS
	82	...	...	...	...				FAS
	83								FAS
	84								FAS
	85								FAS
	86								FAS
	87								FAS
	88								FAS
	89								
	...								
	160	637	638	639	640				

Figure 1 - Bit positions for G.722.1 audio at 32 kbit/s

H.221 Frame	Bit #	Sub-Channel							
		1	2	3	4	5	6	7	8
	1	1	2	3					FAS
	2	4	5	6					FAS
	3	7	8	9					FAS
	4	10	11	12					FAS
First	5	...	...	...					FAS
H.221	6								FAS
Frame	7								FAS
	8								FAS
	9								
	...								
	80	218	219	220					
	81	221	222	223					FAS
	82	224	225	226					FAS
	83	...	...	...					FAS
	84								FAS
Second	85								FAS
H.221	86								FAS
Frame	87								FAS
	88								FAS
	89								
	...								
	160	478	479	480					

Figure 2 - Bit positions for G.722.1 audio at 24 kbit/s

[End Correction]

7.1.5 Clarifications to include revised T.35 country codes

The revised Recommendation T.35 (2000) extends the number of possible country codes to allow more than 254 countries. This is being achieved by introducing a second byte for new countries being reached by an escape code in the first byte of "1111 1111" (0xFF). Countries defined in the first byte are listed in Annex A/T.35 and countries defined in the second byte are listed in Annex B/T.35.

T.35 country codes are used by NS-cap and NS-comm as described in section A.9 - Escape table values (111). In footnote 4, the following text should be added:

[Begin Correction]

[4] Country code consists of two bytes, the first being according to Recommendation T.35 Annex A. The second byte is assigned nationally, unless the first byte is 1111 1111, in which case the second byte shall contain the country code according to T.35 Annex B.The terminal manufacturer code consist of two bytes assigned nationally.

[End Correction]

7.2 Technical and editorial corrections to ITU-T Recommendation H.242

7.2.1 Table 5/H.242 - BAS capabilities that can be included in a valid capability set

Table 5/H.242 is being updated as follows:

[Begin Correction]

Audio	Absent or One or more values[b)] from A-law, m-law, G.722-48, G.722-64, G.728, G.723.1, G.729, G.722.1-24, G.722.1-32

…

[End Correction]

b) See Appendix VII for interpretation of received audio capabilities.

7.2.2 Appendix 6 - Hierarchical capability BAS codes

Appendix 6 is being updated as follows:

[Begin Correction]

The following capability codes are hierarchically structured:

G.711 (A or μ or both) < G.722-64 < G.722-48

G.711 (A or μ or both) < G.728

G.711 (A or μ or both) < G.723.1

G.711 (A or μ or both) < G.729

G.711 (A or μ or both) < G.722.1-24

G.711 (A or μ or both) < G.722.1-32

…

[End Correction]

Note that, while they have not been included previously, G.723.1 and G.729 have been now added to the list for completeness.

7.2.3 Clarifications to include revised T.35 country codes
In Appendix III, two sections are affected by the extension of T.35 country codes (see details in section 7.1.5).

4.2.1 Section III.2 - Subsequent capability exchange, including MBE capability message

Section III.2 is updated as follows:

[Begin Correction]

…

{M} Information will be M-bytes

{byte 1} Country code according to Recommendation T.35 Annex A

{byte 2} Country code assigned nationally, unless the first byte is 1111 1111, in which case this field shall contain the country code according to T.35 Annex B

{bytes 3, 4} Manufacturer code (Company XYZ)

{bytes 5-M} Type identity

…

[End Correction]

4.2.2 Section III.3 Mode switch to non-standard mode using MBE command
Section III.3 is updated as follows:

…

{N} Information will be N-bytes

[Begin Correction]

{byte 1} Country code according to Recommendation T.35 Annex A

{byte 2} Country code assigned nationally, unless the first byte is 1111 1111, in which case this field shall contain the country code according to T.35 Annex B

[End Correction]

{bytes 3, 4} Manufacturer code (Company XYZ)

{bytes 5-N} Type identity

…

H.320 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.

4 IMPLEMENTOR'S GUIDE FOR H.321 V2

_____

To reflect the progress of the SG11 DSS2 signalling work (decision of revised Q.2931 and new Q.2941.2 in December 1999), Recommendation H.321 (02/98) needs the following modifications:

#1 Modification of references

Description: Modify the Q.2931 date, add Q.2941.1 and Q.2941.2.

[Begin correction]

---

2 References

Q.2931 B-ISDN Digital Subscriber Signalling System No. 2 (DSS 2) ñ User Network Interface Layer 3 Specification for Basic Call/Connection (December 1999).

Q.2941.1 B-ISDN Digital Subscriber Signalling System No. 2 - Generic identifier transport (September 1997)

Q.2941.2 B-ISDN Digital Subscriber Signalling System No. 2 - Generic Identifier Transport Extensions (December 1999)

[End Correction]

#2 GIT End Station Identifier

Description: SG11 accepted to define the GIT end station identifier in Q.2941.2. A necessary codepoint has been allocated for this purpose.

[Begin correction]

7.3 Intercommunication between AAL-1 and AAL-5

2) If the AAL type in the SETUP does not match the type of the receiving terminal, a Generic Identifier Transport (GIT) Information Element (IE) may optionally be included in the RELEASE COMPLETE. This GIT IE can contain the address of an AAL-1/AAL-5 Interworking Unit known to the destination terminal that rejected the call. The address shall be contained in the End Station Identifier with Identifier related standard/application (octet 5) = 00000010 and Identifier type (octet 6) = 00000011.

[End Correction]

#3 Broadband Report Type IE`

Description: As part of the Q.2931 revision, SG11 decided that Broadband Report Type IE should be used instead of Notification Indicator IE for the clock source indication in H.321. SG11 also advised us of necessary codepoint values.

[Begin correction]

C.4 Choosing between adaptive and independent clocks

The procedures of this section apply only when a network clock source is not available. They are designed to prevent both ends of a connection from choosing adaptive timing, which would create an unstable loop.

- If an H.321 terminal receives a Q.2931 call-related message with Type of report (00000010) in a Broadband Report Type IE (IE Identifier = 10001001), the transmitter of that terminal shall use an independent clock source.
- When an H.321 terminal without a network clock source sends a SETUP message, Type of report (00000010) shall be included in the Broadband Report Type IE and the transmitter shall prepare to use the adaptive clock of the receiver. It shall revert to an independent clock source if the response to SETUP or any later message contains Type of report (00000010) in a Broadband Report IE.
- An H.321 terminal shall be capable of providing both an adapted clock and an independent clock to its transmitter, whichever is called for in a given connection.

[End Correction]

5 Implementor's Guide for the ITU-T H.324 Recommendation series

Introduction

This document is a text revision of the H.324 version 2 Implementor's Guide. The changes from the previous revision 3 of the Implementor's Guide is one paragraph describing the use of G.722.1 in H.324 systems and changes to section C.8.1.5 clarifying encoding procedures as they appeared and were agreed in Q11-K-05r1 (Red Bank 10/99).

To make the Implementor's Guide more readable, the sections of the existing revision 3 document have been numbered. The sections include:

7. Technical and editorial corrections
    - 7.1 Additions to H.324
    - 7.2 Technical and editorial corrections to H.324 Annex C
    - 7.3 Technical and editorial corrections to H.324 Annex F

8. Implementation clarifications
    - 8.1 Procedures for Call Hold
    - 8.2 Procedures for Explicit Call transfer

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
Conexant Systems Inc.
4311 Jamboree Road
Newport Beach, CA 92660-3095
USA

Tel: +1 949 483 4092
Fax: +1 949 483 6511
Email: tom.geary@connexant.com

Implementor's Guide Editor

Patrick Luthi
PictureTel Corp.
100 Minuteman Road
Andover, MA 01810
USA

Tel: +1 978 292 5000
Fax: +1 978 292 3328
Email: luthip@pictel.com

ITU-T Recommendation H.324 Editor

Mickey Nasiri
Ericsson Telecom
S-125 25 Stockholm
Sweden

Tel: +46 8 404 5591
Fax: +46 8 18 7620
Email:mickey.nasiri@ecs.ericsson.com

Document history

Revision	Date	Description
1	8-11 June 1998	Initial version - Reviewed at the Q.11/SG 16 meeting.
2	22 September 1998	Second version - Completed at the ITU-T Study Group 16 Rapporteurs meeting.
3	24 May 1999	Third version - Completed at the ITU-T Study Group 16 Rapporteurs meeting.
4	7-18 February 2000	Fourth version - Completed at the ITU-T Study Group 16 Rapporteurs meeting.

1. 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.

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 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.

4. 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.

5. References

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

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

– ITU-T Recommendation H.324 Annex F (1998), *Multilink operation*

– ITU-T Recommendation H.223 (1996), *Multiplexing protocol for low bit rate multimedia communication*

– ITU-T Recommendation H.223 Annex D (1999), *Optional multiplexing protocol for low bit rate multimedia mobile communication over highly error-prone channels*

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 Additions to H.324

In order to allow the use of G.722.1 in H.324 systems, a new section 6.7.4 is being added with the following text:

[Begin Correction]

6.7.4 Use of Recommendation G.722.1 for wideband audio

Recommendation G.722.1 may be used for wideband audio applications. G.722.1 frames shall be sent using AL2. Audio frame boundaries within each AL-SDU shall be implied by the ratio of AL-SDU size to G.722.1 frame size at the currently selected G.722.1 bitrate.

[End Correction]

7.2 Technical and editorial corrections to H.324 Annex C

7.2.1 Clarifications to level change procedure

This section describes the editorial corrections to clarify the level change procedure in the H.324 Annex C. The following text at the end of the Chapter C.7 of H.324 Annex C is needed.

[Begin Correction]

Note that after changing from level 0 to some higher levels, MUX-PDU octet alignment shall be preserved. Therefore, the transmitter shall add so many "0" bits after the level change sequence that the first synchronization flag of the new level will be octet aligned. In the transmitter, the reference for the octet alignment is the first transmitted bit. In the receiver, the reference for the octet alignment is the first bit of the first detected synchronization flag in the initial level set-up procedure.

[End Correction]

7.2.2 Additions to Section C.2 - General

A reference to H.223 Annex D is being added to the H.223 Level 3 description as follows:

[Begin Correction]

C.2 General

…

- H.223 Level 1: Described in Annex A/H.223. The HDLC flag in H.223 used to delimit MUX-PDUs in Level 0 is replaced with a longer flag that leads to improved MUX-PDU synchronization. HDLC bit stuffing is not used. The Control Channel Segmentation and Reassembly Layer (CCSRL) is introduced for the transmission of the control channel.

  The transmitter side shall take necessary precaution to prevent possible flag emulation for the control channel. Flag emulation can be prevented, e.g. by detecting N 16-bit flags in each MUX-SDU for the channel and by breaking the SDU into N+1 segments. This may also apply to data channels.

- H.223 Level 2: Described in Annex B/H.223. Includes the features of Annex A/H.223. In addition, the header describing the MUX-PDU contents includes error protection.

- H.223 Level 3: Described in H.223/Annex C. Includes the features of H.223/Annex B. In addition, error protection and other features are provided to increase the protection of the AL-PDUs. Described in H.223/Annex D as an optional definition of H.223/Annex C.

In addition to the hierarchy offered by the level structure, some of the multiplex levels contain options.

Mobile terminals shall support the NSRP and the SRP mode of H.324/Annex A. If both terminals start the session in level 0 initially the SRP mode shall be used. Otherwise both terminals shall start with NSRP mode.

If both terminals in a session support level 3 of H.223, then adaptation layers AL1M, AL2M, and AL3M as defined in level 3 of H.223 may also be used in H.223, H.223 Annex A and B (levels 1 and 2). However, bidirectional channels shall use either the H.223 adaptation layers, or the adaptation layers for level 3 of H.223, but not a mixture of the two.

…

[End Correction]

7.2.3 Additions to Section C.4 – Interworking

A reference to Annex D is being added to Section C.4 as follows:

[Begin Correction]

C.4 Interworking

Since all mobile terminals support H.223 level 0, no interworking function is needed when communicating with an H.324 terminal that does not support any of the robust multiplexing annexes (Annexes A, B, C and D of Recommendation H.223).

[End Correction]

7.2 Technical and editorial corrections to H.324 Annex F

7.2.1 Clarification to Section F.5.2.2.1 – Responder request to add additional connections

To clarify the order of the procedures of Annex F, a reference to Section F.5.2.1 is being added to section F.5.2.2.1 as follows:

[Begin Correction]

At any time after exchange of call information according to Section F.5.2.1, the responder may request that the initiator add physical connections. This shall be done using the **MultilinkRequest.addConnection** message in H.245.

…

[End Correction]

8. 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.

8.1 Procedures for Call Hold (CH)

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

8.1.1 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.

8.1.2 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.

8.2 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.

8.2.1 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:** **EMAIL:**	
AFFECTED RECOMMENDATIONS:	
DESCRIPTION OF PROBLEM:	
SUGGESTIONS FOR RESOLUTION:	

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

6 IMPLEMENTOR'S GUIDE FOR H.310 V2

To reflect the progress of the SG11 DSS2 signalling work (decision of new Q.2941.2 in December 1999), Recommendation H.310 (09/98) needs the following modifications:

#1 Modification of references

Description: Add Q.2941.2.

[Begin correction]

---

2 References

After [32], add the following:

[33] ITU-T Recommendation Q.2941.2 (1999) *B-ISDN Digital Subscriber Signalling System No. 2 - Generic Identifier Transport Extensions*

and renumber the existing [33] through [46] to [34] through [47].

[End Correction]

#2 TABLE C.2

Description:
- Delete the note stating that the End Station is to be defined by SG11.
- Insert the End Station value code.

[Begin correction]

TABLE C.2

GIT - Terminal A to GW

IE parameter	Code	Semantics
Identifier related standard	00000010	Recommendation H.310
Identifier type	00000010	Resource
Value (2 octets)	e.g. 00000000 00000000	H.245 resourceID (the lowest possible value)
Identifier type	00000011	End Station
Value (length dependent on maximum length allowed for called party number IE)	As per octets 5-* of called party number IE	ATM address of Terminal C

[End Correction]

#3 TABLE C.4

Description: _ Delete the note stating that the End Station is to be defined by SG11.

_ Insert the End Station value code.

[Begin correction]

TABLE C.4

GIT - Terminal C to GW

IE parameter	Code	Semantics
Identifier related standard	00000010	Recommendation H.310
Identifier type	00000010	Resource
Value (2 octets)	e.g. 00000000 00000000	H.245 resourceID (the lowest possible value)
Identifier type	00000011	End Station
Value (length dependent on maximum length allowed for called party number IE)	As per octets 5-* of called party number IE	ATM address of Terminal A

[End Correction]

_____