INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Q.2631.1

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(10/2003)

SERIES Q: SWITCHING AND SIGNALLING

Broadband ISDN – Common aspects of B-ISDN application protocols for access signalling and network signalling and interworking

IP connection control signalling protocol – Capability Set 1

ITU-T Recommendation Q.2631.1

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
General aspects	Q.2000–Q.2099
Signalling ATM adaptation layer (SAAL)	Q.2100–Q.2199
Signalling network protocols	Q.2200–Q.2299
Common aspects of B-ISDN application protocols for access signalling and network signalling and interworking	**Q.2600–Q.2699**
B-ISDN application protocols for the network signalling	Q.2700–Q.2899
B-ISDN application protocols for access signalling	Q.2900–Q.2999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Q.2631.1

IP connection control signalling protocol – Capability Set 1

Summary

This Recommendation specifies the inter-node protocol and nodal functions that support the dynamic establishment, modification and release of individual IP connections.

The IP connection control signalling protocol specified in this Recommendation can operate in public or private networks over a range of signalling transport protocol stacks.

It also provides maintenance capabilities, carriage of user-plane protocol stack information and carriage of an identifier to link the connection control protocol with other higher layer control protocols.

Source

ITU-T Recommendation Q.2631.1 was approved by ITU-T Study Group 11 (2001-2004) under the ITU-T Recommendation A.8 procedure on 14 October 2003.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation Q.2631.1

IP connection control signalling protocol – Capability Set 1

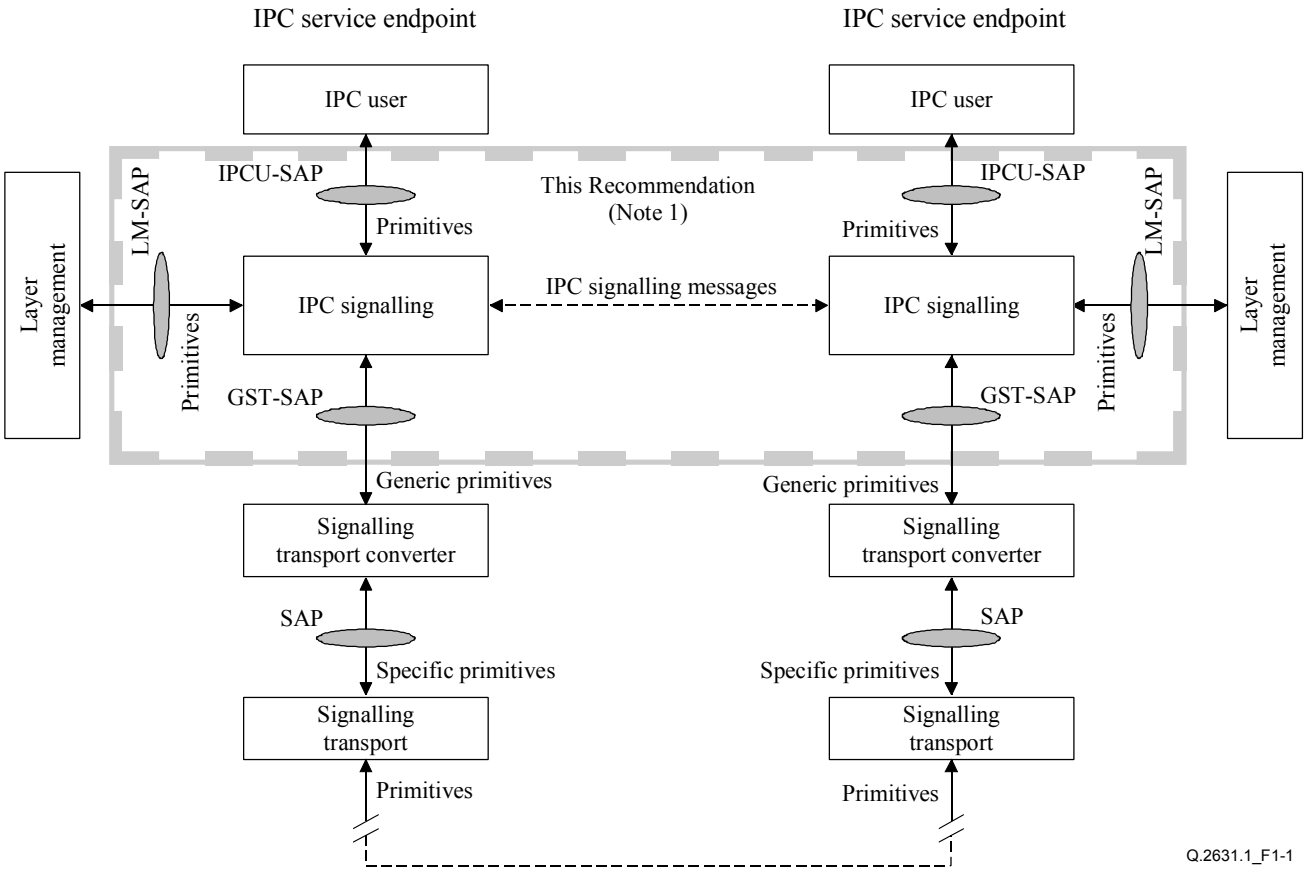
1 Scope

This Recommendation describes the IP connection control signalling protocol that supports the dynamic establishment, modification and release of individual IP connections. It also describes the maintenance procedures, the framework of the protocol, and the interactions between an IPC signalling entity and:

- the signalling protocol user;
- a signalling transport converter; and
- layer management.

The scope of this Recommendation is illustrated in Figure 1-1. The IPC signalling protocol can be deployed over a range of signalling transport protocol stacks.

This Recommendation is based on the requirements defined in ITU-T Technical Report TRQ.2415 [25] "*Signalling requirements for IP connection control in radio access networks Capability Set 1*".



NOTE 1 – The entities and Service Access Points (SAP) bounded by the grey broken line indicate the extent of the definitions specified in this Recommendation.

Figure 1-1/Q.2631.1 – Functional architecture of IPC signalling

2 References

2.1 Normative references

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

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

[2] ITU-T Recommendation X.210 (1993), *Information technology – Open Systems Interconnection – Basic Reference Model: Conventions for the definition of OSI services*.

[3] ITU-T Recommendation Q.2150.0 (2001), *Generic signalling transport service*.

[4] IETF RFC 791 (1981), *Internet Protocol*.

[5] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[6] IETF RFC 768 (1980), *User Datagram Protocol*.

[7] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[8] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[9] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

[10] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behaviour)*.

[11] IETF RFC 3513 (2003), *Internet Protocol Version 6 (IPv6) Addressing Architecture*.

[12] ITU-T Recommendation Q.850 (1998), *Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part*.

[13] ITU-T Recommendation Q.2610 (1999), *Usage of cause and location in B-ISDN user part and DSS2*.

[14] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.

[15] ITU-T Recommendation X.213 (2001), *Information Technology – Open Systems Interconnection – Network service definition*.

[16] ITU-T Recommendation Q.542 (1993), *Digital exchange design objectives – Operations and maintenance*.

[17] ITU-T Recommendation Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

2.2 Informative references

[20] ITU-T Recommendation Q.2630.1 (1999), *AAL type 2 signalling protocol – Capability Set 1*.

[21] ITU-T Recommendation Q.2630.2 (2000), *AAL type 2 signalling protocol – Capability Set 2*.

[22] ITU-T Recommendation Q.2150.1 (2001), *Signalling transport converter on MTP3 and MTP3b*.

[23] ITU-T Recommendation Q.2150.2 (2001), *Signalling Transport Converter on SSCOP and SSCOPMCE*.

[24] ITU-T Recommendation Q.2150.3 (2002), *Signalling Transport Converter on SCTP*.

[25] ITU-T Q-series Recommendations – Supplement 43 (2003), *Technical Report TRQ.2415: Transport control signalling requirements – Signalling requirements for IP connection control in radio access networks Capability Set 1*.

[26] ITU-T Q-series Recommendations – Supplement 44 (2003), *Technical Report TRQ.2800: Transport control signalling requirements – Signalling requirements for AAL type 2 to IP interworking, Capability Set 1*.

[27] IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

[28] 3GPP TS 25.414, *3rd Generation Partnership Project, Technical Specification Group Radio Access Network, UTRAN Iu interface data transport and transport signalling (Release 5)*.

[29] 3GPP TS 25.426, *3rd Generation Partnership Project, Technical Specification Group Radio Access Network, UTRAN Iur and Iub interface data transport & transport signalling for DCH data streams (Release 5)*.

3 Definitions

This Recommendation is based upon the concepts developed in ITU-T Recs X.200 [1] and X.210 [2].

In addition, this Recommendation defines the following terms:

3.1 IP connection: The logical user plane communication facility between two IPC nodes, which is controlled by the IPC signalling protocol. An IP connection is designated by a pair of IP address/port number combinations.

3.2 IPC node: A physical entity that contains an IPC signalling entity.

3.3 IPC user: The user of the IPC signalling protocol. An IPC user resides at an IPC service endpoint.

3.4 IPC signalling protocol: Control plane functions for establishing, modifying and releasing IP connections and the maintenance functions associated with the IPC signalling.

3.5 IPC signalling transport: A facility for carrying IPC signalling messages.

3.6 IPC signalling endpoint: The termination point of IPC signalling transport.

3.7 IPC service endpoint: A functional entity which includes the IPC signalling endpoint and the IPC user.

3.8 IP transfer capability: Information that describes the attributes of the IP connection.

3.9 IP transport type: Information that describes the IP transport protocol stack used for the IP connection.

3.10 field: Information carried in a parameter in a message. A field can have fixed or variable length data.

3.11 generic signalling transport: The function that enables an IPC signalling entity to communicate with a peer IPC signalling entity independently of the underlying signalling transport.

3.12 local IP address: IP address to be used by the peer IPC node to direct the user traffic.

3.13 local UDP port number: UDP port number to be used by the peer IPC node to direct the user traffic.

3.14 parameter: Information carried in a message. A parameter has a fixed, defined set of fields.

3.15 signalling association: A signalling capability that exists between two adjacent IPC nodes to control the IP connections. There may be one or more signalling associations between two adjacent IPC nodes.

3.16 signalling transport: A signalling link or network that connects two IPC nodes.

3.17 signalling transport converter: A function that converts the services provided by a particular signalling transport to the services required by the generic signalling transport.

3.18 subfield: The smallest unit of information in a field that has its own functional meaning.

4 Abbreviations

This Recommendation uses the following abbreviations:

ACC	Automatic Congestion Control
ANI	Adjacent IPC Node Identifier
CAU	Cause Parameter
CFN	ConFusioN message
DEA	Destination Endpoint Address
DEAE	Destination Endpoint E.164 Address
DEAX	Destination Endpoint X.213 Address
DS	Differentiated Services
DSAID	Destination Signalling Association Identifier
DSCP	Differentiated Services Code Point
ECF	Establish Confirm Message
ERQ	Establish Request Message
GST	Generic Signalling Transport
ID	Identifier
IP	Internet Protocol
IPC	IP Connection Control
IPCU	IPC User
IPQoS	IP Quality of Service
IPTA	IP Transport Sink Address
IPTT	IP Transport Type
LM	Layer Management
LSB	Least Significant Bit
M	Mandatory
MOA	Modification Acknowledge message

MOD	Modification Request message
MOR	Modification Reject message
MSB	Most Significant Bit
MSTC	Modify Support for Transfer Capability
O	Optional
OSAID	Originating Signalling Association Identifier
PHB	Per-Hop forwarding Behaviour
PTC	Preferred Transfer Capability
PTC-DBW	Dedicated Bandwidth Preferred Transfer Capability
PTC-SBW	Statistical Bandwidth Preferred Transfer Capability
QoS	Quality of Service
REL	Release Request Message
RES	Reset Request Message
RLC	Release Confirm Message
RSC	Reset Confirm Message
RTP	Real-Time Protocol
SAID	Signalling Association Identifier
SAP	Service Access Point
SDU	Service Data Unit
STC	Signalling Transport Converter
SUGR	Served User Generated Reference
SUT	Served User Transport
TC	Transfer Capability
TC-DBW	Dedicated Bandwidth Transfer Capability
TCI	Test Connection Indication
TC-SBW	Statistical Bandwidth Transfer Capability
UDP	User Datagram Protocol

5 General framework of the IPC signalling protocol

The IP connection control signalling protocol provides the signalling capability to establish, modify and release virtual connections in an IP environment. These services are accessible via the IPC User Service Access Point (IPCU-SAP).

The IPC signalling protocol also provides maintenance functions associated with the IPC signalling. These functions are accessible via the Layer Management Service Access Point (LM-SAP).

Two peer IPC signalling entities rely on the generic signalling transport service to provide assured data transfer between them and service availability indications. These services are accessible via the Generic Signalling Transport Service Access Point (GST-SAP).

NOTE – Primitives over the IPCU-SAP, GST-SAP and LM-SAP are used for descriptive purpose only. They do not imply a specific implementation.

Both peer IPC signalling entities provide the same set of services.

IPC signalling messages are analysed only in IPC service endpoints (see Figure 1-1).

IPC signalling messages are exchanged between peer protocol entities using the generic signalling transport service. The IPC signalling is independent of the signalling transport, although an assured data transport is required and a message size limit applies. The generic signalling transport service used is defined in ITU-T Rec. Q.2150.0 [3]. To adapt the generic signalling transport services to a specific signalling transport service, a signalling transport converter may be needed. The specification of signalling transport converters is beyond the scope of this Recommendation (see ITU-T Recs Q.2150.1 [22], Q.2150.2 [23], and Q.2150.3 [24]).

5.1 Interface between the IPC signalling entity and the IPC user

5.1.1 Service provided by the IPC signalling entity

The IPC signalling entity provides the following services to the IPC user across the IPCU-SAP:

- Establishment of IP connections;
- Release of IP connections; and
- Modification of IP connection resources.

The IPC signalling entity is independent of the IPC user.

5.1.2 Primitives between IPC signalling entity and the IPC user

The IPCU-SAP primitives are used:

1) by the originating IPC user to initiate IP connection establishment and by either of the IPC users to initiate the release of a connection;
2) by the terminating IPC signalling entity to indicate an incoming IP connection establishment request to the terminating IPC user and by either of the IPC signalling entities to notify its corresponding IPC user of the release of a connection;
3) by either IPC user to initiate an IP connection resource modification and by the modification terminating IPC user to respond to a modification request;
4) by either IPC signalling entity to indicate a modification of the IP connection resource to its corresponding IPC user and to notify the modification initiating IPC user of the successful or unsuccessful modification.

NOTE – When sending a primitive between the signalling protocol and its user, the primitive needs to be associated with a particular IP connection instance. The mechanism used for this binding is considered to be an implementation detail and, therefore, is outside the scope of this Recommendation.

The services are provided through the transfer of primitives, which are summarized in Table 5-1, and are defined after the table.

The IPC user passes information in parameters in the primitives. Some of those parameters are mandatory and some are optional; the appropriate usage of the parameters is described in clause 8.

Table 5-1/Q.2631.1 – Primitives and parameters exchanged between the IPC signalling entity and the IPC user

Primitive	Type			
Generic name	Request	Indication	Response	Confirm
ESTABLISH	DEA, SUGR, SUT, MSTC, TC, PTC, IPQOS, IPTT, CP	SUGR, SUT, MSTC, TC, PTC, IPQOS, IPTT, CP	MSTC	MSTC
RELEASE	Cause	Cause	Not defined	Cause
MODIFY	TC	TC	–	–
MODIFY-REJECT	Not defined	Not defined	Cause	Cause
– This primitive has no parameters.				

a) **ESTABLISH.request**:

This primitive is used by the originating IPC user to initiate the establishment of a new IP connection and optionally request the capability for subsequent modification to be performed on this IP connection.

b) **ESTABLISH.indication**:

This primitive is used by the terminating IPC signalling entity to indicate an incoming IP connection establishment request to the terminating IPC user and optionally indicate that subsequent modification may be performed on this IP connection.

c) **ESTABLISH.response**:

This primitive is used by the terminating IPC user to indicate to the terminating IPC signalling entity that the establishment request has been successful.

d) **ESTABLISH.confirm**:

This primitive is used by the originating IPC signalling entity to indicate to the originating IPC user that the IP connection (which was previously requested by the originating IPC user) has successfully been established and optionally indicate that the established connection is capable of subsequent modification.

e) **RELEASE.request**:

This primitive is used by the IPC user to initiate clearing of an IP connection.

f) **RELEASE.indication**:

This primitive is used by the IPC signalling entity to indicate that an IP connection has been released.

g) **RELEASE.confirm**:

This primitive is used by the originating IPC signalling entity to indicate to the originating IPC user that an establishment request has been unsuccessful.

h) **MODIFY.request**:

This primitive is used by either IPC user to initiate the modification of the IP connection resource.

i) **MODIFY.indication**:

This primitive is used by the modify receiving IPC signalling entity to indicate that modification of the IP connection resource has been requested.

j) **MODIFY.response**:

This primitive is used by the modify receiving IPC user to indicate to the IPC signalling entity that the modification request has been successful.

k) **MODIFY.confirm**:

This primitive is used by either IPC signalling entity to indicate that the IP connection resource modification (which was previously requested by the IPC user) has successfully been performed

l) **MODIFY-REJECT.response**:

This primitive is used by the modify receiving IPC user to indicate to the IPC signalling entity that the IP connection resource modification has been rejected.

m) **MODIFY-REJECT.confirm**:

This primitive is used by the modify sending IPC signalling entity to indicate that the IP connection resource modification (which was previously requested by the IPC user) has been rejected.

5.1.3 Parameters between IPC signalling entity and the IPC user

a) **Destination Endpoint Address (DEA)**

This parameter carries the endpoint address of the destination. It can have the form of an E.164 [14] address or an X.213 [15] address, and is transported unmodified to the destination IPC user.

b) **Served User Generated Reference (SUGR)**

This parameter carries a reference provided by the originating IPC user and this reference is transported unmodified to the destination IPC user.

c) **Served User Transport (SUT)**

This parameter carries the user data that is transported unmodified to the destination IPC user.

d) **Transfer Capability (TC)**

This parameter gives an indication of the resources required for the IP connection. This parameter can have the form of either:

- Dedicated Bandwidth Transfer Capability (see ITU-T Rec. Y.1221 [17]); or
- Statistical Bandwidth Transfer Capability (see ITU-T Rec. Y.1221 [17]).

e) **Cause**

This parameter describes the reason for the release of the IP connection. It also may indicate the reason why an IP connection could not be established or why a modification of an IP connection was rejected.

f) **Modify Support for Transfer Capability (MSTC)**

This parameter gives an indication that the transfer capability of the IP connection may need to be modified during the lifetime of the IP connection (ESTABLISH.request) or is permitted to be modified (ESTABLISH.indication and ESTABLISH.confirm).

g) **Preferred Transfer Capability (PTC)**

This parameter gives an indication that the Transfer Capability shall be set as indicated in this parameter if the modification of the Transfer Capability is permitted. This parameter can have the form of either:

- Dedicated Bandwidth Transfer Capability (see ITU-T Rec. Y.1221 [17]); or
- Statistical Bandwidth Transfer Capability (see ITU-T Rec. Y.1221 [17]).

h) **Quality of Service (IPQoS)**

This parameter indicates a request for an IP connection with a specified Quality of Service.

i) **IP Transport Type (IPTT)**

This parameter indicates a request for an IP connection with a specified IP transport protocol stack.

j) **Connection Priority (CP)**

This parameter carries information to indicate the priority level of the connection request.

5.2 Interface between the IPC signalling entity and the generic signalling transport

5.2.1 Service provided by the generic signalling transport service

The generic signalling transport service is specified in ITU-T Rec. Q.2150.0 [3]. For convenience, a summary of the primitives for accessing the service is reproduced in Table 5-2. In the event of any difference between this table and the definitions in ITU-T Rec. Q.2150.0 [3], the definitions in ITU-T Rec. Q.2150.0 [3] take precedence.

Table 5-2/Q.2631.1 – Primitives and parameters of the generic signalling transport sublayer

Primitive	Type			
Generic name	Request	Indication	Response	Confirm
START-INFO	not defined	Max_Length CIC_Control	not defined	not defined
IN-SERVICE	not defined	Level	not defined	not defined
OUT-OF-SERVICE	not defined	(Note 1)	not defined	not defined
CONGESTION	not defined	Level	not defined	not defined
TRANSFER	Sequence Control STC User Data Priority (Note 2)	STC User Data Priority (Note 2)	not defined	not defined

NOTE 1 – This primitive has no parameters.

NOTE 2 – This parameter is a national option (and the use of this parameter is not supported by all signalling transports).

On the establishment of a signalling transport converter entity and the associated signalling transport converter user entity, for example at power up, the initial conditions are the same as if an OUT-OF-SERVICE.indication primitive had been conveyed across this SAP. Also, at this time the START-INFO.indication is sent to the signalling entity.

NOTE – The CIC_Control parameter of the START-INFO.indication is ignored by the IPC signalling entity.

5.2.2 State transition diagram for sequences of primitives of the generic signalling transport service

This clause defines the constraints on the sequences in which the primitives may occur at the layer boundaries of the generic signalling transport service. The sequences are related to the states at one generic signalling transport endpoint between the generic signalling transport service provider and its user. The possible overall sequences of primitives are shown in the state transition diagram, Figure 5-1.

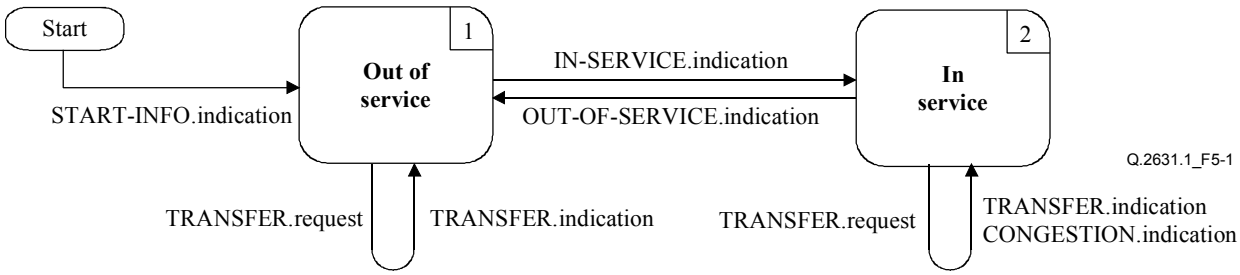


Figure 5-1/Q.2631.1 – State transition diagram for sequences of primitives between the GST and its user

This model assumes that a request primitive is never issued at the same time as an indication primitive. The model also assumes that the primitives are serviced immediately and in zero time.

5.3 Interface between the IPC signalling entity and layer management

5.3.1 Service provided by layer management

This interface provides the internal interface to the network management system.

5.3.2 Primitives between IPC signalling entity and layer management

The primitives are summarized in Table 5-3 and are defined after the table.

Table 5-3/Q.2631.1 – Primitives and parameters exchanged between the IPC signalling entities and layer management

Primitive	Type			
Generic name	Request	Indication	Response	Confirm
RESET	ANI, IPTA	ANI, IPTA	Not defined	–
STOP-RESET	ANI, IPTA	Not defined	Not defined	Not defined
ERROR	Not defined	ANI, IPTA, Cause	Not defined	Not defined
– This primitive has no parameters.				

NOTE – When sending a primitive between the IPC signalling entity and layer management, the primitive needs to be associated with a particular management action instance. The mechanism used for this binding is considered to be an implementation detail and, therefore, is outside the scope of this Recommendation.

a) **RESET.request**:

A primitive to request either IPC signalling entity to reset a particular IP connection, or all IP connections associated with a signalling association to the "Idle" state, and to indicate this to the peer IPC signalling entity.

b) **RESET.indication**:

A primitive indicating that the IPC signalling entity has reset a particular IP connection, or all IP connections associated with a signalling association to the "Idle" state on the request of the peer IPC signalling entity.

c) **RESET.confirm**:

A primitive indicating that the IPC signalling entity has successfully informed the peer IPC signalling entity of the resetting of a particular IP connection, or all IP connections associated with a signalling association.

d) **STOP-RESET.request**:

A primitive to request the IPC signalling entity to stop a reset procedure.

e) **ERROR.indication**:

A primitive to indicate any operational errors in the IPC signalling procedures.

5.3.3 Parameters between IPC signalling entity and layer management

a) **IP Transport Address (IPTA)**

This parameter allows for the identification of:

i) all IP connections associated with a signalling association; or

ii) a particular IP connection.

b) **Cause**

This parameter gives the reason of an operational error.

c) **Adjacent IPC Node Identifier (ANI)**

This parameter is used to unambiguously indicate an adjacent IPC node.

6 Forward and backward compatibility

The compatibility mechanism remains unchanged for all capability sets and/or subsets of the IPC protocol defined in this Recommendation. It is based on forward compatibility information associated with all signalling information.

The compatibility method eases the network operation, for example:

- For the typical case of an IPC signalling protocol mismatch during a network upgrading.
- To interconnect two networks on a different functional level.
- For networks using a different subset of the same IPC protocol, etc.

NOTE – An IPC node may be at a different functional level due to having implemented a different capability set or another subset of the protocol specified in this Recommendation.

The forward compatibility mechanism specified in 6.2 and 8.1 applies to this and future capability sets of this Recommendation.

6.1 Backward compatibility rules

Compatible interworking between IPC protocol capability sets should be optimized by adhering to the following rules when specifying a new capability set (release):

1) Existing protocol elements, i.e., procedures, messages, parameters and subfield values, should not be changed unless a protocol error needs to be corrected, or it becomes necessary to change the operation of the service that is being supported by the protocol.
2) The semantics of a message, a parameter, or of a field and subfield within a parameter should not be changed.
3) Established rules for formatting and encoding messages and parameters should not be modified.

6.2 Forward compatibility mechanism

Compatibility between this and future capability sets will be guaranteed, in the sense that any two capability sets can be interconnected directly with each other, if the following requirements are fulfilled:

i) *Protocol compatibility*

Connections between any two IPC protocols do not fail for the reason of not satisfying protocol requirements.

ii) *Service and functional compatibility*

This feature may be considered as compatibility typically between originating and destination IPC nodes.

iii) *Resource control and management compatibility*

For these functions, at least a backward notification is needed, if correct handling is not possible.

7 Format and coding of the IPC signalling protocol

7.1 Coding conventions for the IPC signalling protocol

7.1.1 Principles

The following principles shall apply for the coding of the IPC signalling protocol:

a) The order of coding of messages shall consist of "destination signalling association identifier", "message identifier", "message compatibility", and any parameters.

b) Messages shall carry zero or more parameters.

c) The sequence of parameters is unconstrained.

d) The order of coding of parameters shall consist of "parameter identifier", "parameter compatibility", "parameter length", and any fields.

e) Parameters shall carry zero or more fields.

f) A parameter shall always consist of the same sequence of fields.

g) If new fields need to be added to a parameter or the length of a fixed size field needs to be changed, the modifications shall be carried in a new parameter (different parameter identifier); the existing parameter shall remain unchanged.

h) Any sequence of fixed size fields and variable size fields is permissible.

i) Fixed length fields shall consist of the "field" only; no length is indicated.

j) Variable length fields shall consist of "field length" and "field".

k) Fields shall be multiples of one octet.

l) Fields are composed of one or more subfields.

m) Reserved subfields shall be coded all zeroes and need not be interpreted by the receiver.

n) If there is no information to be carried in a variable size field, its length shall be set to zero, i.e., only the field length octet will be present.

o) If there is no information to be carried in a fixed size field, its content shall be set to zero in all octets.

p) The presence or the interpretation of a field shall not depend on the value of a field in another parameter.

Consistent with the above coding principles, it is further specified that:

- The message length shall allow for lengths of up to 4000 octets.
- The parameter length shall allow for lengths of up to 255 octets.

7.1.2 General format of messages

The general format of a message is shown in Table 7-1.

NOTE – No "message length" needs to be carried in the message itself; the length of information passed via a primitive implicitly defines its length and the assured data transfer assures that no octets are lost or gained in transport.

Table 7-1/Q.2631.1 – IPC message format

	8	7	6	5	4	3	2	1	Octet
Header	Destination signalling association identifier								4
	Message identifier								1
	Message compatibility								1
Payload	Parameters								

The message header consists of the destination signalling association identifier field, the message identifier field, and the message compatibility field. The destination signalling association identifier field is coded the same as the signalling association identifier field (see 7.4.2), the coding of the message identifier field is specified in 7.2.1, and the message compatibility field is coded the same as the compatibility field (see 7.4.1).

The message payload consists of zero, one, or more parameters.

7.1.2.1 Bit coding rules

When a field is contained within a single octet, the lowest bit number of the field represents the lowest order value.

When a field spans more than one octet, the order of bit values within each octet progressively decreases as the octet number increases; the lowest bit number associated with the field represents the lowest order value.

7.1.3 General format of parameters

The general format of a parameter is shown in Table 7-2.

Table 7-2/Q.2631.1 – IPC parameter format

	8	7	6	5	4	3	2	1	Octet
Header	Parameter identifier								1
	Parameter compatibility								1
	Parameter length								1
Payload	Fields								

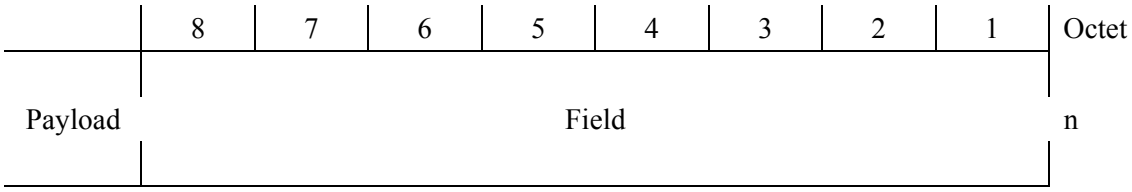
The coding of the parameter identifier field is specified in Table 7-7 and the parameter compatibility field is coded as a compatibility field (see 7.4.1). The coding of the parameter length is a binary value indicating the number of octets in the parameter payload, i.e., the count does not include the octets in the parameter header.

Each parameter has a defined number of fields of defined type and in a particular order.

7.1.4 General format of fixed length fields

The general format of a fixed length field is shown in Table 7-3.

Table 7-3/Q.2631.1 – IPC field – fixed length format

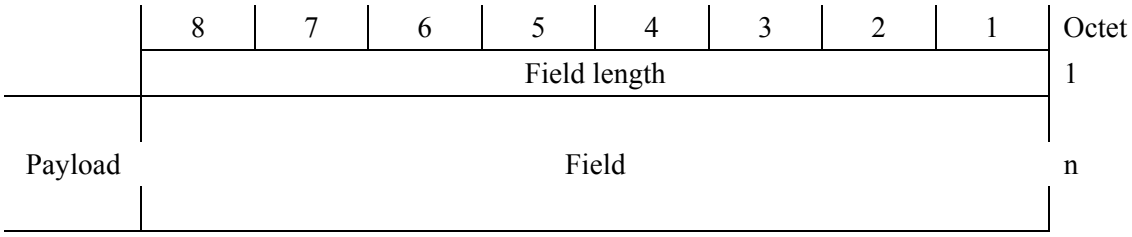


The field type is determined by the location of the field in the particular parameter.

7.1.5 General format of variable length fields

The general format of a variable length field is shown in Table 7-4.

Table 7-4/Q.2631.1 – IPC field – variable length format



The coding of the field length is a binary value indicating the number of octets in the field payload, i.e., the count does not include the field length octet.

The field type is determined by the location of the field in the particular parameter.

7.2 Format and coding of the IPC signalling protocol messages

7.2.1 IPC signalling protocol messages

The IPC signalling protocol messages and their message identifiers are shown in Table 7-5.

Table 7-5/Q.2631.1 – IPC messages and the coding of the message identifiers

Message	Acronym	Message Identifier
Confusion	CFN	0 0 0 0 0 0 1 1
Establish Confirm	ECF	0 0 0 0 0 1 0 0
Establish Request	ERQ	0 0 0 0 0 1 0 1
Modify Acknowledge	MOA	0 0 0 0 1 1 0 0
Modify Reject	MOR	0 0 0 0 1 1 0 1
Modify Request	MOD	0 0 0 0 1 1 1 0
Release Confirm	RLC	0 0 0 0 0 1 1 0
Release Request	REL	0 0 0 0 0 1 1 1
Reset Confirm	RSC	0 0 0 0 1 0 0 0
Reset Request	RES	0 0 0 0 1 0 0 1

7.2.2 Parameters of the IPC signalling protocol messages

The parameters of the IPC signalling protocol messages are shown in Table 7-6. The indications of "mandatory" and "optional" are for information only. The authoritative definition is given in clause 8. If any difference between the indications in this clause and the definitions in clause 8 exists, the definitions in clause 8 take precedence.

Multiple presence of the same parameter in a single message is not permitted.

Table 7-6/Q.2631.1 – Parameters of the IPC signalling protocol messages *(part 1 of 2)*

Parameter	Message						
	ERQ	**ECF**	**REL**	**RLC**	**MOD**	**MOA**	**MOR**
Automatic Congestion Control	–	–	O	O	–	–	–
Cause	–	–	M	(Note 1)	–	–	M
Connection Priority	O	–	–	–	–	–	–
Dedicated Bandwidth Preferred Transfer Capability	(Note 2)	–	–	–	–	–	–
Dedicated Bandwidth Transfer Capability	(Note 3)	–	–	–	(Note 4)	–	–
Destination Endpoint E.164 Address	(Note 5)	–	–	–	–	–	–
Destination Endpoint X.213 Address	(Note 5)	–	–	–	–	–	–
Destination Signalling Association Identifier (Note 6)	(Note 7)	M	M	M	M	M	M
IP QoS	O	–	–	–	–	–	–
IP Transport Sink Address	M	M	–	–	–	–	–
IP Transport Type	O	–	–	–	–	–	–
Modify Support for Transfer Capability	O	O	–	–	–	–	–
Originating Signalling Association Identifier	M	M	–	–	–	–	–
Served User Generated Reference	O	–	–	–	–	–	–
Served User Transport	O	–	–	–	–	–	–
Statistical Bandwidth Preferred Transfer Capability	(Note 2)	–	–	–	–	–	–
Statistical Bandwidth Transfer Capability	(Note 3)	–	–	–	(Note 4)	–	–

M Mandatory parameter

O Optional parameter

– Parameter not present

NOTE 1 – The "Cause" parameter is present in the Release Confirm message if:

a) the RLC is used to reject a connection establishment; or

b) the cause reports unrecognized information received in the REL message.

NOTE 2 – This parameter may only be included if "Modify Support for Transfer Capability" is included. At most, one of these parameters is present in an instance of the message. If present, it must refer to the same transfer capability as the Transfer Capability parameter present in the same Establish Request message.

NOTE 3 – Exactly one of these parameters must be present in an instance of the message.

NOTE 4 – Exactly one of these parameters is present in an instance of the message and only the same parameter that was present in the Establish Request message may be present.

NOTE 5 – Exactly one of these parameters is present in an instance of the message

NOTE 6 – This row designates the Destination Signalling Association Identifier field in the message header.

NOTE 7 – The Destination Signalling Association Identifier field contains the value "unknown".

Table 7-6/Q.2631.1 – Parameters of the IPC signalling protocol messages *(part 2 of 2)*

Parameter	Message		
	RES	**RSC**	**CFN**
Cause	–	(Note 1)	M
Destination Signalling Association Identifier (Note 2)	(Note 3)	M	M
IP Transport Sink Address	M	–	–
Originating Signalling Association Identifier	M	–	–

M Mandatory parameter

O Optional parameter

– Parameter not present

NOTE 1 – The "Cause" parameter is present only if the cause reports unrecognized information received.

NOTE 2 – This row designates the Destination Signalling Association Identifier field in the message header.

NOTE 3 – The Destination Signalling Association Identifier field contains the value "unknown".

The identifiers of the IPC message parameters are defined in Table 7-7.

Table 7-7/Q.2631.1 – Identifiers of the IPC message parameters

IPC parameter	Ref.	Acronym	Identifier
Automatic Congestion Control	7.3.1	ACC	0 0 0 1 1 0 0 1
Cause	7.3.2	CAU	0 0 0 0 0 0 0 1
Connection Priority	7.3.3	CP	0 0 0 1 1 0 1 0
Dedicated Bandwidth Preferred Transfer Capability	7.3.4	PTC-DBW	0 0 0 1 0 0 0 1
Dedicated Bandwidth Transfer Capability	7.3.5	TC-DBW	0 0 0 0 0 1 0 1
Destination Endpoint E.164 Address	7.3.6	DEAE	0 0 0 0 0 0 1 1
Destination Endpoint X.213 Address	7.3.7	DEAX	0 0 0 0 0 1 0 0
IP QoS	7.3.8	IPQOS	0 0 0 1 0 0 0 0
IP Transport Sink Address	7.3.9	IPTA	0 0 0 0 0 0 1 0
IP Transport Type	7.3.10	IPTT	0 0 1 0 0 0 0 0
Modify Support for Transfer Capability	7.3.11	MSTC	0 0 0 0 1 1 1 0
Originating Signalling Association Identifier	7.3.12	OSAID	0 0 0 0 0 1 1 0
Served User Generated Reference	7.3.13	SUGR	0 0 0 0 0 1 1 1
Served User Transport	7.3.14	SUT	0 0 0 0 1 0 0 0
Statistical Bandwidth Preferred Transfer Capability	7.3.15	PTC-SBW	0 0 1 0 0 0 1 1
Statistical Bandwidth Transfer Capability	7.3.16	TC-SBW	0 0 1 0 0 0 0 1

7.3 Parameter specification of the IPC signalling protocol messages

7.3.1 Automatic Congestion Control

The sequence of fields in the Automatic Congestion Control parameter is shown in Table 7-8.

Table 7-8/Q.2631.1 – Sequence of fields in the Automatic Congestion Control parameter

Field No.	Field	Ref.
1	IPC Node Automatic Congestion Level	7.4.3

7.3.2 Cause

The sequence of fields in the Cause parameter is shown in Table 7-9.

Table 7-9/Q.2631.1 – Sequence of fields in the Cause parameter

Field No.	Field	Ref.
1	Cause Value	7.4.4
2	Diagnostics	7.4.5

7.3.3 Connection Priority

The sequence of fields in the Connection Priority parameter is shown in Table 7-10.

Table 7-10/Q.2631.1 – Sequence of fields in the Connection Priority parameter

Field No.	Field	Ref.
1	Priority	7.4.6

7.3.4 Dedicated Bandwidth Preferred Transfer Capability

The sequence of fields in the Dedicated Bandwidth Preferred Transfer Capability parameter is shown in Table 7-11.

Table 7-11/Q.2631.1 – Sequence of fields in the Dedicated Bandwidth Preferred Transfer Capability parameter

Field No.	Field	Ref.
1	Peak bit rate	Note 1
2	Peak token bucket size associated with the Peak bit rate	Note 2
3	Maximum allowed packet size	Note 3
NOTE 1 – This field is coded as a Bit Rate field (see 7.4.11). NOTE 2 – This field is coded as a Token Bucket Size field (see 7.4.18). NOTE 3 – This field is coded as a Packet Size field (see 7.4.12)		

7.3.5 Dedicated Bandwidth Transfer Capability

The sequence of fields in the Dedicated Bandwidth Transfer Capability parameter is shown in Table 7-12.

Table 7-12/Q.2631.1 – Sequence of fields in the Dedicated Bandwidth Transfer Capability parameter

Field No.	Field	Ref.
1	Peak bit rate	Note 1
2	Peak token bucket size associated with the Peak bit rate	Note 2
3	Maximum allowed packet size	Note 3
NOTE 1 – This field is coded as a Bit Rate field (see 7.4.11). NOTE 2 – This field is coded as a Token Bucket Size field (see 7.4.18). NOTE 3 – This field is coded as a Packet Size field (see 7.4.12).		

7.3.6 Destination Endpoint E.164 Address

The sequence of fields in the Destination Endpoint E.164 Address parameter is shown in Table 7-13.

Table 7-13/Q.2631.1 – Sequence of fields in the Destination Endpoint E.164 Address parameter

Field No.	Field	Ref.
1	Nature of Address	7.4.7
2	E.164 Address	7.4.8

7.3.7 Destination Endpoint X.213 Address

The sequence of fields in the Destination Endpoint X.213 Address parameter is shown in Table 7-14.

Table 7-14/Q.2631.1 – Sequence of fields in the Destination Endpoint X.213 Address parameter

Field No.	Field	Ref.
1	X.213 Address	7.4.9

7.3.8 IP QoS

The sequence of fields in the IP QoS parameter is shown in Table 7-15.

Table 7-15/Q.2631.1 – Sequence of fields in the IP QoS parameter

Field No.	Field	Ref.
1	IP QoS Codepoint	7.4.10

7.3.9 IP Transport Sink Address

The sequence of fields in the IP transport address parameter is shown in Table 7-16.

Table 7-16/Q.2631.1 – Sequence of fields in the IP Transport Sink Address parameter

Field No.	Field	Ref.
1	UDP Port Number	7.4.13
2	IP Address	7.4.14

IP address	UDP port number	Meaning
Null	ignored	All IP connections toward an adjacent IPC node associated with an IPC signalling association
Value	Value	The combination of both values uniquely identifies an IP connection between adjacent IPC nodes

A "Null" value of the IP address is never regarded as a valid IP address in an IP network. It is only used to identify all IP connections associated within one IPC signalling association.

7.3.10 IP Transport Type

The sequence of fields in the IP Transport Type parameter is shown in Table 7-17.

Table 7-17/Q.2631.1 – Sequence of fields in the IP Transport Type parameter

Field No.	Field	Ref.
1	IP Transport Protocol Identifier	7.4.15

7.3.11 Modify Support for Transfer Capability

The Modify Support for Transfer Capability parameter has no fields, i.e., the parameter length is always zero.

7.3.12 Originating Signalling Association Identifier

The sequence of fields in the Originating Signalling Association Identifier parameter is shown in Table 7-18.

Table 7-18/Q.2631.1 – Sequence of fields in the Originating Signalling Association Identifier parameter

Field No.	Field	Ref.
1	Originating Signalling Association	Note
NOTE – This field is coded as a Signalling Association Identifier field (see 7.4.2).		

7.3.13 Served User Generated Reference

The sequence of fields in the Served User Generated Reference parameter is shown in Table 7-19.

Table 7-19/Q.2631.1 – Sequence of fields in the Served User Generated Reference parameter

Field No.	Field	Ref.
1	Served User Generated Reference	7.4.16

7.3.14 Served User Transport

The sequence of fields in the Served User Transport parameter is shown in Table 7-20.

Table 7-20/Q.2631.1 – Sequence of fields in the Served User Transport parameter

Field No.	Field	Ref.
1	Served User Transport	7.4.17

7.3.15 Statistical Bandwidth Preferred Transfer Capability

The sequence of fields in the Statistical Bandwidth Preferred Transfer Capability parameter is shown in Table 7-21.

Table 7-21/Q.2631.1 – Sequence of fields in the Statistical Bandwidth Preferred Transfer Capability parameter

Field No.	Field	Ref.
1	Peak bit rate	Note 1
2	Peak token bucket size associated with the Peak bit rate	Note 2
3	Sustainable bit rate	Note 1
4	Sustainable token bucket size associated with the Sustainable bit rate	Note 2
5	Maximum allowed packet size	Note 3
NOTE 1 – This field is coded as a Bit Rate field (see 7.4.11). NOTE 2 – This field is coded as a Token Bucket Size field (see 7.4.18). NOTE 3 – This field is coded as a Packet Size field (see 7.4.12).		

7.3.16 Statistical Bandwidth Transfer Capability

The sequence of fields in the Statistical Bandwidth Transfer Capability parameter is shown in Table 7-22.

Table 7-22/Q.2631.1 – Sequence of fields in the Statistical Bandwidth Transfer Capability parameter

Field No.	Field	Ref.
1	Peak bit rate	Note 1
2	Peak token bucket size associated with the Peak bit rate	Note 2
3	Sustainable bit rate	Note 1
4	Sustainable token bucket size associated with the Sustainable bit rate	Note 2
5	Maximum allowed packet size	Note 3
NOTE 1 – This field is coded as a Bit Rate field (see 7.4.11). NOTE 2 – This field is coded as a Token Bucket Size field (see 7.4.18). NOTE 3 – This field is coded as a Packet Size field (see 7.4.12).		

7.4 Field specification of the IPC signalling protocol parameters

7.4.1 Compatibility

The structure of the compatibility field is shown in Table 7-23; the field is a fixed size field of 1 octet.

Table 7-23/Q.2631.1 – Structure of the compatibility field

8	7	6	5	4	3	2	1	Octet
Reserved					Send notification indicator	Instruction indicator		1

The following codes are used in the subfields of the compatibility information field.

a) *Send notification indicator*

0 Do not send notification.

1 Send notification.

b) *Instruction indicator*

00 Reserved.

01 Discard parameter (see Note).

10 Discard message.

11 Release Connection.

NOTE – When used as message compatibility field, value "01" should not be used. If received, it is interpreted so as to discard the message.

7.4.2 Signalling association identifier

The structure of the Signalling Association Identifier field is shown in Table 7-24; the field is a fixed size field of 4 octets.

Table 7-24/Q.2631.1 – Structure of the signalling association identifier field

8	7	6	5	4	3	2	1	Octet
								1
								2
								3
								4

The coding is implementation dependent.

If the signalling association identifier is used as a destination signalling association identifier that is not known, the field is set to zero indicating the value "unknown".

If the signalling association identifier is used as an originating signalling association identifier, the value zero shall not be used.

7.4.3 IPC node automatic congestion level

The structure of the IPC node automatic congestion level field is shown in Table 7-25; the field is a fixed size field of 1 octet.

Table 7-25/Q.2631.1 – Structure of the IPC node automatic congestion level field

8	7	6	5	4	3	2	1	Octet
IPC node automatic congestion level codepoint								1

The IPC node automatic congestion level codepoint has the following meaning:

0000000 Spare

0000001 Congestion level 1 exceeded

0000010 Congestion level 2 exceeded

0000011 to 1111111 Spare

7.4.4 Cause value

The structure of the cause value field is shown in Table 7-26; the field is a fixed size field of 2 octets.

Table 7-26/Q.2631.1 – Structure of the cause value field

8	7	6	5	4	3	2	1	Octet
Reserved						Coding standard		1
Reserved	Cause							2

Coding standard

00 ITU-T standardized coding as described in ITU-T Recs Q.850 [12] and Q.2610 [13]

01 ISO/IEC standard (Note)

10 National standard (Note)

11 Standard defined for the network (either public of private) present on the network side of the interface (Note)

NOTE – These other coding standards should be used only when the parameter contents cannot be represented with the ITU-T standardized coding.

The procedures defined in clause 8 make use of ITU-T standardized codes described in ITU-T Recs Q.850 [12] and Q.2610 [13]. The codes are listed here for convenience. If there exists any difference in the names and codepoints of the following causes, the definitions in ITU-T Recs Q.850 [12] and Q.2610 [13] take precedence.

Code	Cause Description
1	Unallocated (unassigned) number
3	No route to destination
25	Exchange routing error
31	Normal, unspecified
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
47	Resource unavailable, unspecified
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
99	Information element/parameter non-existent or not implemented
100	Invalid information element contents
102	Recovery on timer expiry
110	Message with unrecognized parameter, discarded
111	Protocol error, unspecified

7.4.5 Diagnostics

The structure of the diagnostics field is shown in Table 7-27; the field is a variable size field.

Table 7-27/Q.2631.1 – Structure of the diagnostic field

8	7	6	5	4	3	2	1	Octet
Field length								1
								2
⋮ Diagnostic ⋮								
								n

The coding is specified in ITU-T Rec. Q.2610 [13] except when associated with one of the following causes:

– Message type non-existent or not implemented;

– Information element/parameter non-existent or not implemented; or

– Message with unrecognized parameter, discarded.

In these cases, the diagnostics field is shown in Table 7-28; the field is a variable size field.

Table 7-28/Q.2631.1 – Structure of the diagnostic field for compatibility causes

8	7	6	5	4	3	2	1	Octet
Field length								1
Message identifier								2
first			Parameter identifier					3
pair			Field number					4
second			Parameter identifier					5
pair			Field number					6
⋮								
last			Parameter identifier					
pair			Field number					n

The diagnostic field for compatibility always starts (after the field length) with an octet containing the copy of the message identifier (of the message that gave rise to a compatibility diagnostic) followed by 0 to 125 octet pairs each containing a parameter identifier and a field number. If the field number octet is zero, the whole parameter is designated.

7.4.6 Priority

The structure of the priority field is shown in Table 7-29; the field is a fixed size field of 1 octet.

Table 7-29/Q.2631.1 – Structure of the priority field

8	7	6	5	4	3	2	1	Octet
Reserved					Priority			1

The priority codepoint has the following meaning:

0 0 0 level 1 (highest)

0 0 1 level 2

0 1 0 level 3

0 1 1 level 4

1 0 0 level 5 (lowest)

1 0 1 to 1 1 1 reserved

7.4.7 Nature of address

The structure of the nature of address field is shown in Table 7-30; the field is a fixed size field of 1 octet.

Table 7-30/Q.2631.1 – Structure of the nature of address field

8	7	6	5	4	3	2	1	Octet
Reserved	Nature of address code							1

The nature of address code has the following meaning:

0000000 Spare

0000001 Subscriber number (national use)

0000010 Unknown (national use) (Note 1)

0000011 National (significant) number

0000100 International number

0000101 Network-specific number (national use) (Note 2)

0000110 to 1101111 Spare

1110000 to 1111110 Reserved for national use

1111111 Spare

NOTE 1 – This codepoint is used when the type of number is indicated using the digits in the E.164 [14] address field. The E.164 address field is organized according to the network dialling plan; e.g., prefix digits might be present; in addition, escape digits may also be present.

NOTE 2 – This codepoint is used to indicate an administration/service number specific to the serving network.

7.4.8 E.164 address

The structure of the E.164 [14] address field is shown in Table 7-31; the field is a variable size field.

Table 7-31/Q.2631.1 – Structure of the E.164 address field

8	7	6	5	4	3	2	1	Octet
Field length								1
Reserved				First hexadecimal digit of address ---- Last hexadecimal digit of address				2 n

7.4.9 X.213 address

The structure of the X.213 [15] address field is shown in Table 7-32; the field is a fixed size field of 20 octets.

Table 7-32/Q.2631.1 – Structure of the X.213 address field

8	7	6	5	4	3	2	1	Octet
NSAP								1
								20

7.4.10 IP QoS codepoint

The structure of the IP QoS codepoint field is shown in Table 7-33.

Table 7-33/Q.2631.1 – Structure of the IP QoS codepoint field

8	7	6	5	4	3	2	1	Octet
DSCP						Reserved		1

The IP QoS codepoint field accommodates the "Differentiated Services Codepoint (DSCP) Values" as specified in RFC 2474 [8], RFC 2597 [9], and RFC 3246 [10] with the following encoding:

000000 Background

000001 to 001001 Spare

001010 AF11

001011 to 010001 Spare

010010 AF21

010011 to 011001 Spare

011010 AF31

011011 Spare

011100 AF32

011101 Spare

011110 AF33

011111 to 101101 Spare

101110 EF

101111 to 111111 Spare

7.4.11 Bit rate

The structure of the bit rate field is shown in Table 7-34; the field is a fixed size field of 6 octets.

Table 7-34/Q.2631.1 – Structure of the bit rate field

8	7	6	5	4	3	2	1	Octet
Bit rate in the forward direction								1
								2
								3
Bit rate in the backward direction								4
								5
								6

A bit rate may be used as a peak CPS bit rate or a sustainable CPS bit rate according to ITU-T Rec. Y.1221 [17]. Allowed bit rates are 0 to 16 384 kbit/s. The granularity is 64 bit/s.

The following values for bit rates in either specified direction are allowed:

0-262144 Corresponding to bit rates of 0-16 Mbit/s

262145-16777215 Spare

7.4.12 Packet size

The structure of the packet size field is shown in Table 7-35; the field is a fixed size field of 4 octets.

Table 7-35/Q.2631.1 – Structure of the packet size field

8	7	6	5	4	3	2	1	Octet
Packet size in the forward direction								1
								2
Packet size in the backward direction								3
								4

A packet size may be used as maximum allowed packet size, in octets, allowed to be sent in the specified direction during the holding time of the connection according to ITU-T Rec. Y.1221 [17]. Allowed packet sizes are 0 to 1500 octets.

When calculating the packet sizes, all the transport headers are included, e.g., IP header, UDP header and, if relevant, RTP header.

As an example, when the transport is UDP over IP, the valid range of this field is:

0 maximum packet size value (used in case of unidirectional connections)

1-28 reserved

29-1500 maximum packet size value

1501-65535 spare

7.4.13 UDP port number

The structure of the UDP port number field is shown in Table 7-36; the field is a fixed size field of 2 octets.

Table 7-36/Q.2631.1 – Structure of the UDP port number field

8	7	6	5	4	3	2	1	Octet
UDP port number								1 2

The UDP port number field represents a port number as specified in [6] to be used for the user data flow.

7.4.14 IP address

The structure of the IP address field is shown in Table 7-37; the field is a variable size field.

Table 7-37/Q.2631.1 – Structure of the IP address field

8	7	6	5	4	3	2	1	Octet
Field length								1
IP address								2 n

Depending on the IP version in use, the length of the IP address field is either 4 (IPv4 [4]) or 16 (IPv6 [5]).

The IP address field represents an address as specified in IPv4 [4] or IPv6 [5] to be used for the user data flow.

An IPv4 [4] IP address written in decimal representation as $d_1.d_2.d_3.d_4$ is represented by d_1 in octet 2……d_4 in octet 5.

An IPv6 address ([5], [11]) represented hexadecimally as $w_1x_1y_1z_1$:…….:$w_8x_8y_8z_8$, is represented by w_1 in the lowest order bits of octet 2……z_8 in the highest order bits of octet 17.

7.4.15 IP transport protocol identifier

The structure of the IP transport protocol identifier field is shown in Table 7-38.

Table 7-38/Q.2631.1 – Structure of the IP transport protocol identifier field

8	7	6	5	4	3	2	1	Octet
Reserved				Transport protocol				1
Reserved	Payload type							2

The transport protocol specifies whether UDP [6], or RTP [7] over UDP [6] is used for the user data flow and has the following encoding:

0000	Spare
0001	UDP
0010	RTP over UDP
0011 to 1111	Spare

The payload type specifies the RTP payload type, as defined in RFC 3550 [7] and is only valid when the transport protocol indicates RTP as one of the transport protocols. In all other cases, the payload type shall be set to zero.

7.4.16 Served user generated reference

The structure of the served user generated reference field is shown in Table 7-39; the field is a fixed size field of 4 octets.

Table 7-39/Q.2631.1 – Structure of the served user generated reference field

8	7	6	5	4	3	2	1	Octet
								1
								2
								3
								4

7.4.17 Served user transport

The structure of the served user transport field is shown in Table 7-40; the field is a variable size field.

Table 7-40/Q.2631.1 – Structure of the served user transport field

8	7	6	5	4	3	2	1	Octet
Field length								1
								2
Served user transport								
								n

The served user transport length can be from 1 to 254 octets.

7.4.18 Token bucket size

The structure of the token bucket size field is shown in Table 7-41; the field is a fixed size field of 4 octets.

Table 7-41/Q.2631.1 – Structure of the token bucket size field

8	7	6	5	4	3	2	1	Octet
Token bucket size in the forward direction								1
								2
Token bucket size in the backward direction								3
								4

A token bucket size may be used as token bucket size, in octets, associated with peak or with sustainable bit rates allowed for the specified direction according to ITU-T Rec. Y.1221 [17]. Allowed values are 0 to 1500 octets for token bucket sizes associated with peak bit rates, and 0 to 3200 octets for token bucket sizes associated with sustainable bit rates.

When calculating the token bucket sizes, all transport headers are included, e.g., IP header, UDP header and, if relevant, RTP header.

As an example, when the transport is UDP over IP, the valid range of this field is:

0	Token bucket size (used in case of unidirectional connections)
1-28	reserved
29-1500	Token bucket size associated with peak or sustainable bit rates
1501-3200	Token bucket size associated with sustainable bit rates
3201-65535	spare

8 Procedure of the IPC signalling protocol

Each IP connection request shall contain an endpoint address which indicates the destination of the intended IP connection instance. This information is used by the originating IPC signalling endpoint to route the IP establish request message to the destination IPC signalling endpoint. In capability set 1, the supported address formats are E.164 [14] and X.213 [15].

It is up to the application area or the operator of a particular network to decide what addressing plan is used in the IP network.

NOTE – Causes in the procedures defined in clause 8 specify which ITU-T standardized code should be used in cause parameters of IPC signalling protocol messages. Implementation dependent non-standardized causes may be used for IPC signalling entity internal processing and for IPCU-SAP, GST-SAP, and LM-SAP cause primitive parameters.

The following procedures may be supported as a network option:

a) Connection Priority;

b) Automatic Congestion Control (see ITU-T Rec. Q.542 [16]).

8.1 Compatibility

8.1.1 General requirements on receipt of unrecognized signalling information

It may occur that an IPC node receives unrecognized signalling information, i.e., messages, parameter types or subfield values. This can typically be caused by the upgrading of the signalling system used by other IPC nodes in the network. In these cases the following compatibility procedures are invoked to ensure the predictable network behaviour.

All messages and parameters shall include a compatibility field generated by the IPC signalling entity.

The procedures to be used on receipt of unrecognized information make use of:

- compatibility field received in the same message as the unrecognized information;
- the cause parameter containing a cause value and diagnostics;
- the confusion message and the release request message (maintaining the signalling association); and
- the release confirm message and the reset confirm message (terminating the signalling association).

The following causes are used:

- "message type non-existent or not implemented";
- "information element/parameter non-existent or not implemented"; or
- "message with unrecognized parameter, discarded".

For all the above causes a diagnostic field is included containing, dependant on the cause, the message identifier and zero, one, or more pairs of parameter identifier and field number.

The procedures are based on the following assumptions:

i) Since IPC nodes can be both national and international nodes, the compatibility mechanism is applicable to the national and international network.

ii) If an IPC node receives a confusion message, a release request message, a release confirm message or a reset confirm message indicating an unrecognized message or parameter received, it assumes interaction with an IPC node supporting a different functional level.

NOTE – An IPC node may be at a different functional level due to having implemented a different capability set or another subset of the protocol specified in this Recommendation.

When an unrecognized parameter or message is received, the IPC signalling entity will find some corresponding instructions contained in the parameter compatibility information or message compatibility field respectively. The message compatibility field contains the instructions specific for the handling of the complete message.

The following general rules apply to the interpretation of these instruction indicators:

a) "Reserved" subfields of the compatibility field are not examined. They may be used by future capability sets of this Recommendation; in this case, the future capability sets will set the currently defined instruction indicators to a reasonable value for IPC nodes implementing the current capability set. This rule ensures that more types of instructions can be defined in the future without creating a backward compatibility problem.

b) At an IPC signalling entity, the IP connection is released, using normal release procedures, if the instruction indicator is set to "release connection".

c) At an IPC signalling entity, if the instruction indicator is set to: "Discard message", or "Discard parameter", the message or parameter is discarded, as instructed. If the send notification indicator is set to "send notification", the appropriate message is issued towards the IPC signalling entity that sent the unrecognized information:

   - A confusion message is sent in response to an establish request message, an establish confirm message or in response to an unrecognized message.
   - The appropriate confirm message is sent in response to a release request message or reset request message.
   - No response is returned in response to a confusion message, release confirm message, or reset confirm message.

d) For the case of an unrecognized parameter, it is possible for the instruction to require that either the unrecognized parameter or the whole message is discarded. This provides for the case where the sending IPC signalling entity determines that it is not acceptable for the message to continue being processed without this parameter.

8.1.2 Procedures for the handling of the unrecognized messages or parameters

If the unrecognized signalling information is received, an ERROR.indication primitive with an appropriate cause (described in the following subclauses) is sent to layer management.

A confusion message must not be issued in response to the following messages:

- Confusion
- Release request
- Release confirm
- Reset request
- Reset confirm

Any unrecognized parameters received in the following messages are discarded:

- Confusion
- Release confirm
- Reset confirm

8.1.2.1 Unrecognized messages

Depending on the instructions received in the message compatibility field, an IPC signalling entity receiving an unrecognized message will either:

a) discard the message;

b) discard the message and send notification; or

c) release the connection.

The release request in case c) and the confusion message in case b) shall include the cause "Message type non-existent or not implemented", followed by a diagnostic field containing only the message identifier.

8.1.2.2 Unrecognized parameters

Unexpected parameters (a parameter in the "wrong" message) are handled like unrecognized parameters.

Depending on the instructions received in the parameter compatibility information field, an IPC signalling entity receiving an unrecognized parameter will either:

a) discard the parameter;

b) discard the parameter and send notification;

c) discard the message;

d) discard the message and send notification; or

e) release the connection.

In case b), the confusion message shall include the cause "Information element/parameter non-existent or not implemented" followed by a diagnostic field containing the message identifier and containing pairs of parameter identifier and field number for each unrecognized parameter; the field number in each pair is set to "zero".

In case d), the confusion message shall include the cause "Message with unrecognized parameter, discarded", followed by a diagnostic field containing the message identifier and a parameter identifier (of the first detected unrecognized parameter which caused the message to be discarded) and a field number set to "zero". A confusion message may refer to multiple unrecognized parameters.

An IPC signalling entity receiving a message including multiple unrecognized parameters shall process the different instruction indicators, associated with those parameters, according to the following order:

1) release the connection;

2) discard the message and send notification;

3) discard the message.

A release request message shall include the cause "Information element/parameter non-existent or not implemented" followed by a diagnostic field containing the message identifier, the parameter identifier (of the first detected unrecognized parameter which caused the connection to be released), and a field number set to "zero".

If a release request message is received containing an unrecognized parameter, depending on the instructions received in the parameter compatibility field the signalling entity will either:

- discard the parameter; or
- discard the parameter and send a cause "Information element/parameter non-existent or not implemented", in the release confirm message; the diagnostic field contains the message identifier and one or more pairs of parameter identifier and field number indicating all parameters that match the cause value; the field number of all pairs contains the null value.

If a reset request message is received containing an unrecognized parameter, depending on the instructions received in the parameter compatibility field, the IPC signalling entity will either:

- discard the parameter; or
- discard the parameter and send a cause "Information element/parameter non-existent or not implemented", in the reset confirm message; the diagnostic field contains the message identifier and one or more pairs of parameter identifier and field number indicating all parameters that match the cause value; the field number of all pairs contains the null value.

8.1.2.3 Unrecognized fields

There exists no specific compatibility information for each field. For all fields contained in a parameter, the compatibility information of the parameter applies.

Any value in a subfield that is marked as "spare", "reserved" or "national use" is regarded as unrecognized and the procedures as stated for unrecognized parameters apply except that the field number is coded in the diagnostics field.

8.1.3 Procedures for the handling of responses indicating unrecognized information has been sent

Action taken on receipt of responses indicating unrecognized information has been sent at an originating or terminating IPC signalling entity will depend on the connection state and the affected service.

The definition of any procedure that is outside the basic connection set-up protocol, as defined in this Recommendation, should include procedures for handling responses that indicate that another IPC signalling entity has received, but not recognized, information belonging to that procedure. The procedure receiving this response should take the appropriate actions.

The default action taken on receipt of a confusion message is to discard the message without disrupting normal connection processing.

8.2 IP connection control procedures

8.2.1 Connection control

8.2.1.1 Successful connection set-up

8.2.1.1.1 Actions at originating IPC signalling entity

When the IPC signalling entity receives an ESTABLISH.request primitive from the IPC user, the following restrictions on the optionality of the parameters of the primitive apply:

- The preferred transfer capability parameter shall only be present if the modify support for transfer capability parameter is also present;
- If a preferred transfer capability parameter is specified, it has to refer to the same transfer capability as the transfer capability parameter (for example, if the transfer capability parameter indicates a dedicated bandwidth transfer capability, the preferred transfer capability, if present, may only indicate a dedicated bandwidth transfer capability).

Upon reception of the ESTABLISH.request primitive from the IPC user, an originating IPC signalling entity instance is created. The originating IPC signalling entity instance analyses the routing information and selects a route with sufficient IP resources to the destination IPC node.

NOTE 1 – Routing typically is based on:

- Addressing information;
- Transfer Capability;
- Automatic congestion control and the congestion level in the routing tables;
- Connection Priority; and
- IP Transport Type.

A local IP transport sink address (i.e., an IP address and UDP port number) and other resources (e.g., indicated by transfer capability and connection priority) are allocated by the originating IPC signalling entity instance.

Under the normal condition, when the network is not congested and the originating IPC signalling entity has the necessary resources to complete it, the connection establishment is processed without special treatments.

NOTE 2 – In times of network congestion, when the originating IPC signalling entity does not have sufficient resources to complete all of the incoming connection establishment requests, as one option, the originating IPC signalling entity may give preferential treatments based on the priority level. The preferential treatment should include access to reserved network resources, e.g.,:

1) the highest priority connections are given access to available network resources including the resources reserved for highest priority connections;
2) the second highest priority connections are given access to available network resources including the resources reserved for the second highest priority connections, except for the resources reserved for the highest priority connections, and so on;

NOTE 3 – Allocation of reserved network resources to specific priority levels is implementation specific, and is not a subject for standardization.

A free signalling association identifier is allocated and an ERQ message (establish request) is sent to the destination IPC node and Timer_ERQ started. The ERQ message contains a destination signalling association identifier field set to the "unknown" value and an originating signalling association identifier parameter. The ERQ message also contains the transfer capability and the destination IP endpoint address as received from the IPC user and the local IP transport sink address.

The destination endpoint address, the transfer capability, the IP QoS, the IP transport type, the modify support for transfer capability, the preferred transfer capability, the served user generated reference and the served user transport shall not be modified by either originating or terminating IPC signalling entities. The served user generated reference and the served user transport are parameters with significance to the IPC user only; therefore, they shall not be examined by either originating or terminating signalling entities.

The following parameters are included in the ERQ message only if they were received from the IPC user: the connection priority, the destination endpoint address; the transfer capability, the IP QoS, the preferred transfer capability, the modify support for transfer capability, the served user generated reference and the served user transport.

NOTE 4 – Through-connection of the transmission path at an IPC node is not specified by this Recommendation. It may be controlled by the IPC user.

If an ECF message (establish confirm) is received, Timer_ERQ is stopped and an ESTABLISH.confirm primitive is sent to the IPC user including a modify support for transfer capability parameter, if received. The handling of transfer capability and modify support for transfer capability parameters is specified in Annex A.

8.2.1.1.2 Actions at terminating IPC signalling entity

Upon receiving an ERQ message (establish request) with the DSAID set to "unknown", a terminating IPC signalling entity instance is created and a Signalling Association Identifier (SAID) is allocated.

The terminating IPC signalling entity instance checks the availability of a suitable local IP transport sink address (i.e., an IP address and UDP port number) and other resources (e.g., indicated by transfer capability and connection priority). The handling of transfer capability and modify support for transfer capability parameters is specified in Annex A.

If a local IP transport sink address and the other resources are available for the new IP connection, they are allocated to the new connection.

Under the normal condition, when the network is not congested and the terminating IPC signalling entity has the necessary resources to complete it, the connection establishment is processed without special treatments.

NOTE 1 – In times of network congestion, when the terminating IPC signalling entity does not have sufficient resources to complete all of the incoming connection establishment requests, as one option, the terminating IPC signalling entity may give preferential treatments based on the priority level. The preferential treatment should include access to reserved network resources, e.g.:

1) the highest priority connections are given access to available network resources including the resources reserved for highest priority connections;
2) the second highest priority connections are given access to available network resources including the resources reserved for the second highest priority connections, except for the resources reserved for the highest priority connections, and so on.

NOTE 2 – Allocation of reserved network resources to specific priority levels is implementation specific, and is not a subject for standardization.

The destination endpoint address, the transfer capability, the IP QoS, the IP transport type, the modify support for transfer capability, the preferred transfer capability, the served user generated reference and the served user transport shall not be modified by either originating or terminating IPC signalling entities. The served user generated reference and the served user transport are parameters with significance to the IPC user only; therefore, they shall not be examined by either originating or terminating signalling entities.

An ESTABLISH.indication primitive is sent to the terminating IPC user to inform it of the new connection establishment request. The terminating IPC signalling entity instance shall pass the transfer capability and, only if they were received in the ERQ message, the following parameters to the terminating IPC user only if they were received in the ERQ message: the connection priority, the destination endpoint address; the transfer capability, the IP QoS, the preferred transfer capability, the modify support for transfer capability, the served user generated reference and the served user transport.

Upon reception of an ESTABLISH.response primitive from the IPC user, the terminating IPC signalling entity instance acknowledges the successful IP connection establishment by returning an ECF message (establish confirm) to the sender of the ERQ message. The ECF message contains both the originating and destination signalling association identifiers and the local IP transport sink address. If modification capability is supported the modify support for transfer capability parameter will also be included. The handling of transfer capability and modify support for transfer capability parameters is specified in Annex A.

NOTE 3 – Through-connection of the transmission path at an IPC nodes is not specified by this Recommendation. It may be controlled by the IPC user.

8.2.1.2 Unsuccessful/abnormal connection set-up

8.2.1.2.1 Actions at originating IPC signalling entity

If the allocation of a local IP transport sink address, the SAID, or other resources for the outgoing IP connection described in 8.2.1.1.1 fails, a RELEASE.confirm primitive is returned to the IPC user with one of the following causes:

- "Unallocated (unassigned) number";
- "No route to destination";
- "Resource unavailable, unspecified";
- "Switching equipment congestion";
- "Network out of order"; or
- "Temporary failure".

If the originating IPC signalling entity cannot complete a high priority connection establishment request even after application of the preferential treatment, a RELEASE.confirm primitive is returned to the IPC user with cause "Resource unavailable, unspecified".

If the ERQ message (establish request) is longer than the signalling transport allows, the IPC user is informed by a RELEASE.confirm primitive containing the cause "Protocol error, unspecified".

If an RLC message (release confirm) is received by the originating IPC signalling entity instance, Timer_ERQ is stopped and the IPC user is informed by a RELEASE.confirm primitive containing the cause received in the release confirm message. If the release confirm message indicates that there has been a change in the level of congestion of the adjacent IPC node, the routing tables in the originating IPC node shall be updated accordingly. The absence of an automatic congestion control parameter indicates that there is no reported congestion in the adjacent IPC node whilst, if the automatic congestion control parameter is present, it indicates whether congestion level 1 or 2 has been exceeded. After the routing tables have been updated, the automatic congestion control parameter is discarded.

In all of the above cases, any resources allocated to the originating IPC signalling entity instance are released and made available for new traffic. The originating IPC signalling entity instance is released.

If Timer_ERQ expires, the IPC user is informed by a RELEASE.confirm primitive containing the cause "Recovery on timer expiry", any resources allocated to the originating IPC signalling entity

instance, and the originating IPC signalling entity instance are released, and a reset procedure is initiated (see 8.2.2.1.1 case 2 a)).

8.2.1.2.2 Actions at terminating IPC signalling entity

Upon reception of an ERQ message (establish request), if resources for the incoming IP connection are not available, or if the SAID allocation fails, an RLC message (release confirm) is returned containing the cause "Resource unavailable, unspecified". If the IPC user indicates that the establishment request has failed (reception of an RELEASE.response primitive from the IPC user), the terminating IPC signalling entity instance sends an RLC message to the peer IPC node, containing the cause received from the IPC user. The terminating IPC signalling entity instance examines the congestion level of the IPC node. If either of the two congestion thresholds is exceeded, an automatic congestion control parameter is included in the RLC message, indicating the level of congestion (congestion level 1 or 2) to the adjacent IPC node.

If the terminating IPC signalling entity cannot complete a high priority connection establishment request even after application of the preferential treatment, an RLC message (release confirm) is returned containing the cause "Resource unavailable, unspecified".

In all of the above cases, any resources allocated to the terminating IPC signalling entity instance are released and made available for new traffic. The terminating IPC signalling entity instance is released.

8.2.1.3 Normal connection release

8.2.1.3.1 Actions at IPC signalling entity that originates the release request

When the IPC signalling entity instance receives a RELEASE.request primitive from the IPC user, a REL message (release request) is sent and Timer_REL is started. The REL message contains the cause received from the IPC user, which shall be "Normal, unspecified" in case of normal connection release.

If an RLC message (release confirm) is received Timer_REL is stopped. If the RLC message indicates that there has been a change in the level of congestion of the adjacent IPC node, the routing tables in the IPC node shall be updated accordingly. The absence of an automatic congestion control parameter indicates that there is no reported congestion in the adjacent IPC node whilst, if the automatic congestion control parameter is present, it indicates whether congestion level 1 or 2 has been exceeded. After the routing tables have been updated, the automatic congestion control parameter is discarded.

Any resources allocated to the IPC signalling entity instance are released and made available for new traffic. The IPC signalling entity instance is released.

8.2.1.3.2 Actions at IPC signalling entity that receives the release request

Upon receiving a REL message (release request), a RELEASE.indication primitive is sent to the IPC user to inform it of the connection release request. The RELEASE.indication primitive contains the cause received in the REL message.

The IPC signalling entity instance acknowledges the successful IP connection release by returning a RLC message (release confirm) to the sender of the REL message. The IPC signalling entity instance examines the congestion level of the IPC node. If either of the two congestion thresholds is exceeded, an automatic congestion control parameter is included in the RLC message, indicating the level of congestion (congestion level 1 or 2) to the adjacent IPC node.

Any resources allocated to the IPC signalling entity instance are released and made available for new traffic. The IPC signalling entity instance is released.

8.2.1.4 Abnormal connection release

If Timer_REL expires, any resources allocated to the IPC signalling entity instance, and the IPC signalling entity instance are released, and a reset procedure is initiated (see 8.2.2.1.1 case 2 a)).

8.2.1.5 Release request collision

In the case of release request collision, i.e., a REL message is received by an IPC signalling entity instance whilst waiting for a response to a REL message already sent, Timer_REL is stopped and an RLC message is immediately returned to the peer IPC signalling entity instance. Any resources allocated to the IPC signalling entity instance are released and made available for new traffic. The IPC signalling entity instance is released.

8.2.1.6 Successful modification

8.2.1.6.1 Actions at IPC signalling entity that originates the modification request

When the IPC signalling entity instance receives a MODIFY.request primitive from the IPC user, the following restrictions on the optionality of the parameters of the primitive apply:

- The transfer capability parameter must refer to the same transfer capability as the transfer capability parameter in the ESTABLISH.request primitive (for example, if the transfer capability parameter in the ESTABLISH.request primitive indicated a dedicated bandwidth transfer capability, the transfer capability parameter in the MODIFY.request primitive may only indicate a dedicated bandwidth transfer capability).

The IPC signalling entity checks the availability of resources indicated by the IPC user. If the resources are available for the IP connection, they are reserved. A MOD message (modify request) is sent to the peer IPC signalling entity instance and Timer_MOD is started. The MOD message contains the transfer capability parameter provided by the IPC user.

If a MOA message (modify acknowledge) is received by the IPC signalling entity instance, Timer_MOD is stopped and the reserved additional resources are allocated to the connection, or resources no longer required for this IP connection are freed. A MODIFY.confirm primitive is sent to the IPC user to indicate the successful modification.

8.2.1.6.2 Actions at IPC signalling entity that receives the modification request

Upon receiving a MOD message (modify request) the IPC signalling entity instance checks the availability of resources indicated in the MOD message. If the resources are available for the connection, they are reserved.

A MODIFY.indication primitive is sent to the IPC user to inform it of the modification request. The transfer capability received in the MOD message shall be passed to the IPC user.

Upon reception of a MODIFY.response primitive from the IPC user, the IPC signalling entity instance acknowledges the successful modification by returning a MOA message (modify acknowledge) to the sender of the MOD message. The reserved additional resources are allocated to the connection, or resources no longer required for this IP connection are freed.

8.2.1.7 Unsuccessful modification

8.2.1.7.1 Actions at IPC signalling entity that originates the modification request

If the required resources are not available, a MODIFY-REJECT.confirm primitive is returned to the IPC user with the cause "Resource unavailable, unspecified".

If a MOR message (modify reject) is received, all additional resources reserved for the modification request are freed. A MODIFY-REJECT.confirm primitive is sent to the IPC user with the cause received in the MOR message.

If Timer_MOD expires, the IPC user is informed by a RELEASE.indication primitive containing the cause "Recovery on timer expiry", any resources allocated to the IPC signalling entity instance, and the IPC signalling entity instance are released, and a reset procedure is initiated (see 8.2.2.1.1 case 2 a)).

8.2.1.7.2 Actions at IPC signalling entity that receives the modification request

If the required resources are not available, an MOR message (modify reject) is returned to the peer IPC node with the cause "Resource unavailable, unspecified".

If the IPC user indicates that the modification request has failed (reception of an MODIFY-REJECT.response primitive from the IPC user), all additional resources reserved for the modification request are freed and the IPC signalling entity instance sends a MOR message to the peer IPC node, containing the cause received from the IPC user.

8.2.1.8 Modification collision

In the case of modification collision, i.e., a MOD message is received by an IPC signalling entity instance whilst waiting for a response to a MOD message already sent, Timer_MOD is stopped and a MOR message is immediately returned to the peer IPC signalling entity instance. All additional resources reserved for the modification request are freed.

8.2.1.9 Connection release during modification

When an IPC signalling entity instance receives either a RELEASE.request primitive from the IPC user or a REL message (release request) from the peer IPC node whilst a modification request is being processed, the IPC signalling entity instance shall continue with normal connection release procedures.

8.2.2 Maintenance control

8.2.2.1 Reset

The reset procedure is invoked under abnormal conditions such as when the current status of the IP connection is unknown or ambiguous, for example, an IPC node that has suffered memory mutilation will not know the status of one or several IP connections. All the affected IP connections and any associated resources (e.g., bandwidth, etc.) between the two adjacent IPC nodes shall be released. The resources are made available for new traffic.

The reset procedure covers the following two cases:

1) Case 1: Reset all IP connections associated with a signalling association between two adjacent IPC nodes.

2) Case 2: Reset a single IP connection between two adjacent IPC nodes.

The reset procedure should be initiated when:

a) Signalling anomalies are detected by the IPC signalling entity:

- Timer "Timer_ERQ" expiry – Action: Reset the single IP connection associated with the originating IPC signalling entity instance.
- Timer "Timer_REL" expiry – Reset the single IP connection associated with either originating or terminating IPC signalling entity instance.
- Timer "Timer_MOD" expiry – Reset the single IP connection associated with either originating or terminating IPC signalling entity instance.

b) Maintenance action is required to recover from abnormal conditions such as loss or ambiguity of association information (e.g., caused by memory mutilation) between SAID(s) and the connection status of either a specific IP connection, or all IP connections associated with a signalling association between two IPC nodes – Action: Reset a single IP connection or all IP connections associated with a signalling association between two adjacent IPC nodes respectively.

The reset procedures take precedence over the modification procedures.

8.2.2.1.1 Actions at reset initiating IPC node

When a request for reset is received from either layer management (via the LM-SAP interface) or due to a timer expiry, a maintenance IPC signalling entity instance is created and an SAID allocated to it.

Reset procedures can be initiated to reset:

1) all IP connections associated with a signalling association between two adjacent IPC nodes,

2) a single IP connection between two adjacent IPC nodes.

For case 1, layer management passes a RESET.request together with the indication "All IP connections associated with a signalling association" to the maintenance IPC signalling entity instance. The maintenance IPC signalling entity instance starts Timer_RES and sends a RES message (reset request) containing an indication that all IP connections associated with a signalling association are to be reset.

For case 2, there are two possible sub-cases, one due to timer expiry and the other due to layer management action:

2-a) After the expiry of Timer_ERQ, Timer_REL, or Timer_MOD, the IPC signalling entity starts Timer_RES and sends a RES message (reset request) containing a specific IP transport sink address.

2-b) Layer management passes a RESET.request together with the indication "a specific IP connection" to the maintenance IPC signalling entity instance. The maintenance IPC signalling entity instance starts Timer_RES and sends a RES message (reset request) containing the local IP transport sink address of the affected IP connection.

In cases 1 and 2-b, the maintenance IPC signalling entity instance informs any affected IPC user with a RELEASE.indication primitive with the cause "Temporary failure".

If an RSC message (reset confirm) is received, Timer_RES is stopped. Any affected resources are made available for new connections. The SAID allocated to the maintenance IPC signalling entity instance is released and made available for new traffic. The maintenance IPC signalling entity instance is released.

In case 2-a, a RESET.indication primitive with the local IP transport sink address parameter is sent to layer management; in all other cases, a RESET.confirm primitive is sent to the layer management.

8.2.2.1.2 Actions at reset responding IPC node

When a RES message (reset request) is received, a maintenance IPC signalling entity instance is created and an SAID allocated to it.

1) If an indication that all IP connections associated with a signalling association must be reset is received, then all IP connections associated with a signalling association between the two adjacent IPC nodes are reset.

2) If an indication that a specific IP connection must be reset is received, only that IP connection is reset.

If resources have been assigned to any of the IP connections that are reset, any affected resources are made available for new connections. Layer management is informed about the receipt of the reset request by sending a RESET.indication primitive with the same IP transport sink address parameter that was received in the RES message. Any affected IPC user is informed with a RELEASE.indication primitive with the cause "Temporary failure".

A RSC message (reset confirm) is returned to the sender of the RES message, the maintenance IPC signalling entity instance is released and the allocated SAID is made available for new traffic.

8.2.2.1.3 Abnormal reset procedures

If the SAID allocation fails at the reset initiating IPC node, an ERROR.indication primitive including the cause "Switching equipment congestion" and the IPTA parameter is sent to layer management. The maintenance IPC signalling entity instance is released.

If the SAID allocation fails at the reset responding IPC node, the maintenance IPC signalling entity instance is released and no further action is taken.

If Timer_RES expires following the initial sending of the RES message, Timer_RES is restarted and the maintenance IPC signalling entity will re-send the RES message, containing the same parameters as in the first sending of the RES message. The maintenance IPC signalling entity shall send an ERROR.indication primitive to layer management including the cause "Recovery on timer expiry " and the IPTA parameter.

If Timer_RES expires following the second sending, or any subsequent sending of the RES message, Timer_RES is restarted and the maintenance IPC signalling entity will resend the RES message, containing the same parameters as in the first sending of the RES message.

Upon receiving a STOP-RESET.request primitive with adjacent ANI identifier and IP transport sink address parameters from layer management, Timer_RES is stopped. Any affected resources are made available for new connections. The SAID allocated to the maintenance IPC signalling entity instance, and the maintenance IPC signalling entity instance, are released and made available for new traffic.

8.2.2.2 Transmission fault handling

Fully digital transmission systems are provided between all IPC nodes. They have some inherent fault indication features that give an indication to the IPC node when faults are detected on the transmission level. On receipt of a fault indication from layer management, the routing function in the node inhibits selection of affected IP transport sink addresses for the period that the fault condition persists. No special action is required for active IP connections.

8.2.2.3 IPC signalling congestion control

On receipt of a CONGESTION.indication primitive from the generic signalling transport service, the IPC signalling entity instance should alter traffic load (e.g., connection attempts) toward the affected IPC nodes to align with the congestion level indicated by the primitive.

8.2.2.4 Adjacent IPC node availability

On receipt of an OUT-OF-SERVICE.indication primitive from the generic signalling transport service, the following action is required:

All IP transport sink addresses associated with the affected adjacent IPC node are marked as unavailable in the routing function prohibiting new connection establishments to that IPC node. Already established IP connections need not be released even though signalling messages cannot be sent to the affected IPC node.

On receipt of an IN-SERVICE.indication primitive from the generic signalling transport service, the following action is required:

All IP transport sink addresses associated with the affected adjacent IPC node are again marked available in the routing function. Reset procedures that may have started during the period of signalling isolation continue and ensure that affected IP connections are returned to a state whereby the resources are available for new IP connections. Already, established IP connections are unaffected.

8.3 General protocol rules

8.3.1 Error handling

If a parameter is present more than once in a message where this parameter is allowed only once, only the first parameter shall be processed; all subsequent instances of the parameter shall be ignored.

When receiving a message, which does not contain the minimum set of parameters required to continue processing, a protocol error is reported to layer management with an ERROR.indication primitive with a cause "Mandatory information element is missing" and the message is discarded.

8.3.2 Handling of signalling association identifiers

The following rules relating to Signalling Association Identifiers (SAID) apply:

- The IPC signalling entity instance that does not issue the value of such a field is not allowed to modify it, but shall use it in the destination signalling association identifier field in the header of a messages directed towards the issuer.
- When a message is received at the generic signalling transport service access point (GST-SAP), the destination signalling association identifier field of the incoming message is used to distribute the messages to the appropriate IPC signalling entity instance.
- If a received message contains a destination signalling association identifier set to the "unknown" value and an originating signalling association identifier, a new terminating IPC signalling entity instance, or a new maintenance IPC signalling entity instance is created and marked with a newly allocated signalling association identifier. The originating signalling association identifier parameter in the first response message issued by the new IPC signalling entity instance will inform the peer IPC signalling entity instance of the newly allocated signalling association identifier.
- If an IPC signalling entity instance sends a message to its peer IPC signalling entity instance, the message includes the signalling association identifier of the peer in the destination signalling association identifier field.
- If a new maintenance IPC signalling entity instance is created as a result of an incoming maintenance message, no signalling association identifier is allocated for it and no originating signalling association identifier parameter is conveyed to the peer IPC signalling entity instance in the first (and only) message issued by the new maintenance IPC signalling entity instance.

The sequence control parameter of the TRANSFER.request primitive across the GST-SAP is allocated on a cyclic basis per IPC signalling entity instance.

All messages are sent in a TRANSFER.request primitive. All messages are received in a TRANSFER.indication primitive.

8.3.3 General protocol error handling

If a message is received that is too short to contain a complete message (i.e., less than 6 octets), it shall be ignored.

The message is discarded and layer management informed with an ERROR.indication in the following cases:

- If the parameter length points beyond the end of the message, cause "Message with unrecognized parameter, discarded" is indicated.
- If the field length points beyond the end of the parameter, cause "Message with unrecognized parameter, discarded" is indicated.
- If an unrecognized message containing a destination signalling association identifier set to the "unknown" value, cause "Message type non-existent or not implemented" is indicated.

  NOTE – If an unrecognized message containing a valid destination signalling association identifier is received, the message is conveyed to the addressed IPC signalling entity instance as if it were a recognized message.
- If the message contains a destination signalling association identifier with an illegal/invalid value, cause "Invalid information element contents" is indicated.
- If the message is considered unexpected by the signalling procedures, cause "Invalid message, unspecified" is indicated.
- If a mandatory originating signalling association identifier parameter is not present, cause "Mandatory information element is missing" is indicated.
- If the originating signalling association identifier field is set to "zero", cause "Invalid information element contents" is indicated.

8.4 List of timers

The timers used in the procedures described in 8.2 are listed in Table 8-1 together with a timeout value range, their cause for setting the timer, resetting the timer, and the action at expiry of the timer.

Table 8-1/Q.2631.1 – List of Timers

Timer	Time-out value	Cause for initiation	Normal termination	At expiry
Timer_ERQ	5-30 s (t1)	When an ERQ message is sent	At the receipt of ECF message	Release all resources and the IP connection, send RES message.
Timer_REL	2-60 s (t2)	When an REL message is sent	At the receipt of RLC message	Release resources, send RES message.
Timer_RES	2-60 s (t3)	When an RES message is sent	At the receipt of RSC message	At first expiry: Repeat RES message, restart Timer_RES, inform layer management. At subsequent expiry: Repeat RES message, restart Timer_RES.
Timer_MOD	5-30 s (t6)	When a MOD message is sent	At the receipt of MOA message	Release all resources and the IP connection, send RES message.
NOTE – In the diagnostic field associated with a cause field indicating "Recovery on timer expiry", the timer number is included. Timer_ERQ is coded as the IA5 character "1"; Timer_MOD is coded as the IA5 character "6".				

Annex A

Handling of the transfer capability in conjunction with the connection set-up and modification procedures

NOTE – In this annex the terms "Transfer Capability" and "Preferred Transfer Capability" and the abbreviations "TC" and "PTC" do not distinguish between the different types of transfer capabilities, i.e., dedicated bandwidth and statistical bandwidth.

A.1 Preferred transfer capability parameter present

When an Establish Request (ERQ) message includes the following parameters:

- Preferred Transfer Capability (PTC);
- Transfer Capability (TC); and
- Modify Support for Transfer Capability (MSTC).

the connection admission control at all IPC nodes shall initially be based on the most demanding of the preferred transfer capability and the transfer capability ("max PTC/TC"). The concept of "demanding" depends on the connection admission control algorithm in use, which is outside the scope of this Recommendation.

At a terminating IPC node the following applies:

Upon reception of the ESTABLISH.response primitive from the IPC user, the existence of a modify support for transfer capability parameter is checked:

– If the IPC user indicates that modification is supported, the preferred transfer capability is used for connection admission control, and the ECF message (establish confirm) shall contain the modify support for transfer capability parameter.

– If the IPC user indicates that modification is not supported, the transfer capability is used for connection admission control, and the ECF message (establish confirm) shall not contain the modify support for transfer capability parameter.

At an originating IPC node the following applies:

Upon reception of the ECF message (establish confirm), the existence of a modify support for transfer capability parameter is checked:

– If the ECF message contains a modify support for transfer capability parameter, the preferred transfer capability is used for connection admission control, and the ESTABLISH.confirm primitive sent to the originating IPC user shall contain the modify support for transfer capability parameter.

– If the ECF message does not contain a modify support for transfer capability parameter, the transfer capability is used for connection admission control, and the ESTABLISH.confirm primitive sent to the originating IPC user shall not contain the modify support for transfer capability parameter.

A.2 Preferred transfer capability parameter not present

When an Establish Request (ERQ) message includes the following parameters:

- Transfer Capability (TC), and
- Modify Support for Transfer Capability (MSTC),

the connection admission control at all IPC nodes shall be based on the transfer capability.

At a terminating IPC node the following applies:

Upon reception of the ESTABLISH.response primitive from the IPC user, the existence of a modify support for transfer capability parameter is checked:

– If the IPC user indicates that modification is supported, the ECF message (establish confirm) shall contain the modify support for transfer capability parameter.

– If the IPC user indicates that modification is not supported, the ECF message (establish confirm) shall not contain the modify support for transfer capability parameter.

At an originating IPC node the following applies:

Upon reception of the ECF message (establish confirm) the existence of a modify support for transfer capability parameter is checked:

– If the ECF message contains a modify support for transfer capability parameter, the ESTABLISH.confirm primitive sent to the originating IPC user shall contain the modify support for transfer capability parameter.

– If the ECF message does not contain a modify support for transfer capability parameter, and the ESTABLISH.confirm primitive sent to the originating IPC user shall not contain the modify support for transfer capability parameter.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2004