INTERNATIONAL TELECOMMUNICATION UNION

ITU-T G.7713.3/Y.1704.3

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2003)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital terminal equipments – Operations, administration and maintenance features of transmission equipment

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

Internet protocol aspects – Operation, administration and maintenance

Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

ITU-T Recommendation G.7713.3/Y.1704.3

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DIGITAL TERMINAL EQUIPMENTS	G.7000–G.7999
General	G.7000–G.7099
Coding of analogue signals by pulse code modulation	G.7100–G.7199
Coding of analogue signals by methods other than PCM	G.7200–G.7299
Principal characteristics of primary multiplex equipment	G.7300–G.7399
Principal characteristics of second order multiplex equipment	G.7400–G.7499
Principal characteristics of higher order multiplex equipment	G.7500–G.7599
Principal characteristics of transcoder and digital multiplication equipment	G.7600–G.7699
Operations, administration and maintenance features of transmission equipment	**G.7700–G.7799**
Principal characteristics of multiplexing equipment for the synchronous digital hierarchy	G.7800–G.7899
Other terminal equipment	G.7900–G.7999
DIGITAL NETWORKS	G.8000–G.8999

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

ITU-T Recommendation G.7713.3/Y.1704.3

Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

Summary

This Recommendation specifies the signalling mechanism and protocol for distributed call and connection management based on GMPLS CR-LDP. This signalling protocol is applicable at the UNI, I-NNI and E-NNI and provides for automated call and connection operations relating to ASTN and ASON. Routing, DCN usage, and automatic discovery are beyond the scope of this Recommendation. Items covered in this Recommendation include:

– CR-LDP messages;

– CR-LDP attributes; and

– CR-LDP signal flows.

This Recommendation meets the requirements of ITU-T Rec. G.7713/Y.1704 and is functionally similar to ITU-T Recs G.7713.1/Y.1704.1 and G.7713.2/Y.1704.2.

Source

ITU-T Recommendation G.7713.3 was approved by ITU-T Study Group 15 (2001-2004) under the ITU-T Recommendation A.8 procedure on 16 March 2003.

History

This Recommendation forms part of a suite of Recommendations covering the full functionality of the automatic switched transport network (ASTN).

Document history	
Issue	**Notes**
0.1	Version 0.1 of G.7713.3/Y.1704.3 (05/2002)
0.2	New text on SPC, signal flow diagram, label scope, removed crankback
0.3	Revisions from drafting in Q14/15 interim meeting – Ottawa Oct. 7-11, 2002
0.4	Editorial revisions for Geneva meeting in January 2003
0.5	Revisions based on contributions at the SG15 meeting in Geneva, January 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 G.7713.3/Y.1704.3

Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

1 Scope

This Recommendation provides the signalling mechanism for distributed call and connection management (DCM) using constraint-based routed label distribution protocol (CR-LDP).

ITU-T Recs G.807/Y.1302 and G.8080/Y.1304 together specify the requirements and architecture for a dynamic optical network in which optical service is established using a control plane. ITU-T Rec. G.7713/Y.1704 specifies the detailed requirements for the signalling procedures in the ASON control plane in a protocol-neutral manner.

CR-LDP is a protocol within the Multi-Protocol Label Switching (MPLS) framework and is also recognized as a method of transporting IP over ATM in ITU-T Rec. Y.1310. Extensions to the scope of MPLS to include TDM switching and transport, and optical multiplexing hierarchies are contained in the Generalized MPLS (GMPLS) framework of which there is a protocol neutral functional description. GMPLS CR-LDP referred to in this Recommendation is CR-LDP adapted to the GMPLS framework.

In this Recommendation, the use of the term "GMPLS" refers only to a framework and functional description. The term "GMPLS CR-LDP", or simply "CR-LDP", refers to a specific protocol that was developed within the GMPLS framework. Extensions to GMPLS CR-LDP were developed for the OIF UNI-01.0 specification.

This Recommendation describes the use of the GMPLS CR-LDP protocol as an instantiation of data call and connection management (ITU-T Rec. G.7713/Y.1704) within the ASON (ITU-T Rec. G.8080/Y.1304) framework. It covers the use of CR-LDP for basic call/connection procedures, messages, and signalling over the various reference points. Extensions to GMPLS CR-LDP for compliance to ITU-T Rec. G.7713/Y.1704 are also included in this Recommendation. Routing, DCN usage, and automatic discovery are beyond the scope of this Recommendation.

This Recommendation initially focuses on the support of Soft Permanent Connections (SPC) services. Protocol specifications to support basic switched connections (SC) services are also included.

2 References

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

– ITU-T Recommendation E.360.1 (2002), *Framework for QoS routing and related traffic engineering methods for IP-, ATM-, and TDM-based multiservice networks*.

– ITU-T Recommendation G.703 (2001), *Physical/electrical characteristics of hierarchical digital interfaces*.

– ITU-T Recommendation G.707/Y.1322 (2000), *Network node interface for the Synchronous Digital Hierarchy (SDH)*.

– ITU-T Recommendation G.709/Y.1331 (2003), *Interfaces for the Optical Transport Network (OTN)*.

– ITU-T Recommendation G.803 (2000), *Architecture of transport networks based on the Synchronous Digital Hierarchy (SDH)*.

– ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

– ITU-T Recommendation G.807/Y.1302 (2001), *Requirements for the Automatic Switched Transport Network (ASTN)*.

– ITU-T Recommendation G.872 (2001), *Architecture of optical transport networks*.

– ITU-T Recommendation G.7713/Y.1704 (2001), *Distributed Call and Connection Management (DCM)*.

– ITU-T Recommendation G.7714/Y.1705 (2001), *Generalized automatic discovery techniques*.

– ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture of the Automatically Switched Optical Network (ASON)*.

– ITU-T Recommendation T.50 (1992), *International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange*.

– ITU-T Recommendation Y.1310 (2000), *Transport of IP over ATM in public networks*.

– IETF RFC 3036 (2001), *LDP specification*.

– IETF RFC 3212 (2002), *Constraint-Based LSP setup using LDP*.

– IETF RFC 3471 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) – Signalling Functional Description*.

– IETF RFC 3472 (2003), *Generalized Multi-Protocol Label Switching (GMPLS) Signalling – Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*.

– IETF RFC 3480 (2003), *Signalling Unnumbered Links in CR-LDP (Constraint-Routing Label Distribution Protocol)*.

– IETF RFC 3479 (2003), *Fault tolerance for the Label Distribution Protocol (LDP)*.

– IETF RFC 3478 (2003), *Graceful Restart Mechanism for Label Distribution Protocol*.

– OIF UNI-01.0 (2001), *User Network Interface (UNI) 1.0 signalling specification*.

3 Terms and definitions

The following terms are defined in ITU-T Rec. G.8080/Y.1304:

– connection controller;

– link resource manager;

– subnetwork point;

– protocol controller;

– routing controller;

– subnetwork point pool.

The following term are defined in ITU-T Rec. G.807/Y.1302:

– Soft permanent connection

This Recommendation defines the following terms:

3.1 hello: A message sent by a signalling protocol controller to advertise its presence to other signalling protocol controllers.

3.2 CR-LDP peers: Two protocol controllers implementing CR-LDP that have established communication with each other.

3.3 CR-LDP session: The control communication instance between two CR-LDP peers.

3.4 label: This term is the same as a G.8080/Y.1304 SNP.

3.5 downstream on demand: A label advertisement procedure by which the upstream node is responsible for requesting the label mapping.

3.6 ordered control mode: A node initiates the transmission of a label mapping only when the label mapping from the downstream node is received.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ASON	Automatic Switched Optical Network
CR-LDP	Constraint-based Routed Label Distribution Protocol
DCN	Data Communications Network
E-NNI	Exterior NNI
GMPLS	Generalized Multi-Protocol Label Switching
I-NNI	Interior NNI
ISO	International Organization for Standardization
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switch Router
NNI	Network Node Interface
SNP	Subnetwork Point
SNPP	Subnetwork Point Pool
SPC	Soft Permanent Connection
TLV	Type, Length, Value (encoding)
TNA	Transport Network Address

5 Conventions

In this Recommendation, the use of the term "GMPLS" refers only to a framework and functional description. The term "GMPLS CR-LDP", or simply "CR-LDP", refers to a specific protocol that was developed within the GMPLS framework. Extensions to GMPLS CR-LDP were developed for the OIF UNI-01.0 specification.

6 Assumptions

ITU-T Rec. G.8080/Y.1304 defines a UNI Transport Resource Addresses for the bearer links at the UNI reference point. For this Recommendation, an instantiation of those addresses will follow the OIF Transport Network Address (TNA) from OIF UNI-01.0 which complies with G.8080/Y.1304 architecture. Allowable address formats in the OIF TNA are IPv4, IPv6, and NSAP addresses.

Call routing services are assumed to be available that associate a UNI Transport Resource Addresses with internal routable addresses. This is not within the scope of this Recommendation.

Addressing of transport resources in the protocol is done by SNPP identifiers. A pair of these would identify an SNPP link. SNPP names are defined from transport name spaces (see clause 10/G.8080/Y.1304) and it is important to note that control plane names/addresses are not used for these. For example, neither routing controller nor connection manager identifiers are used for bearer link names.

The terms Quality of Service (QoS), Class of Service (CoS), and Grade of Service (GoS) with respect to the transport plane are used in this Recommendation in the sense of ITU-T Rec. E.360.1. It is expected that ASON specific characteristics and parameters will be associated with these terms in later versions of this Recommendation.

7 Overview and applications

7.1 CR-LDP overview

GMPLS CR-LDP uses attributes defined in RFC 3036 (LDP Specification) and RFC 3212 (Constraint-Based LSP Setup Using LDP). Extensions to CR-LDP signalling required to support generalized MPLS (GMPLS) are contained in RFC 3471 and RFC 3472.

There are four categories of LDP messages as defined in RFC 3036:

- Discovery messages, used to announce and maintain the presence of a network element.
- Session messages, used to establish, maintain, and terminate sessions between CR-LDP peers.
- Advertisement messages, used to create, change, and delete label mappings (or connections).
- Notification messages, used to provide advisory information and to signal error information.

LDP and CR-LDP were developed for use in data networks where the call concept does not exist. Support of connection control could be achieved through the use of the already existing LDP messages. The support of call control requires the introduction of a new message category for this purpose:

- Call control messages, for use in the call control procedure.

Call control messages are a new LDP message category that is introduced specifically for this Recommendation.

Discovery messages provide a mechanism whereby network elements indicate their presence in a network by sending a Hello message periodically. Hello messages are transmitted over UDP to the CR-LDP port. The IP multicast address corresponding to "all routers on this subnet" is used as the destination IP address. When a network element chooses to establish a session with another network element (whose address is learned via the Hello message), it uses the LDP initialization procedure over TCP. Upon successful completion of the initialization procedure, the two network elements become LDP peers and may begin exchanging advertisement messages.

LDP uses TCP transport for session, advertisement and notification messages, i.e., for everything but the UDP-based discovery mechanism. The use of TCP for transport allows CR-LDP to maintain a hard state property. The term "hard state" means that the representation of the state of an entity persists until an explicit action is taken to change it. TCP also allows CR-LDP to make use of the TCP provided mechanisms for reliable transmission and flow control, hence there is no need to build these important features at the LDP level.

LDP can operate in a number of modes depending on the label distribution mode (*independent* or *ordered*), label retention mode (*conservative* or *liberal*), and label advertisement mode (*downstream on demand* or *downstream unsolicited*). These modes are defined in RFC 3036. The only mode of operation for CR-LDP shall be downstream on demand, ordered control.

CR-LDP supports explicit and loose routing.

In the absence of carrier-grade equipment, i.e., state is lost during failure, CR-LDP employs a graceful restart mechanism by which a failed node reconstructs its state from information learned from the other nodes during the restart.

7.2 Support for basic call identifier

To support the call model described in ITU-T Rec. G.7713/Y.1704, CR-LDP is extended to include call control in addition to a connection. This enables multiple connections to be associated with a single call, changes to existing connections, and call-related billing. The main CR-LDP extension for the support of call control across the UNI and E-NNI is the introduction of the Call Id TLV as defined in 9.4.

7.3 CR-LDP at UNI reference point

CR-LDP is one of two protocol instances specified in OIF UNI-01.0 and serves as an example of CR-LDP at a UNI. CR-LDP UNI extensions allow for the setup, teardown, and query of connections. Connection setup, teardown, and modification utilize specified LDP messages. Connection querying is accomplished using the Query and Query Response messages.

The OIF UNI-01.0 does not include the concept of call and connection separation. So, applying the OIF UNI version of CR-LDP to ITU-T Rec. G.7713/Y.1704 requires additional changes. It does however, contain call information elements that are reused in this Recommendation.

Support of TCP/IP is needed in the DCN for CR-LDP messages. Use of TCP provides signalling channel resilience and this may need to be coordinated with signalling network recovery procedures (if present) as per 6.2/G.7713/Y.1704. Use of TCP for session, advertisement and notification messages fits well with use of the DCN in ITU-T Rec. G.7713/Y.1704 in that signalling channel resilience is not part of the actual CR-LDP protocol but is a separate function.

7.4 CR-LDP at I-NNI reference point

CR-LDP is used across the I-NNI for connection control procedures as specified in ITU-T Recs G.8080/Y.1304 and G.7713/Y.1704. Additional messages, attributes, and procedures are added to support call control at the I-NNI and they need to pass through the I-NNI.

7.5 CR-LDP at E-NNI reference point

CR-LDP is used across the E-NNI for call and connection control procedures as specified in ITU-T Recs G.8080/Y.1304 and G.7713/Y.1704. Additional messages are added to support call control at the E-NNI.

The E-NNI reference point includes call control. This enables actions to be taken on the connection within a domain bounded by call controllers. For example, a connection failure occurs within a domain and it propagates to a UNI and E-NNI. Those endpoints re-establish a connection without propagating the connection failure beyond the E-NNI. This is a form of re-routing domain.

Different actions result when a call is received on an E-NNI depending on its direction. If the E-NNI receives a call from within the network, it establishes call state and continues the connection across the E-NNI bearer link(s). If the E-NNI receives a call from the other end of the reference point, it continues the connection into the network. In both cases, it maintains the association between the call and its connection(s).

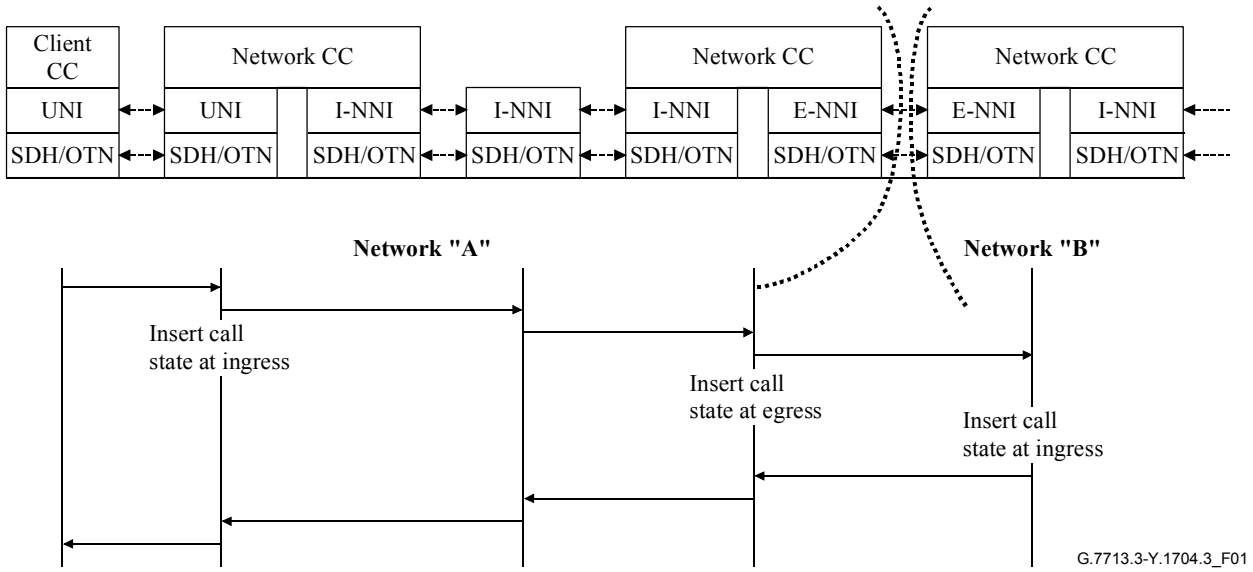


Figure 1/G.7713.3/Y.1704.3 – Progression of signalling

Figure 1 shows the progression of signalling from a client through network A and crossing the network A boundary to network B. Of particular interest in Figure 1 is the insertion of call states at the ingress and egress points of two networks. Call states are inserted before connection setup proceeds.

At the ingress NE of network A, UNI signalling messages are intercepted from a Client Call Controller (CCC) by a Network call control (NCC) which determines if the incoming call/connection can be accepted. Once the call is accepted, call state is inserted at the ingress NE and UNI messages are translated to the equivalent I-NNI signalling messages. I-NNI signalling proceeds across network A until it reaches the egress NE, where a call state is inserted there. Translation of the I-NNI signalling to E-NNI signalling that crosses network A boundary to network B is performed by Network Call Control associated with the E-NNI in Network A.

7.6 CR-LDP support for SPC

An SPC service assumes that both source and destination user-to-network connection segments are provisioned while the network connection segment is set up via the control plane. For example when the initial request is received from an external source (e.g., from management system), there is an implicit assumption that the control plane has adequate information to determine the specific destination (network-to-user) link connection to use. Support for SPC in CR-LDP is provided by making use of the Egress Label as defined in OIF UNI-01.0.

7.7 Defect handling

There are different types of defects that may affect the control plane. These defects may range from a simple signalling channel failure to multiple control plane node failures. The control plane needs to support appropriate behaviours to recover from these defects, initially attempting to recover from failures based on local control plane mechanisms, local interaction with the transport plane, and subsequently attempting to recover based on control plane interactions with external components.

General guidelines for defect handling include:

- Control plane failures are notified to the management plane. The management plane may direct the control plane to take certain actions due to the failure. These actions may include cleaning up of partial connections, release of certain connections, or other protocol-specific actions for state maintenance and recovery.
- A control plane node may provide a persistent storage of relevant information, such as call and connection state information, configuration information, and control plane neighbour information.
- After repair if connection/call states cannot be recovered, the control plane node may communicate with an external component to attempt state information recovery. External components may include neighbour control plane nodes or a persistent storage provided by a centralised (e.g., management plane) component.
- A control plane node notifies the management plane of the inability to recover (subset of) relevant information (e.g., inability to synchronize state of connections). The management plane may respond with the following actions (the default control plane action should be to retain the connections):
  - Release the impacted connections.
  - Retain the impacted connections. In this case, a connection may remain non-synchronized from the control plane perspective; however, the connection may remain valid.
- A control plane node (after recovering from node failure) may not be able to recover neighbour connection state from its local persistent storage and thus may lose information on connections. In this case the control plane node should request an external controller (e.g., the management system) for information to recover the connections. Similarly call state may be unrecovered and require management intervention to resolve. Specifics of the interactions between the control plane and management plane are beyond the scope of this Recommendation.

Thus, as a general rule:

- A control plane failure must not result in the release of established connections. Setup requests in the process of been completed may be removed (either during the failure or after recovery from failure). Established connections associated with a pending release request must be released (either during the failure or after recovery from failure).
- Additional actions by the control plane may be dependent on provisioned default behaviour for a particular type of connection.

However, a transport plane node failure may result in the release of established connections. This depends on the type of connection and the service level associated with each connection. For example, a "best-effort unprotected" connection may be released during a transport plane node failure while a "protected" connection must be restored (or maintained) based on the service level specification associated with that connection. Note that even in the case of a protected connection, the original connection may be released while a new connection is set up (this also depends on the type of protection used for the particular connection).

Three types of failures might occur. Those are signalling channel failure, bearer link failure, and nodal (crossconnect) failure. Failure recovery usually involves state recovery and resynchronization with adjacent NEs.

Signalling channel failure disrupts the flow of the control messages between two or more nodes. This failure condition should have no impact on established connections in the sense that those connections should continue in the active state without disruption. Upon recovery connection states must be resynchronized with adjacent NEs. Those connections that were partially established must be terminated.

The failure of the bearer link disrupts the flow of the data. Failure of the data plane needs to be communicated to the control plane for the appropriate action to be taken. Among the possible actions are the termination of connections that are affected by the link failure, re-routing of connections through other links or other nodes. The specific action taken for each connection depends on the protection requirements of a connection.

Nodal failure is similar to link failure. Nodal failure is implicitly communicated to the control plane through the loss of communication with the failed node. In this case the affected connection must be terminated or re-routed through other nodes.

8 GMPLS CR-LDP messages

All CR-LDP messages have a common structure that uses a Type-Length-Value (TLV) encoding scheme as illustrated in Figure 2. The number of bits allocated for each field is as shown. The Value part of a TLV-encoded object, or TLV for short, may itself contain one or more TLVs. The Length field specifies the length of the Value field in octets. The meaning of U and F bits is defined in RFC 3036.

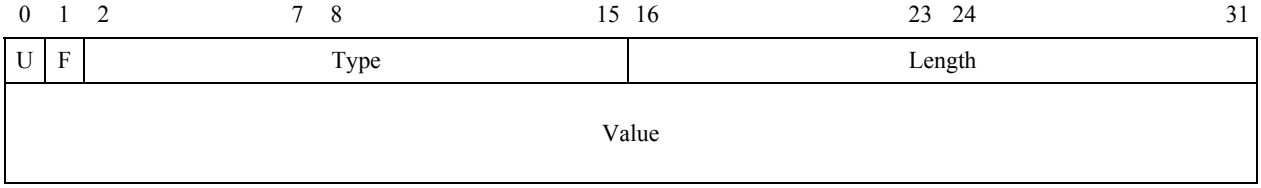


Figure 2/G.7713.3/Y.1704.3 – Structure of a TLV encoding scheme

Table 1 gives a summary the set of messages defined for CR-LDP along with their scope, function and source reference.

Table 1/G.7713.3/Y.1704.3 – Messages defined for CR-LDP

Message	Scope	Ref. point	Function	Source
Label Request	End-to-End	All	Sent by the calling party requesting the setup of a connection with certain attributes	RFC 3036
Label Mapping	End-to-End	All	Sent by the called party indicating the setup of a connection with the attributes given in Label Request message.	RFC 3036
Initialization	Local	All	For establishing LDP peers between network elements	RFC 3036

Table 1/G.7713.3/Y.1704.3 – Messages defined for CR-LDP

Message	Scope	Ref. point	Function	Source
Hello	Local	All	For peer discovery	RFC 3036
KeepAlive	Local	All	For maintenance of LDP session	RFC 3036
Label Release	End-to-End	All	Signals the teardown of a connection in the downstream direction	RFC 3036
Label Withdraw	End-to-End	All	Signals the teardown of a connection in the upstream direction	RFC 3036
Label Abort	End-to-End	All	Aborts an outstanding request	RFC 3036
Notification	Local or end-to-end	All	Notification of advisory or error information	RFC 3036
Query	Local for UNI and E-NNI. End-to-End for I-NNI	All	Gathers information about a connection	
Query Reply	Local for UNI and E-NNI. End-to-End for I-NNI	All	The queried information is encoded in a Query Reply message.	
Partial Query Reply	End-to-End	I-NNI	Same as Query Reply. It is sent in response to a Query message that have not traversed the whole route	
Call Setup	Local	UNI, E-NNI	Sent by the calling party requesting the set up of a call with certain attributes	New
Call Release	Local	UNI, E-NNI	Sent by the calling party requesting the set up of a call with certain attributes	New
NOTE – The term 'all' means UNI, E-NNI and I-NNI.				

The following messages are numbered from the RFC 3036 LDP namespace as allocated by the Internet Assigned Numbers Authority (IANA).

```
0x0500 = Call Setup
0x0501 = Call Release
```

Table 2 summarizes the various CR-LDP TLVs relevant to the call and connection control. It shows the various TLVs together with the purpose for each of them and in what message they might be included.

Table 2/G.7713.3/Y.1704.3 – Call and connection control TLVs

TLV name	Purpose	Message	Source
Generalized Label TLV	Identifies label assigned by a node to a particular connection	Label Request, Label Mapping Query, Query Response	RFC 3471
Suggested Label TLV	Upstream nodes suggest a set of labels for use by downstream nodes	Label Request	RFC 3471
Upstream Label TLV	The label used in the upstream direction for a bidirectional connection	Label Request	RFC 3471
Acceptable Label Set TLV	Indicates acceptable label values	Notification	RFC 3471
Label Set TLV	Limits the label choices of a downstream node	Label Request	RFC 3471
Generalized Label Request TLV	Communicates the characteristics required to support the connection being requested	Label Request	RFC 3471
Waveband Switching TLV	Label value in case of waveband switching	Label Mapping	RFC 3471
Protection TLV	Protection requirements for the connection being requested	Label Request	RFC 3472
Admin Status TLV	Indicates administrative state of a connection	Notification	RFC 3472
ER TLV	Describes the explicit route	Label Request, Query Reply, Partial Query Reply	RFC 3036; RFC 3212
Source Id TLV	Identifies the TNA address of the client source	Label Request, Label Mapping	OIF UNI-01.0
Dest Id TLV	Identifies the TNA address of the client destination	Label Request, Label Mapping	OIF UNI-01.0
Local Connection Id TLV	Identifies connections locally across the UNI	Label Request, Label Mapping, Label Withdraw, Label Release, Notification	OIF UNI-01.0
Egress Label TLV	Used across the UNI to indicate the label to be used at the destination client	Label Request, Label Mapping, Label Release, Label Withdraw, Status, Status Request, Notification	OIF UNI-01.0
Diversity TLV	Indicates the diversity attributes of the requested connection	Label Request, Label Mapping	OIF UNI-01.0
Contract Id TLV	Format and meaning will be determined by the service provider	Initialization	OIF UNI-01.0

Table 2/G.7713.3/Y.1704.3 – Call and connection control TLVs

TLV name	Purpose	Message	Source
UNI Service Level TLV	Indicates the service level agreement at the UNI. Values are assigned by service provider	Label Request, Label Mapping	OIF UNI-01.0
Call Id TLV	Identifies call across a single carrier network	Call Setup, Label Request, Label Mapping, Label Release, Label Withdraw	New
Call Capability TLV	Identifies capability of requested call.	Call Setup	New
SONET/SDH Traffic Parameters TLV	Traffic parameters of the requested SONET/SDH connection	Label Request, Label Mapping	IETF
Crankback TLV	Carries information back to source node regarding the location of connection setup failure	Notification	New
Feedback TLVs	Carries information back to source node regarding resource availability	Notification, Label Mapping, Label Withdraw	IETF, new

8.1 Call Setup message

The format of the Call Setup message is shown in Figure 3. The Call Id TLV and the Call Capability TLV are described in clause 9.

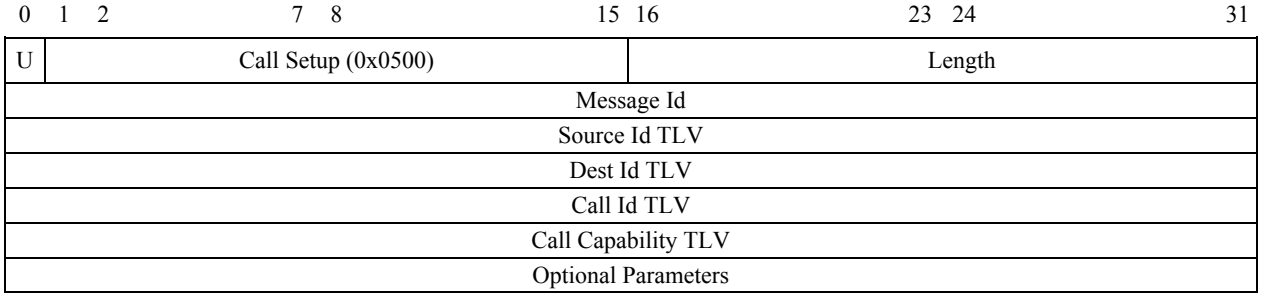


Figure 3/G.7713.3/Y.1704.3 – Structure of call setup message

The procedure for the Call Setup message is:

The Calling party initiates a call setup by sending the Call Setup message. The Call Setup message SHALL contain all the information required by the network to process the call. In particular, the Calling and Called party addresses.

The Call Setup message MUST include call identifier TLV. The call control entity shall identify the call using the selected identifier for the lifetime of the call.

The Call Setup message shall progress through the network to the called party. The called party may accept or reject the incoming call. An LDP Notification message with the appropriate status

code (to be defined) shall be used to inform the calling party whether the setup is successful. The call can be rejected by either the network, e.g., for policy reasons, or by the called party.

8.2 Call Release message

The format of the Call Release message is:

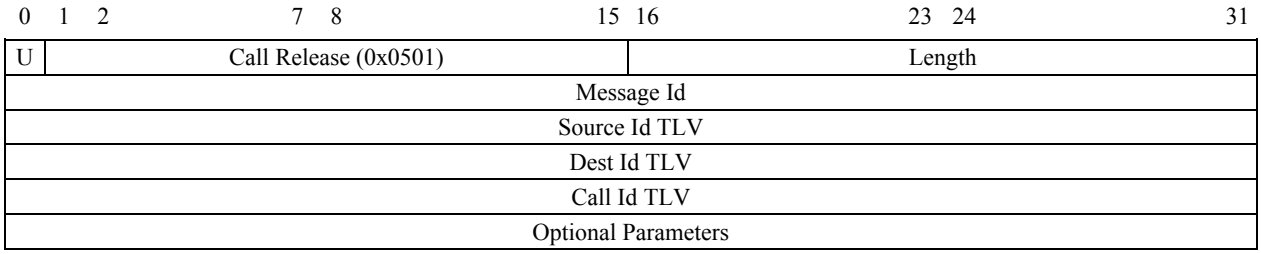


Figure 4/G.7713.3/Y.1704.3 – Structure of call release message

The Call Release message is sent by any entity of the network (client or network) to indicate the desire to terminate an existing call. The Call Release message shall contain all the information required by the network to process the call. In particular the Calling and Called party addresses.

The Call Release message also signals the need to delete all connections associated with the call as identified by the Call Id. Connection deletion in CR-LDP is implemented using Label Withdraw and/or Label Release messages. Therefore in an effort to keep the connection deletion procedure of CR-LDP intact, the reception of the Call Delete message by a network entity will trigger that entity to send a Label Withdraw or Label Release message depending on the direction of which Call Delete message has been received. Label Release or Label Withdraw messages will release or withdraw all connection labels that are associated to the call as identified by the Call Id TLV.

8.3 Label Request message

The format and the procedure of the Label Request message are as given in the OIF UNI-01.0, RFC 3036 and RFC 3212.

The Label Request message is used to signalling new connection, a new call (if logical separation of call/connection is being done), or modify an existing call. The Label Request message must include a Source Id TLV, a Destination Id TLV, Generalized label Request TLV, Connection Id TLV, and Call Id TLV. Absence of one or more of those TLVs will result in the termination of the setup process and a notification to the source.

The Label Request message may optionally include, Egress Label TLV, Upstream Label TLV, Suggested Label TLV, Label Set TLV, Diversity TLV.

8.4 Label Mapping message

The format and the procedure of the Label Mapping message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

The Label Mapping message carries label information and propagates in a direction opposite to that of the Label Request message. Label Mapping message could be viewed as a confirmation that the setup request was successful. The Label Mapping message must include, Generalized Label TLV, Connection Id TLV, and Call Id TLV. To correlate a mapping message to the corresponding request message, a Label Mapping message must include the identity of the Label Request message (Label Request Message Id TLV) to which it is the response.

8.5 Initialization message

The format and the procedure of the Initialization message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

The initialization message is exchanged between two CR-LDP peers as part of the CR-LDP session establishment procedure. The Initialization message specifies values proposed by the sending node for parameters that must be negotiated at the LDP session level, e.g., KeepAlive Time, etc.

8.6 Hello message

The format and the procedure of the Hello message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

The Hello messages are exchanged as part of the CR-LDP discovery mechanism. Both basic and extended discovery mechanisms are supported in this Recommendation.

8.7 KeepAlive message

The format and the procedure of the KeepAlive message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

A node sends KeepAlive messages as part of a mechanism that monitors the integrity of the CR-LDP session transport connection.

8.8 Label Release message

The format and the procedure of the Label Release message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212. The added procedure in the context of a Call Release message is as given in 10.3.

The Label Release message is used for connection release in the downstream direction. It is also used to acknowledge a connection release request in the upstream direction. In this case the delete request is confirmed by the use of LDP Notification message with the status code "delete_success".

8.9 Label Withdraw message

The format and the procedure of the Label Withdraw message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212. The added procedure in the context of Call Release message is as given in 10.3.

The Label Withdraw message is used for connection release in the upstream direction. The Label Release message is used to acknowledge the withdrawal of the label (releasing the connection) by the upstream node.

8.10 Label Abort message

The format and the procedure of the Label Abort message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

Label Abort message maybe used to abort an outstanding Label Request message.

8.11 Notification message

The format and the procedure of the Notification message are as given in OIF UNI-01.0, RFC 3036 and RFC 3212.

The Notification message is used by a node to notify its peers of advisory or error conditions.

8.12 Query, Query Reply, and Partial Query reply messages

The connection query functionality defined in ITU-T Rec. G.7713/Y.1704 is implemented with the use of the CR-LDP Query and Query-Reply messages. A Partial Query-Reply message is also defined. The format of the Query message is as shown in Figure 5:

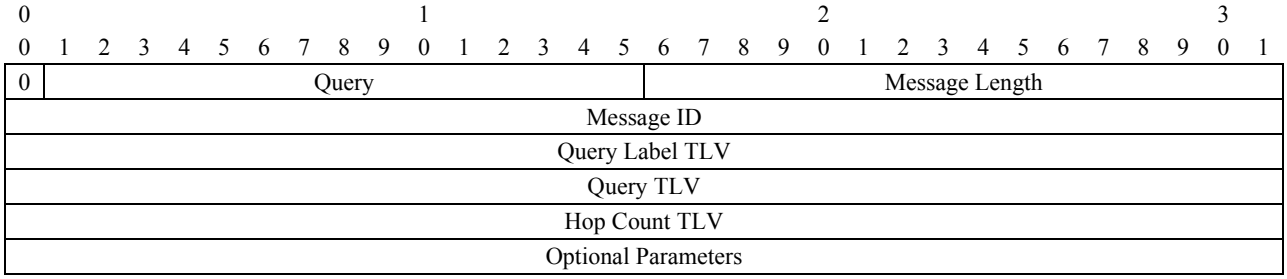


Figure 5/G.7713.3/Y.1704.3 – Query Message format

The format of the Query-Reply and the Partial Query-Reply messages is as shown in Figure 6:

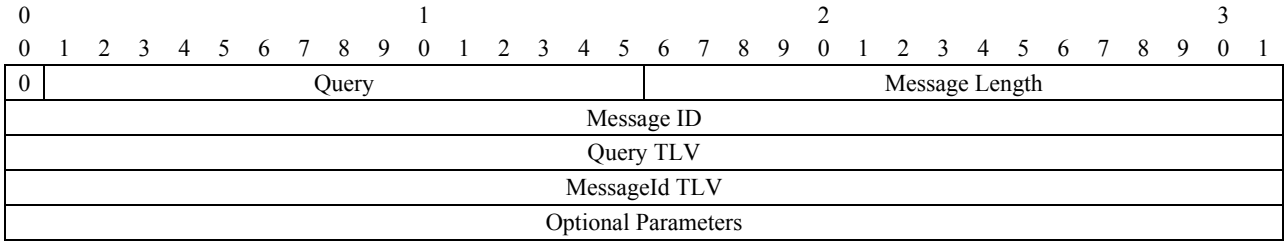
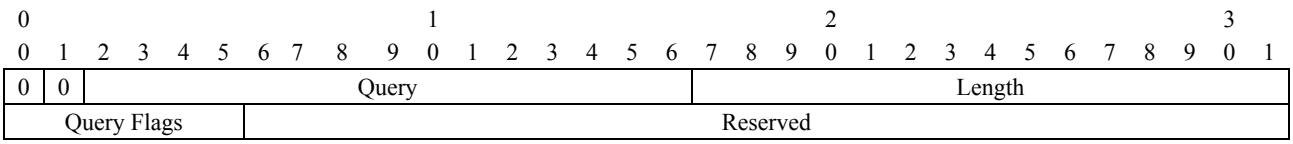


Figure 6/G.7713.3/Y.1704.3 – Query Reply message format

The Query message is sent by a network entity to gather information about a particular connection. The connection to be queried is identified by its label in the Query Label TLV. A connection controller along the path of the connection that receives the message must replace the incoming label with the outgoing label in the query Label TLV. The Query message includes a Query TLV that indicates the relevant connection parameters to be queried. Currently those parameters are defined:

- connection bandwidth;
- labels that are associated to each hop in the connection path;
- The NEs which form the connection that is queried. Each connection controller that receives the Query Reply message has to encode the current hop in the ER-TLV.



Query Flags can be set according to what the Query is used for. A query flag is set when it is 1.

Q8	Reserved	Q4	Q3	Q2	Q1

They can be:

– Q1 : query the bandwidth; if set, the connection controller that receives the Query message has to encode the bandwidth that is available on the link (unused bandwidth);

– Q2 : query the labels which are associated to each hop in the path;

– Q3 : query the NEs which form the connection which is queried; if set, the connection controller that received the Query-Reply message has to encode the current hop or hops (in its span of control) in the ER-TLV;

– Q4 : not used for ASON;

– Q8 : if set, the ingress requests partial query-replies; each connection controller along the path is signalled to send a Partial Query Reply.

The reserved bits need to be set to zero on transmission and must be ignored on receipt. They might be used in the future to signal other types of queried information.

The Query Label TLV is used to encode the labels used along the path which is queried.

NOTE – Query Label TLV is used in both Query and Query Reply. It is a required parameter in the Query message and it is an optional parameter in Query Reply message. When being used in the Query message, it carries the label or stack of labels which are being followed and queried. When being used in the Query Reply message, it carries the list of labels which make up the queried path.

The format for the Query Label TLV is as shown in Figure 7:

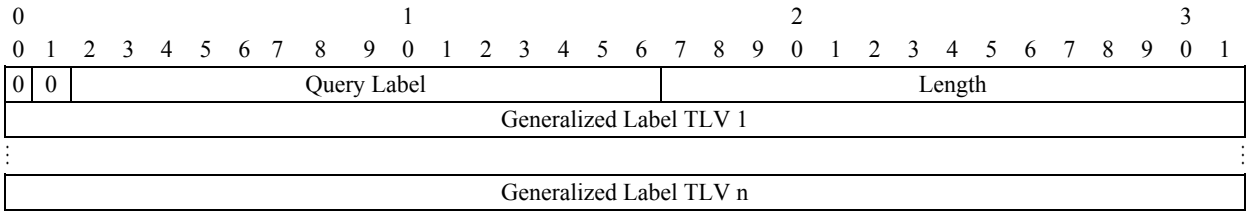


Figure 7/G.7713.3/Y.1704.3 – Query Label TLV format

The Query-Reply message is sent in the upstream direction by the egress connection manager that receives the Query message. The egress node has to encode into the Query-Reply message a MessageId TLV. The mapping between Query and Query-Reply message is done based on the Message Id.

The Partial Query-Reply message is initiated by connection managers along the path of the queried connection. The message is generated only if the following rules apply:

- if the Query message asked for partial replies;
- if the connection manager is configured to provide partial replies.

The Partial Query-Reply message procedure is similar to the Query-Reply procedure.

Across the UNI and the E-NNI, the Query message is initiated in either direction. For example across the UNI the Query message could be generated by the end system or the connection manager connected to it. A Query-Reply message is always sent in the other direction. The use of the Partial Query-Reply is not allowed at the UNI and the E-NNI. The Query-Reply message will include connection parameters that are requested by the Query message. For both the UNI and E-NNI, the

scope of the Query message is limited to the single hop between the two connection managers involved.

At the I-NNI the Query message is initiated by the ingress connection manager. The Query-Reply message is sent by the egress connection manager that receives the Query message. The Query-Reply message propagates in the upstream direction collecting connection parameters that were indicated in the Query message. The use of the Partial Query-Reply message is allowed at the I-NNI. A connection manager that contains connection state could generate a Partial Query-Reply message as long as it satisfies the two conditions mentioned above.

9 GMPLS CR-LDP attributes

This clause provides the TLVs for the various CR-LDP messages. Table 2 provides a description of the TLVs defined for CR-LDP in the context of GMPLS.

The following TLVs are numbered from the RFC 3036 LDP namespace as allocated by IANA:

```
0x0831 = Op-Sp Call ID TLV
0x0832 = GU Call ID TLV
0x0833 = Call Capability TLV
0x0834 = Crankback TLV
```

9.1 Source Id TLV

The format and procedure of the Source ID TLV is as defined in OIF UNI-01.0.

9.2 Dest Id TLV

The Dest Id TLV is as defined in OIF UNI-01.0.

9.3 ER TLV

Acceptable "hop TLVs" that can be contained in the ER TLV are the ER-Hop TLVs [RFC 3212] but with no AS number or LSPID types. To comply with control and transport plane separation, the IPv4 address of the type 1 and the IPv6 address of the type 2 Hop TLVs are not control plane names (e.g., routing controllers) but rather transport plane names.

9.4 Call Id TLV

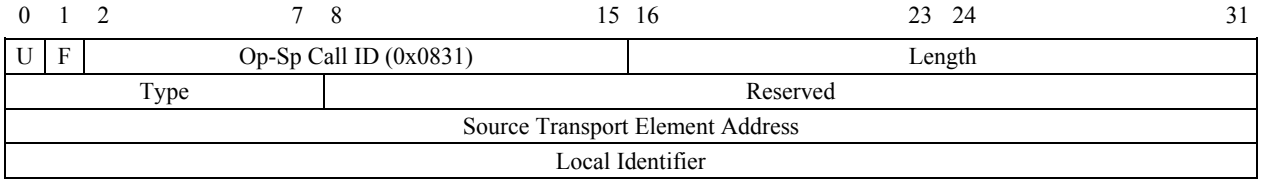
An established call may be identified by a Call Id. The Call Id is a globally unique identifier that is set by the source network. The structure for the call identifier (to guarantee global uniqueness) is to concatenate a globally unique fixed Id (composed of country code, carrier code, unique access point code) with an operator specific Id (where the operator specific Id is composed of a source transport network element address – and a local identifier).

Therefore, a generic CALL_Id with global uniqueness includes <global Id> (composed of <country code> plus <carrier code> plus <unique access point code>) and <operator specific Id> (composed of <source transport network element address> plus <local identifier>). For a CALL_Id that only requires operator specific uniqueness only the <operator specific Id> is needed, while for a CALL_Id that requires to be globally unique both <global ID> and <operator specific Id> are needed.

The <global Id> shall consist of a three-character International Segment (the <country code>) and a twelve-character National Segment (the <carrier code> plus <unique access point code>). These characters shall be coded according to ITU-T Rec. T.50. The International Segment (IS) field provides a 3 character ISO 3166 Geographic/Political Country Code. The country code shall be based on the three-character uppercase alphabetic ISO 3166 Country Code (e.g., USA, FRA).

The National Segment (NS) field consists of two sub-fields: the ITU Carrier Code followed by a Unique Access Point Code. The ITU Carrier Code is a code assigned to a network operator/service provider, maintained by the ITU-T Telecommunication Standardization Bureau in association with ITU-T Rec. M.1400. This code shall consist of 1-6 left-justified characters, alphabetic, or leading alphabetic with trailing numeric. The unique access point code shall be a matter for the organization to which the country code and ITU carrier code have been assigned, provided that uniqueness is guaranteed. This code shall consist of 6-11 characters, with trailing NULL, completing the 12-character National Segment.

The format of the operator specific CALL_Id:



The format of the Globally Unique Call_Id:

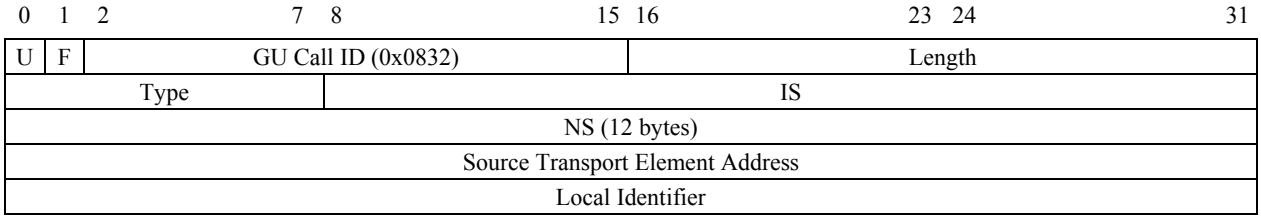


Figure 8/G.7713.3/Y.1704.3 – Structure of the Call Id TLV

In both cases, a "Type" field is defined to indicate the type of format used for the source transport network element address. The Type field has the following meaning:

For Type = 0x01, the source transport network element address is 4 bytes;

For Type = 0x02, the source transport network element address is 16 bytes;

For Type = 0x03, the source transport network element address is 20 bytes;

For type = 0x04, the source transport network element address is 6 bytes;

For type = 0x7f, the source transport network element address has the length defined by the vendor;

The Source Transport Element Address is an address of the transport network element (SSN) controlled by the source network. It can be 4, 6, 16, or 20 bytes long as determined by the type;

The local identifier is a 64-bit identifier that remains constant over the life of the call.

Note that if the source transport network element address is assigned from an address space that is globally unique, then the operator-specific CALL_Id may also be used to represent a globally unique CALL_Id. However, this is not guaranteed since this address may be assigned from an operator-specific address space.

The following processing rules are applicable to the CALL_ID object:

– For initial calls, the calling/originating party call controller must set the CALL_Id values to all-zeros.

– For a new call request, the source network call controller (SNCC) sets the appropriate type and value for the CALL_Id.

– For an existing call (in case CALL_Id is non-zero) the SNCC verifies existence of the call.
– The CALL_Id object on all messages MUST be sent from ingress call controller to egress call controller by all other (intermediate) controllers without alteration.
– The destination user/client receiving the request uses the CALL_Id value as reference to the requested call between the source user and itself. Subsequent actions related to the call uses the CALL_Id as the reference identifier.

9.5 Call Capability TLV

The format of the Call Capability TLV is as shown in Figure 9:

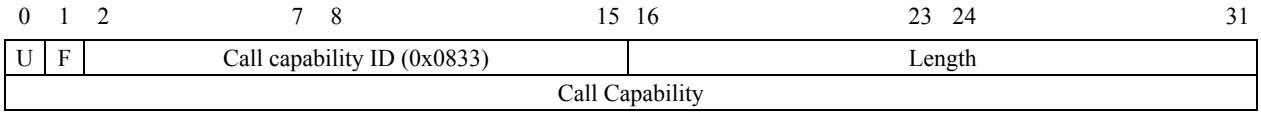


Figure 9/G.7713.3/Y.1704.3 – Structure of the Call Capability TLV

The Call Capability TLV is used to explicitly indicate the configuration potential of the call. Its contents and procedure are a local matter between call controllers (client to network and/or network to network).

9.6 Generalized Label Request TLV

The format and the procedure of the Generalized Label Request TLV is as specified in RFC 3471 and RFC 3472.

9.7 Generalized Label TLV

The format and the procedure of the Generalized Label TLV is as specified in RFC 3471 and RFC 3472.

9.8 Upstream Label TLV

The format and the procedure of the Upstream Label TLV is as specified in RFC 3471 and RFC 3472.

9.9 Acceptable Label TLV

The format and the procedure of the Acceptable Label TLV is as specified in RFC 3471 and RFC 3472.

9.10 Label Set TLV

The format and the procedure of the Label Set TLV is as specified in RFC 3471 and RFC 3472.

9.11 Suggested Label Set TLV

The format and the procedure of the Suggested Label Set TLV is as specified in RFC 3471 and RFC 3472.

9.12 Admin Status TLV

The format and the procedure of the Admin Status TLV is as specified in RFC 3471 and RFC 3472.

9.13 Contract Id TLV

The format and the procedure of the Contract Id TLV is as defined in OIF UNI-01.0.

9.14 UNI Service TLV

The format and the procedure of the UNI Service TLV is as defined in OIF UNI-01.0. The service level sub-object can be used to identify specific levels of Class of Service to be provided to the call/connection requested. The value and interpretation of specific classes of service is defined by carriers, in agreement with clients in the case of switched connections.

9.15 Feedback TLV

The format and the procedure of the Feedback TLV is as specified in Appendix III.

9.16 Local Connection Id TLV

The format and the procedure of the Local Connection Id TLV is as specified in OIF UNI-01.0

9.17 Protection TLV

The format and the procedure of the Protection TLV is as specified in OIF UNI-01.0

9.18 Diversity TLV

The format and the procedure of the Diversity TLV is as specified in OIF UNI-01.0

9.19 Status TLV

The status TLV is as defined in RFC 3036 and RFC 3212.

9.20 Interface TLV

The Interface ID TLV is defined in RFC 3471 and is used to provide context to the various label TLVs. For example, an unnumbered link. In Label Request messages, the Interface ID TLV accompanies the Upstream and Suggested Label TLVs. For the Label Mapping message, the Interface ID TLV accompanies the Generalized Label TLV. Additional contexts (sub-TLVs within the Interface ID TLV) may be needed in the future for more complex contexts like groups of links.

As with Hop TLVs, the IP addresses used within the Interface ID TLV should refer to transport names and not control plane names. This is because the Interface ID TLV is an encoding of a G.8080/Y.1304 SNPP id.

10 Call and connection control procedures using CR-LDP

This clause describes the basic call and connection control operations using CR-LDP. The procedures described in this Recommendation are, for the most part, general for UNI, I-NNI, and E-NNI. Explicit mention will be made where differences arise.

10.1 CR-LDP discovery and session initialization

CR-LDP discovery is the process by which CR-LDP nodes automatically discover one another. Automatic discovery eliminates the need for explicit configuration activity. CR-LDP employs a Hello mechanism to enable discovery. Hello messages are exchanged using the UDP protocol (the only CR-LDP message that is not transported using TCP). The Hello procedure, including extended Hello, as defined in RFC 3036 is directly applicable here with no modification.

CR-LDP session initialization is executed by the exchange of the Initialization message. Initialization messages carry information that is relevant to nodal capabilities, e.g., support for Fault Tolerant operation. The Initialization message procedure as described in RFC 3036 is directly applicable here without modification.

10.2 Call setup using CR-LDP

As previously mentioned, LDP and CR-LDP as defined, respectively, in RFC 3036 and RFC 3212 do not support the call and connection control separation as defined in ITU-T Recs G.8080/Y.1304 and G.7713//Y.1704. Extensions (i.e., new messages and new TLVs) are defined in this Recommendation to support this separation.

Two call setup models are applicable. The first is a call setup request that has no connection associated with it. The signalling message in this case includes information that is only related to call parameters, e.g., source and destination addresses. Connections associated with this call can subsequently be set up using the connection setup procedure described in 10.4.

In the second call setup model, the call setup request carries with it a request for connection setup. This may be a desirable feature to expedite the process of a connection setup. Subsequent connections can be set up using the connection setup procedure described in 10.4.

CR-LDP supports both call setup models.

In the case of the first call setup model, a new CR-LDP message, the Call Setup message, is introduced. The Call Setup message is sent by the calling party and progresses through the network until it reaches the destination (called party). A Notification message is sent back to the calling party indicating the success or failure of the call setup. Call setup may fail for a number of reasons, in which case the Notification message must also include the reason for the failure. Figure 10 shows a successful call set up sequence for the first model.

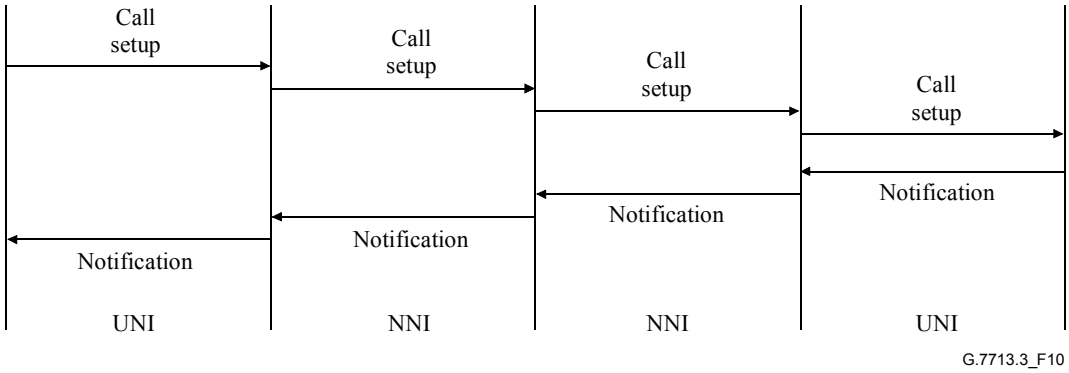


Figure 10/G.7713.3/Y.1704.3 – Call setup with no associated connection

The second model for call setup allows for the setup of connections using the same request. Connection setup in CR-LDP is carried out using the LDP Label Request and Label Mapping messages. Since label assignment is needed, then the same messages for connection setup are used for call setup in this case. In this case, the Label Request message will carry both call and connection parameters, e.g., connection traffic parameters. Figure 11 shows the call and connection setup for the second model. The Notification message back to the called party is used to confirm the setup of the connection and its readiness.

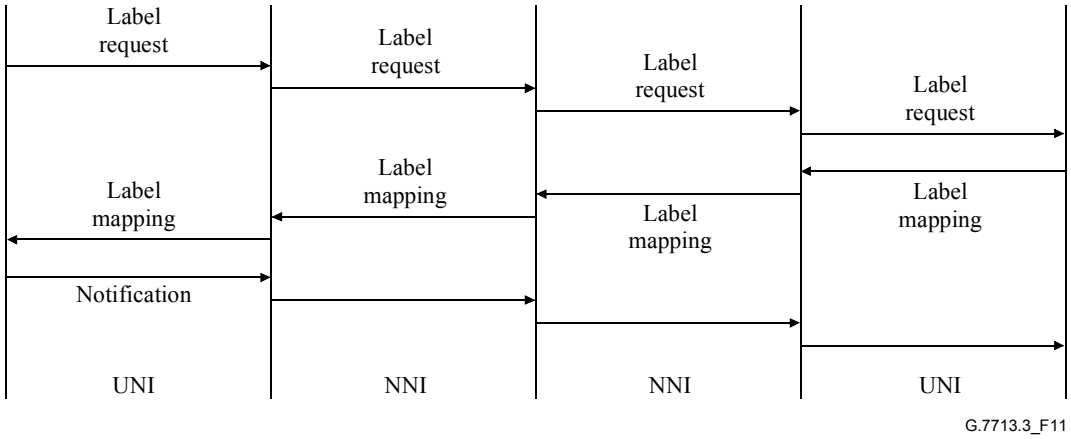


Figure 11/G.7713.3/Y.1704.3 – Call setup with associated connection

Subsequent connection setup and teardown can take place at anytime following completion of the call setup. There is the need for a mechanism to associate connections and calls and this is achieved by using the Call Id as defined before.

An important application of the call and connection separation is the ability to set up a call with multiple connections for the purpose of protection, e.g., 1+1. Figure 12 shows the message sequence for call setup with two connections associated to it.

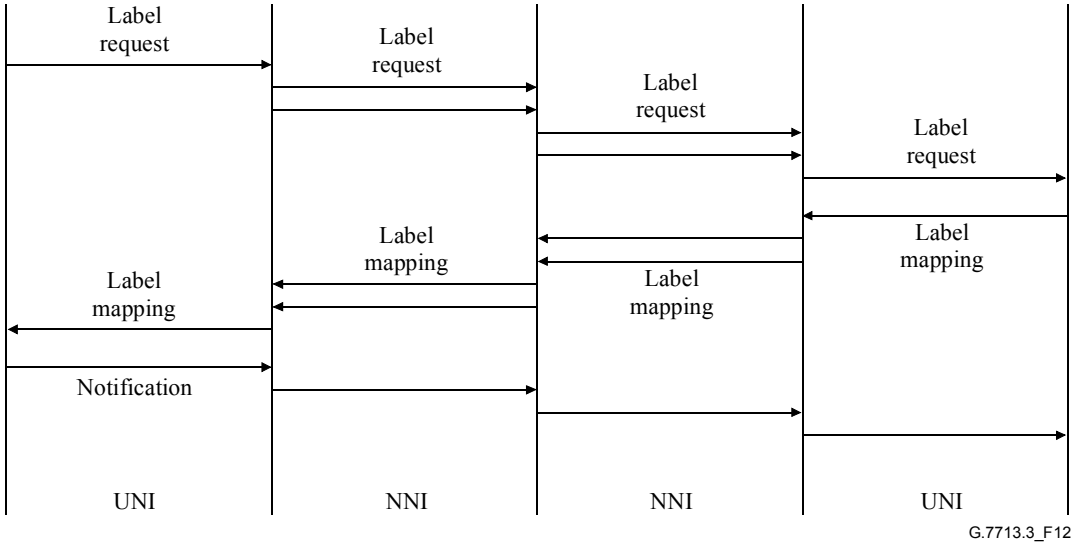


Figure 12/G.7713.3/Y.1704.3 – 1+1 application using CR-LDP

Figure 12 follows the same procedure as for the case shown in Figure 11. The difference is in the need to set up two connections simultaneously. This is achieved by generating two Label Request messages at the NNI to account for the two connections.

10.3 Call Release using CR-LDP

A new CR-LDP message, Call Release, is introduced for call teardown irrespective of the model used for setup. The call teardown operation must result in the teardown of all connections associated with the call. Connection teardown (see 10.6) in CR-LDP is achieved by the use of Label Release and Label Withdraw messages. The same procedure is used for connection deletion. When a Call Release message is received, it triggers the CR-LDP connection release mechanism by sending Label Release or Label Withdraw messages as required. Figure 13 shows the graceful release mechanism. The Notification message includes the Admin_Status TLV to turn off the alarm before the release of connections.

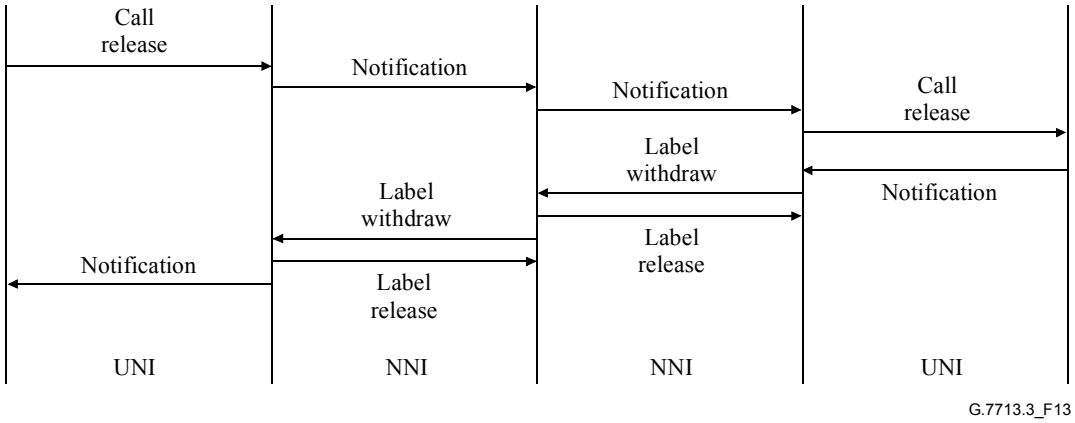


Figure 13/G.7713.3/Y.1704.3 – Call release initiated by calling party

The call teardown process is assumed to be complete when the initiator of the Call Release message receives a Notification message confirming completion of the process. The called party sends this Notification message after ensuring that it has deleted all connection associated with that call.

In some instances non-graceful (no set off of alarms is performed beforehand) release of connections is needed. Figure 14 shows the signalling flow for the non-graceful call/connection release initiated by the source where there are two connections associated with the call.

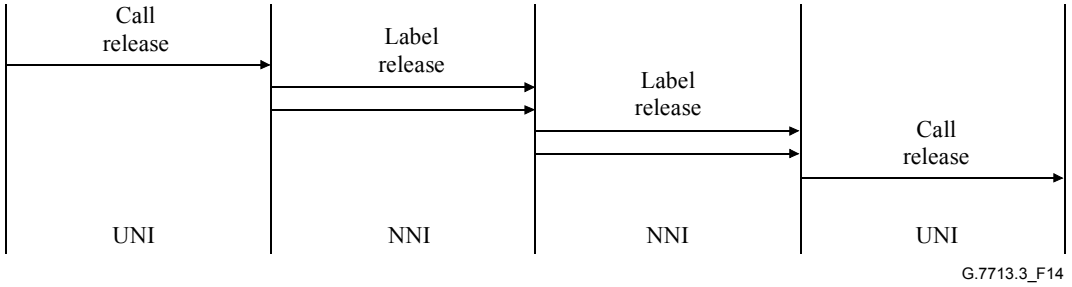


Figure 14/G.7713.3/Y.1704.3 – Non-graceful call release initiated by source

Non-graceful call/connection release initiated by the destination is shown in Figure 15.

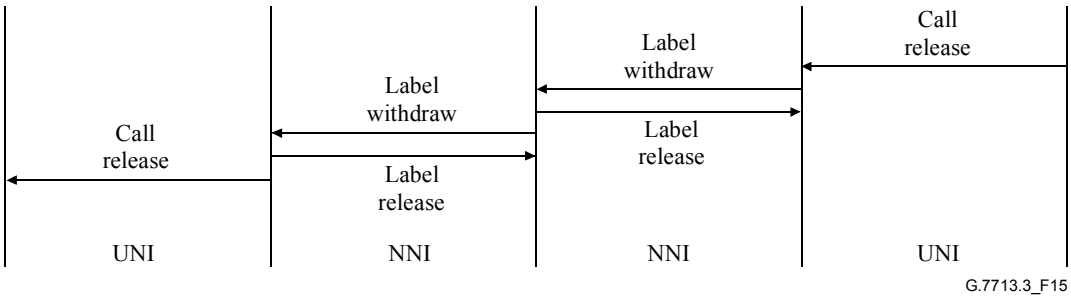


Figure 15/G.7713.3/Y.1704.3 – Non-graceful call release initiated by destination

10.4 Connection setup using CR-LDP

Connection setup is achieved in CR-LDP by using the Label Request and Label Mapping messages. The Label Request message is transmitted in the forward direction and carries connection parameters. This message may also carry call parameters, e.g., for the case where call setup is accompanied by connection setup. The Label Request message requests the assignment of a label for the requested connection at each of the nodes along the path. This label represents an SNP.

The setup of a connection assumes that a call has been established or is in the process of being established. The Label Request message includes a call identification element that is used for call and connection association. Call identification is assigned by the network and its scope is unique within a single network (may include multiple domains).

ASON connections are bidirectional. As specified in GMPLS, a bidirectional connection is signalled by the inclusion of the Upstream Label in the Label Request message. Reception of the Label Request message by the destination signifies a successful reservation, i.e., all the requested connection attributes of the bidirectional connection can be satisfied. However, it does not imply that the connection is available for data transport. The connection is only available when the configuration of intermediate cross-connects is complete. The configuration of any intermediate cross-connects is likely to require some time to complete and, depending on the technology used, this delay may be significant, e.g., in the order of 10's or 100's of ms.

The destination sends a Label Mapping message in response to the Label Request, but not before it has set up its own switch fabric. If it so desires, the destination may indicate to the source that a reservation confirmation indication is needed. The reservation confirmation indication is implemented using the LDP Notification message with the status code "reservation_confirm".

Contention for labels may occur between two bidirectional connection setup requests travelling in opposite directions. This contention occurs when both sides allocate the same resources (labels) at effectively the same instant. To resolve contention, the node with the higher node Id will succeed and must issue a Notification message with a "Routing problem/Label allocation failure" indication. Upon receipt of such an error message, the other node should try to allocate a different Upstream label (and a different Suggested Label if used) to the bidirectional path. However, if no other resources are available, the node must proceed with standard error handling.

Figure 16 shows the connection setup sequence using CR-LDP.

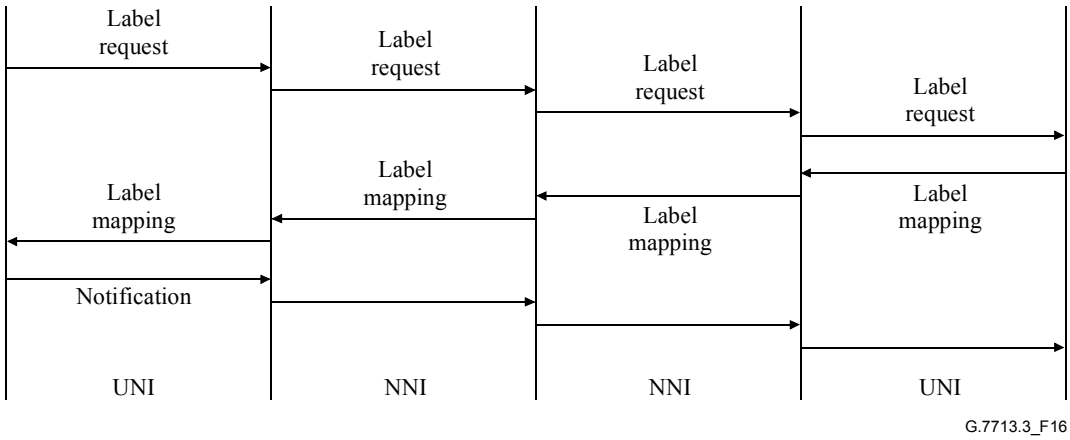


Figure 16/G.7713.3/Y.1704.3 – Connection setup

The connection create request might fail for a number of reasons, e.g., insufficient or no bandwidth available, no physical connectivity, SLA violation, connection rejected by far end client. In this case failure of the create request is indicated to the source using the LDP Notification message with the status code reflecting the reason for the failure, e.g., resources unavailable. Figure 17 shows a create request rejection by the network.

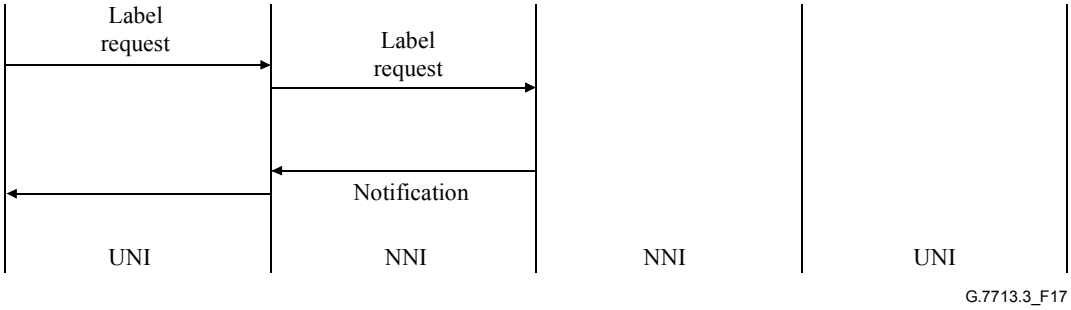


Figure 17/G.7713.3/Y.1704.3 – Setup request rejection by network

Should a client desire to abort the connection create process after sending the Label Request message, an LDP Abort message must be sent as defined in section 3.5.9 of RFC 3036. Specifically, the Message Id used in the Label Request Message is used in the Abort Message as the temporary local connection identifier.

10.5 Connection modification using CR-LDP

Connection modification in CR-LDP is achieved by the calling party sending a new Label Request message that includes the identity of the connection to be modified, as well as an indication that this is a modification request (as opposed to a new setup request). An action flag is associated with the Local Connection Id TLV to indicate if the Label Request message is for a new setup or for modification.

Connection modification is only allowed for already existing connections. The Label Request message includes those parameters that need to be changed, e.g., connection traffic parameters. It follows the same procedure as in the case of a new connection setup.

10.6 Connection release using CR-LDP

LDP employs two mechanisms whereby a node may inform its peer to stop using a particular label. The first method is based on the use of Label Withdraw message and it is used to signal to a peer that the peer may not continue to use a specific label mapping that the node has previously advertised. The second method is based on the use of Label Release message and it is sent to signal to a peer that the CR-LDP connection controller no longer needs a specific label mapping previously requested and/or advertised by the peer.

The CR-LDP extensions for G.7713/Y.1704 make use of the Label Release and Label Withdraw messages for connection deletion. The choice of which message to use depends on the entity that initiates the deletion. The Label Withdraw message is used for the case where the connection deletion is in the upstream direction. As per the LDP procedure in section 3.5.10 of RFC 3036, Label Release message is used in this case to acknowledge the delete request.

The Label Release message is used for the cases where connection deletion is in the downstream direction. In this case the delete request is confirmed by the use of LDP Notification message with the status code "delete_success".

Figures 18 and 19 show graceful connection deletion requests by the source and destination respectively. Figure 18 shows that the delete request is preceded by an LDP Notification with the Admin_Status TLV indicating a connection release. In optical networks, indication of bearer failure (e.g., AIS) can propagate faster than the delete request. Thus downstream nodes will receive this and potentially alarm on it. This alarm could be used to incorrectly trigger restoration and/or protection activity. To address this issue, a Notification message should be sent along the connection's route to inform all nodes of the intended deletion. Upon the receipt of this message, each node should disable its alarm reporting and protection mechanisms on the indicated connection.

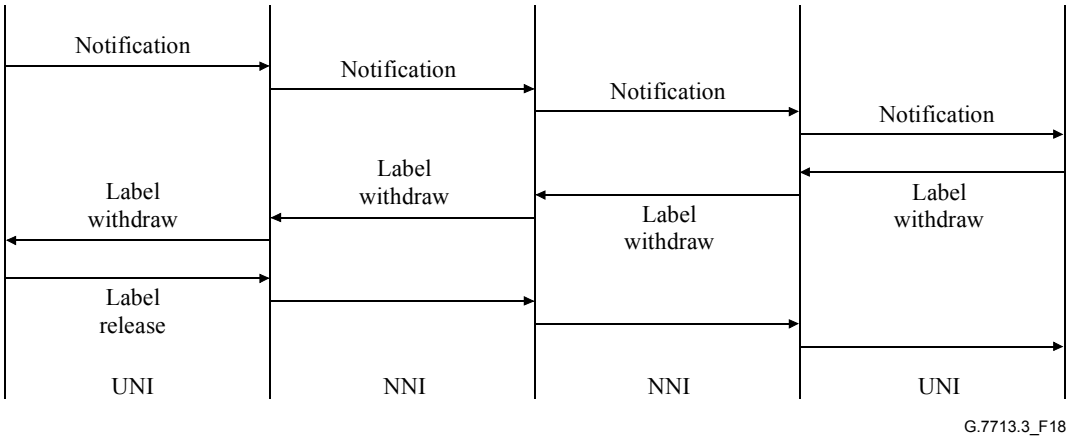


Figure 18/G.7713.3/Y.1704.3 – Connection deletion initiated by the source

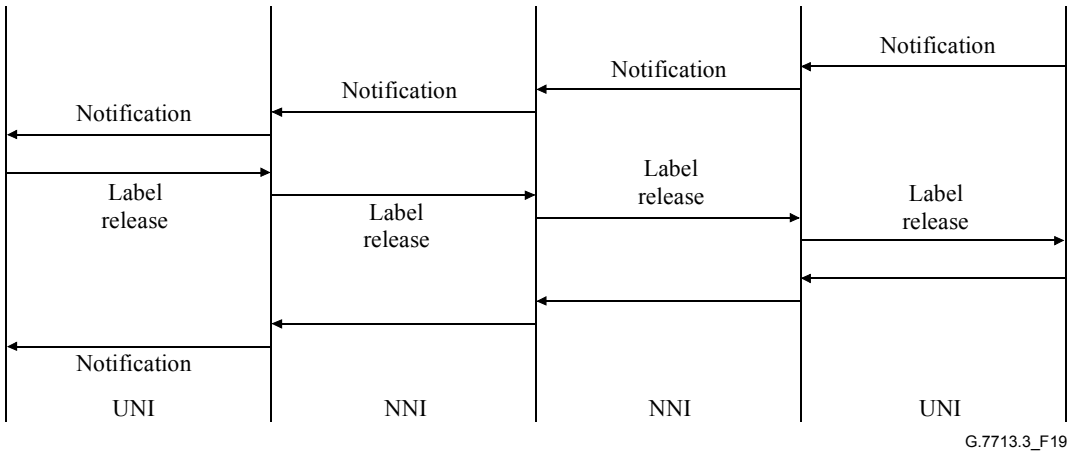


Figure 19/G.7713.3/Y.1704.3 – Connection deletion initiated by the destination

Figure 20 shows a connection deletion scenario initiated by the network or from a forced deletion request from an OAM entity. In this case both Label Withdraw and Label Release messages are used to initiate the deletion request.

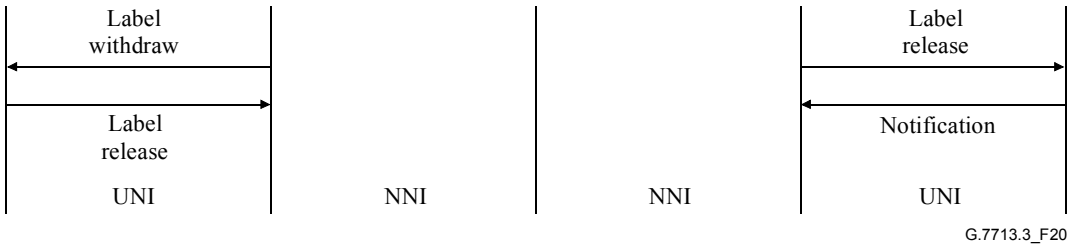


Figure 20/G.7713.3/Y.1704.3 – Network-initiated connection deletion

10.7 Feedback using CR-LDP

To improve the probability of successful connection setup, CR-LDP employs feedback mechanisms to allow for better decision making regarding the selection of explicit routes.

Feedback is a mechanism by which a source node knows about the success or failure of its path selection by receiving feedback from the paths it is attempting to set up. This information can be incorporated into subsequent route computations which greatly improves the accuracy of the overall routing solution by significantly reducing database discrepancies.

10.7.1 Dependencies on routing

Call and connection controllers query the routing controller in order to obtain path information. Because of this, signalling is dependent on routing to set up connections. Call control may query routing for two paths in response to a single call request, and then initiate two connections with the results. For a single connection setup, connection controllers could query routing at every subnetwork if step-by-step routing is being used.

10.7.2 Feedback mechanism

As connections are established in an ASON network, bandwidth on links become reserved for connections that are set up. For example, the number of STM-1s allocated to trails in a STM-64 link. Path selection in routing operates more effectively when bandwidth utilization information in the network is current. Stale information can result in calls being blocked because path selection operated on a network view that was more optimistic of its resources. In this case as the connection

is being set up, signalling encounters a node that is unable to reserve another link for the connection. The opposite condition can occur when network information is pessimistic. In this case, path selection may block the call at ingress because it thinks there is insufficient bandwidth to begin with when, in fact, there could exist sufficient bandwidth in the network for the connection.

Keeping routing information sufficiently current can require a high amount of routing control information to be passed continuously. This might well be prohibitive in the signalling network (DCN).

A mechanism called "feedback" is designed to alleviate the difficulty of balancing call blocking against frequency and volume of routing information updates. The feedback mechanism stores link information (e.g., utilization) in signalling messages that flow back to call/connection controller sources. These are Label Mapping, Label Release, Label Withdraw and Notification messages. When the message is received at the source, the link information is included with the topology information. Path calculation uses the more current information when invoked.

Note that the feedback mechanism only benefits path selection functions that depend on full topology information. This implies that it is only applicable to routing protocol controllers that exchange and store full topology information.

A good example of how feedback can reduce call blocking is when a connection setup fails due to lack of resources at an intermediate link. Information about that link's utilization is fed back to the source node. A subsequent call request to the same destination will not progress to the same intermediate link because path selection will use the current information it has to disqualify that link.

While path selection uses link information obtained from feedback, the routing controller does not propagate them to peer routing controllers. Routing information received from peer routing controllers that is newer than information received from feedback always overrides (and removes) feedback information.

Feedback changes the relationship between signalling and routing in that routing is now assisted by feedback. Routing is not made dependent on signalling for its operation, but the effectiveness of path selection and hence call setup is improved through the use of the feedback mechanism.

Appendix III describes an encoding for containing feedback information.

10.8 Failure detection and recovery in CR-LDP

CR-LDP employs a Keep Alive mechanism to maintain connectivity between peers. Every node keeps a KeepAlive timer for each peer that it resets every time it receives LDP message. Specific KeepAlive message can be exchanged between peers to when the flow of LDP messages is low to keep the timer from expiry. Timer expiry is an indication that a peer has been lost as a result of failure.

Failure may be due to loss of communication, i.e., loss of the signalling channel or due to the loss of the nodal control plane, i.e., a node is down. A failed node may or may not preserve connection state. A node that is provisioned with backup copies of software and/or redundant hardware will be able to maintain the connection state and is called a carrier-grade node. It cannot be assumed that a non carrier-grade node will retain any state, however, as a minimum it should be able to retain its forwarding state. Inability to do this means that recovery from failures would not be possible.

In both types of failure there is the need for the recovery of the LDP session (re-establishment of TCP session and recovery of lost control messages). Following this step there is the need to resynchronize connection state between peers in those cases where state has been lost.

CR-LDP FT operation assumes carrier-grade nodes are available. It recovers the lost LDP session by assigning sequence numbers to CR-LDP messages and employing a message acknowledgement mechanism. CR-LDP messages that are lost during the failure are detected by absence of their acknowledgments and retransmitted upon the re-establishment of the LDP session.

State resynchronization across the UNI is achieved locally at both sides of the interface by means of Status and Status Response message. The resynchronization procedure is described at the OIF UNI-01.0.

Across the NNI state resynchronization could be achieved by using Query and Query Reply messages. Those messages have end-to-end scope within the network and can collect information pertaining to connection states. Resynchronization could also be achieved by using the LDP restart procedure as defined in RFC 3478. During NNI resynchronization, the network could initiate connection deletion towards one direction only for cleaning up inconsistent connections. In this case, the network either initiates a Label Release message towards to tail end of connection, or initiates Label Withdraw message towards to head end of connection.

For non carrier-grade nodes there is no mechanism to restore the failed LDP session. A new LDP session has to be initiated using the normal LDP procedure. State synchronization at the UNI could be achieved using the same procedure as described in OIF UNI-01.0. At the NNI state synchronization could be achieved using Query and Query reply messages.

When the transport plane of a node fails (while the control plane is still functioning), it is advisable that the failed node initiate the signalling procedure to release calls and connections that are passing by it. The procedure to follow to achieve this goal is shown in Figure 21.

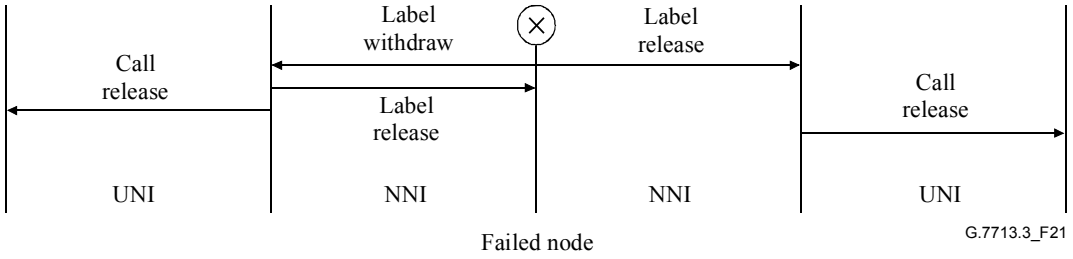


Figure 21/G.7713.3/Y1704.3 – Call/Connection release upon nodal bearer failure

11 Error sequences

In addition to those error codes that are defined in RFC 3036 and RFC 3212, the following error codes are defined specifically for this Recommendation:

```
0x04000009 = Invalid SNP ID
0x0400000a = Calling Party busy
0x0400000b = Unavailable SNP ID
0x0400000c = Invalid SNPP ID
0x0400000d = Unavailable SNPP ID
0x0400000e = Failed to create SNC
0x0400000f = Failed to establish LC
0x04000010 = Invalid A End-User Name
0x04000011 = Invalid Z End-User Name
0x04000012 = Invalid CoS
0x04000013 = Unavailable CoS
0x04000014 = Invalid GoS
0x04000015 = Unavailable GoS
0x04000016 = Failed Security Check
0x04000017 = TimeOut
0x04000018 = Invalid Call Name
```

```
0x04000019 = Failed to Release SNC
0x0400001a = Failed to Free LC
```

Annex A

Technology-specific terminology updates

The terminology used in [RFC 3471] for the Generalized Label Request TLV are updated to align with the ITU-T transport terminology. Note that no technical or procedural modifications are made. Tables A.1 and A.2 provide the updated terminology for the relevant fields applicable for ASON (LSP Encoding Type, and Generalized Payload ID):

Table A.1/G.7713.3/Y.1704.3 – Terminology update for LSP ENCODING Type within the Generalized Label Request TLV

Value	Type (in the RFC)	Updated type terminology
5	SDH ITU-T G.707/Y.1322/SONET ANSI T1.105	SDH ITU-T G.707/Y.1322
7	Digital Wrapper	OTN ITU-T G.709/Y.1331 ODUx
8	Lambda (photonic)	OTN ITU-T G.709/Y.1331 OCh

Table A.2/G.7713.3/Y.1704.3 – Values and types of the Generalized Payload ID within the Generalized Label Request TLV

Value	Type
0	Unknown
1	Reserved
2	Reserved
3	Reserved
4	Reserved
5	Asynchronous mapping of 139 264 kbit/s (P4x) into VC-4
6	Asynchronous mapping of 44 736 kbit/s (P32x) into VC-3
7	Asynchronous mapping of 34 368 kbit/s (P31x) into VC-3
10	Asynchronous mapping of 6 312 kbit/s (P21x) into VC-2
11	Bit synchronous mapping of 6 312 kbit/s (P21x) into VC-2
13	Asynchronous mapping of 2 048 kbit/s (P12x) into VC-12
14	Byte synchronous mapping of 2 048 kbit/s (P12s) into VC-12
15	Byte synchronous mapping of 31 * 64 kbit/s (P0) into VC-12
16	Asynchronous mapping of 1 544 kbit/s (P11x) into VC-11
17	Bit synchronous mapping of 1 544 kbit/s (P11x-bit) into VC-11
18	Byte synchronous mapping of 1 544 kbit/s (P11s) into VC-11

Table A.2/G.7713.3/Y.1704.3 – Values and types of the Generalized Payload ID within the Generalized Label Request TLV

Value	Type
25	Multiplexing of SDH LOVC via TUG-2 into a VC-3
26	Multiplexing of SDH LOVC via TUG-3s into a VC-4
27	Multiplexing of SDH HOVC into STM-N
28	POS – No Scrambling, 16-bit CRC
29	POS – No Scrambling, 32-bit CRC
30	POS – Scrambling, 16-bit CRC
31	POS – Scrambling, 32-bit CRC
41	FDDI mapping into VC-4
42	DQDB mapping into VC-4

Annex B

TLV code points

Code points for TLVs introduced by the OIF UNI-01.0 and not in RFCs 3036 and 3212 are listed below:

```
0x0960 = IPv4 Source ID TLV
0x0961 = IPv6 Source ID TLV
0x0962 = NSAP Source ID TLV
0x0963 = IPv4 Destination ID TLV
0x0964 = IPv6 Destination ID TLV
0x0965 = NSAP Destination ID TLV
0x0966 = Egress Label TLV
0x0967 = Local Connection ID TLV
0x0968 = Diversity TLV
0x0969 = Contract ID TLV
0x0970 = UNI Service Level TLV
```

Annex C

Label scope

C.1 Scope of the label

Labels provide information that are useful only to the CC/LRM using them. Labels may have an associated structure imposed on them for local use. Once the labels are transmitted to another CC or LRM, the structure of a label should no longer be important. This issue does not present a problem in a simple point-to-point connection between two control plane-enabled nodes. However, once a subnetwork is introduced between these nodes (where the subnetwork provides rearrangement capability for the signals), label scoping becomes an issue. Figure C.1 illustrates the case of a connection traversing a non-control-plane rearrangeable subnetwork (e.g., label rearrangement may

be performed via a management system). There is an implicit assumption that the non-control-plane connections already exist prior to any connection request.

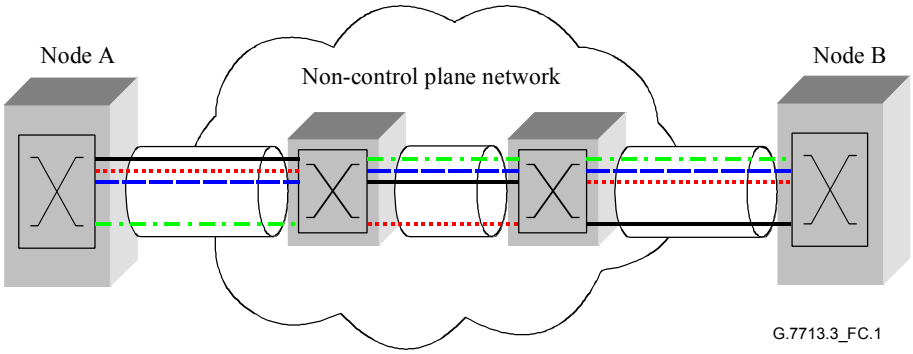


Figure C.1/G.7713.3/Y.1704.3 – Example Link where labels are rearranged via non-control plane network

The only characteristic of a label that is important once it is transmitted is the format of the label and the uniqueness of the label values. Characteristics such as the structure of the label are no longer important or useful. In fact, imposing structure of a label outside of the local space may result in restrictions to the architecture of a network.

C.2 A label association function

In order to support the capability to map a received label value to a locally significant label value, an additional function is needed as part of the local process: that of label association. This function takes as input a received label value and provides as output a locally significant label value. As such, this function may be considered generally to provide a table lookup function.

The information necessary to allow mapping from received label value to a locally significant label value may be derived in several ways:

– via manual provisioning of the association;

– via automatic discovery of the association.

Either method may be used. In the case of automatic discovery of the association, this implies that the discovery mechanism operates at the SNP level, as per ITU-T Rec. G.7714/Y.1705. Note that in the simple case where two NEs may be directly connected, no association may be necessary. In such instances, the label association function provides a one-to-one mapping of the input-to-output label values.

Appendix I

Mapping of messages

I.1 Mapping of UNI messages

See Table I.1.

Table I.1/G.7713.3/Y.1704.3 – Mapping of UNI messages

	UNI messages	GMPLS CR-LDP
Call Setup messages	CallSetupRequest	Label Request
	CallSetupIndication	Label Mapping
	CallSetupConfirm	Notification
Call Release messages	CallReleaseRequest	Label Release or Label Withdraw
	CallReleaseIndication	Label Release or Notification
Call Query messages	CallQueryRequest	Query
	CallQueryIndication	Query Reply
Call notification message	CallNotify	Notification

I.2 Mapping of E-NNI messages

See Table I.2.

Table I.2/G.7713.3/Y.1704.3 – Mapping of E-NNI messages

	E-NNI messages	GMPLS CR-LDP
Call Setup messages	CallSetupRequest	Label Request
	CallSetupIndication	Label Mapping
	CallSetupConfirm	Notification
Call Release messages	CallReleaseRequest	Label Release or Label Withdraw
	CallReleaseIndication	Label Release or Notification
Call Query messages	CallQueryRequest	Query
	CallQueryIndication	Query Reply
Call notification message	CallNotify	Notification

Appendix II

Mapping of attributes

II.1 Mapping of UNI attributes

See Table II.1.

Table II.1/G.7713.3/Y.1704.3 – UNI attributes list

	Attributes	Format	Scope	CR-LDP TLVs
Identity attributes	A-end user name	String	End-to-end	Source ID TLV
	Z-end user name	String	End-to-end	Dest ID TLV
	Initiating CC/CallC name	String	Local	Source Node ID (in the IP/TCP headers)
	Terminating CC/CallC name	String	Local	Destination Node ID (in the IP/TCP headers)
	Connection name	String	Local	GENERALIZED_LABEL, UPSTREAM_LABEL
	Call name	String	End-to-end	Call Id TLV
Service attributes	SNP ID	String	Local	GENERALIZED_LABEL, UPSTREAM_LABEL, EGRESS_LABEL, LABEL_SET, ACCEPTABLE_LABEL_SET
	SNPP ID	String	Local	Source/destination TNA
	Directionality	String	Local	(Implied by UPSTREAM_LABEL)
Policy attributes	CoS	String	End-to-end	Service Level TLV, Contract ID TLV, Diversity TLV
	GoS	String	End-to-end	Same as CoS above
	Security	String	Local	Using LDP security Procedure
Additional attributes of GMPLS	Implied layer information			GENERALIZED_LABEL_REQUEST
	To support graceful release in 10.3 and 10.6			ADMIN_STATUS
	To handle subclause 6.2 in ITU-T Rec. G.7713/Y.1704, for robustness			KeepAlive, TCP reliable transmission
	For status/error code			Status
	For robustness			Relies on TCP reliable transmission and flow control mechanisms
Failure notification related attributes	Status			Status TLV LDP Fault Tolerance
Inter-domain provisioning related attributes	As listed in E-NNI Table II.2			

II.2 Mapping of E-NNI attributes

See Table II.2.

Table II.2/G.7713.3/Y.1704.3 – E-NNI attributes list

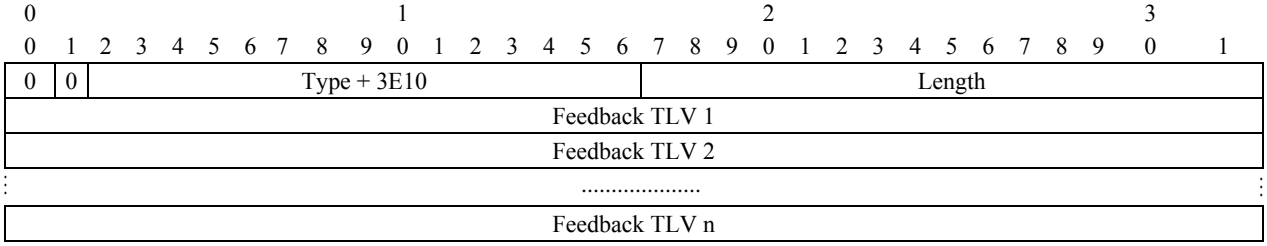
	Attributes	Format	Scope	CR-LDP TLVs
Identity attributes	A-end user name	String	End-to-end	Source ID TLV
	Z-end user name	String	End-to-end	Dest ID TLV
	Initiating CC/CallC name	String	Local	Source Node ID (in the IP/TCP headers)
	Terminating CC/CallC name	String	Local	Destination Node ID (in the IP/TCP headers)
	Connection name	String	Local	GENERALIZED_LABEL, UPSTREAM_LABEL
	Call name	String	End-to-end	Call Id TLV
Service attributes	SNP ID	String	Local	GENERALIZED_LABEL, UPSTREAM_LABEL, EGRESS_LABEL, LABEL_SET, ACCEPTABLE_LABEL_SET
	SNPP ID	String	Local	Interface ID TLV
	Directionality	String	Local	(Implied by UPSTREAM_LABEL)
Policy attributes	CoS	String	End-to-end	Service Level TLV, Contract ID TLV, Diversity TLV
	GoS	String	End-to-end	Same as CoS above
	Security	String	Local	Using LDP security Procedure
Additional attributes of GMPLS	Implied layer information			GENERALIZED_LABEL_REQUEST
	To support graceful release in 10.3 and 10.6			ADMIN_STATUS
	To handle subclause 6.2 in ITU-T Rec. G.7713/Y.1704 for robustness			KeepAlive, TCP reliable transmission
	For status/error code			Status
	For robustness			Relies on TCP reliable transmission and flow control mechanisms
Failure notification related attributes	Status			Status TLV LDP Fault Tolerance

Appendix III

Feedback list TLV

Connection management (signalling) benefits from feedback when there is a higher probability that the path computation function returns valid paths when resources exist, and no paths when resources do not exist. The feedback mechanism in signalling assists by providing more current routing information to the routing function which in turn supports path computation.

The information passed back to routing is transparent to connection management. However, a TLV is needed by connection management to contain this information. This is defined below in the Feedback List TLV.



Type

A fourteen-bit field carrying the value of the Feedback List TLV Type.

Length

Specifies the length of the value field in bytes.

Feedback TLVs

One or more Feedback TLVs.

NOTE – For bidirectional connections, there are two Feedback TLVs for both directions at one OCC in the Feedback List TLV.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE AND INTERNET PROTOCOL ASPECTS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	**Y.1700–Y.1799**
Charging	Y.1800–Y.1899

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

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 and Internet protocol aspects**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2003