International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3302.1

(10/2010)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

Recommendation ITU-T Q.3302.1

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
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	**Q.3300–Q.3369**
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3302.1

Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

Summary

Recommendation ITU-T Q.3302.1 specifies the resource connection initiation protocol (RCIP) for use to carry resource control requests and responses between transport resource control physical entities within the same domain. This protocol is designed to be able to support signalling along a chain of control elements in an operator's network for a collection of most commonly used QoS models and requirements, including (but not limited to) traffic specification, priority, multiprotocol label switching (MPLS) labels and virtual switching connection information. A multimedia service call traversing the network, which comprises one or more sessions (each having application/user-specific QoS specification), will get desired QoS treatment in the data plane (i.e., the chain of transport physical entities), through the appropriate configuration of the transport physical entities by the transport resource control physical entities.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3302.1	2007-03-09	11
2.0	ITU-T Q.3302.1v2	2010-10-14	11

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Q.3302.1

Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

1 Scope

This Recommendation defines the resource connection initiation protocol (RCIP), for signalling control information between peer TRC-PEs (Rp interface) in a single operator's network. The requirements for the Rp interface are defined in clause 8.6 of [ITU-T Y.2111] and in [ITU-T Q-Sup.51].

The possible methods of configuration and notification between the transport physical entities (T-PE) and the transport resource control are out of scope of this Recommendation. RCIP specifies control plane signalling among transport resource control physical entities (TRC-PEs) in an operator's network.

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

[ITU-T Q.2981] Recommendation ITU-T Q.2981 (1999), *Broadband integrated services digital network (B-ISDN) and broadband private integrated services network (B-PISN) – Call control protocol*.

[ITU-T Q-Sup.51] ITU-T Q-series Recommendations – Supplement 51 (2004), *Signalling requirements for IP-QoS*.

[ITU- T T.50] Recommendation ITU-T 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 Y.1291] Recommendation ITU-T Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks.*

[IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 connection [ITU-T G.805]: A "transport entity" which consists of an associated pair of "unidirectional connections" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 bearer: A connection for the transport of user plane information between users involved in a communication. (Derived from [ITU-T Q.2981])

3.2.2 bearer control function (BCF): A functional entity that performs the Resource and Admission Control functions. (Derived from [ITU-T Q.2981])

NOTE – BCF is identical to RACF, can be PD-FE, TRC-FE, or both.

3.2.3 downstream TRC-PE: The entity which receives the resource request from an upstream TRC-PE.

3.2.4 flow information: Information necessary to identify an IP data flow.

3.2.5 IP data stream: A sequence of packets sent to convey communication between the two endpoints identified by the flow information. It is an instance of bearer.

3.2.6 RCIP resource connection: A control signalling relationship maintained in all TRC-PEs between (and including) the source TRC-PE and the destination TRC-PE in support of a specific IP data stream.

NOTE – The messages sent along the RCIP resource connection can carry one or more pieces of resource reservation information for that IP data stream.

3.2.7 RCIP transport channel: A signalling transport connection maintained between two TRC-PE peers, within which multiple RCIP resource connections can be multiplexed.

3.2.8 service control function (SvCF): A functional entity that provides value-added service functionality. (Derived from [ITU-T Q-Sup.51])

3.2.9 session control function (SeCF): A functional entity that provides the call/session control functionality. (Derived from [ITU-T Q-Sup.51])

3.2.10 source TRC-PE: The TRC-PE which receives a resource request based on service, sent by the PD-PE or the previous hop source-seeking TRC-PE.

NOTE – The source address of the media flow belongs to the TRC-PE domain that is under its administration.

3.2.11 transport physical entity (T-PE): An entity that performs stream classification, switching and forwarding and is capable of enforcing a QoS guarantee. (Derived from [ITU-T Q-Sup.51])

3.2.12 upstream TRC-PE: The entity which sends the resource request to a downstream TRC-PE.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACCT Protocol Connection Establishment Accept; an RCIP message

AH Authentication Header

AUP AUdit resPonse; an RCIP message

AUR AUdit Request; an RCIP message

BCD Binary-Coded Decimal

BCF Bearer Control Function

CLOSE	Protocol Connection Establishment Close; an RCIP message
DNS	Domain Name System
ESP	Encapsulation Security Payload
HMAC	Hash-based Message Authentication Code
ID	Identifier
IP	Internet Protocol
KA	Keep-Alive; an RCIP message
kbps	kilobit per second
LSP	Label Switched Path
mbps	megabit per second
MPLS	MultiProtocol Label Switching
OPEN	Protocol Connection Establishment Open; an RCIP message
OVE	OVErload indication; an RCIP message
PD-PE	Policy Decision Physical Entity
QoS	Quality of Service
RA	Resource Acceptance; an RCIP message
RACF	Resource Admission Control Functions
RCIP	Resource Connection Initiation Protocol
REJ	Resource REJection; an RCIP message
RLP	Resource reLease resPonse; an RCIP message
RLR	Resource reLease Request; an RCIP message
RR	Resource Request; an RCIP message
SCE	Session/Service Control Entity
SF	Switching Function
TLS	Transport Layer Security
T-PE	Transport Physical Entities
TRC-PE	Transport Resource Control Physical Entity

5 Protocol design principles

5.1 Introduction

[ITU-T Q-Sup.51] describes the control information flows between BCFs which is depicted in Figure 5-1. Rp interface is defined in [ITU-T Y.2111] between TRC-FE instances, as shown in Figure 5-2. Separation between data plane (transport functions) and control plane (bearer control functions, or BCFs) is an important feature in the NGN and RCIP architectures. BCF interacts with border session/service control entities (SCEs) and interior transport physical entities (T-PEs) in order to apply resource reservation made in the control plane to achieve the service in the data plane, and to get feedback from T-PEs or SCEs for (re) negotiating reservations. The basic protocol architecture for RCIP is shown in Figure 5-1.

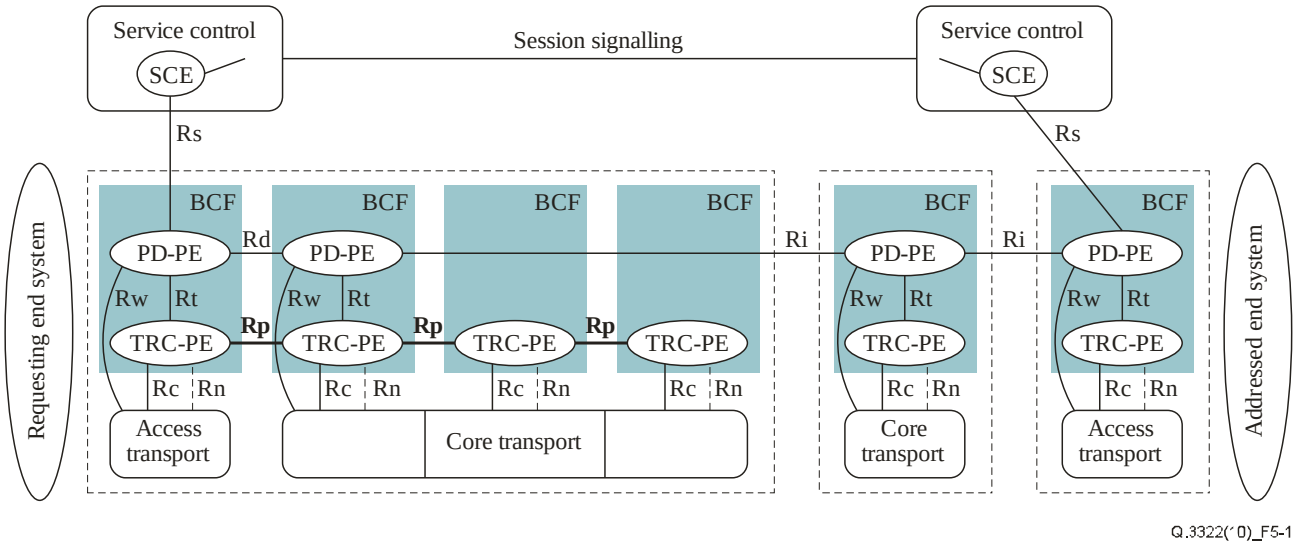
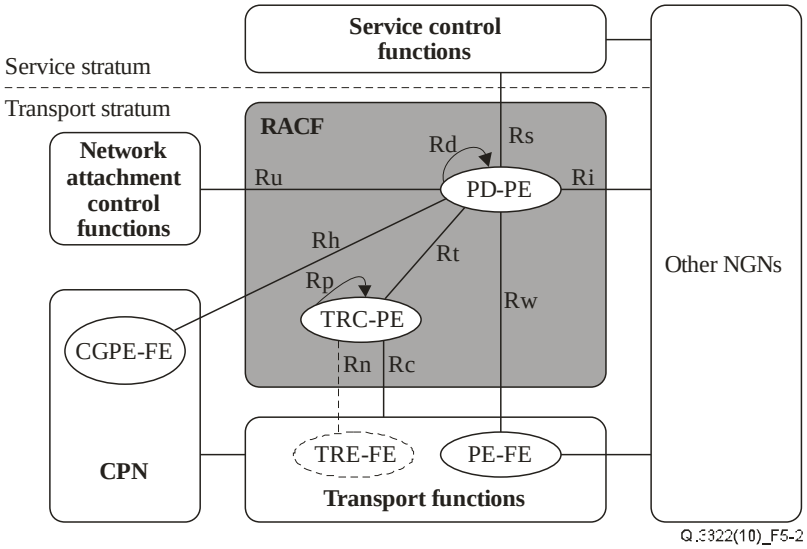


Figure 5-1 – Basic protocol architecture



NOTE – This figure is derived from Figure 5 of [ITU-T Y-2111].

Figure 5-2 – Generic resource and admission control functional architecture in NGN

In the IP network, TRC-PE(s) are used to manage all logical bearer networks in all managed areas. In each TRC-PE, the topology and resources in each logical bearer network is recorded and managed respectively.

Internally, RCIP maintains a resource connection for the resource reservation from a source T-PE to a destination T-PE. For example, an RCIP resource connection can reserve resource for a multimedia service call which has an audio session and a video session.

Each RCIP resource connection message contains reservation information or control information related to an RCIP resource connection. It is transported reliably over a secure RCIP transport channel which is a half-permanent hop-by-hop communication channel. As RCIP operates within an operator's network, it is assumed that all TRC-PEs have a pre-configured signalling path between any source TRC-PE and destination TRC-PE pair.

Clause 7.2 of [ITU-T Y.1291] describes the QoS routing of control plane mechanisms, which is an important feature of RCIP.

5.2 Protocol overview

RCIP protocol (Figure 5-3) is designed to be able to support signalling along a chain of control elements (preconfigured TRC-PEs) in an operator's network for a collection of the most commonly used QoS models and requirements, including (but not limited to) traffic specification, priority, MPLS labels and virtual switching connection information. A multimedia service call traversing the network, which comprises one or more sessions (each having application/user-specific QoS specification), will get desired QoS treatment in the data plane (i.e., the chain of T-PEs), through appropriate configuration of the T-PEs by TRC-PEs. The possible methods of configuration and notification between the T-PE and the TRC-PE are out of the scope of RCIP. RCIP specifies control plane signalling among TRC-PEs in an operator's network.

Upon receiving a SCE's request of QoS requirements, a TRC-PE located in the network edge, herein called the source TRC-PE, will initiate resource reservation towards another TRC-PE in the same operator's network where the service call leaves (i.e., destination TRC-PE). The intermediate TRC-PEs perform admission control, and if they succeeds, perform appropriate resource reservation until the destination TRC-PE is reached. Upon successful reservation in the destination TRC-PE, a corresponding resource acceptance will be issued, traversing through the same set of TRC-PEs in the reverse direction, confirming the resource reservation request previously made. The reserved resources will be released using an explicit release-response mechanism. Any TRC-PE initializing resource reservation and any TRC-PE which failed to provide required reservation, (e.g., due to a failure in admission control or being pre-empted by new higher-priority resource requests), can issue a release towards the TRC-PE to release the reserved resource.

Between two adjacent RCIP peers, RCIP messages are securely and transparently transmitted over an RCIP transport channel. An RCIP transport channel is established and maintained as a half-permanent virtual circuit, and reused by all traversing RCIP messages (which can belong to any RCIP resource connection).

In addition, RCIP allows asynchronous overload notifications by any TRC-PE. Such a notification is triggered in a TRC-PE by high processing overloads.

Between two TRC-PE(s) there is one RCIP transport channel. There can be many service messages carried on a single RCIP transport channel as shown below.

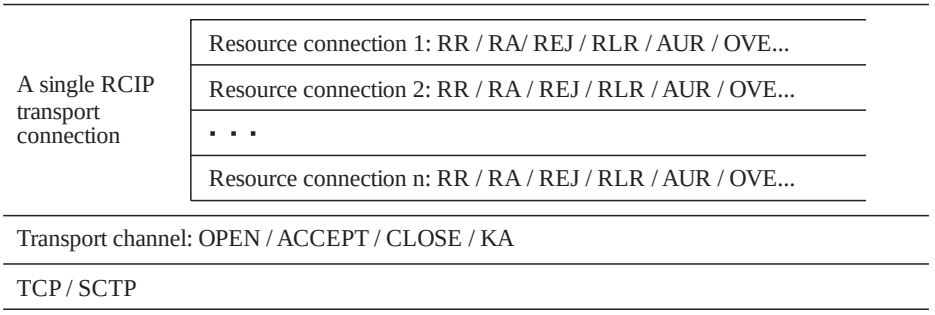


Figure 5-3 – RCIP protocol overview

RCIP specifies the following messages and objects:

RCIP resource connection messages:

– Resource Request (RR)
– Resource Acceptance (RA)
– Resource Rejection (REJ)
– Resource Release Request (RLR)

– Resource Release Response (RLP)
– Overload Indication (OVE)
– Audit Request (AUR)
– Audit Response (AUP)

RCIP transport channel messages:

– Protocol Connection Establishment Open (OPEN)
– Protocol Connection Establishment Accept (ACCT)
– Protocol Connection Establishment Close (CLOSE)
– Keep Alive (KA)

RCIP main objects:

– Connection ID
– Flow Information
– Flow Traffic Information
– LSP Connection Information
– V-Switching Connection Information
– Reason Code
– Overload Indication
– Result Indication
– Data Consistency
– Aggregate Resource Information

Each RCIP message includes header information which specifies the message. Related to each message, there are a number of mandatory and optional objects as described in clause 7.

5.3 Roles of TRC-PE

The roles of TRC-PE [ITU-T Q-Sup.51] are shown in Figure 5-4, which is only a sketch map. A TRC-PE can act as one or more of these roles at the same time.

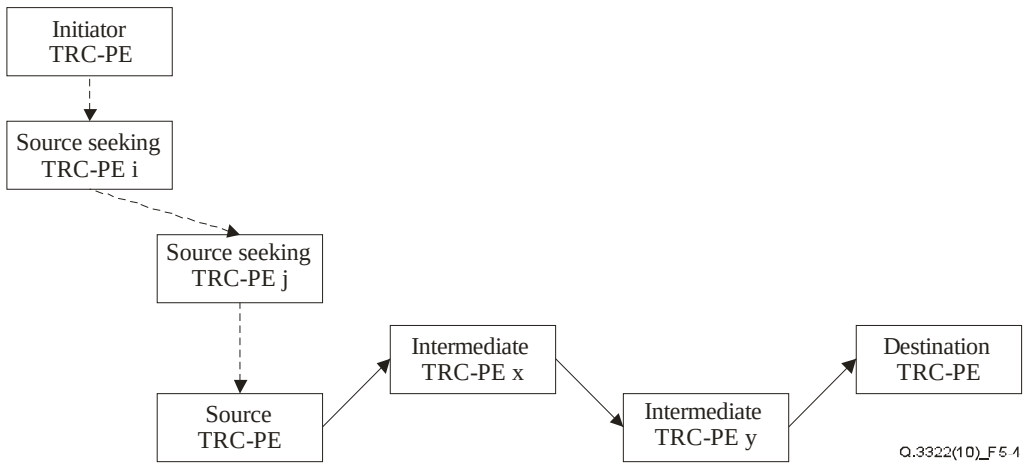


Figure 5-4 – Roles of TRC-PE

Initiator TRC-PE	The initiator TRC-PE receives a QoS request sent by the SCE through the PD-PE. For the MPLS case it performs service routing, while for the non-MPLS case, it performs the identification of the logical path.
Source-seeking TRC-PE	The source-seeking TRC-PE receives a QoS request sent by the previous hop TRC-PE, and queries the "Source TRC-PE" route to find out the next hop TRC-PE, to which it will transfer the request. The difference between the source-seeking TRC-PE and the intermediate TRC-PE is that the former transfers a request for resources according to the managed area to which the source address of the service message stream belongs.
Source TRC-PE	The source TRC-PE receives a resource request based on the service message, sent by the SCE or the previous hop source-seeking TRC-PE. The source address of the media flow belongs to the TRC-PE domain that is under its administration.
Intermediate TRC-PE	The intermediate TRC-PE receives a resource request based on the service message, sent by the previous hop TRC-PE, queries the TRC-PE route table, provides distribution of resources in the local domain, and transfer the RESOURCE request to the next hop TRC-PE.
Destination TRC-PE	The destination TRC-PE receives a resource request based on the service message, sent by the previous hop TRC-PE. When it finds out that the destination IP of the media flow belongs to the TRC-PE domain that is under its administration, if the request is bidirectional, the destination TRC-PE will deliver the routing result of the resource path from the destination to the source directly to the edge router, and return a response message of the resource path from the source to the destination and then to the previous hop TRC-PE.

6 Basic protocol operation

6.1 REQUEST

The REQUEST operation is used to request reservation of resources between a downstream TRC-PE and an upstream TRC-PE. The REQUEST operation transfers the flow information, and QoS parameter objects, which describe the desired resources to be allocated. After the TRC-PE receives the request, it will calculate the resources and select the route in the corresponding logic bearer network for the media flow according to the source address, destination address and QoS requirements carried in the request. A request is sent in a hop-by-hop fashion. This means that a given reservation is realized via a series of requests between adjacent TRC-PEs, and the given TRC-PE takes the previous TRC-PE as the source of the RR.

Every TRC-PE has two logical TRC-PE routing tables, one is for TRC-PE routing of source-seeking procedure (and can be one hop or multi hops), the other is for TRC-PE routing for resource reservation procedure. The recipient TRC-PE records the addressing identification address of the source TRC-PE so as to correctly send responses and enable the event notification to find the upstream node.

One call may need multiple data streams. For example, a video phone usually needs an audio flow session and a video flow session. In order to establish the QoS connections of all streams in a call at a single attempt of connection, one request needs to carry the QoS requirement information of multiple streams. One RCIP message includes one or more groups of flow information (e.g., 5-tuple), while the RCIP message as a whole corresponds to one call/or resource connection (e.g., the video call including both video and audio sessions).

In one request, the network may fail to meet the QoS requirements, but some available resources may still exist. In this case, the SCE can specify in the request, whether to accept the services with lower QoS as required. Correspondingly, TRC-PE can also specify it as the information between TRC-PE(s) is from SCE via PD-PE. A request can be partially met.

When necessary, the network can remove the resources of existing non-emergency calls/sessions to meet the QoS resources for the emergency call/session. This is achieved by using an urgent flag in the resource request for emergency calls. When there is no available resource in a TRC-PE, TRC-PE can determine whether to pre-empt or tear down the low priority resource connection.

In the REQUEST operation, Resource Request (RR) message is used in one direction, and Resource Acceptance (RA) message and Resource Rejection (REJ) message are used in the other direction.

6.2 MODIFY

The MODIFY operation is used at the request of upstream TRC-PE, to modify the bandwidth, port, or protocol type. Repetitive modifications are allowed. Bandwidth modification falls into decrement modification or increment modification. Decrement modification is expected to be performed successfully in most cases, while increment modification may fail due to a lack of resources to meet the new requirement. When modification fails, the previous connection may be recovered or the service connection may be released.

The MODIFY operation utilizes the Resource Request (RR) message with Modify Flag, Resource Acceptance (RA) message and Resource Rejection (REJ) message.

6.3 AUDIT

The AUDIT operation is used to synchronize the TRC-PE(s) in the status of a QoS request. The AUDIT operation is a mechanism to check the consistency of the RCIP resource connections in peer TRC-PE(s).

The information obtained through the AUDIT operation can be used for the management control process of the TRC-PE(s). Note that the AUDIT operation will not change the status of the existing reserved resources, nor establish the status of the upstream TRC-PE which originates the query.

If the audit response fails, the corresponding RCIP resource connection shall be released. TRC-PE releases resources locally, sends resource release to the upstream or downstream peer TRC-PE, not including the TRC-PE which sends the audit response.

The AUDIT message contains only one connection ID object, so as to allow the audited TRC-PE to feedback the information. The Audit Request (AUR) and Audit Response (AUP) messages are utilized in the AUDIT operation.

6.4 NOTIFY

The NOTIFY operation is used to notify the asynchronous events (from a TRC-PE to another TRC-PE).

The information carried by the NOTIFY operation is usually related to conditions. One example of NOTIFY is unavailable LSP or unavailable downstream TRC-PE due to overload conditions. In such case, the upstream TRC-PE can be handled in two ways: to release the call or not. If the call is not released, QoS will be interrupted for the call.

The Overload Indication (OVE) message is utilized in the NOTIFY operation.

6.5 RELEASE

The RELEASE operation is used by the upstream TRC-PE requests to request the downstream TRC-PE for releasing the resources that have been requested for allocation.

The Resource Release Request (RLR) message and Resource Release Response message (RLP) are utilized in the RELEASE operation.

6.6 TRC-PE source-seeking

The TRC-FE source-seeking operation is used to find the source TRC-PE (e.g., IP address, digits from 0 and 9, URL), based on the source address of the media flow which requests the reserve resource.

In order to hide the network topology of the bearer control layer to the service control layer, the SCE does not need to know where the source TRC-PE for each call is located. The SCE simply initiates a request to any TRC-PE and the request will be transferred to the appropriate source TRC-PE via the TRC-PE source-seeking TRC-PE process, so that a normal process of resource reservation can be started.

There are two ways to complete the source-seeking process:

1) The first is a piggyback method whereby the resolution function is integrated within TRC-PE. The TRC-PE is called source-seeking TRC-PE and acts as the resource reservation request proxy. When a TRC-PE, which is called initiator TRC-PE, receives a request from SCE, it initiates a Resource Request and forwards it to the source-seeking TRC-PE. The source-seeking TRC-PE is responsible for resolving the source TRC-PE's address and transmits the Resource Request to the source TRC-PE.
2) The second is an independent method where the resolution function is separated from TRC-PE. The resolution function is responsible for resolving the source TRC-PE's address and returning it to initiator TRC-PE. Initiator TRC-PE then initiates a resource request to the source TRC-PE directly. This method is out of the scope of this Recommendation.

The Resource Request message (RR) is utilized in the TRC-PE source-seeking operation.

7 Basic procedure

7.1 Resource connection establishment

In an IP network supporting MPLS or DiffServ, the network administrator can divide the service with QoS requirements into several categories according to the service category or QoS degree. According to the topology and flow rule of each QoS service, the network administrator can use the MPLS LSP technology to preset a route and logical bearer network independent of other services and set the bandwidth and QoS attribute for each label switched path (LSP) used to constitute a logical bearer network. Thus, QoS in a bearer network level for a media flow can be guaranteed by applying provider-specific resource admission control and path selection. The best effort traffic without QoS requirements can be forwarded following traditional IP routing without applying any QoS mechanisms.

In order to establish an RCIP resource connection (i.e., make successful reservation of necessary QoS resources) for a call in a provider network, a resource request is first generated in a source TRC-PE.

The Resource Request (RR) message is sent to a downstream TRC-PE. This message is detected on the downstream TRC-PE. The downstream TRC-PE carries out resource computation, TRC-PE route selection and admission control depending on the topology and resource usage of the logic bearer network [ITU-T Y.2111]. The downstream TRC-PE checks the availability of resources in its local domain, and if they are available and preliminarily reserved, the request is passed to the next TRC-PE towards the destination TRC-PE. The previously described procedure is performed in every TRC-PE. When the request has a chain of TRC-PEs, from the destination TRC-PE on, the downstream TRC-PE provides feedback results of resource admission control to the upstream TRC-PE. At the same time it provides the results of route selection (MPLS multi-layer label representing a given path), flow ID and QoS parameter to the corresponding edge router. On the basis of its received Resource Request (RR) message, the TRC-PE creates a new Resource Request (RR) message which is forwarded to the next TRC-PE.

The same handling process can be implemented at the nearest TRC-PE on the RCIP signalling path until the destination TRC-PE is reached.

On the destination TRC-PE, it is impossible for the last TRC-PE on the signalling path to send a further Resource Request (RR) message, thus a reply or reject message as acknowledgement is mandatory.

Appendix I provides examples of message flows with unidirectional and bidirectional RCIP resource connection setup.

7.2 Resource connection tear-down

If an RCIP resource connection is no longer needed or resources are reduced on the connection, the TRC-PE sends a Resource Release Request (RLR) message to the interconnected TRC-PE. When the interconnected TRC-PE receives a RLR, it performs the following actions:

– Decides if resources shall be released;

– Sends an RLR message to other TRC-PEs involved in the connection, releases the actual resources in the node and sends a successful Resource Release Response (RLP) message to the sending TRC-PE of the RLR.

7.3 Overload control

There might be situations where a given TRC-PE is overloaded due to high processing. To ensure timely responses, and to increase the effective throughput at high loads, it is necessary for entities external to the given TRC-PE to reduce the rate of new signalling requests to a level at which throughput can be maximised. The protocol provides a minimal yet effective procedure to achieve this. The overloaded TRC-PE node could propagate this information to all the neighbouring TRC-PE nodes. The exact behaviour of the TRC-PE node receiving such an indication is implementation- specific. However, it is expected to reduce the originating traffic towards the overloaded TRC-PE node until an explicit notification is received, indicating that the overload situation has ceased.

8 Protocol format

8.1 General

This clause describes the message formats and objects exchanged between TRC-PE(s). See Figure 8-1. All fields in an RCIP message must be transmitted in network-byte order.

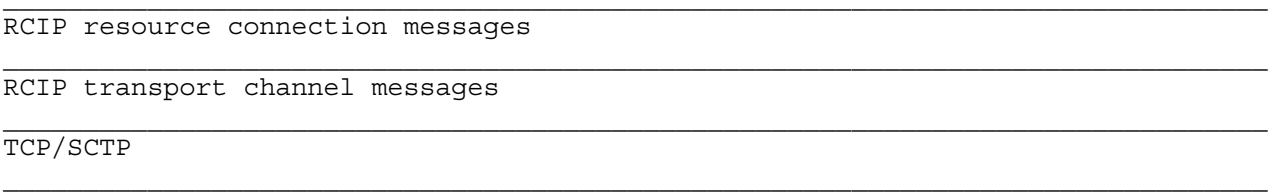


Figure 8-1 – RCIP messages exchanged between TRC-PE(s)

8.2 RCIP message format

The general RCIP message format is shown in Figure 8-2. Each message is comprised of a message header and message content consisting of one or more objects. See clause 8.2.1 for a description of the message header, and clause 8.4 for a description of the general structure of an object.

Table 8-1 in clause 8.4 lists the object types that are required in each RCIP message type.

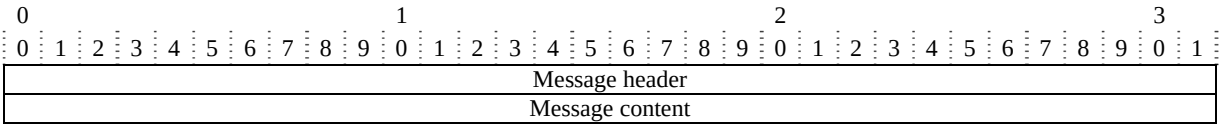


Figure 8-2 – RCIP message format

8.2.1 RCIP message header

Figure 8-3 shows the structure of the RCIP message header.

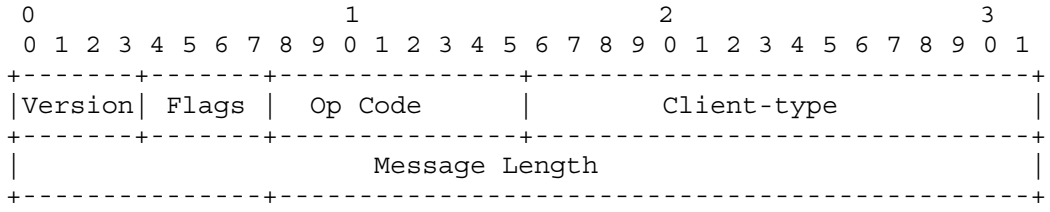


Figure 8-3 – RCIP message header

The fields in the header are:

Version: 4 bits

RCIP version number. The current version is 1.

Flags: 4 bits

Defined flag values:

| proxy | modify | converse | urgent |

Reserved: 0.

0x8 Proxy Flag Bit

This flag is set when the message is from the source-seeking TRC-PE, not the message sent to the next TRC-PE.

0x4 Modify Flag Bit

This flag is set when the message is modifying the information of the same request or response, e.g., bandwidth modification.

0x2 Converse Flag Bit

This flag is used in Resource Release Request (RLR) message. This flag is set when the message is converse RLR, Op Code is 11 = Request for resources to support the service. Converse means that the direction of this RLR is in the converse direction with RR.

0x1 Urgent Flag Bit

This flag is used to represent the priority of the message. When the urgent flag is 0, the RCIP resource connection may be released when necessary; when the urgent flag is 1, the RCIP resource connection should not be released except in manual reconfiguration.

All other values are reserved and are set to "0".

NOTE – 0xm indicates hexadecimal notation.

Op code: 8 bits

0-5 = reserved

6 = Protocol Connection Establishment Open (OPEN) message

7 = Protocol Connection Establishment Accept (ACCT) message

8 = Protocol Connection Establishment Close (CLOSE) message

9 = Keep Alive (KA) message

10 = reserved

11 = Resource Request (RR) message

12 = Resource Acceptance (RA) message

13 = Resource Rejection (REJ) message

14 = Resource Release Request (RLR) message

15 = Resource Release Response (RLP) message

16 = Overload Indication (OVE) message

17 = Audit Request (AUR) message

18 = Audit Response (AUP) message

Client-type: 16 bits

The Client-type identifies the policy client. Interpretation of all encapsulated objects is relative to the client-type.

0x0 KA

0x1 TRC-PE during source-seeking process

0x4 TRC-PE not in the source-seeking process

For KA Messages, the client-type in the header must always be set to 0 as the KA is used for connection verification (not per client session verification).

For the messages between source TRC-PE, intermediate TRC-PE and destination TRC-PE, the client-type in the header must always be set to 0x4.

For the messages between initiator TRC-PE, source-seeking TRC-PE, and source TRC-PE, the client-type in the header must always be set to 0x1.

Message length: 32 bits

The size of a message is in octets, which includes the standard RCIP header and all encapsulated objects. Messages are required to be aligned on 4-octet boundaries.

If the length is not the integral times of 4 bytes, filling is needed. The filling bits are all set to "0".

When sending to the network, the version is sent first; when receiving from the network, the version is received first.

8.3 RCIP messages

8.3.1 RCIP resource connection messages

8.3.1.1 Resource Request (RR)

The Resource Request (RR) message, indicated by the Op code set to 11, is sent by an upstream TRC-PE to the downstream TRC-PE to request the bearer resource for the RCIP resource connection.

```
Resource Request = <RCIP_HEADER>
                     <Connection ID>
                   1*{Media Profile}
                     [Data Consistency Information]
```

In the flow profile object, if the RR message is bidirectional, both forward flow traffic descriptor and backward flow traffic descriptor are carried; if the RR message is unidirectional, either forward flow traffic descriptor or backward flow traffic descriptor is carried. Flow profile contains a profile for a part of resource reservation information including flow ID, flow information, flow traffic descriptor (multiple groups of forward flow traffic descriptor and multiple groups of backward flow traffic descriptor), LSP connection information (needed when Proxy flag is set to 0).

8.3.1.2 Resource Acceptance (RA)

The Resource Acceptance (RA) message, indicated by the Op code set to 12, is sent by a downstream TRC-PE to the upstream TRC-PE in response to the Resource Request message.

```
Resource Acceptance = <RCIP_HEADER>
                      <Connection ID>
                    1*{Media Profile}
                      [Data Consistency Information]
```

8.3.1.3 Resource Rejection (REJ)

The Resource Rejection (REJ) message, indicated by the Op code set to 13, is sent by a downstream TRC-PE to the upstream TRC-PE in rejection response to the Resource Request message.

```
Resource Rejection = <RCIP_HEADER>
                     <Connection ID>
                     {Reason Code}
                     [Data Consistency Information]
```

8.3.1.4 Resource Release Request (RLR)

The Resource Release Request (RLR) message, indicated by the Op code set to 14, can be sent from an upstream TRC-PE to the downstream TRC-PE with the converse flag set to 0, and can also be sent from a downstream TRC-PE to the upstream TRC-PE with the converse flag set to 1.

```
Resource Release Request = <RCIP_HEADER>
                     <Connection ID>
                     {Reason Code}
                     [Data Consistency Information]
```

8.3.1.5 Resource Release Response (RLP)

The Resource Release Response (RLP) message, indicated by the Op code set to 15, is sent from a downstream TRC-PE to the upstream TRC-PE, in response to the RLR message with converse flag set to 0. There is no response message to the Converse Resource Release Request message, as in this case it is already the abnormal release.

```
Resource Release Response = <RCIP_HEADER>
```

```
                    <Connection ID>
                    {Reason Code}
                    [Data Consistency Information]
```

8.3.1.6 Overload Indication (OVE)

The Overload Indication (OVE) message, indicated by the Op code set to 16, is sent from a TRC-PE to the peer TRC-PE, including overload and recovery.

```
Overload Indication = <RCIP_HEADER>
                    {Overload Indication}
                    [Data Consistency Information]
```

8.3.1.7 Audit Request (AUR)

The Audit Request (AUR) message, indicated by the Op code set to 17, is sent from a TRC-PE to the peer TRC-PE, in order to check whether the RCIP resource connection exists.

```
Audit Request = <RCIP_HEADER>
                    <Connection ID>
                    [Data Consistency Information]
```

8.3.1.8 Audit Response (AUP)

The Audit Response (AUP) message, indicated by the Op code set to 18, is sent from a TRC-PE to the peer TRC-PE, in response to the Audit Request message.

```
Audit Response = <RCIP_HEADER>
                    <Connection ID>
                    {Result Indication}
                    [Data Consistency Information]
```

8.3.2 RCIP transport channel messages

8.3.2.1 Protocol Connection Establishment Open (OPEN)

The OPEN message, indicated, by the Op code set to 6, is sent from client TRC-PE to the server TRC-PE, in order to set up the RCIP transport channel.

```
OPEN = <RCIP_HEADER>
          <Identity Identification>
          [Authentication Information]
          [Data Consistency Information]
```

8.3.2.2 Protocol Connection Establishment Accept (ACCT)

The ACCT message indicated, by the Op code set to 7, is sent from server TRC-PE to the client TRC-PE, in response to OPEN message with the value of Keep-Alive Timer. Upon receiving ACCT message, the RCIP transport channel is set up.

```
ACCT = <RCIP_HEADER>
          {Keep-Alive Timer}
          [Data Consistency Information]
```

8.3.2.3 Protocol Connection Establishment Close (CLOSE)

The CLOSE message, indicated by the Op code set to 8, is sent from a TRC-PE to the peer TRC-PE, in order to close the corresponding RCIP transport channel.

```
CLOSE = <RCIP_HEADER>
{Reason Code}
     [Data Consistency Information]
```

8.3.2.4 Keep Alive (KA)

The keep alive (KA) message is sent from a TRC-PE to the peer TRC-PE, in order to check the data consistency between the two TRC-PEs.

```
KA = <RCIP_HEADER>
     [Data Consistency Information]
```

8.4 RCIP object format

Figure 8-4 provides the format for the RCIP object. It consists of a four-octet (32-bit word) header followed by object content. Object content may be null. Object content is required to be a multiple of 32-bit words. Padding is required in case content length is not an integral multiple of 32-bit words. If necessary, padding bits are all set to "0".

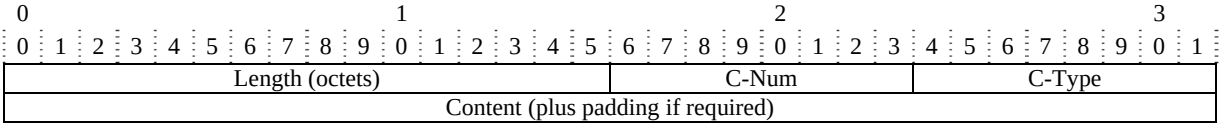


Figure 8-4 – RCIP object format

Length: two octets

The length describes the number of octets (including the header) that makes up the object. If the length in octets does not fall on a 32-bit word boundary, padding must be added to the end of the object so that it is aligned to the next 32-bit boundary before the object can be sent on the wire. On the receiving side, a subsequent object boundary can be found by simply rounding up the previously stated object length to the next 32-bit boundary.

C-num: 8 bits

C-Num identifies the class of information contained in the object:

1 = Connection ID

2 = Flow ID

3 = Flow Information

4 = Flow Traffic Descriptor

5 = LSP Connection Information

6 = Authentication Information

7 = Reason Code

8 = Identity Identification

9 = Keep-Alive Timer

10 = Data Consistency Information

11 = V-Switching connection information

12 = Overload-Indication Object

13 = Flow Profile Object

14 = Result Identification Object

15= ITU-T E.164 Number

16= Resource State

17= TRC-PE Sequence Object

18= Media Profile Object

19= Media Profile ID Object

20= Aggregate resource profile object

C-type: 8 bits

C-Type identifies the subtype or version of the information contained in the object.

C-Type values identify variant structures within a specific class of information represented by a C-num.

Table 8-1 lists the object types found in each message type. The clause numbers describing the messages and objects are shown in parentheses after the names. The final column indicates whether these objects are mandatory (M) or optional (O) in the given message, and adds the further qualifier "m" if multiple instances of the object are allowed.

Table 8-1 – Object types found in each message type

Message Type	Objects	M/O
RR (8.3.1.1)	Connection ID (8.5.1)	M
	Media Profile (8.5.18)	Mm
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
RA (8.3.1.2)	Connection ID (8.5.1)	M
	Media Profile (8.5.18)	Mm
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
REJ (8.3.1.3)	Connection ID (8.5.1)	M
	Reason Code (8.5.7)	M
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
RLR (8.3.1.4)	Connection ID (8.5.1)	M
	Reason Code (8.5.7)	M
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
RLP (8.3.1.5)	Connection ID (8.5.1)	M
	Reason Code (8.5.7)	M
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
OVE (8.3.1.6)	Overload Indication (8.5.12)	M
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
AUR (8.3.1.7)	Connection ID (8.5.1)	M
	Data Consistency (8.5.10)	O

Message Type	Objects	M/O
AUP (8.3.1.8)	Connection ID (8.5.1)	M
	Result Indication (8.5.14)	O
	Data Consistency (8.5.10)	O

8.5 RCIP objects

8.5.1 Connection ID (ConnID)

The connection ID object corresponds to each call. A unique value for Connection ID is set by the initiator TRC-PE. If the connection ID object appears in a message, it means that the message is pertaining to the RCIP resource connection identified by the connection ID. When a TRC-PE sees an RCIP message containing such an object, it can create or find the corresponding connection ID internally, and does the corresponding process.

8.5.1.1 IPv4 connection ID (IPv4ConnID)

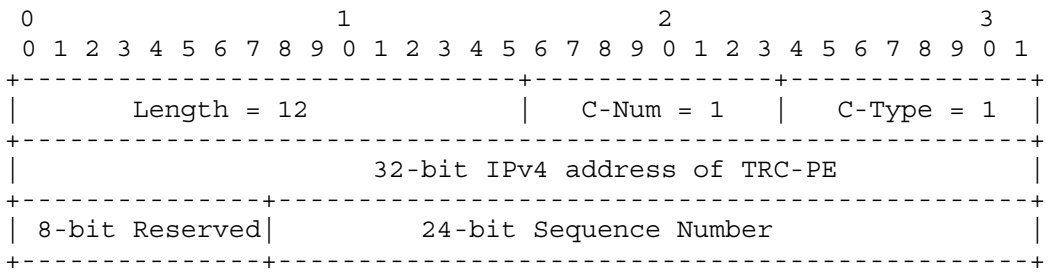


Figure 8-5 – IPv4 connection id object content

C-Num = 1

C-Type = 1, IPv4 connection ID.

The connection ID consists of two parts. One part is the 32-bit TRC-PE identification (ordinarily IPv4 address), the other part is the 24-bit sequence number, allocated by the TRC-PE for the resource request. See Figure 8-5.

8.5.1.2 IPv6 connection ID (IPv6ConnID)

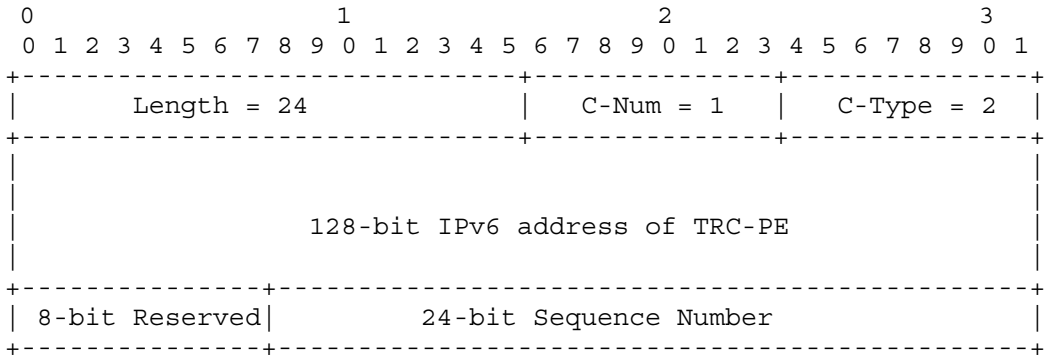


Figure 8-6 – IPv6 connection id object content

C-Num = 1

C-Type = 2, IPv6 connection ID.

The connection ID consists of two parts. One part is the 128-bit TRC-PE identification (ordinarily IPv6 address), the other part is the 24-bit sequence number allocated by the TRC-PE for the resource request. See Figure 8-6.

8.5.2 Flow ID (FlowID)

The purpose of this object is to identify a flow within a RCIP resource connection. A flow ID object is unique within one RCIP resource connection; its integer value ranges from 1 to 4294967296. It is a sub-object of flow profile object, carried in Resource Request and Acceptance, to identify a flow within a RCIP resource connection. When a TRC-PE sees one RCIP message containing such an object, it can create or find the corresponding flow ID within one RCIP resource connection, and does the corresponding process. See Figure 8-7.

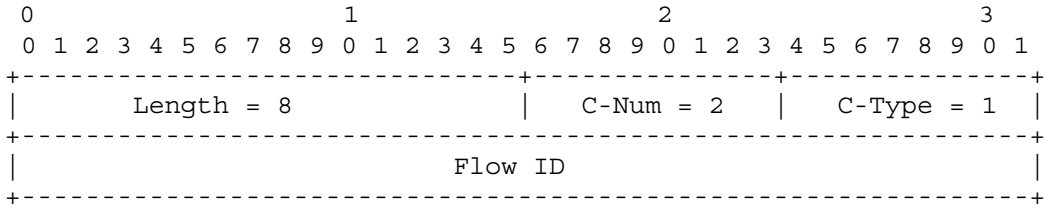


Figure 8-7 – Flow ID object content

C-Num = 2

C-Type = 1, Flow ID.

8.5.3 Flow information (FlowInfo)

The flow information object is a sub-object of flow profile object, carried in Resource Request and Acceptance. When a TRC-PE sees one RCIP message containing such an object, it can get the key information to identify an IP data stream, and carries out the corresponding process.

8.5.3.1 IPv4 flow information (IPv4FlowInfo)

The purpose of this object is to identify an IPv4 data stream. See Figure 8-8.

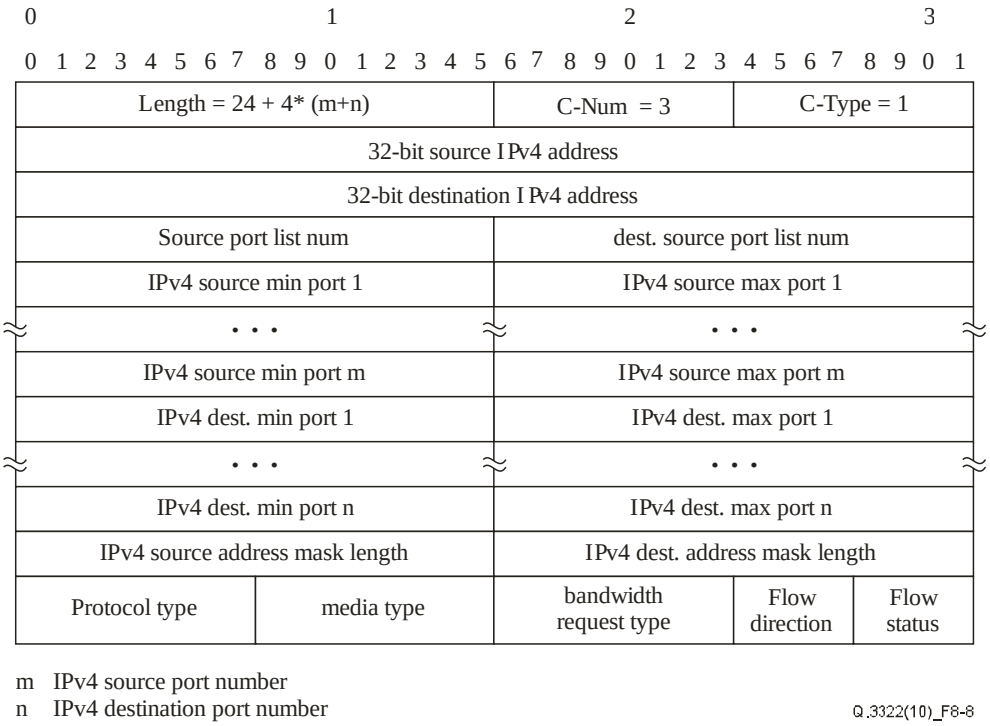


Figure 8-8 – IPv4 flow information object content

C-Num = 3

C-Type = 1, IPv4 Flow Information.

IPv4 Flow information includes source IPv4 address, destination IPv4 address, service type, protocol type, bandwidth request type (normal, degradation), flow direction (bidirectional, forward, backward), and flow status.

Media type mainly includes audio and video for different bandwidth requirements, e.g., AUDIO (0), VIDEO (1), DATA (2), APPLICATION (3), CONTROL (4), TEXT (5), MESSAGE (6), and OTHER (0xFFFFFFFF).

The most familiar application is providing service to multiple terminals within one network segment during a videoconference. When the mask length is 0, it means a single IP address, the max length of the mask is 32.

Protocol type:

0x0 = IP

0x1 = TCP

0x2 = UDP

Media type:

0x0 = audio

0x1 = video

0x2 = data

0x3 = application

0x4 = control

0x5 = text

0x6 = message

0xFFFFFFFF = other

Bandwidth request type may be one of following:

Normal (0): no special requirements to handle this type of request.

Degradation (1): when necessary, it can degrade the QoS via applying lower bandwidth to the call/session.

The flow status describes whether the IP flow(s) are enabled or disabled. The following values are defined:

Enable (2)

This value shall be used to enable all associated IP flow(s).

Enabled-forward (0)

This value shall be used to enable all associated IP flow(s) in the forward direction and disable all associated IP flow(s) in the backward direction when the flow direction is set to the value of "bidirectional".

Enabled-backward (1)

This value shall be used to enable all associated IP flow(s) in the backward direction and disable all associated IP flow(s) in the forward direction when the flow direction is set to the value of "bidirectional".

Disable (3)

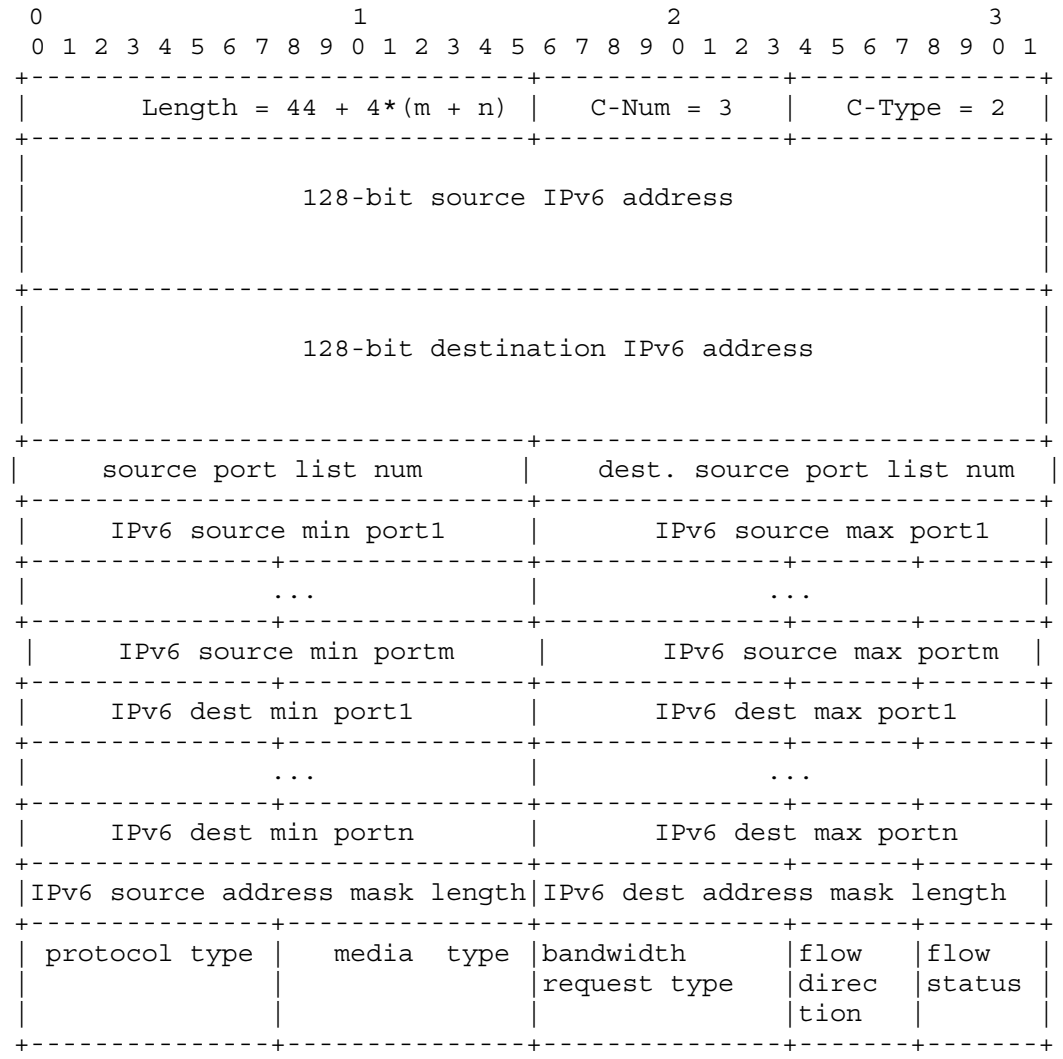
This value shall be used to disable all associated IP flow(s).

Remove (4)

The IP filters for the associated IP flow(s) shall be removed.

8.5.3.2 IPv6 flow information (IPv6FlowInfo)

The purpose of this object is to identify an IPv6 data stream. See Figure 8-9.



m IPv6 source port number.
n IPv6 destination port number.

Figure 8-9 – IPv6 flow information object content

C-Num = 3

C-Type = 2, IPv6 Flow Information.

IPv6 flow information (IPv6FlowInfo) object includes source IPv6 address, destination IPv6 address, service type, protocol type, bandwidth request type (normal, degradation), flow direction (bidirectional, forward, backward), and flow status.

When the mask length is 0, it means a single IP address, the max length of the mask is 64.

Bandwidth request type may be one of following:

Normal (0): no special requirements to handle this type of request.

Degradation (1): when necessary, it can degrade the QoS via allowing applying lower bandwidth to the call/session.

The flow state describes whether the IP flow(s) are enabled or disabled. The following values are defined:

Enable (2)

This value shall be used to enable all associated IP flow(s).

Enabled-forward (0)

This value shall be used to enable all associated IP flow(s) in the forward direction and disable all associated IP flow(s) in the backward direction when the flow direction is set to the value of "bidirectional".

Enabled-backward (1)

This value shall be used to enable all associated IP flow(s) in the backward direction and disable all associated IP flow(s) in the forward direction when the flow direction is set to the value of "bidirectional".

Disable (3)

This value shall be used to disable all associated IP flow(s).

Remove (4)

The IP filters for the associated IP flow(s) shall be removed.

8.5.4 Flow traffic descriptor (FlwTrafDscr)

The flow traffic descriptor (FlwTrafDscr) object is a sub-object of Flow Profile Object, carried in Resource Request and Resource Acceptance messages. When a TRC-PE sees a RCIP message containing such an object, it can get the key information about description of the service quality requirements of a stream, and carries out the corresponding process. It is allowed to use further version of RCIP to specify this object. The version number is in the RCIP header.

8.5.4.1 Forward flow traffic descriptor (FwdFlwTrafDscr)

The purpose of this object is to identify the forward flow traffic features. See Figure 8-10.

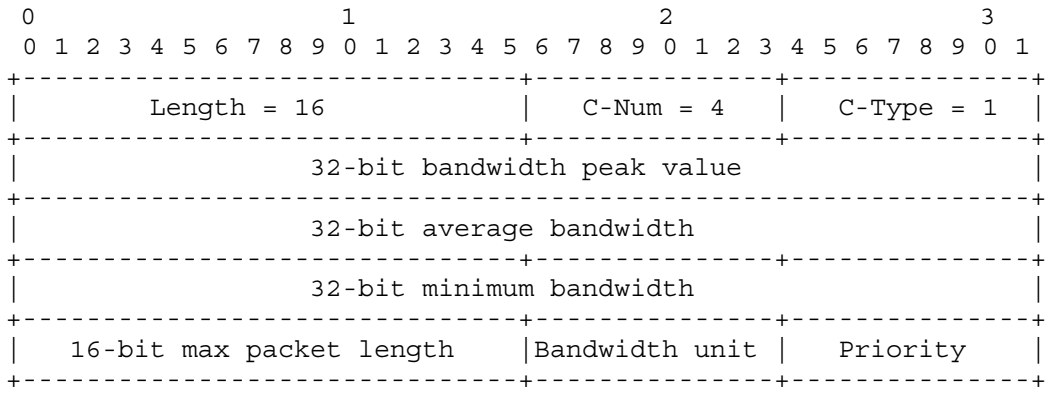


Figure 8-10 – Forward flow traffic descriptor object content

C-Num = 4

C-Type = 1, Forward Flux Descriptor.

The forward flow traffic descriptor (FwdFlwTrafDscr) object includes forward bandwidth peak value, average bandwidth (32 bits, the max is 4 Gbit/s based on 1 bit/s), and max packet length (16 bits, max value is 65535 bytes). The bandwidth units are bit/s (1), kbit/s (2), and Mbit/s (3). The value of priority ranges from 0 to 7 to identify the priority of the flow.

8.5.4.2 Backward flow traffic descriptor (BwdFlwTrafDscr)

The purpose of this object is to identify the backward flow traffic features. See Figure 8-11.

The backward flow traffic descriptor (BwdFlwTrafDscr) object includes backward bandwidth peak value, average bandwidth (32 bits, the max is 4 Gbit/s based on 1 bit/s), and max packet length (16 bits, max value is 65535 bytes). Bandwidth units are bit/s (1), kbit/s (2), and Mbit/s (3).

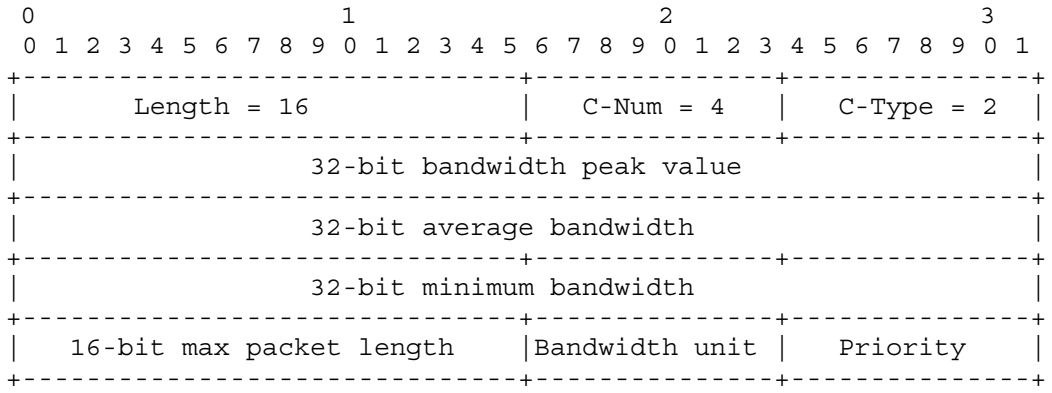


Figure 8-11 – Backward flow traffic descriptor object content

C-Num = 4

C-Type = 2, Backward Flow Traffic Descriptor.

8.5.5 LSP connection information (LSPconn)

In MPLS case, the connection information which is from the border router in this domain to the next hop border router is LSP label stack. LSP connection information (LSPconn) object is a sub-object of flow profile object, carried in Resource Request (RR) and Resource Acceptance (RA) messages.

8.5.5.1 IPv4 forward LSP connection information (IPv4FwdLSPconn)

The purpose of this object is to identify the IPv4 forward LSP connection information. See Figure 8-12.

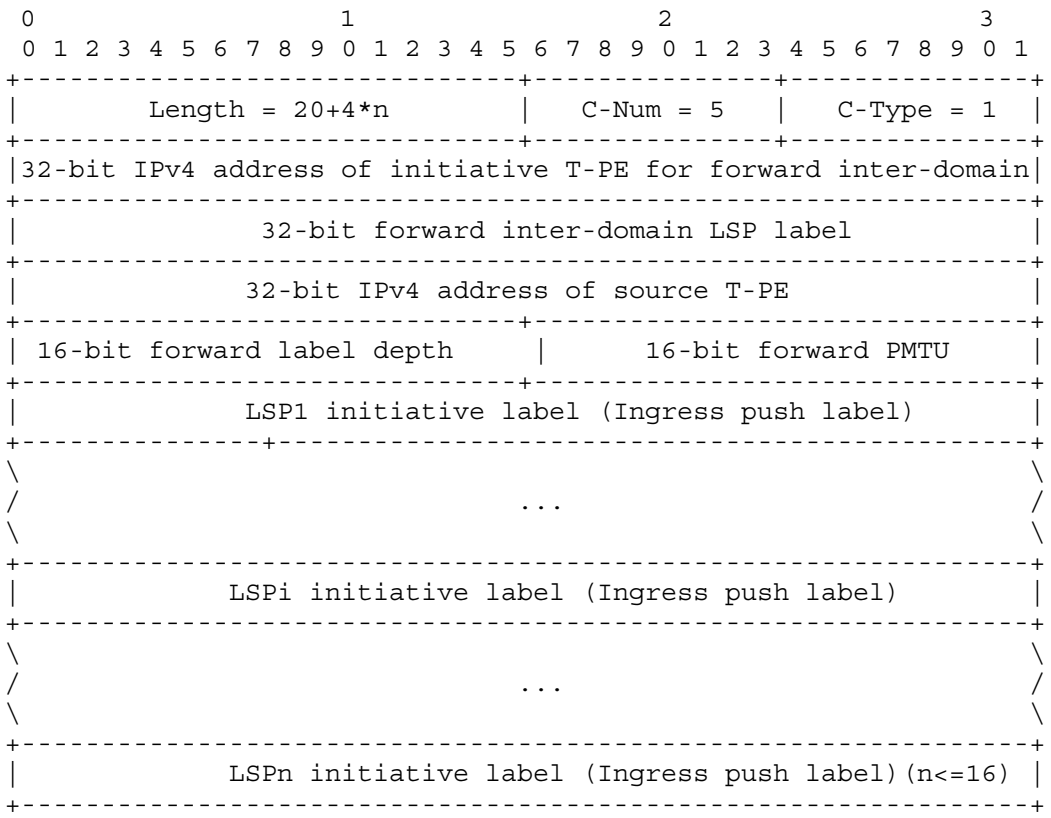


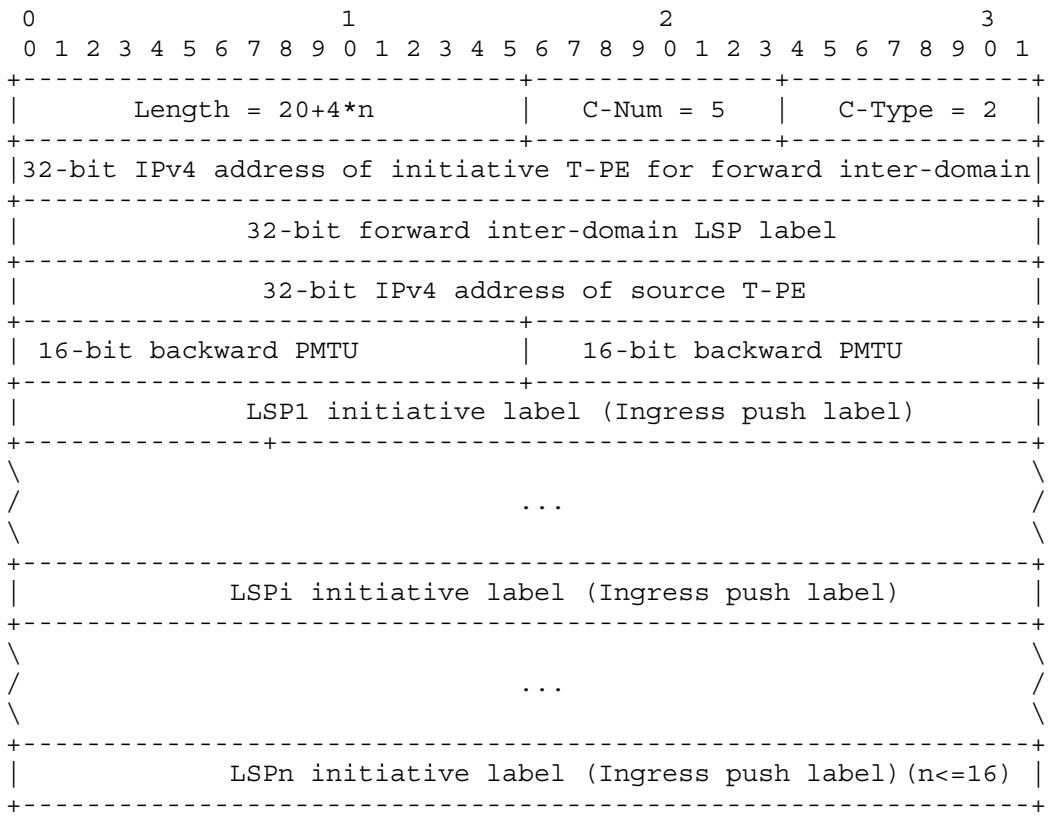
Figure 8-12 – IPv4 forward LSP connection information object content

C-Num = 5

C-Type = 1, IPv4 forward LSP connection information.

8.5.5.2 IPv4 backward LSP connection information (IPv4BwdLSPconn)

The purpose of this object is to identify the IPv4 backward LSP connection information. See Figure 8-13.



n LSP number.

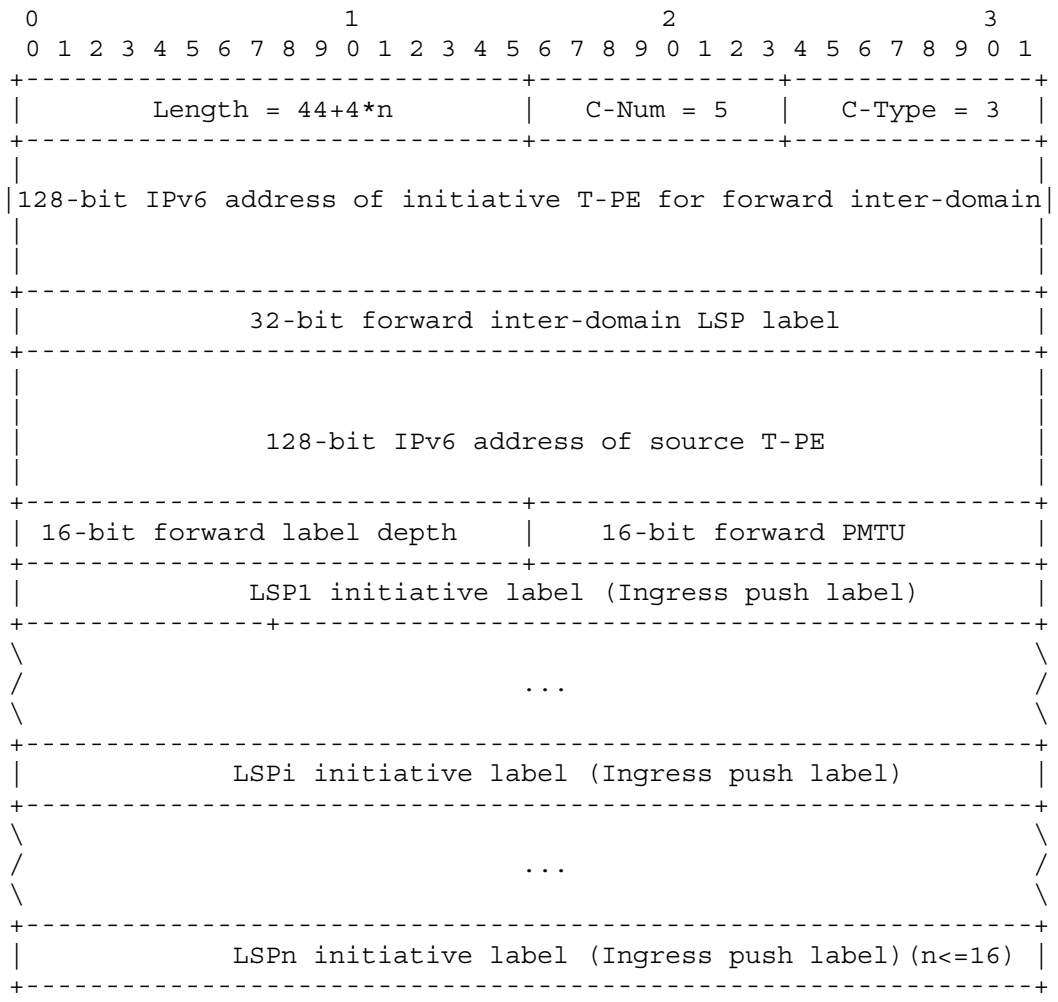
Figure 8-13 – IPv4 backward LSP connection information object content

C-Num = 5

C-Type = 2, IPv4 backward LSP connection information.

8.5.5.3 IPv6 forward LSP connection information (IPv6FwdLSPconn)

The purpose of this object is to identify the IPv6 forward LSP connection information. See Figure 8-14.



n LSP number.

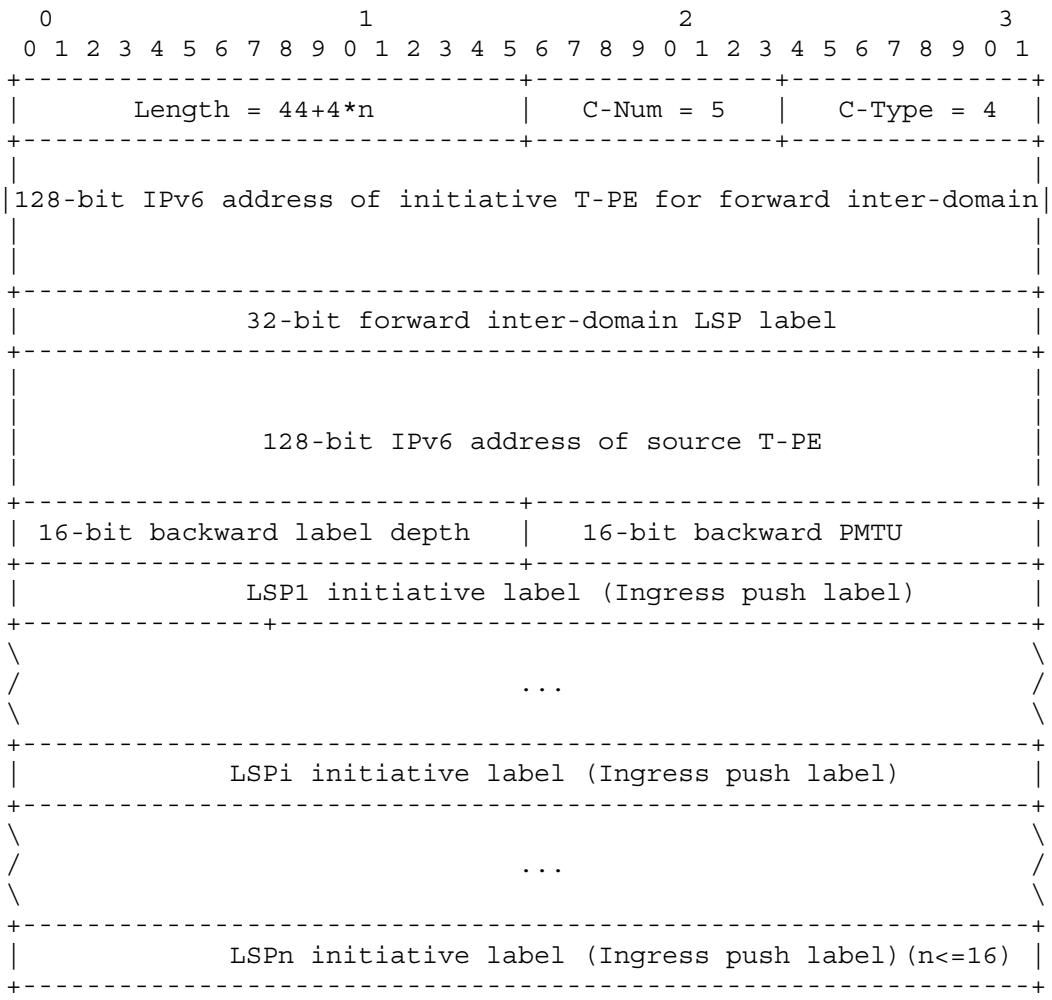
Figure 8-14 – IPv6 forward LSP connection information object content

C-Num = 5

C-Type = 3, IPv6 forward LSP connection information.

8.5.5.4 IPv6 backward LSP connection information (IPv6BwdLSPconn)

The purpose of this object is to identify the IPv6 backward LSP connection information. See Figure 8-15.



n LSP number.

Figure 8-15 – IPv6 backward LSP connection information object content

C-Num = 5

C-Type = 4, IPv6 backward LSP connection information.

8.5.6 Authentication information (AuthInfo)

The purpose of this object is to authenticate the peers. See Figure 8-16.

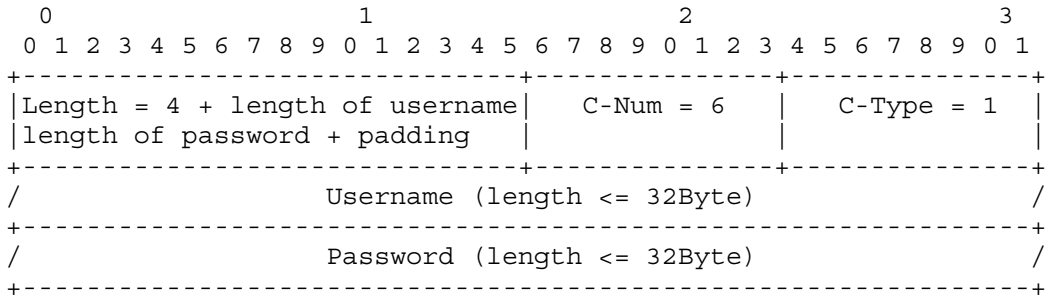


Figure 8-16 – Authentication information object content

C-Num = 6

C-Type = 1, Authentication Information.

Username and password should be carried in the OPEN message, for authentication of peers.

8.5.7 Reason code (ReasonCode)

The reason code (ReasonCode) object specifies the reason why the request state was deleted. It appears in the Resource Release Request (RLR) message. See Figure 8-17.

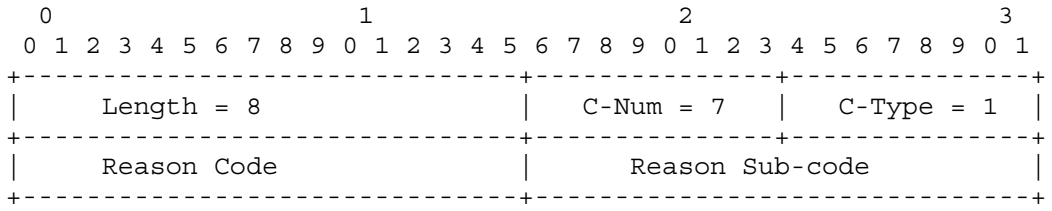


Figure 8-17 – Reason code object content

C-Num = 7, C-Type = 1

Reason code:

0 = Operating normally

1 = Router operation failed

2 = Connection interrupted

3 = Insufficient Resources

4 = Bandwidth mode not supporting

5 = Path unavailable

6 = Timeout

7 = Illegal operation

8 = Unknown object

9 = Upgrade needed

10= Authentication failed

11= Configuration process

12= TCP connection interrupted

13= Abnormal interruption

14= Message error

15= Loop request

16= Distribution failure

17= Others

The reason sub-code field is reserved for more detailed client-specific reason codes.

8.5.8 Identity identification (IdentityIdentification)

Identity identification adopts only International Alphabet No.5 string format [ITU-T T.50]. In a general way, this is the static IP address of TRC-PE. When the TRC-PE adopts dynamic IP address, identity identification object can use domain name system (DNS) domain name. It is used in OPEN message. TRC-PE should do a validity check including domain name, identifier and address. See Figure 8-18.

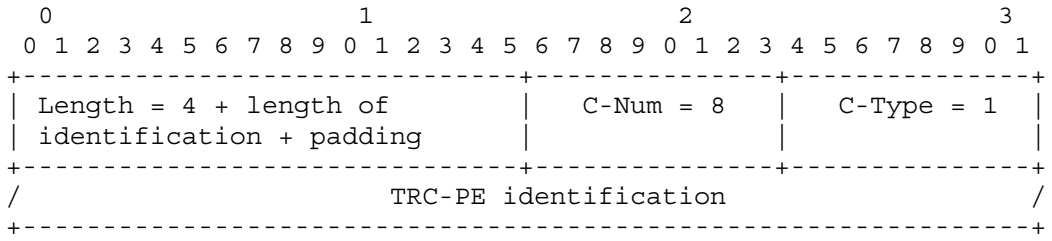


Figure 8-18 – Identity identification object content

C-Num = 8, C-Type = 1

8.5.9 Keep-alive timer (KATimer)

The Keep-Alive Timer object is used to specify the maximum time interval over which an RCIP transport channel message is recommended in order to be sent or received. See Figure 8-19. The units are in seconds. It is used in ACCT message. Times are encoded as 2 octet integer values and are in units of seconds. The timer value is treated as a delta. The TRC-PE compares the KA Timer value which the ACCT message carries, with local KA Timer value; select the smaller value as the KA Timer value between them. If the TRC-PE does not accept the KA Timer value, the CLOSE message is sent to disconnect. The range of finite timeouts is 1 to 65535 seconds represented as an unsigned two-octet integer.

The KA Timer is used only on the RCIP transport channel, i.e., between two TRC-PEs.

Scope of KA Timer values: 0-65535

Default: 45 seconds

The value of zero implies infinity, that means TRC-PE does not check the KA message, and does not send any KA message.

A KA message is sent per 1/3 KA Timer.

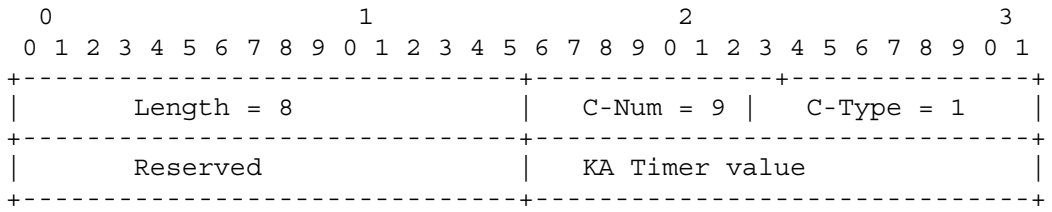


Figure 8-19 – Keep-alive timer object content

C-Num =9,

C-Type = 1, Keep-alive timer value

8.5.10 Data consistency (DataConsistency)

The purpose of this object is to verify the consistency of the RCIP message. See Figure 8-20.

In order to ensure message integrity, TRC-PEs adopt HMAC technology [b-IETF RFC 2104] and compute the message digests to be appended at the end of an RCIP message, using the shared key and cryptographic algorithm to verify the consistency.

The data consistency message includes a 32-bit Key ID, a 32-bit sequence number and a 96-bit message digest.

A 32-bit Key ID is used to identify a specific key shared between TRC-PEs and the cryptographic algorithm to be used.

The sequence number is initiated during an initial OPEN message and is then incremented by one each time a new message is sent over the TCP connection in the same direction. If the sequence number reaches the value of 0xFFFFFFFF, the next increment will simply roll over to a value of zero to avoid the replay attack.

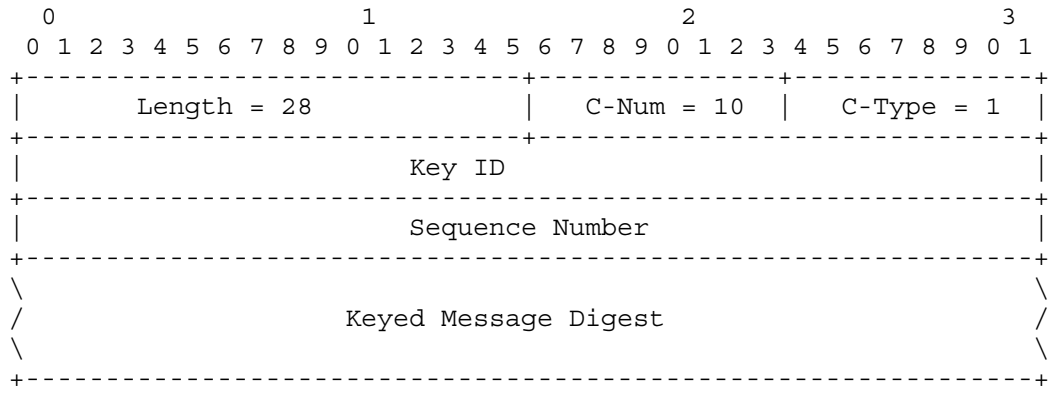


Figure 8-20 – Data consistency object content

C-Num = 10,

C-Type = 1, HMAC digest

8.5.11 V-switching connection information (VSConnInfo)

The purpose of this object is to identify the v-switching connection information. See Figure 8-21.

V-switching connection information object includes the connection information of In V-switching and the Out V-switching.

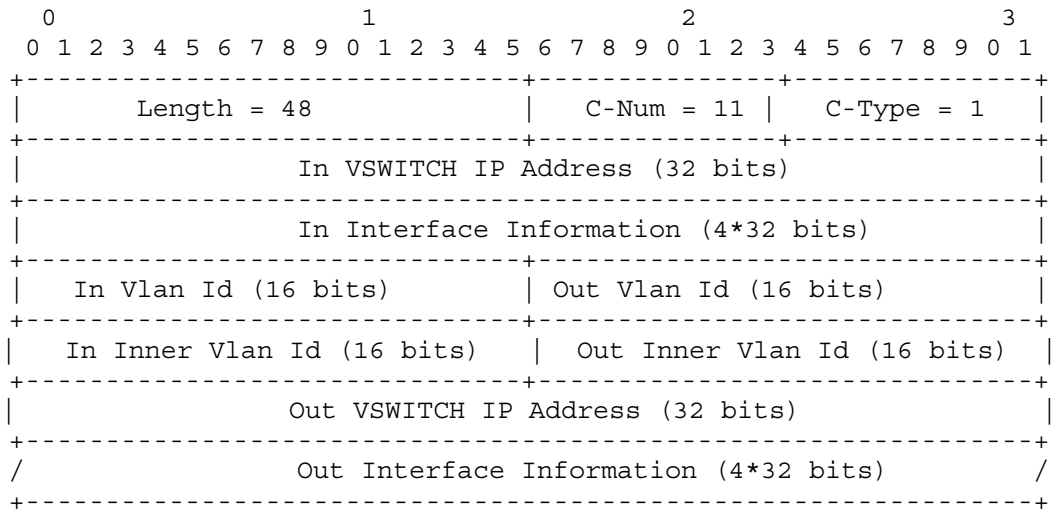


Figure 8-21 – V-switching connection information object content

C-Num = 11,

C-Type = 1, V-switching connection information

In/Out Inner Vlan Id means null if presented as 0xFFFF.

8.5.12 Overload indication (Overload-Indication)

The purpose of overload indication object is to indicate whether overload information is carried in the Overload Indication message. See Figure 8-22.

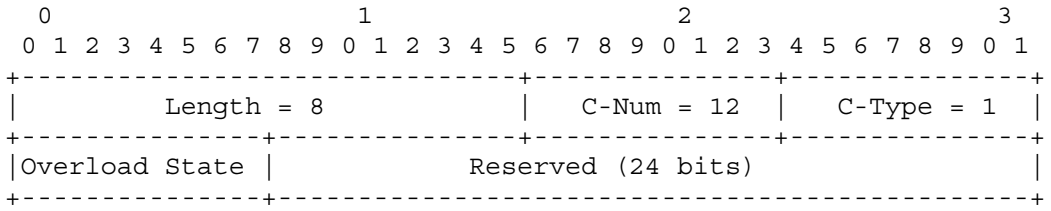


Figure 8-22 – Overload indication object content

C-Num = 12,

C-Type = 1, Overload Indication.

Overload State:

0 – overload recovered (no overload)

1 – Overload happened

8.5.13 Flow profile (FlowProfile)

The flow profile object is carried in Resource Request and Resource Response messages. It can appear one or more times in a Resource Request or Resource Response messages.

8.5.13.1 Flow profile for MPLS case (FlowPro4MPLS)

The purpose of this object is to provide the flow profile in MPLS case. See Figure 8-23.

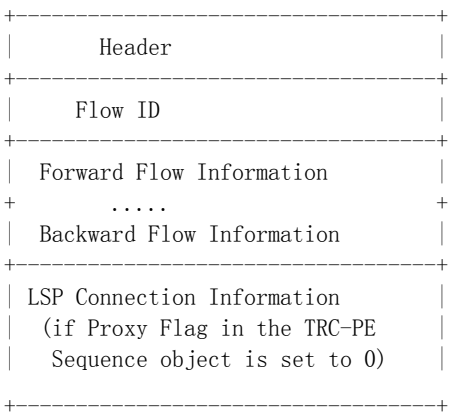


Figure 8-23 – Flow profile for MPLS case object content

C-Num = 13

C-Type = 1, Flow profile for MPLS case.

The content includes flow ID, flow information, flow traffic descriptor (multiple groups of forward flow traffic descriptor and multiple groups of backward flow traffic descriptor), LSP connection information (needed only when Proxy flag is set to 0).

8.5.13.2 Flow profile for V-switching case (FlowPro4V-Switching)

The purpose of this object is to provide the flow profile in V-Switching case.

C-Num = 13

C-Type = 2, Flow profile for V-switching case.

The content includes flow ID, digits from 0 to 9, flow traffic descriptor (multiple groups of forward flow traffic descriptor and multiple groups of backward flow traffic descriptor), V-switching connection information (needed only when Proxy flag is set to 0).

8.5.14 Result indication (Result Indication)

The result indication (Result Indication) object is needed to indicate the result of success/failure in the audit message. See Figure 8-24.

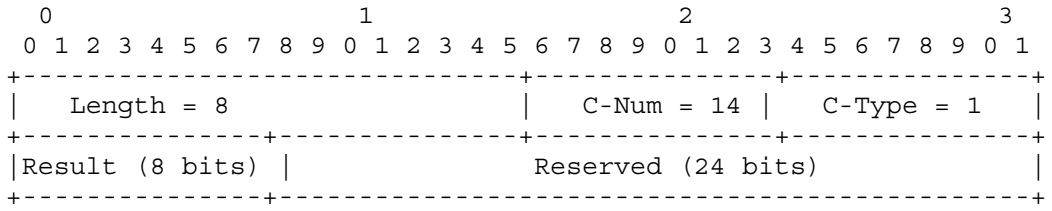


Figure 8-24 – Result indication object content

C-Num = 14

C-Type = 1, Result Indication.

Result:

0 – Success

1 – Non-success

8.5.15 Digits string (DigitsString)

The digits string (DigitsString) object is a sub-object of V-switching logical path information object, carried in the Resource Request and Resource Response messages. See Figure 8-25.

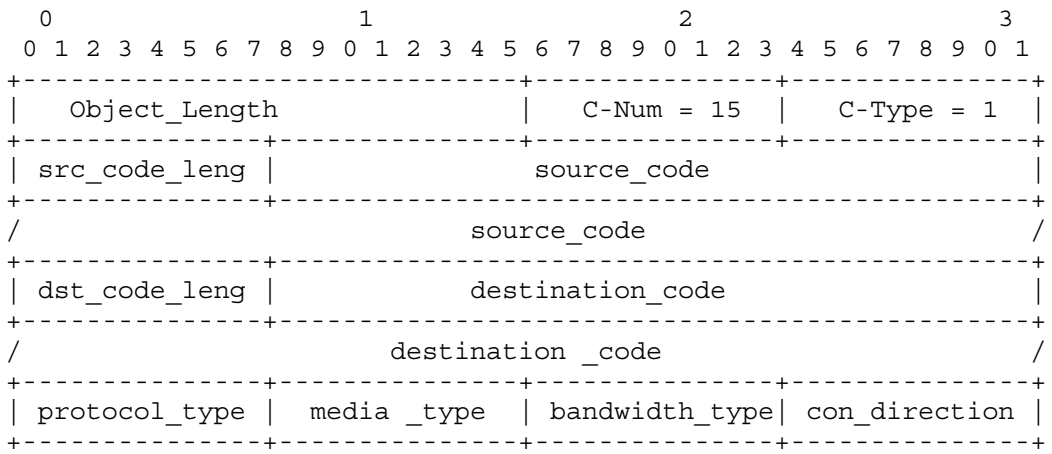


Figure 8-25 – Digits string object content

object_length: length of the object in octet

C-Num = 15

C-Type = 1

object_length = 16 + (src_code_length + 1)/2/4*4 + (dst_code_length + 1)/2/4*4 (divide exactly)

source_code: source number (BCD code)

destination_code: destination number (BCD code)

src_code_length: amount of source numbers

dst_code_length: amout of destination numbers

The following values are the same with the flow-info objects:

procotol_type: protocol type

media_type: media type

bandwidth_type: bandwidth request type

con_direction: connection direction

Bidirectional: 0

Forwarding: 1

Backwarding: 2

8.5.16 Resource state (RrcState)

8.5.16.1 Connection resource state (ConnRrcState)

The purpose of this object is to identify the resource state of the connection.

Connection resource state code includes OK(0), flow aging(1), LSP unavailable(2), Vlan-switching interface unavailable(3), inexistence of one connection ID(4), connection resource unmatchable(5); suggest release(6), the hops of source seeking beyond the specification limitation(7), query timeout(8). See Figure 8-26.

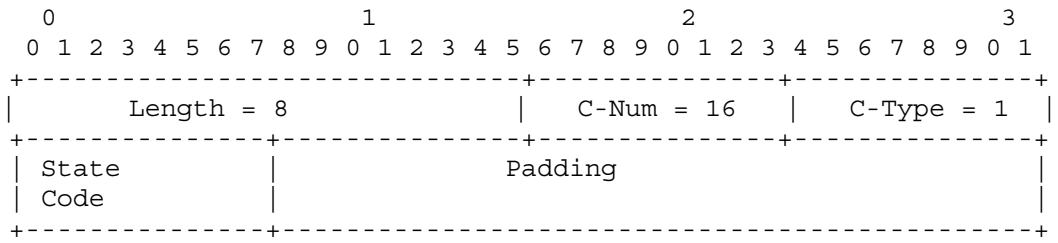


Figure 8-26 – Connection resource state object content

C-Num = 16

C-Type = 1, Connection resource state.

8.5.16.2 Node state (NodeState)

The purpose of this object is to identify the state of the node. See Figure 8-27.

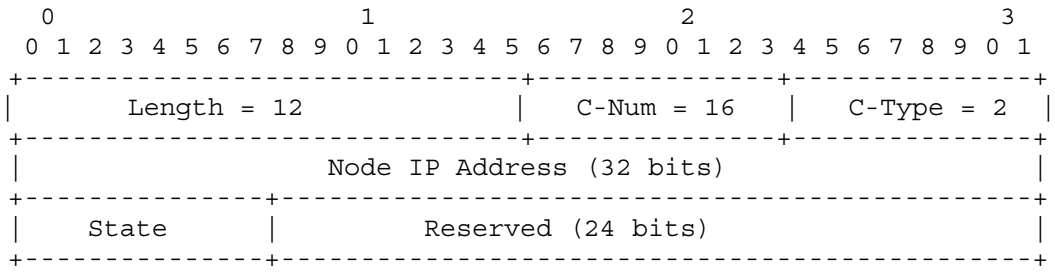


Figure 8-27 – Node state object content

C-Num = 16

C-Type = 2, Node state.

The node state denotes as follows:

0 = disabled

1 = enabled

2 = overload

3 = holding

FF = inexistence

8.5.16.3 LSP resource state (LspRrcState)

The purpose of this object is to identify the state of the LSP resource. See Figure 8-28.

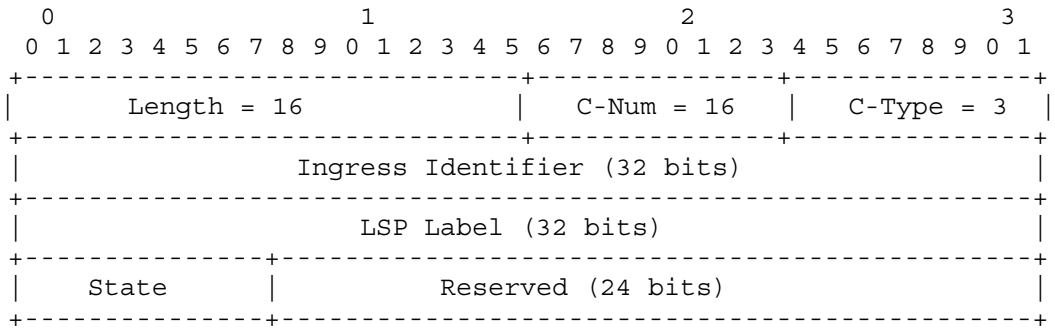


Figure 8-28 – LSP resource state object content

C-Num = 16

C-Type = 3, LSP resource state.

The LSP resource state denotes as follows:

0 = disabled

1 = enabled

FF = inexistence

8.5.16.4 Interface state (IntState)

The purpose of this object is to identify the state of the interface. See Figure 8-29.

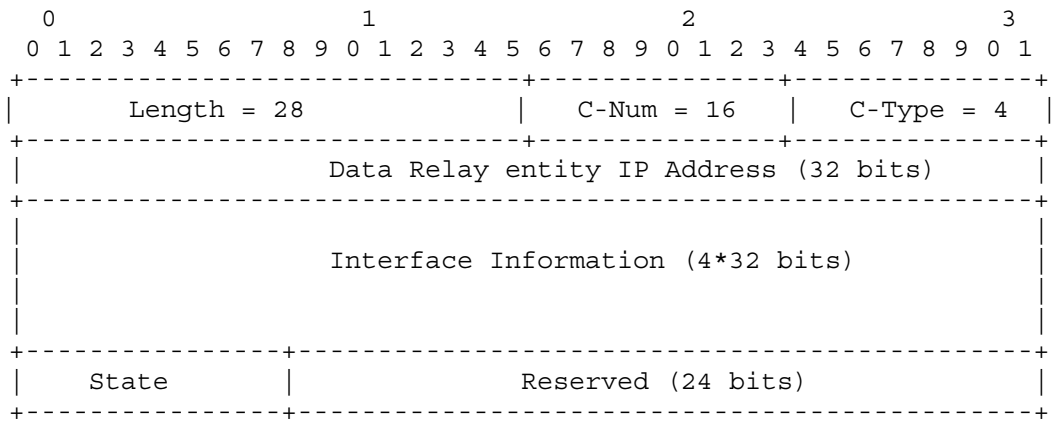


Figure 8-29 – Interface state object content

C-Num = 16

C-Type = 4, Interface state.

The interface state denotes as follows:

0 = disabled

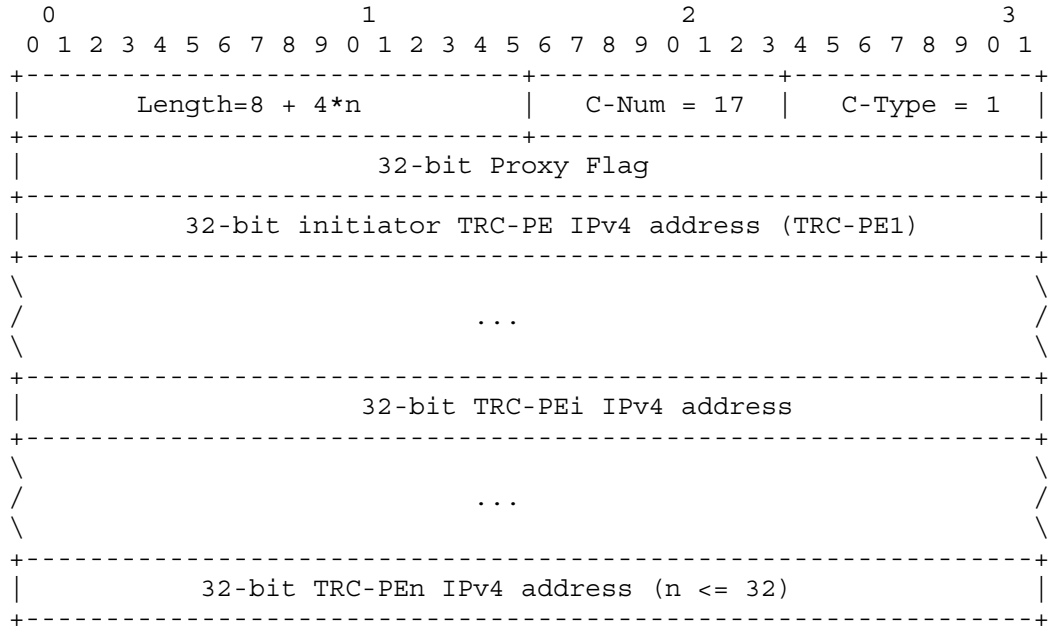
1 = enabled

FF = inexistence

8.5.17 TRC-PE sequence (TRC-PESequence)

8.5.17.1 IPv4 TRC-PE sequence (IPv4TRC-PESequence)

The purpose of this object is to define the IPv4 TRC-PE sequence. See Figure 8-30.



n TRC-PE list number.

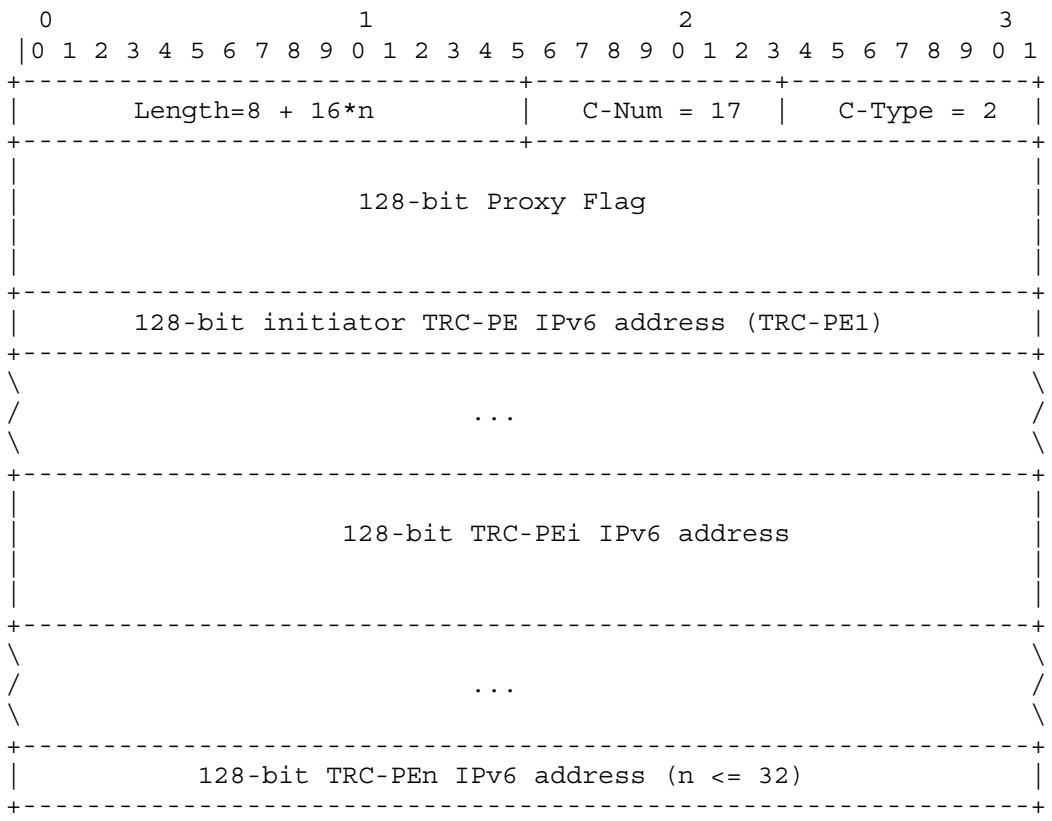
Figure 8-30 – IPv4 TRC-PE sequence object content

C-Num = 17

C-Type = 1, IPv4 TRC-PE sequence.

8.5.17.2 IPv6 TRC-PE sequence (IPv6TRC-PESequence)

The purpose of this object is to define the IPv6 TRC-PE sequence. See Figure 8-31.



n TRC-PE list number.

Figure 8-31 – IPv6 TRC-PE sequence object content

C-Num = 17

C-Type = 2, IPv6 TRC-PE sequence.

8.5.18 Media profile (MediaProfile)

The purpose of this object is to provide the service information for a single media component within an application session. The media profile object is carried in Resource Request and Resource Response messages. It can appear one or more times in Resource Request or Resource Response messages.

C-Num = 18

C-Type = 1, media profile.

The content includes one media profile ID object and one or more flow profile objects.

8.5.19 Media profile ID (MediaProfileID)

The purpose of this object is to identify the media component within an application session. See Figure 8-32.

The media profile ID object is a sub-object of media profile object, carried in Resource Request and Resource Response messages.

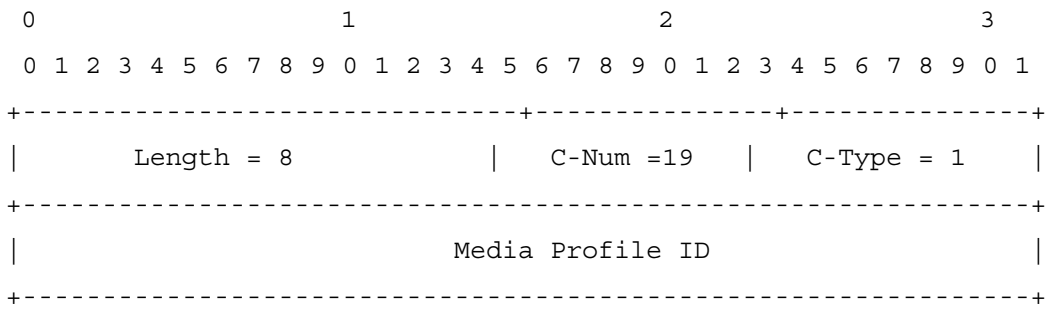


Figure 8-32 – Media profile ID object content

C-Num = 19

C-Type =1, media profile ID.

8.5.20 Aggregate resource information

The aggregate resource information object is a sub-object of aggregate resource profile object, carried in aggregate Resource allocation request and Resource Response messages. See Figure 8-33.

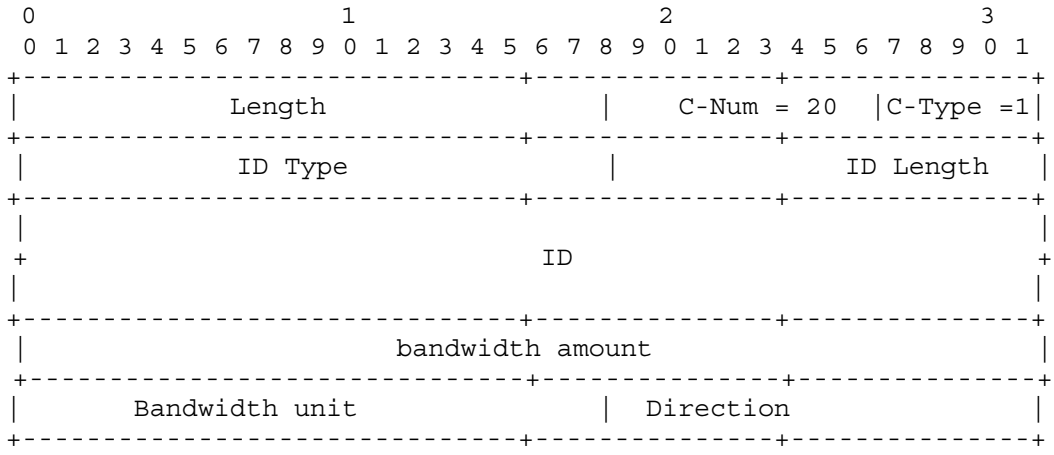


Figure 8-33 – Aggregate resource information object content

Length: the length of this object.

C-Num = 20

C-Type = 1, aggregate resource information.

ID type: the type of identifier, 0 for logical access ID, 1 for physical access ID, 2 for logical aggregation ID, 3 for physical aggregation ID.

ID length: the length of ID.

ID: the identifier value of the resource in the access/aggregation network.

Bandwidth amount: the aggregate bandwidth description.

Bandwidth unit: the unit of bandwidth amount.

9 Performance considerations

9.1 Performance requirement

It is important to consider processing delays in order to meet minimum requirements for entire call delays. Therefore, RCIP is recommended to establish, maintain and clear the QoS request messages whose quantities should be kept to a minimum. Simultaneously, it is recommended to choose the signalling message form through which a minimum message handling delay can be reached.

10 Other considerations

10.1 Integrity

In order to prevent the messages from being illegally changed or attacked during the transmission, HMAC (hash-based message authentication code) technology is used between TRC-PE(s) for calculating the message abstract, which is to be attached to the message. The shared key value and algorithm are used for verifying the integrity. HMAC technology supports HMAC-MD5-96. The data integrity message is composed of the KEY_ID, sequence number and abstract. The KEY_ID describes the key value and algorithm shared by both parties. The sequence number is initialized when opening the message. The subsequent messages are added sequentially. When the messages overflow, the sequence number resumes from 0, so as to prevent replay attacks from occurring.

10.2 Protocol transport and maintenance

The TCP or SCTP port number assignment for RCIP is 2225.

In order to ensure a reliable transmission for the service connection resources between the TRC-PE(s), the RCIP protocol connection needs to be established between the TRC-PE(s) for bearing the service connection resources messages. The protocol connection maintains the status through the heartbeat mechanism. The RCIP protocol connection should be persistent: the connection should be re-established automatically even if the connection, for any reason, goes down.

10.3 Connection ID

One RCIP resource connection corresponds to one connection ID. One call may have many connections, e.g., a bidirectional call needs to establish two connections.

Connection ID is used for specifying a connection. It can ensure correct operations for connections with the same connection ID. When the system needs service requirements such as signalling tracing, statistics charging, the connection ID will identify and specify, thus maintaining correct operations.

11 Security considerations

To establish a semi-permanent connection between the two opposite ends of the RCIP, the client side verifies the establishment to the server. This can be accomplished by carrying verification information in the RCIP message, configuring the verification scheme at the client side, and configuring the user at the server. The verification methods include, but are not limited to, plain text verification, and MD5 verification [IETF RFC 1321].

The RCIP protocol provides a data consistency object that can achieve authentication, message integrity, and replay prevention. All RCIP implementations are required to support the RCIP data consistency object and its mechanisms as described in this Recommendation. To ensure that the client is communicating with the correct server requires authentication of the client and server using a shared secret and consistent proof that the connection remains valid. The shared secret requires, at a minimum, manual configuration of keys (identified by a Key ID) shared between the client and its server. The key is used in conjunction with the contents of an RCIP message to calculate a message

digest which is part of the data consistency object. The data consistency object is then used to validate all RCIP messages sent over the TCP connection between a client and a server.

Key maintenance is outside the scope of this Recommendation. In general, it is good practice to regularly change keys to maintain security. Furthermore, it is good practice to use localized keys specific to a particular client such that a stolen client cannot compromise the security of an entire administrative domain.

The RCIP data consistency object also provides sequence numbers to avoid replay attacks. The server chooses the initial sequence number for the client and the client chooses the initial sequence number for the server.

These initial numbers are then incremented with each successive message sent over the connection in the corresponding direction. The initial sequence numbers are recommended to be chosen such that they are monotonically increasing and are never repeated for a particular key.

Security between the client and server may be provided by IP security (IPSec). In this case, the IPSec authentication header (AH) is recommended to be used for the validation of the connection; additionally IPSec encapsulation security payload (ESP) may be used to provide both validation and secrecy.

Transport layer security (TLS) may be used for both connection-level validation and privacy.

Annex A

A cross-reference matrix for objects and messages in ITU-T Q.3302.1

(This annex forms an integral part of this Recommendation.)

Legend:
M) Mandatory object
O) Optional object
1) Part of flow profile for MPLS case object
2) Part of flow profile for V-switching case object

Object	Connection ID	Flow ID	Flow Information	Flow Traffic Descriptor	LSP Connection Information	Authentication Information	Reason Code	Identity Identification	Keep-Alive Timer	Data Consistency Information	V- Switching connection information	Overload Indication	Flow Profile	Result Indication	DIgit String	Resource State	TRC-PE Sequence	Media Profile	Media Profile ID
grouped object													G						
part of group		Y	Y	Y	Y						Y				Y				
Op-Code	Code point	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
OPEN	6						**O**		**M**		**O**									
ACCT	7									**M**	**O**									
CLOSE	8							**M**			**O**									
KA	9										**O**									
RR	11	**M**	**1/2**	**1**	**1/2**	**1**					**O**			**M**		**2**			**M**	**M**
RA	12	**M**	**1/2**	**1**	**1/2**	**1**					**O**			**M**		**2**			**M**	**M**
REJ	13	**M**						**M**			**O**									
RLR	14	**M**						**M**			**O**									
RLP	15	**M**						**M**			**O**									
OVE	16										**O**		**M**							
AUR	17	**M**									**O**									
AUP	18	**M**									**O**				**M**					

Appendix I

An information flow example

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

I.1 TRC-PE source-addressing information flows

The initiator TRC-PE performs the seeking of the real source TRC-PE. The initiator TRC-PE checks if the source address of flow information in the QoS request received from SCE, belongs to the management of the managed area of which the initiator TRC-PE takes charge. When it finds that the source address of stream information in the QoS request does not belong to its managed area, it issues information flow 1.

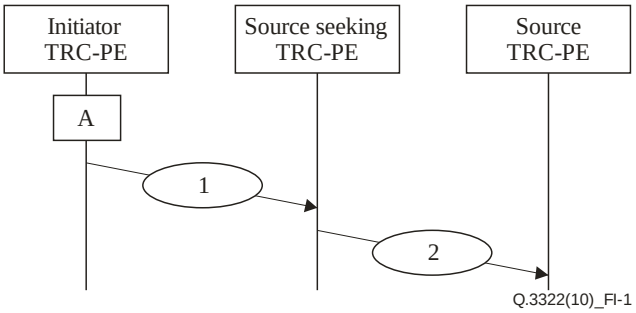


Figure I.1 – TRC-PE source-addressing information flows

The flows illustrated in Figure I.1 are as follows:

Sequence A

The initiator TRC-PE performs the seeking of the real source TRC-PE. The initiator TRC-PE checks whether the source address of stream information in the QoS request received from SCE belongs to the management of the managed area of which the initiator TRC-PE takes charge. When it finds that the source address of stream information in the QoS request does not belong to its managed area, it issues information flow 1.

1 IP Setup-Request.ready Initiator TRC-PE to source-seeking TRC-PE

Table I.1 – Information elements for information flow 1

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter

Processing upon receipt: The source-seeking TRC-PE checks if the source address of stream information in the QoS request belongs to the management of the managed area of which the source-seeking TRC-PE takes charge. When it finds that the source address of stream information in the QoS request does not belong to its managed area, it acts as a source-seeking TRC-PE. The source-seeking TRC-PE queries the "Source TRC-PE" route to find out the next hop TRC-PE, to which it will transfer the request. Then it issues information flow 2.

2 IP Setup-Request.ready Source-seeking TRC-PE to source TRC-PE

Table I.2 – Information elements for information flow 2

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter

Processing upon receipt: The TRC-PE checks whether the source address of stream information in the QoS request belongs to the management of the managed area of which the TRC-PE takes charge. When it finds that the source address of flow information in the QoS request belongs to its managed area, the process of addressing source TRC-PE is completed and this TRC-PE acts as a source TRC-PE.

I.2 Unidirectional QoS path establishment information flows

There are two approaches in the QoS path establishment procedures. The difference is the existence of the provisional response from TRC-PE to SCE, by which the TRC-PE notifies SCE that the resource allocation is successful, just before confirming the local policies to the corresponding T-PE. When the SCE receives the provisional response, then it changes the state of the service control from "waiting for the successful completion of resource allocation", to the next state with issuing the awaited service control messages. This approach can be applied when the resource management is integrated with service control in which the completion of the resource allocation is required before the progress and completion of the session establishment. Some VoIP services may require the completion of resource allocation before the called party's state transition into the alerting.

In the following, the scenario when the resource request is processed without the provisional response is called "1-phase case". If the request is processed with this response, it is called "2-phase case".

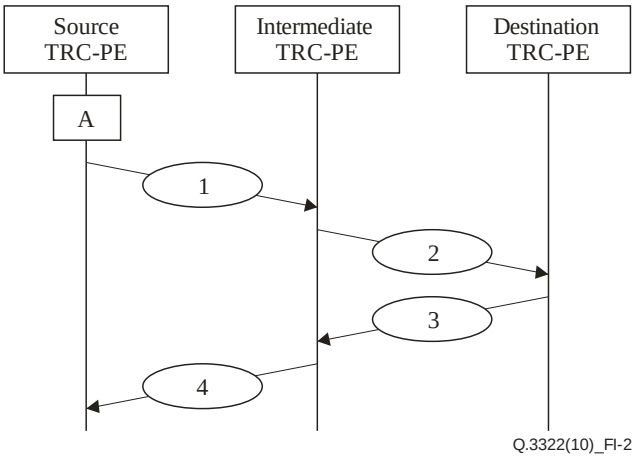


Figure I.2 – Forward unidirectional QoS path establishment information flows

The flows illustrated in Figure I.2 are as follows:

A

The source TRC-PE (also an initiator TRC-PE) allocates the path resources of the local domain. It then issues information flow 1.

1 IP Setup-Request.ready Source TRC-PE to intermediate TRC-PE

Table I.3 – Information elements for information flow 1

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Path information selected in the local domain (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE allocates the intermediate path resources. It then issues information flow 2.

2 IP Setup-Request.ready Intermediate TRC-PE to destination TRC-PE

Table I.4 – Information elements for information flow 2

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Path information selected in the local domain and the previous domains (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The result of the destination TRC-PE route decides the final path resource. The destination TRC-PE responds to the intermediate TRC-PE. It then issues information flow 3.

3 IP Setup-Request.commit Destination TRC-PE to intermediate TRC-PE

Table I.5 – Information elements for information flow 3

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE responds to the source TRC-PE. It then issues information flow 4.

4 IP Setup-Request.commit Intermediate TRC-PE to source TRC-PE

Table I.6 – Information elements for information flow 4

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: It then issues an information flow to the Source T-PE or SCE (only for 2-phase case).

I.3 Bidirectional QoS path establishment information flows

There are two methods to establish a bidirectional QoS path supporting symmetric QoS requests; one is to allocate the path of the two directions at one time, which can be applied when the transport plane is able to perform the explicit routing for reducing the time of the signalling procedures (see clause I.3.1); the other is to use two, unidirectional information flows (see clause I.3.2).

The differences between unified-allocated forward-and-backward-resource information flows and separately-allocated forward-and-backward-resource information flows are:

– Path information of two directions is needed for the source TRC-PE and intermediate TRC-PE to initiate a resource request. For a bidirectional path with unified-allocated forward-and-backward-resource information flows, both forward and backward paths are needed.

– Path information of two directions is needed for the destination TRC-PE and intermediate TRC-PE to initiate a resource response.

– The destination TRC-PE needs to deliver a piece of QoS configuration information from the called to the caller to the destination T-PE.

I.3.1 Unified-allocated forward-and-backward-resource information flows

NOTE – The flows drawn in dashed lines are used only in the 2-phase case.

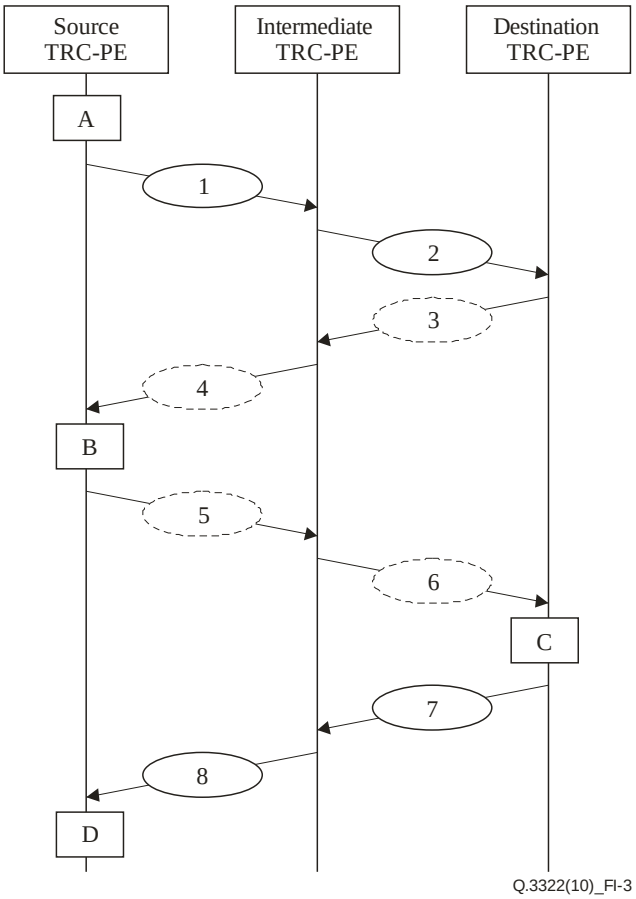


Figure I.3 – Bidirectional QoS path establishment information flows with unified-allocated signalling path

The flows illustrated in Figure I.3 are as follows:

Sequence A

The source TRC-PE allocates the path resources of the local domain. It then issues information flow 1.

1 IP Setup-Request.ready Source TRC-PE to intermediate TRC-PE

Table I.7 – Information elements for information flow 1

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Path information selected in the local domain (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE allocates the intermediate path resources. It then issues information flow 2.

2 IP Setup-Request.ready Intermediate TRC-PE to destination TRC-PE

Table I.8 – Information elements for information flow 2

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Path information selected in the local domain and the previous domains (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The result of the destination TRC-PE route decides the final path resource. The TRC-PE responds to the intermediate TRC-PE. It then issues information flow 3.

3 IP Setup-Request.commit Destination TRC-PE to intermediate TRC-PE (only in 2-phase case)

Table I.9 – Information elements for information flow 3

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE responds to the source TRC-PE. It then issues information flow 4.

4 IP Setup-Request.commit Intermediate TRC-PE to source TRC-PE (only in 2-phase case)

Table I.10 – Information elements for information flow 4

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The source TRC-PE issues information flow to SCE.

Sequence B

In a 2-phase case, the source TRC-PE receives the information flow from SCE, and information flow 5 is issued to control the configuration information of the opposite side T-PE.

5 IP Setup-Request.ready Source TRC-PE to intermediate TRC-PE (only in 2-phase case)

Table I.11 – Information elements for information flow 5

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE finds out the next hop until the destination TRC-PE. It then issues information flow 6.

6 IP Setup-Request.ready Intermediate TRC-PE to destination TRC-PE (only in 2-phase case)

Table I.12 – Information elements for information flow 6

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more addresses, protocol and port tuples) QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The destination TRC-PE controls the destination T-PE for the stream in the direction from the destination T-PE to the source T-PE. Upon getting a piece of complete path resource information, the destination TRC-PE forms a piece of stream QoS configuration information to deliver a piece of configuration information to the destination T-PE. It then issues an information flow to destination T-PE.

Sequence C

The destination T-PE installs the configuration information to control the data stream transfer. It then issues an information flow back to destination TRC-PE.

7 IP Setup-Request.commit Destination TRC-PE to intermediate TRC-PE

Table I.13 – Information elements for information flow 7

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate TRC-PE responds to the source TRC-PE. It then issues information flow 8.

8 IP Setup-Request.commit Intermediate TRC-PE to Source TRC-PE

Table I.14 – Information elements for information flow 8

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Accepted QoS parameter Whole path information (for the MPLS case) Address information of the inter-domain interface (for the non-MPLS case)

Sequence D

The source TRC-PE issues an information flow to control the stream QoS configuration information of the source T-PE. When there is no need to wait for the whole path information, after receiving the information flow (which is the response for "backward message flows", as well as the information flow which is the response for "forward message flows"), the source and initiator TRC-PE issues the information flows which are sent to SCE.

I.3.2 Separately-allocated forward-and-backward-resource information flows

Figure I.4 shows the separately-allocated forward-and-backward-resource information flows. For the backward information flows, if both the calling and called party SCE take part in the procedure, we can use the second figure; if only one of the calling and called party SCE take part in the procedure, we can use the third figure.

If either the calling party or called party SCE takes part in the procedure, two parallel unidirectional information flows are used, as described in clause I.2 with the following exceptions:

– The TRC-PE receiving information flow from SCE splits the signalling sequence into two sequences with opposite directions.

  In the 2-phase case, this split is also performed after receiving an information flow from SCE.

– The TRC-PE receiving information flow 1 also waits for the response of each sequence (information flow from source T-PE and S8), and then consolidates these two signalling sequences into a single sequence.

  In the 2-phase case, this consolidation is also performed before issuing an information flow to SCE.

– To perform the resource control in the direction where the initiator TRC-PE is not the source TRC-PE, the source TRC-PE seeking flows (described in clause I.1) are applied as described with information flows (S1, S2, S3, S4, S5, S6, S7, S8.)

NOTE – The flows drawn in dashed lines are used only in the 2-phase case.

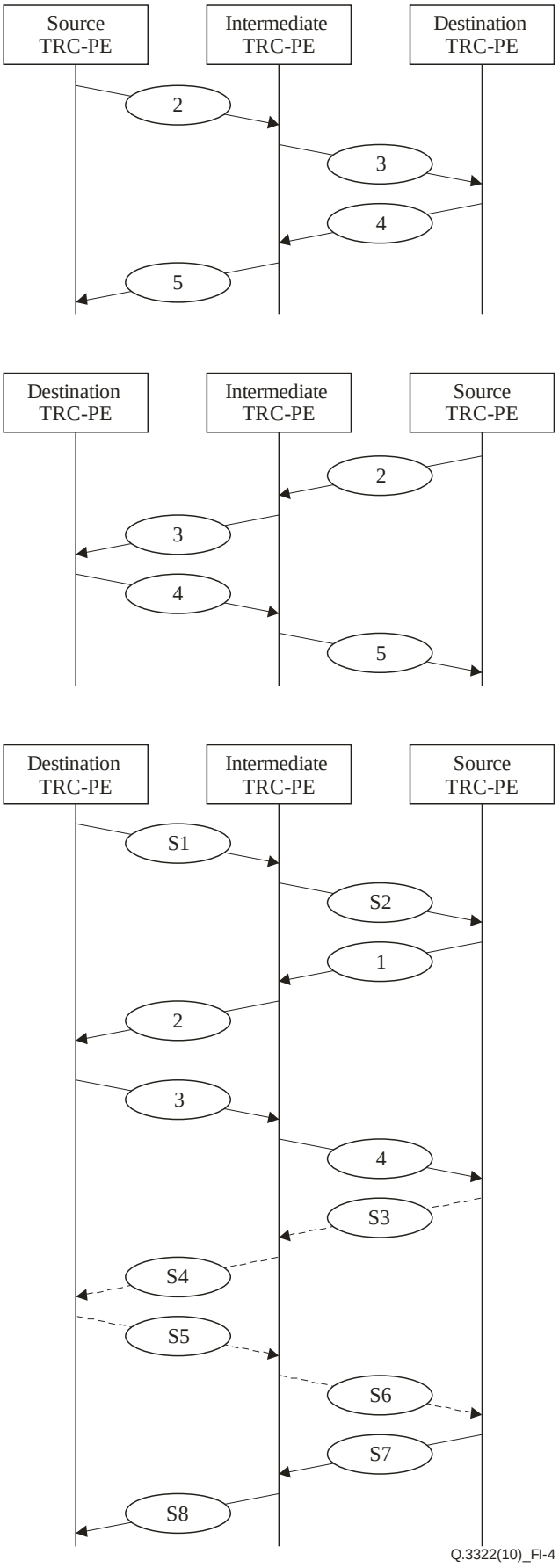


Figure I.4 – Separately-allocated forward-and-backward-resource information flows

Appendix II

Element components not supported in this Recommendation

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

– Reservation holding time (optional)
– Resource control session information (optional)
– Network class of service (optional)
– IP QoS handling class (optional)
– Event notification indication (request for) (optional).

Bibliography

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2012