International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3302.1

(03/2007)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

---

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

ITU-T Recommendation Q.3302.1

ITU-T

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.

ITU-T Recommendation Q.3302.1

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

Summary

ITU-T Recommendation Q.3302.1 specifies the resource connection initiation protocol for use in carrying resource control requests and responses between transport resource control physical entities within the same domain. This protocol is designed 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, 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 appropriate configuration of the transport physical entities by the transport resource control physical entities.

Source

ITU-T Recommendation Q.3302.1 was approved on 9 March 2007 by ITU-T Study Group 11 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, 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/.

CONTENTS

Page

ITU-T Recommendation Q.3302.1

Resource control protocol No. 2 – 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.Sup51].

The possible methods of configuration and notification between the transport physical entities (T-PE) and the transport resource control are out of scope of RCIP. RCIP only specifies the 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] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

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

[ITU-T Q.Sup51] ITU-T Q-series Supplement 51 (2004), *Signalling requirements for IP-QoS*.

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

[ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.

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: Bearer is 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): The BCF is 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 upstream TRC-PE: The entity which sends the resource request to a downstream TRC-PE.

3.2.4 destination TRC-PE

NOTE – The destination TRC-PE receives a resource request based on service, 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 a bidirectional one, 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 the response message of the resource path from the source to the destination to the previous hop TRC-PE.

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

3.2.6 flow information: The flow information is the information necessary to identify an IP data flow, as defined in clause 8.3.3.

3.2.7 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.

3.2.8 RCIP resource connection: An RCIP resource connection is 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.

3.2.9 RCIP transport channel: An RCIP transport channel is a signalling transport connection maintained between two TRC-PE peers, within which multiple RCIP resource connections can be multiplexed.

3.2.10 service control function: The SvCF (service control function) is a functional entity that provides value-added service functionality. (Derived from [ITU-T Q.Sup51])

3.2.11 session control function: The SeCF (session control function) is a functional entity that provides the call/session control functionality. (Derived from [ITU-T Q.Sup51])

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

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

3.2.13 transport physical entity: The T-PE (transport physical entity) is an entity that performs stream classification, switching and forwarding and is capable of enforcing a QoS guarantee. (Derived from [ITU-T Q.Sup51])

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACCT	Accept
AUP	RCIP AUdit resPonse
AUR	RCIP AUdit Request
BCF	Bearer Control Function
KA	Keep-Alive

MPLS	MultiProtocol Label Switching
OVE	OVErload indication
PD-PE	Policy Decision Physical Entity
RA	Resource Acceptance message
RACF	Resource Admission Control Functions
RCIP	Resource Connection Initiation Protocol
REJ	resource REJection message
RLP	Resource reLease resPonse message
RLR	Resource reLease Request message
RR	Resource Request message
SCE	Session/Service Control Entity
SF	Switching Function
T-PE	Transport Physical Entity
TRC-PE	Transport Resource Control Physical Entity

5 Protocol design principles

5.1 Introduction

[ITU-T Q.Sup51] describes the control information flows between BCFs as shown in Figure 5-1, and [ITU-T Y.2111] defines the Rp interface between TRC-FE instances within a domain as shown in Figures 5-1 and 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 SCEs and interior 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.

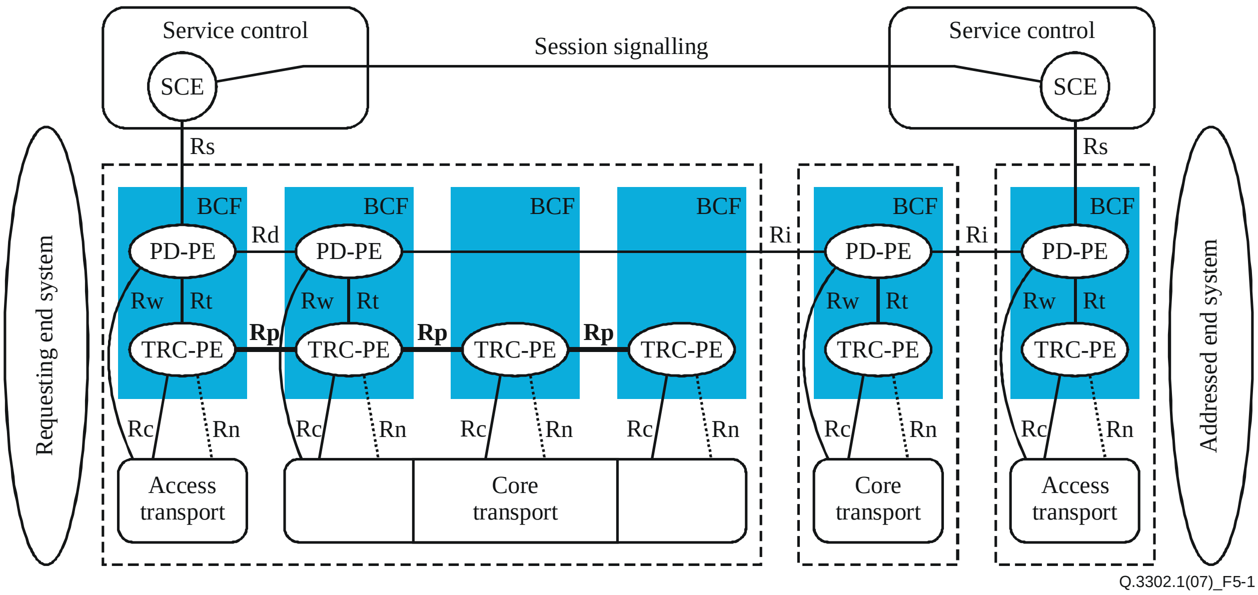


Figure 5-1 – Basic protocol architecture

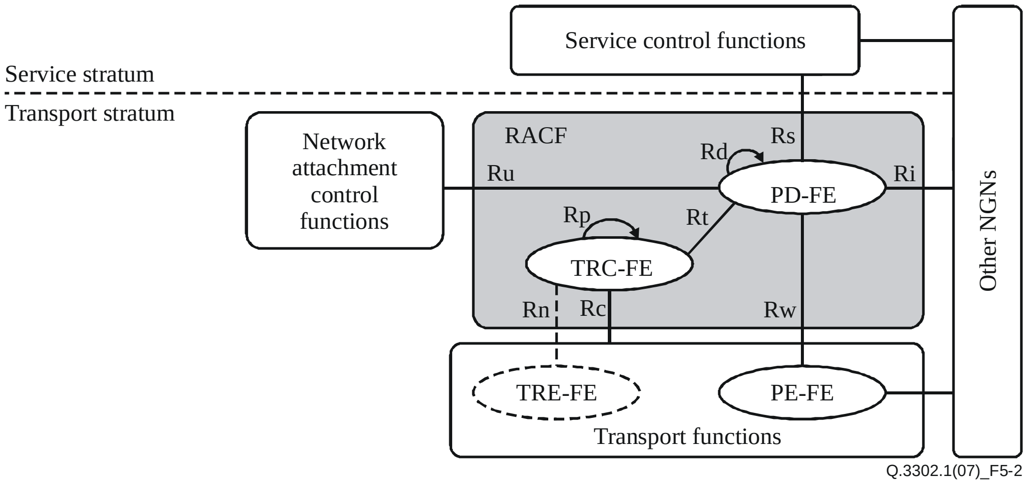


Figure 5-2 (Derived from Figure 5/Y.2111) – Generic resource and admission control functional architecture in NGN

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 are 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, a RCIP resource connection can reserve resource for a multimedia call which has an audio session and a video session.

Each RCIP resource connection message contains reservation information or control information related to a 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 to the destination TRC-PE pair.

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

5.2 Protocol overview

The RCIP protocol 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 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 scope of RCIP. RCIP only specifies the 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 it 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 due to 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. It is shown as below.

```
__________________________________________________________________________
          |    ---------------------------------------------------------
          |    Resource Connection 1: RR/ RA/ REJ/ RLR/ AUR/OVE…
          |    ---------------------------------------------------------
A single  |    Resource Connection 2: RR/ RA/ REJ/ RLR/ AUR/OVE…
RCIP      |    ---------------------------------------------------------
Transport      |    …
Connection     |    ---------------------------------------------------------
          |    Resource Connection n: RR/ RA/ REJ/ RLR/ AUR/OVE…
          |    ---------------------------------------------------------
__________________________________________________________________________
Transport Channel: OPEN/ ACCEPT/ CLOSE/ KA
__________________________________________________________________________
TCP/SCTP

__________________________________________________________________________
```

RCIP specifies the following message types and objects:

RCIP resource connection message types:

- 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 message types:

- OPEN;
- ACCT;
- CLOSE;
- Keep alive.

RCIP main objects:

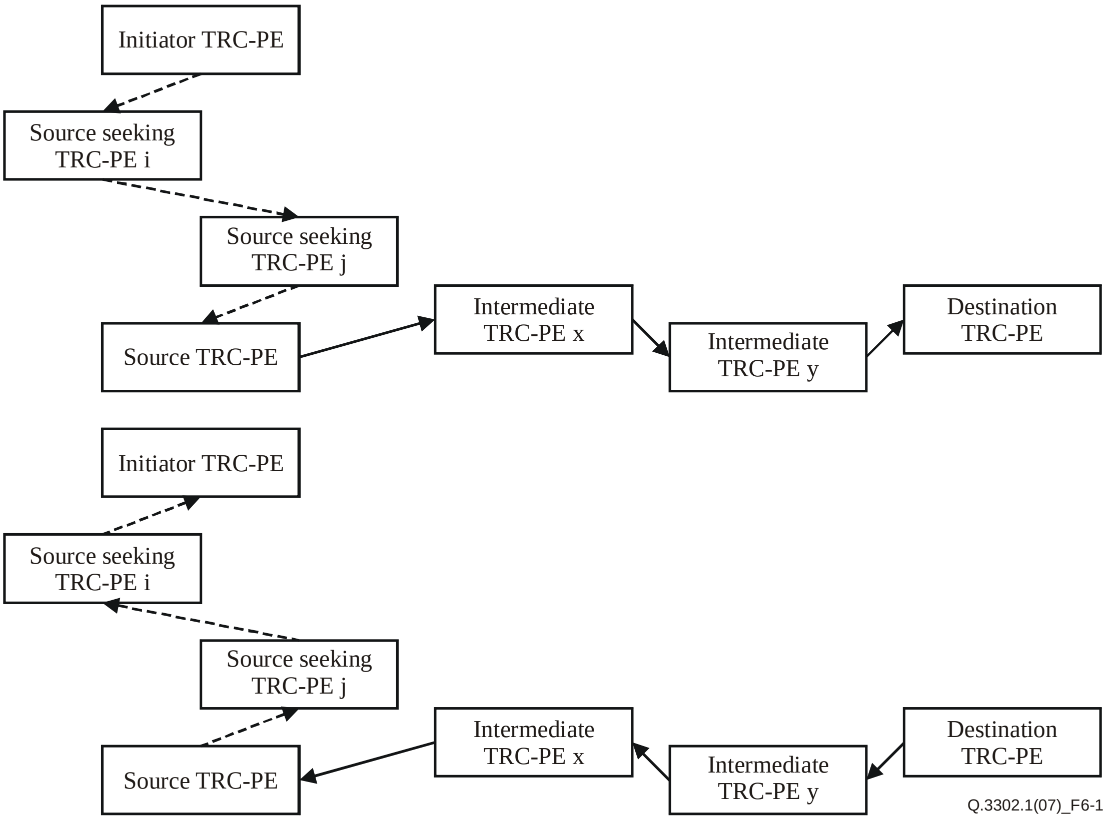
- Connection ID;
- Flow Information;
- Flow Traffic Information;
- LSP Connection Information;
- V-Switching Connection Information;
- Reason Code;
- Overload Indication;
- Result Indication;
- Data Consistency.

Each RCIP message includes header information which specifies the message type. Related to each message type, there are a number of mandatory and optional objects. See clause 7 for details.

6 Basic protocol operation

6.1 Roles of TRC-PE

The roles of TRC-PE [ITU-T Q.Sup51] are shown in Figure 6-1, which is only a sketch map. A TRC-PE can perform one or more of the roles at the same time.



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 which the source address of the service stream belongs to.
Source TRC-PE	The source TRC-PE receives a resource request based on service, sent by the SCE or the source-seeking TRC-PE from the previous hop. 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 service, 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 service, 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 a bidirectional one, 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 the response message of the resource path from the source to the destination to the previous hop TRC-PE.

Figure 6-1 – Roles of TRC-PE

6.2 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 resource 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 the source-seeking procedure (can be one hop or multi hops), the other is for TRC-PE routing for resource reservation procedure. In implementation, the two logic routing tables can be combined into one physical table.

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/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, it 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, the TRC-PE can determine to pre-empt and tear down the low priority resource connection.

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

6.3 MODIFY

Some services may need to modify the QoS requirements during the service operation. According to the upstream TRC-PE request, the present TRC-PE modifies the bandwidth, port, protocol type, and so on, except the addresses used for the previous application. Repetitive modifications are enabled.

Bandwidth modification falls under increment modification and decrement modification. Decrement modification is expected to be performed successfully in most cases, while increment modification may fail due to there being insufficient resources to meet the new requirement. When modification fails, one may recover the previous connection or release the service connection. But carrying on with this reservation may be quite difficult to implement.

RR (Resource Request) message with Modify Flag, Resource Acceptance message (RA) and Resource Rejection message (REJ) message are involved in this MODIFY operation.

6.4 AUDIT

In order to synchronize the TRC-PE(s) in the status of a QoS request, the AUDIT operation is defined. This mechanism is used 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 result audit response fails, the corresponding RCIP resource connection shall be released. TRC-PE releases resource locally, sends resource release to the upstream or downstream peer TRC-PE, not including the TRC-PE who sends the audit response.

The AUDIT message contains only one Connection ID Object, so as to allow the audited TRC-PE to feed back the information. AUR (Audit Request) and AUP (Audit Response) messages are involved in this AUDIT operation.

6.5 NOTIFY

The protocol must allow the notification of 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 handle in two ways: to release the call or not. If the call remains, the QoS will be interrupted for the call. OVE (Overload Indication) message is involved in this NOTIFY operation.

6.6 RELEASE

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

RLR (Resource release Request) message and Resource Release Response message (RLP) are involved in RELEASE operation.

6.7 TRC-PE source seeking

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

Source seeking is a process to find the source TRC-PE (e.g., IP address, digits from 0 and 9, URL) based on source address of the media flow which request to reserve resource.

There are two ways to complete the process.

One is in a piggyback way, in which the resolution function is integrated within the TRC-PE. The TRC-PE is called the source-seeking TRC-PE and act as the resource reservation request proxies. When a TRC-PE, which is called the 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 for transmitting the resource request to the source TRC-PE.

The other is an independent way, in which the resolution function is separate 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 way is out of the scope of this Recommendation.

RR (Resource Request) message is involved in this TRC-PE source-seeking operation.

7 Basic procedure

7.1 Resource connection establishment

In an IP network supporting MPLS and/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 to set the bandwidth and QoS attribute for each 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 a 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 message (RR) 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 according to 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 provisionally reserved, the request is passed on to the next TRC-PE towards the destination TRC-PE. The previously described procedure is performed in every TRC-PE. When the request has chain of TRC-PEs, from the destination TRC-PE on, the downstream TRC-PE feedbacks the result of resource admission control to upstream while at the same time it tells the result 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 message (RR), a TRC-PE creates a new Resource Request message (RR) 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 message (RR); a reply/reject message as acknowledgement is mandatory.

Some paragraphs and example message flow figures with unidirectional and bidirectional RCIP resource connection set-up are shown in Appendix I, which is derived from [ITU-T Q.Sup51].

7.2 Tear down a resource connection

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

– Decide if resource shall be released.
– If they are to be released, a RLR is sent to other TRC-PEs involved in the connection, release the actual resources in the node and a successful Resource Release Response message (RLP) is sent to the TRC-PE which sent the RLR.
– Otherwise, a RLR is sent to other TRC-PEs involved in the connection and a successful response is sent to the TRC-PE which sent the RLR.

7.3 Overload control

There might be situations where a given TRC-PE is overloaded due to high processing overloads. To ensure timely responses, and 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 the level at which throughput can be the maximal. 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 overload situation has ceased.

8 Protocol format

RCIP resource connection messages
RCIP transport channel messages
TCP/SCTP

This clause describes the message formats and objects exchanged between TRC-PE(s).

All fields in an RCIP packet MUST be transmitted in network byte order.

Each RCIP message consists of the RCIP header followed by a number of typed objects. For example, the connection Resource Request message (RR) from TRC-PE to TRC-PE consists of HEADER and Connection ID Object, Flow Profile Object.

8.1 Common HEADER

Each RCIP message consists of the RCIP header followed by a number of type-length-value (TLV) encoded objects.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Version |  Flags  |     Op Code       |        Client-type            |
|                        Message Length                                 |
```

The fields in the header are:

Version: 4 bits

RCIP version number. Current version is 1.

Flags: 4 bits

Defined flag values (if all other flags is set to 0):

| 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 towards 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 only used in Resource Release Request message (RLR). 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 manual reconfiguration.

Op Code: 8 bits

0-5: reserved

6 = Protocol Connection Establishment Open (OPEN)

7 = Protocol Connection Establishment Accept (ACCT)

8 = Protocol Connection Close (CLOSE)

9 = Keep Alive (KA)

10: reserved

11 = Resource Request message **(RR)**

12 = Resource Acceptance message **(RA)**

13 = Resource **Rej**ection message **(REJ)**

14 = Resource Release Request message **(RLR)**

15 = Resource Release Response message **(RLP)**

16 = Overload Indication message **(OVE)**

17 = Audit Request message **(AUR)**

18 = Audit Response message **(AUP)**

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 the 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

Size of message in octets, which includes the standard RCIP header and all encapsulated objects. Messages MUST be aligned on 4-octet boundaries.

If the length is not the integral times of 4 bytes, filling is needed.

In the above scheme, when sending to the network, version is sent first; when receiving from the network, version is received first.

8.2 RCIP message format

8.2.1 RCIP resource connection messages

8.2.1.1 Resource Request message (RR)

The Resource Request 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*{Flow Profile}
                   [Data Consistency Information]
```

In the Flow Profile Object, if the resource request is bidirectional, both Forward Flow Traffic Descriptor and Backward Flow Traffic Descriptor are carried; if the resource request is unidirectional, either Forward Flow Traffic Descriptor or Backward Flow Traffic Descriptor is carried. Flow Profile contains profile for a piece 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 only when Proxy flag is set to 0).

8.2.1.2 Resource Acceptance message (RA)

The Resource Acceptance 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, with a piece of success information.

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

In the Flow Profile Object, if the Resource Acceptance is bidirectional, both Forward Flow Traffic Descriptor and Backward Flow Traffic Descriptor are carried; if the Resource Acceptance is unidirectional, either Forward Flow Traffic Descriptor or Backward Flow Traffic Descriptor is carried.

8.2.1.3 Resource Rejection message (REJ)

The Resource Rejection 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]
```

8.2.1.4 Resource Release Request message (RLR)

The Resource Release Request 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; it 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]
```

8.2.1.5 Resource Release Response message (RLP)

The Resource Release Response 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 Resource Release Request 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]
```

8.2.1.6 Overload Indication message (OVE)

The Overload Indication 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]
```

8.2.1.7 Audit Request message (AUR)

The Audit Request 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]
```

8.2.1.8 Audit Response message (AUP)

The Audit Response 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]
```

8.2.2 RCIP transport channel messages

8.2.2.1 OPEN message (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]
```

8.2.2.2 ACCT message (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, RCIP transport channel is set up.

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

8.2.2.3 CLOSE message (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]
```

8.2.2.4 Keep Alive message (KA)

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

8.3 RCIP object formats

All the objects follow the same object format; each object consists of one or more 32-bit words with a four-octet object header, using the following format:

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Length (octets)																C-Num								C-Type							
Object contents																															

The length is a two-octet value that describes the number of octets (including the header) that compose 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 previous stated object length to the next 32-bit boundary.

Typically, C-Num identifies the class of information contained in the object, and the C-Type identifies the subtype or version of the information contained in the object.

C-num: 8 bits

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 = E.164 Number

16 = Resource State

17 = TRC-PE Sequence Object

C-type: 8 bits

Values defined per C-num.

8.3.1 Connection ID Object (ConnID)

The Connection ID Object is corresponding 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 the message is pertaining to the RCIP resource connection identified by the connection ID. When a TRC-PE sees a RCIP message containing such an object, it can create or find the corresponding connection ID internally, and does the corresponding process.

8.3.1.1 IPv4 Connection ID Object (IPv4ConnID)

C-Num = 1

C-Type = 1, IPv4 Connection ID.

Connection ID consists of two parts. One part is the 32-bit TRC-PE identification (ordinarily IPv4 address), the other part is the 32-bit sequence number allocated by the TRC-PE for the resource request.

Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Length = 12		C-Num = 1	C-Type = 1
32 bits IPv4 address of TRC-PE			
8 bits Reserved	24 bits Sequence Number		

8.3.1.2 IPv6 Connection ID Object (IPv6ConnID)

C-Num = 1

C-Type = 2, IPv6 Connection ID.

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.

Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
Length = 24		C-Num = 1	C-Type = 2
128 bits IPv6 address of TRC-PE			
8 bits Reserved	24 bits Sequence Number		

8.3.2 Flow ID Object (FlowID)

Flow ID Object is unique within one RCIP resource connection; value arranges 1 to biggest integer. 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 a RCIP message containing such an object, it can create or find the corresponding Flow ID within a RCIP resource connection, and does the corresponding process.

C-Num = 2

C-Type = 1, Flow ID.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Length = 8																C-Num = 2								C-Type = 1							
Flow ID																															

8.3.3 Flow Information Object (FlowInfo)

It is a sub-object of Flow Profile Object, carried in Resource Request and Acceptance. When a TRC-PE sees a RCIP message containing such an object, it can get the key information to identify an IP data stream, and does the corresponding process.

8.3.3.1 IPv4 Flow Information Object (IPv4FlowInfo)

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, 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 television conference. When the mask length is 0, it means a single IP address; the maximum 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 the 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.

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

– Enable (1)

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

– Enabled-forward (2)

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 (3)

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 (4)

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

– Remove (5)

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

<table>
<tr><td colspan="5">0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td></tr>
<tr><td colspan="2">Length = 24 + 4 * (m + n)</td><td>C-Num = 3</td><td colspan="2">C-Type = 1</td></tr>
<tr><td colspan="5">32 bits source IPv4 address</td></tr>
<tr><td colspan="5">32 bits destination IPv4 address</td></tr>
<tr><td colspan="2">source port count</td><td colspan="3">dest port count</td></tr>
<tr><td colspan="2">IPv4 source min port1</td><td colspan="3">IPv4 source max port1</td></tr>
<tr><td colspan="2">…</td><td colspan="3">…</td></tr>
<tr><td colspan="2">IPv4 source min portm</td><td colspan="3">IPv4 source max portm</td></tr>
<tr><td colspan="2">IPv4 dest min port1</td><td colspan="3">IPv4 dest max port1</td></tr>
<tr><td colspan="2">…</td><td colspan="3">…</td></tr>
<tr><td colspan="2">IPv4 dest min portn</td><td colspan="3">IPv4 dest max portn</td></tr>
<tr><td colspan="2">IPv4 source address mask length</td><td colspan="3">IPv4 dest address mask length</td></tr>
<tr><td>protocol type</td><td>media type</td><td>bandwidth request type</td><td>flow direction</td><td>flow status</td></tr>
</table>

8.3.3.2 IPv6 Flow Information Object (IPv6FlowInfo)

C-Num = 3

C-Type = 2, IPv6 Flow Information.

IPv6 flow information 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 maximum length of the mask is 64.

Bandwidth request type may be one of the 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.

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

– Enable (1)

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

– Enabled-forward (2)

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 (3)

  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 (4)

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

– Remove (5)

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

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Length = 44 + 4 * (m + n)		C-Num = 3	C-Type = 2	
128 bits source IPv6 address				
128 bits destination IPv6 address				
source port count		dest port count		
IPv6 source min port1		IPv6 source max port1		
…		…		
Ipv6 source min portn		IPv6 source max portn		
IPv6 dest min port1		IPv6 dest max port1		
…		…		
IPv6 dest min portn		IPv6 dest max portn		
IPv6 source address mask length		IPv6 dest address mask length		
protocol type	media type	bandwidth request type	flow direction	flow status

8.3.4 Flow Traffic Descriptor Object (FlwTrafDscr)

It is a sub-object of Flow Profile Object, carried in Resource Request and Acceptance. 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 does the corresponding process. It is allowed to use further version of RCIP to specify this object. Version number is in RCIP header.

8.3.4.1 Forward Flow Traffic Descriptor Object (FwdFlwTrafDscr)

C-Num = 4

C-Type = 1, Forward Flux Descriptor.

Forward Flow Traffic Descriptor includes forward bandwidth peak value, average bandwidth (32 bits, the maximum is 4 Gbit/s based on 1 bit/s), maximum packet length (16 bits, maximum value is 65535 bytes). Bandwidth unit is 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.

0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 (bits 0–15)	6 7 8 9 2 0 1 2 3 (bits 16–23)	4 5 6 7 8 9 3 0 1 (bits 24–31)
Length = 16	C-Num = 4	C-Type = 1
32 bits bandwidth peak value		
32 bits average bandwidth		
32 bits minimum bandwidth		
16 bits max packet length	Bandwidth unit	Priority

8.3.4.2 Backward Flow Traffic Descriptor Object (BwdFlwTrafDscr)

C-Num = 4

C-Type = 2, Backward Flow Traffic Descriptor.

Backward Flow Traffic Descriptor includes backward bandwidth peak value, average bandwidth (32 bits, the maximum is 4 Gbit/s based on 1 bit/s), maximum packet length (16 bits, maximum value is 65535 bytes). Bandwidth unit is bit/s (1), kbit/s (2), and Mbit/s (3).

0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 (bits 0–15)	6 7 8 9 2 0 1 2 3 (bits 16–23)	4 5 6 7 8 9 3 0 1 (bits 24–31)
Length = 16	C-Num = 4	C-Type = 2
32 bits bandwidth peak value		
32 bits average bandwidth		
32 bits minimum bandwidth		
16 bits max packet length	Bandwidth unit	Priority

8.3.5 LSP Connection Information Object (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. It is a sub-object of Flow Profile Object, carried in Resource Request and Acceptance.

8.3.5.1 IPv4 Forward LSP Connection Information Object (IPv4FwdLSPconn)

C-Num = 5

C-Type = 1, IPv4 Forward LSP Connection Information.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Length = 20 + 4 * n	C-Num = 5	C-Type = 1
32 bits IPv4 address of initiative T-PE for forward inter-domain		
32 bits forward inter-domain LSP label		
32 bits IPv4 address of source T-PE		
16 bits forward label depth	16 bits forward PMTU	
LSP1 initiative label (Ingress push label)		
…		
LSPi initiative label (Ingress push label)		
…		
LSPn initiative label (Ingress push label) (n ≤ 16)		

8.3.5.2 IPv4 Backward LSP Connection Information Object (IPv4BwdLSPconn)

C-Num = 5

C-Type = 2, IPv4 Backward LSP Connection Information.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Length = 20 + 4 * n	C-Num = 5	C-Type = 2
32 bits IPv4 address of initiative T-PE for forward inter-domain		
32 bits forward inter-domain LSP label		
32 bits IPv4 address of source T-PE		
16 bits backward label depth	16 bits backward PMTU	
LSP1 initiative label (Ingress push label)		
…		
LSPi initiative label (Ingress push label)		
…		
LSPn initiative label (Ingress push label) (n ≤ 16)		

8.3.5.3 IPv6 Forward LSP Connection Information Object (IPv6FwdLSPconn)

C-Num = 5

C-Type = 3, IPv6 Forward LSP Connection Information.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

Length = 44 + 4 * n	C-Num = 5	C-Type = 3
128 bits IPv6 address of initiative T-PE for forward inter-domain		
32 bits forward inter-domain LSP label		
128 bits IPv6 address of source T-PE		
16 bits forward label depth	16 bits forward PMTU	
LSP1 initiative label (Ingress push label)		
…		
LSPi initiative label (Ingress push label)		
…		
LSPn initiative label (Ingress push label) (n ≤ 16)		

8.3.5.4 IPv6 Backward LSP Connection Information Object (IPv6BwdLSPconn)

C-Num = 5

C-Type = 4, IPv6 Backward LSP Connection Information.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

Length = 44 + 4 * n	C-Num = 5	C-Type = 4
128 bits IPv6 address of initiative T-PE for forward inter-domain		
32 bits forward inter-domain LSP label		
128 bits IPv6 address of source T-PE		
16 bits backward label depth	16 bits backward PMTU	
LSP1 initiative label (Ingress push label)		
…		
LSPi initiative label (Ingress push label)		
…		
LSPn initiative label (Ingress push label) (n ≤ 16)		

8.3.6 Authentication Information Object (AuthInfo)

C-Num = 6

C-Type = 1, Authentication Information.

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

0 – 15	16 – 23	24 – 31
Length = 4 + length of username length of password + padding	C-Num = 6	C-Type = 1
Username (length ≤ 32 byte)		
Password (length ≤ 32 byte)		

8.3.7 Reason Code Object (ReasonCode)

This object specifies the reason why the request state was deleted. It appears in the Resource Release Request message (RLR).

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

C-Num = 7

C-Type = 1.

0 – 15	16 – 23	24 – 31
Length = 8	C-Num = 7	C-Type = 1
Reason Code	Reason Sub-code	

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

8.3.8 Identity Identification Object (IdentityIdentification)

C-Num = 8, C-Type = 1

Only identity identification adopts the T.50 International Alphabet No. 5 string format; in a general way it is the static IP address of TRC-PE. When the TRC-PE adopts dynamic IP address, identity identification can use DNS domain name. It is used in OPEN message. TRC-PE should do validity check including domain name, identifier and address.

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 4 + length of identification + padding		C-Num = 8	C-Type = 1
TRC-PE identification			

8.3.9 Keep-Alive Timer Object (KATimer)

Times are encoded as 2-octet integer values and are in units of seconds. The timer value is treated as a delta.

C-Num = 9

C-Type = 1, Keep-alive timer value

Keep-Alive Timer object is used to specify the maximum time interval over which a RCIP transport channel message MUST be sent or received. The unit is in seconds. It is used in ACCT messages. The TRC-PE compares the KA Timer value which the ACCT message carries with local KA Timer value and selects the smaller value as the KA Timer value between them. If the TRC-PE does not accept the KA Timer value, CLOSE message is sent to disconnect. The range of finite timeouts is 1 to 65535 seconds represented as an unsigned two-octet integer.

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

Scope of KA Timer values: 0 to 65535

Default: 45 seconds

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

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

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 8		C-Num = 9	C-Type = 1
Reserved		KA Timer value	

8.3.10 Data Consistency Object (DataConsistency)

In order to ensure message integrity, TRC-PEs adopt the HMAC technology computing the message digests to be appended at the end of a RCIP message, use the shared key and cryptographic algorithm to verify the consistency, supporting HMAC-MD5-96.

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.

C-Num = 10

C-Type = 1, HMAC digest.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

Length = 28	C-Num = 10	C-Type = 1
Key ID		
Sequence Number		
Keyed Message Digest		

8.3.11 V-switching Connection Information Object (VSConnInfo)

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

C-Num = 11

C-Type = 1, V-switching Connection Information.

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

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

Length = 48	C-Num = 11	C-Type = 1
In VSWITCH IP Address (32 bits)		
In Interface Information (4 * 32 bits)		
In Vlan Id (16 bits)	Out Vlan Id (16 bits)	
In Inner Vlan Id (16 bits)	Out Inner Vlan Id (16 bits)	
Out VSWITCH IP Address (32 bits)		
Out Interface Information (4 * 32 bits)		

8.3.12 Overload Indication Object (Overload-Indication)

Overload Indication Object indicates whether overload happens, carried in Overload Indication message.

C-Num = 12

C-Type = 1, Overload Indication.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

Length = 8	C-Num = 12	C-Type = 1
Overload State	Reserved (24 bits)	

Overload State:

0 – Overload recovered (no overload)

1 – Overload happened

8.3.13 Flow Profile Object (FlowProfile)

Flow Profile Object is carried in Resource Request and Response. It can appear one or more times in a Resource Request or Response.

8.3.13.1 Flow Profile for MPLS caseObject (FlowPro4MPLS)

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).

8.3.13.2 Flow Profile for V-Switching case Object (FlowPro4V-Switching)

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).

8.3.14 Result Indication Object (ResultIdentification)

It is needed to indicate the result of success/failure in the audit message.

C-Num = 14

C-Type = 1, Result Indication.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Length = 8		C-Num = 14	C-Type = 1
Result (8 bits)	Reserved (24 bits)		

Result:

0 – Success

1 – Non-success

8.3.15 Digits String Object (DigitsString)

DigitsString is a sub-object of V-Switching Logical Path Information Object, carried in the Resource Request and Response.

C-Num = 15

C-Type = 1

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Object_Length		C-Num = 15	C-Type = 1
src_code_leng	source_code		
source_code			
dst_code_leng	destination_code		
destination_code			
protocol_type	media_type	bandwidth_type	con_direction

object_length: object length

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: amount 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

8.3.16 Resource State Object (RrcState)

8.3.16.1 Connection Resource State Object (ConnRrcState)

C-Num = 16

C-Type = 1, Connection Resource State.

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).

0 1 2 3 4 5 6	7 8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 8		C-Num = 16	C-Type = 1
State Code	Padding		

8.3.16.2 Node State Object (NodeState)

C-Num = 16

C-Type = 2, Node State.

The node state denotes the following.

0 = disabled

1 = enabled

2 = overload

3 = holding

FF = inexistence

0 1 2 3 4 5 6	7 8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 12		C-Num = 16	C-Type = 2
Node IP Address (32 bits)			
State	Reserved (24 bits)		

8.3.16.3 LSP Resource State Object (LspRrcState)

C-Num = 16

C-Type = 3, LSP Resource State.

The LSP Resource State denotes the following.

0 = disabled

1 = enabled

FF = inexistence

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 16		C-Num = 16	C-Type = 3
Ingress Identifier (32 bits)			
LSP Label (32 bits)			
State	Reserved (24 bits)		

8.3.16.4 Interface State Object (IntState)

C-Num = 16

C-Type = 4, Interface State.

The Interface State denotes the following.

0 = disabled

1 = enabled

FF = inexistence

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 28		C-Num = 16	C-Type = 4
Data Relay entity IP Address (32 bits)			
Interface Information (4 * 32 bits)			
State	Reserved (24 bits)		

8.3.17 TRC-PE Sequence Object (TRC-PESequence)

8.3.17.1 IPv4 TRC-PE Sequence Object (IPv4TRC-PESequence)

C-Num = 17

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

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3	4 5 6 7 8 9 0 1
Length = 8 + 4 * n		C-Num = 17	C-Type = 1
32 bits Proxy Flag			
32 bits initiator TRC-PE IPv4 address (TRC-PE1)			
…			
32 bits TRC-PEi IPv4 address			
…			
32 bits TRC-PEn IPv4 address (n ≤ 32)			

8.3.17.2 IPv6 TRC-PE Sequence Object (IPv6TRC-PESequence)

C-Num = 17

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

Bits 0–15	Bits 16–23	Bits 24–31
Length = 8 + 16 * n	C-Num = 17	C-Type = 2
128 bits Proxy Flag		
128 bits initiator TRC-PE IPv6 address (TRC-PE1)		
…		
128 bits TRC-PEi IPv6 address		
…		
128 bits TRC-PEn IPv6 address (n ≤ 32)		

9 Performance considerations

9.1 Performance requirements

Performance requirements must consider processing delays to meet the requirements for the entire call delays. So RCIP needs to establish, maintain and clear the QoS request messages whose quantity should be kept at the minimum. At the same time, the signalling message form being chosen should achieve the minimum message handling delay.

10 Other issues

10.1 Integrity

In order to prevent the messages from being illegally changed or attacked during the transmission, the HMAC 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 to verify the integrity. The HMAC technology supports HMAC-MD5-96. The data integrity message is composed of 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 attack.

10.2 Security

To establish a semi-permanent connection between the two opposites ends of the RCIP, the client side needs to verify it 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.

The RCIP protocol provides a Data Consistency object that can achieve authentication, message integrity, and replay prevention. All RCIP implementations MUST support the RCIP Data Consistency object and its mechanisms as described in this Recommendation. To ensure 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 minimally requires 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 a 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 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 will not 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 SHOULD be chosen such that they are monotonically increasing and never repeat 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) SHOULD 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.

10.3 Protocol transport and maintenance

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 resource messages. The protocol connection maintains the status through the heartbeat mechanism. The RCIP protocol connection should be persistent, once the connection is down due to any reason, the connection should be re-established automatically.

10.4 Connection ID

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

Connection ID is used for specifying a connection. It can ensure the correction operation on the connections with the same connection ID. When the system needs service requirements such as signalling tracing, statistics charging, the connection ID plays a role of identifying.

Annex A

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

(This annex forms an integral part of this Recommendation)

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

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

Appendix I

An example message flow

(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 which the initiator TRC-PE takes charge of. 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.

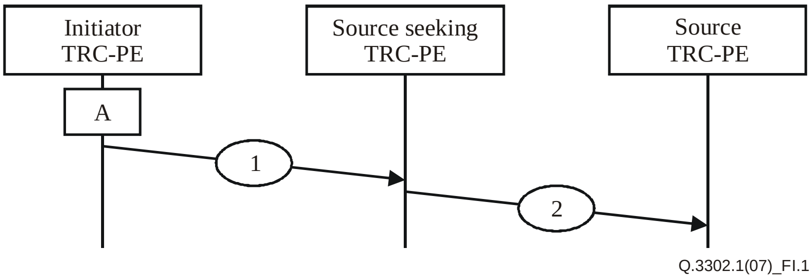


Figure I.1 – TRC-PE source addressing information flows

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

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 which the initiator TRC-PE takes charge of. 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

User information	Connection information
IP Streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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 which the source-seeking TRC-PE takes charge of. 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

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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 which the TRC-PE takes charge of. 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 between them is the existence of a provisional response from TRC-PE to SCE, by which the TRC-PE notifies to 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".

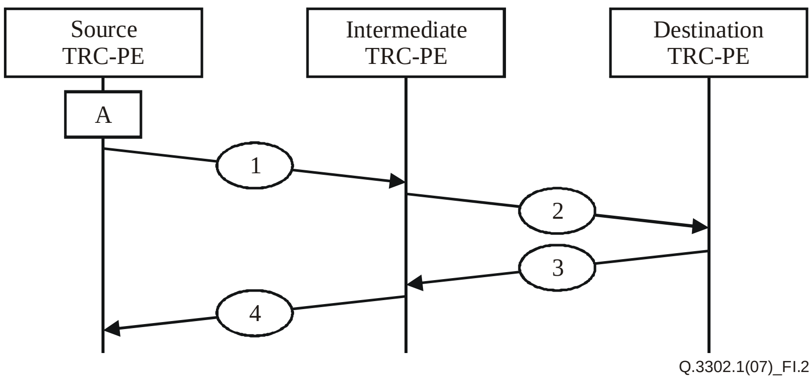


Figure I.2 – Forward unidirectional QoS path establishment information flows

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

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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

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

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 the 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 in the case that the transport plane has a capability to perform the explicit routing for reducing the time of the signalling procedures (see I.3.1); the other is to use two unidirectional information flows (see 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 for both 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 for both directions is also 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 party 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 in Figure I.3 are used only in the 2-phase case.

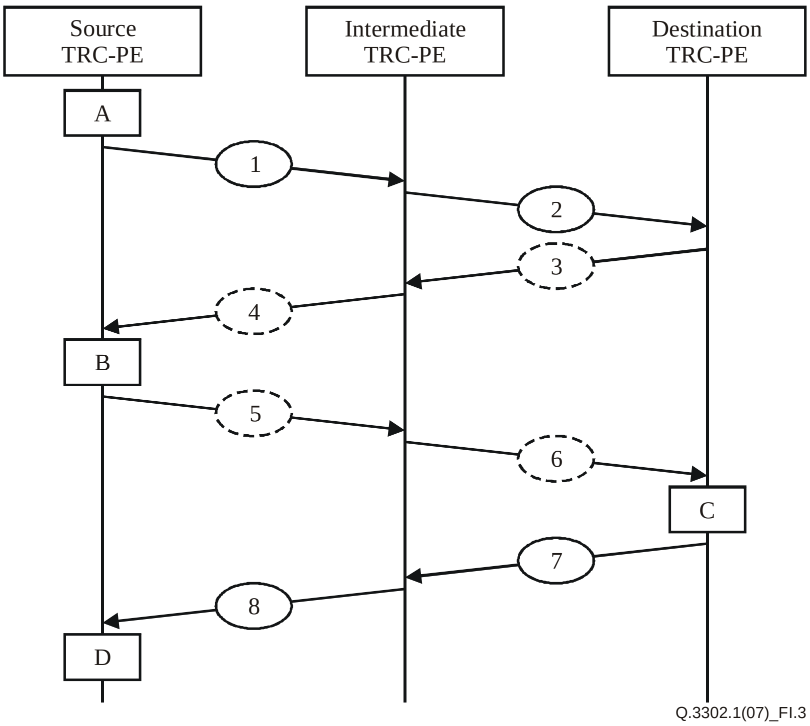


Figure I.3 – Bidirectional QoS path establishment information flows with unified-allocated signalling path

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

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

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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)

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)

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 an information flow to SCE.

B

In 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)

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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)

User information	Connection information
IP streams description information Service type (optional) Gating information	Connection ID Stream information (a set of one or more Address, 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.

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

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

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)

D

The source TRC-PE issues an information flow to control the stream QoS configuration information of the source T-PE. For the case where there is no need to wait for the whole path information and quick process, 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 an information flow to SCE.

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

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

In the case of one of the calling and called parties' SCE taking part in the procedure, this is performed with two parallel unidirectional information flows described in clause I.2 except the following points:

– The TRC-PE receiving an 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.

– For performing resource control in the direction where the initiator TRC-PE is not the source TRC-PE, the flows seeking the source TRC-PE (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.

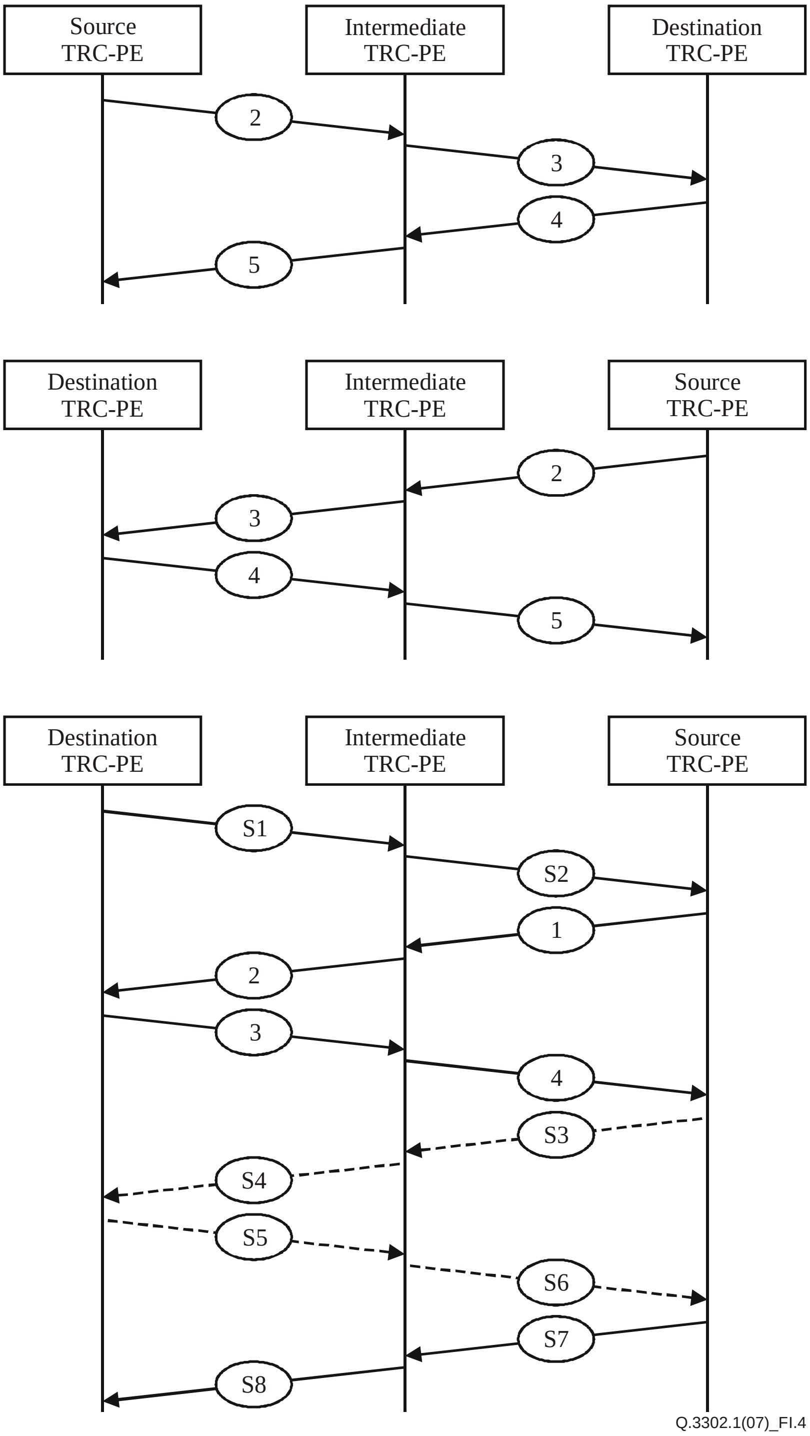


Figure I.4 – Separately allocated forward-and-backward-resource information flows

Appendix II

Element components not supported in RCIP v1

(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).

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	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, 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, 2008