International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3304.2

(08/2012)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity and a transport physical entity: SNMP alternative

Recommendation ITU-T Q.3304.2

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 next generation networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3304.2

Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity and a transport physical entity: SNMP alternative

Summary

Recommendation ITU-T Q.3304.2 specifies the profile of a variant of the resource control protocol No. 4 (rcp4) that uses the simple network management protocol (SNMP) at the Rc interface, i.e., between the transport resource control physical entity (TRC-PE) and the transport physical entity (T-PE) in the resource and admission control functional block. This protocol operates across the Rc reference point, as defined in Recommendation ITU-T Y.2111. The interface is used for checking the network topology and resource status information of an access or a core network.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3304.2	2007-10-29	11
2.0	ITU-T Q.3304.2 v2	2012-08-13	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/.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Q.3304.2

Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity and a transport physical entity: SNMP alternative

1 Scope

This Recommendation provides the Stage 3 technical specifications for a protocol variant which uses the simple network management protocol (SNMP) to satisfy the requirements for information transfer across the Rc reference point, as defined in clause 8.3 of [ITU-T Y.2111]. This protocol allows the transport resource control physical entity (TRC-PE) to collect network topology and resource status information from elements of an access or a core 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 Q.3300 v2] Recommendation ITU-T Q.3300 v2 (2010), *Architectural framework for the Q.33xx series of Recommendations*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

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

[IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 transport physical entity (T-PE) [ITU-T Q.3300]: A term used to refer to any device implementing the transport functions in the limited sense provided in clause 7.2.4 of [ITU-T Y.2111] (i.e., those with which the RACF interacts).

3.1.2 transport resource control physical entity (TRC-PE) [ITU-T Q.3300]: A device that implements the transport resource control functional entity (TRC-FE) as defined in clause 7.2.3.3 of [ITU-T Y.2111].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DoS Denial of Service

MIB Management Information Base

NACE Network Attachment Control Entity

OID Object ID

PD-PE Policy Decision Physical Entity

PE-PE Policy Enforcement Physical Entity

SCE Service Control Entity

SNMP Simple Network Management Protocol

T-PE Transport Physical Entity

TRC-PE Transport Resource Control Physical Entity

TRE-PE Transport Resource Enforcement Physical Entity

5 Conventions

None.

6 Rc interface

The Rc interface allows a transport resource control physical entity (TRC-PE) to collect network topology and resource status information about an access or a core network. The Rc interface is relevant to a transport physical entity (T-PE) at the network boundary or inside the network.

6.1 Rc reference model

The Rc interface, as shown in Figure 6-1, is defined between the TRC-PE and T-PE.

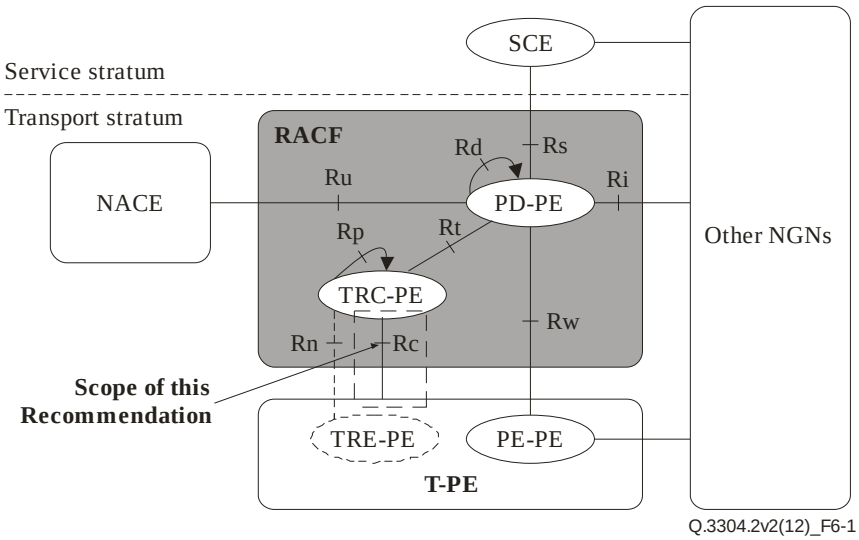

Figure 6-1 – Rc reference model

7 Protocol specification

SNMPv2 [IETF RFC 3416] shall apply to the Rc interface, where the TRC-PE acts as an SNMP manager and the transport elements are SNMP agents. The TRC-PE issues the SNMP-get (resource query message) to the T-PE and collects the resource information by retrieving interface information. If a change has occurred in the operational status or administrative status at the interfaces of the T-PE, the change is reported by the SNMP-trap (resource state report message) issued by the T-PE, and the TRC-PE then updates its resource information.

8 Protocols and messages

8.1 Resource query message

The TRC-PE collects interface information by issuing the SNMP-get to transport elements, as shown in [IETF RFC 3416]. The interface information to be retrieved corresponds to the object IDs (OIDs) under OID:1.3.6.1.2.1. The management information bases (MIBs) and OIDs associated with SNMP-get are shown in Appendix I.

8.2 Resource state report message

The change in the operational status at the interfaces of the transport element is reported to the TRC-PE by the SNMP-trap [IETF RFC 3416]. The generic SNMP-trap can be used for resource state report messages. SNMP-traps with generic trap Type 2 (linkDown) and generic trap Type 3 (linkUp) are utilized. The OIDs associated with the SNMP-trap are shown in Appendix I.

9 Security considerations

There might be several possible security threats at the Rc interface, such as denial of service (DoS), message disclosure by unauthorized snooping, and unauthorized message creation and modification.

In general, an attacker can surreptitiously intercept information, attempt to create unauthorized information, and/or send modified or reordered information. There might be a risk that an attacker can impersonate an SNMP manager and illicitly acquire and tamper with the information. Even though the information is encrypted, a reply attack might be possible.

For these security threats, operators need to be aware that no sufficient authentication and encryption mechanisms are provided between the SNMP manager (TRC-PE) and SNMP agents (T-PE) in the SNMP version 2 framework. To minimize the risk, the SNMP entity needs to be properly configured so that only authorized SNMP managers and agents can access information and exchange it with each other. Particular attention to the credence and information integrity is necessary.

Therefore, it is recommended that the implementers consider security features, such as authentication and encryption mechanisms, at the application level in the case where SNMP messages are open to an insecure domain in order to prevent possibilities of attacks from such a domain. At the same time, operators need to consider physical and/or logical SNMP traffic separation, packet filtering from an unauthorized SNMP manager (TRC-PE) and SNMP agents (T-PE). Operators should note that a long-term solution would be to consider implementing the SNMP version 3 framework and its security control model described in [b-IETF RFC 3414] and [b-IETF RFC 3415]. However, that is outside of the scope of this Recommendation.

Appendix I

Management information base

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

The following Tables I.1, I.2 and I.3 shows the management information base (MIB) referenced respectively in [b-IETF RFC 1213], [b-IETF RFC 4293] and [b-IETF RFC 2863].

Table I.1 – Management information base [b-IETF RFC 1213]

RFC	MIB object	Type	Object identifier
1213	mib-2		1.3.6.1.2.1
	System		1.3.6.1.2.1.1
	sysDescr	SCALAR	1.3.6.1.2.1.1.1
	sysObjectID	SCALAR	1.3.6.1.2.1.1.2
	sysName	SCALAR	1.3.6.1.2.1.1.5
	Interface		1.3.6.1.2.1.2
	ifTable	TABLE	1.3.6.1.2.1.2.2
	ifEntry	ENTRY	1.3.6.1.2.1.2.2.1
	ifIndex	TABULAR	1.3.6.1.2.1.2.2.1.1
	ifDescr	TABULAR	1.3.6.1.2.1.2.2.1.2
	ifType	TABULAR	1.3.6.1.2.1.2.2.1.3
	ifSpeed	TABULAR	1.3.6.1.2.1.2.2.1.5
	ifPhysAddress	TABULAR	1.3.6.1.2.1.2.2.1.6
	ifAdminStatus	TABULAR	1.3.6.1.2.1.2.2.1.7
	ifOperStatus	TABULAR	1.3.6.1.2.1.2.2.1.8

Table I.2 – Management information base [b-IETF RFC 4293]

RFC	MIB object	Type	Object identifier
4293	mib-2		1.3.6.1.2.1
	Ip		1.3.6.1.2.1.4
	ipv6IpForwarding	SCALAR	1.3.6.1.2.1.4.25
	ipAddressTable	TABLE	1.3.6.1.2.1.4.34
	ipAddressEntry	ENTRY	1.3.6.1.2.1.4.34.1
	ipAddressAddrType	TABULAR	1.3.6.1.2.1.4.34.1.1
	ipAddressAddr	TABULAR	1.3.6.1.2.1.4.34.1.2
	ipAddressIfIndex	TABULAR	1.3.6.1.2.1.4.34.1.3
	ipAddressPrefix	TABULAR	1.3.6.1.2.1.4.34.1.5

Table I.3 – Management information base [b-IETF RFC 2863]

RFC	MIB object	Type	Object identifier
2863	mib-2		1.3.6.1.2.1
	ifMIBObjects		1.3.6.1.2.1.31.1
	ifIXTable	TABLE	1.3.6.1.2.1.31.1.1
	ifIXEntry	ENTRY	1.3.6.1.2.1.31.1.1.1
	ifName	TABULAR	1.3.6.1.2.1.31.1.1.1.1
	ifHighSpeed	TABULAR	1.3.6.1.2.1.31.1.1.1.15
	ifStackTable	TABLE	1.3.6.1.2.1.31.1.2
	ifStackEntry	ENTRY	1.3.6.1.2.1.31.1.2.1
	ifStackStatus	TABULAR	1.3.6.1.2.1.31.1.2.1.3

Bibliography

[b-IETF RFC 1213] IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

[b-IETF RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB*.

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 4293] IETF RFC 4293 (2006), *Management Information Base for the Internet Protocol (IP)*.

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, 2013