

3GPP2 C.S0038-B

Version 1.0

Version Date: 30 March 2009



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Signaling Conformance Specification for High Rate Packet Data Air Interface

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Copyright © 2009 3GPP2.

No Text.

CONTENTS

1		
2	FOREWORD.....	xi
3	SCOPE.....	xiii
4	REFERENCES.....	xv
5	1 Overview	1-1
6	1.1 Objectives.....	1-1
7	1.2 Requirements Language	1-1
8	1.3 Document Organization	1-1
9	1.4 Abbreviations, Acronyms and Terms	1-2
10	1.5 Notation.....	1-6
11	2 Default Signaling Application Tests.....	2-1
12	2.1 Default Signaling Link Protocol Tests	2-1
13	2.1.1 Access Network Tests.....	2-1
14	2.1.2 Access Terminal Tests	2-4
15	3 Default Packet Application Tests	3-1
16	3.1 Radio Link Protocol Tests	3-1
17	3.1.1 Access Network RLP Tests	3-1
18	3.1.2 Access Terminal RLP Tests.....	3-5
19	3.2 Location Update Protocol Tests.....	3-10
20	3.2.1 Access Network Tests.....	3-10
21	3.2.2 Access Terminal Tests	3-10
22	3.3 Flow Control Protocol Tests.....	3-11
23	3.3.1 Access Network Tests.....	3-11
24	3.3.2 Access Terminal Tests	3-12
25	4 Multi-flow Application Protocol Tests	4-1
26	4.1 Radio Link Protocol Tests	4-1
27	4.1.1 Access Network RLP Tests	4-1
28	4.1.2 Access Terminal RLP Tests.....	4-5
29	4.2 Data Over Signaling Protocol Tests.....	4-11
30	4.2.1 Access Network Tests.....	4-11
31	4.2.2 Access Terminal Tests	4-14

1	4.3 Location Update Protocol Tests.....	4-16
2	4.3.1 Access Network Tests.....	4-17
3	4.3.2 Access Terminal Tests	4-17
4	4.4 Flow Control Protocol Tests.....	4-19
5	4.4.1 Access Network Tests.....	4-19
6	4.4.2 Access Terminal Tests	4-20
7	5 Stream Layer Protocol Tests	5-1
8	5.1 Default Stream Protocol Tests.....	5-1
9	5.1.1 Access Network Tests.....	5-1
10	5.1.2 Access Terminal Tests	5-1
11	6 Session Layer Tests	6-1
12	6.1 Default Session Management Protocol Tests	6-1
13	6.1.1 Access Network Tests.....	6-1
14	6.1.2 Access Terminal Tests	6-4
15	6.2 Default Address Management Protocol Tests	6-5
16	6.2.1 Access Network Tests.....	6-5
17	6.2.2 Access Terminal Tests	6-7
18	6.3 Default Session Configuration Protocol Tests	6-14
19	6.3.1 Access Network Tests.....	6-14
20	6.3.2 Access Terminal Tests	6-15
21	7 Connection Layer Tests	7-1
22	7.1 Default Air-Link Management Protocol Tests	7-1
23	7.1.1 Access Network Tests.....	7-1
24	7.1.2 Access Terminal Tests	7-3
25	7.2 Default Initialization State Protocol Tests.....	7-4
26	7.2.1 Access Network Tests.....	7-4
27	7.2.2 Access Terminal Tests	7-5
28	7.3 Default Idle State Protocol Tests	7-7
29	7.3.1 Access Network Tests.....	7-7
30	7.3.2 Access Terminal Tests	7-8
31	7.4 Enhanced Idle State Protocol Tests	7-11
32	7.4.1 Access Network Tests.....	7-11

1	7.4.2 Access Terminal Tests	7-13
2	7.5 Default Connected State Protocol Tests.....	7-16
3	7.5.1 Access Network Tests.....	7-16
4	7.5.2 Access Terminal Tests	7-17
5	7.6 Default Route Update Protocol Tests	7-18
6	7.6.1 Access Network Tests.....	7-18
7	7.6.2 Access Terminal Tests	7-19
8	7.7 MC Route Update Protocol Tests.....	7-22
9	7.7.1 Access Network Tests.....	7-22
10	7.7.2 Access Terminal Tests	7-23
11	7.8 Overhead Messages Protocol Tests	7-29
12	7.8.1 Access Network Tests.....	7-29
13	7.8.2 Access Terminal Tests	7-31
14	8 Security Layer Tests	8-1
15	8.1 DH Key Exchange Protocol Tests	8-1
16	8.1.1 Access Network Test	8-1
17	8.1.2 Access Terminal Test.....	8-2
18	8.2 SHA-1 Authentication Protocol Tests.....	8-4
19	8.2.1 Access Network Test	8-4
20	8.2.2 Access Terminal Test.....	8-5
21	8.3 Security Protocol Tests	8-6
22	8.3.1 Access Network Test	8-6
23	8.3.2 Access Terminal Test.....	8-7
24	9 Mac Layer Tests.....	9-1
25	9.1 Default Control Channel MAC Protocol Tests.....	9-1
26	9.1.1 Access Network Test	9-1
27	9.1.2 Access Terminal Test.....	9-2
28	9.2 Enhanced Control Channel MAC Protocol Tests.....	9-3
29	9.2.1 Access Network Test	9-3
30	9.2.2 Access Terminal Test.....	9-6
31	9.3 Default Access Channel MAC Protocol Tests.....	9-6
32	9.3.1 Access Network Tests.....	9-6

1	9.3.2 Access Terminal Tests	9-7
2	9.4 Enhanced Access Channel MAC Protocol Tests	9-8
3	9.4.1 Access Network Tests.....	9-8
4	9.4.2 Access Terminal Tests	9-9
5	9.5 Default Forward Traffic Channel MAC Protocol Tests	9-10
6	9.5.1 Access Network Tests.....	9-10
7	9.5.2 Access Terminal Tests	9-12
8	9.6 Enhanced Forward Traffic Channel MAC Protocol Tests	9-13
9	9.6.1 Access Network Tests.....	9-13
10	9.6.2 Access Terminal Tests	9-14
11	9.7 Default Reverse Traffic Channel MAC Protocol Tests	9-16
12	9.7.1 Access Network Tests.....	9-16
13	9.7.2 Access Terminal Tests	9-17
14	9.8 Subtype 3 Reverse Traffic Channel MAC Protocol	9-18
15	9.8.1 Access Network Tests.....	9-18
16	9.8.2 Access terminal Tests.....	9-18
17	9.9 MultiCarrier Reverse Traffic Channel MAC Protocol	9-41
18	9.9.1 Access Network Tests.....	9-41
19	9.9.2 Access terminal Tests.....	9-41
20	10 Physical Layer Tests.....	10-1
21	10.1 Transmitter Tests	10-1
22	10.1.1 Access Network Tests.....	10-1
23	10.1.2 Access Terminal Tests	10-2
24	10.2 Demodulation of the Reverse Activity Channel	10-5
25	10.2.1 Access Network Tests.....	10-5
26	10.2.2 Access Terminal Tests	10-5
27	11 Broadcast Protocol Tests	11-1
28	11.1 Generic Broadcast Protocol Tests.....	11-1
29	11.1.1 Access Network Tests.....	11-1
30	11.1.2 Access Terminal Tests	11-1
31	12 Figures	12-1
32	13 Annex (Informative).....	13-1

TABLES

1		
2	Table 9.8.2.1.3-1 T2PMaxPilotStrength.....	9-20
3	Table 9.8.2.1.3-2 BucketFactor	9-20
4	Table 9.8.2.1.3-3 T2PInflowRange	9-21
5	Table 9.8.2.1.3-4 T2PUp and T2PDn.....	9-22
6	Table 9.8.2.1.4-1 End to End Minimum Standard.....	9-23
7	Table 9.8.2.1.4-2 Minimum Requirement for TxT2P Ramping Up.....	9-24
8	Table 9.8.2.1.4-3 Minimum Requirement for TxT2P Ramping Down	9-25
9	Table 9.8.2.2.3-1 T2PInflowRange	9-27
10	Table 9.8.2.2.3-2 BucketFactor	9-27
11	Table 9.8.2.2.3-3 T2Pup and T2PDn	9-28
12	Table 9.8.2.2.4-1 Minimum Requirement for Fixed Allocation TxT2P Ramping	9-29
13	Table 9.8.2.3.3-1 T2PInflowRange	9-30
14	Table 9.8.2.4.3-1 T2PMaxPilotStrength.....	9-32
15	Table 9.8.2.4.3-2 BucketFactor	9-32
16	Table 9.8.2.4.3-2 T2PInflowRange	9-32
17	Table 9.8.2.4.3-3 T2PUp and T2PDn.....	9-33
18	Table 9.8.2.4.4-1 Minimum Requirement for T2PInflow Decay.....	9-34
19	Table 9.8.2.5.3-1 T2PMaxPilotStrength.....	9-35
20	Table 9.8.2.5.3-2 BucketFactor	9-36
21	Table 9.8.2.5.3-3 T2PInflowRange	9-36
22	Table 9.8.2.5.3-4 T2PUp and T2PDn.....	9-37
23	Table 9.8.2.5.4-1 Minimum Requirement for T2PInflow Decay.....	9-38
24	Table 9.8.2.6.3-1 T2PMaxPilotStrength.....	9-39
25	Table 9.8.2.6.3-2 BucketFactor	9-39
26	Table 9.8.2.6.3-3 T2PUp and T2PDn.....	9-40
27	Table 10.1.2.1.3-1 \hat{I}_{or} / I_{oc} and I_{oc}	10-3
28	Table 10.1.2.2.3-1 Pilot	10-4
29	Table 10.2.2.1.3-1 \hat{I}_{or} / I_{oc} and I_{oc}	10-6
30	Table 10.1.2.2.3-2 Pilot.....	10-7
31	Table 10.1.2.2.3-3 RABOffset and RABLength.....	10-7

- 1 No Text.
- 2

FIGURES

1
2
3
4
5
6
7
8
9
10
11
12
13

Figure 12.1 Conformance Requirements for Testing PermittedPayloadPS_k 12-1

Figure 12.2 Functional Setup for FTC Redundant ACK..... 12-1

Figure 12.3 Functional Setup for Reverse Traffic Channel Response to ARQ Channel
and Demodulation of the Reverse Activity Channel Tests 12-2

Figure 12.4 Functional Setup for one FTC response to ACK channel and Connection
Security and Session Layer Tests 12-2

Figure 12.5 Functional Setup for Routing of *UATIAssignment* and
TrafficChannelAssignment Messages Tests 12-3

- 1 No Text.
- 2

1
2
3
4
5
6
7
8
9

FOREWORD

(This foreword is not part of this Standard)

This standard was prepared by Technical Specification Group C of the Third Generation Partnership Project 2 (3GPP2). This standard is a companion to the cdma2000^{®1} high rate packet data standards. This specification provides a set of procedures that the access terminal and the access network can use to conduct the signaling conformance tests in a laboratory environment.

¹ “cdma2000[®] is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000[®] is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.”

- 1 No Text.
- 2

SCOPE

1
2
3
4
5
6
7

(This scope is not part of this Standard)

These technical requirements form a standard for signaling conformance in cdma2000 high rate packet data systems. These requirements ensure that compliant access terminals and compliant access networks can execute tests in meeting the objectives stated in 1.1.

1 No Text.

2

REFERENCES

The following standards and documents contain provisions, which, through reference in this text, constitute provisions of this specification. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. References [1] to [4] are normative references, while reference [5] is informative.

[1] 3GPP2 C.S0024-B, *cdma2000 High Rate Packet Data Air Interface Specification*.

[2] 3GPP2 C.S0044-A v1.0, *Interoperability Specification for cdma2000 Air Interface*.

[3] 3GPP2 C.S0054-0, *cdma2000 High Rate Broadcast-Multicast Packet Data Air Interface Specification*.

[4] 3GPP2 C.S0029-B. *Test Application Specification (TAS) for High Rate Packet Data Air Interface*

[5] 3GPP2 C.R1001-F, *Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards, Release F. (Informative reference)*

1 No Text.

1 OVERVIEW

1.1 Objectives

The objective of the test procedures contained herein is to demonstrate that access terminal/access network implementation of signaling functionality in a cabled test environment at nominal levels is in conformance with [1].

1.2 Requirements Language

“Shall” and “shall not” identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the standard. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical, or causal.

1.3 Document Organization

This document is organized into the following sections:

- Section 1 Overview: This section describes the document scope and objectives as well as document organization, list of acronyms and notations.
- Section 2 Default Signaling Application Tests: This section describes the test setups, procedures and minimum requirements for the Default Signaling Network Protocol (SNP), and the Default Signaling Link Protocol (SLP).
- Section 3 Default Packet Application Tests: This section includes test setups, procedures and minimum requirements for the Radio Link Protocol (RLP), Location Update Protocol, and Flow Control Protocol.
- Section 4 Multi-Flow Packet Application Tests: This section includes test setups, procedures and minimum requirements for the Radio Link Protocol (RLP), Data Over Signaling Protocol, Location Update Protocol, and Flow Control Protocol.
- Section 5 Stream Layer Tests: This section describes the test setups, procedures, and minimum requirements for the Default Stream Protocol.
- Section 6 Session Layer Tests: This section describes the test setups, procedures, and minimum requirements for the Default Session Management Protocol, the Default Address Management Protocol, and the Default Session Configuration Protocol.
- Section 7 Connection Layer Tests: This section describes the test setups, procedures, and minimum requirements for the Default Air-Link Management Protocol, Default Initialization State Protocol, Default Idle State Protocol, Enhanced

1 Idle State Protocol, Default Connected State Protocol, Default Route Update Protocol,
2 Default Packet Consolidation Protocol, and Overhead Messages Protocol.

- 3 • Section 8 Security Layer Tests: This section includes test setups, procedures, and
4 minimum requirements for the DH Key Exchange Protocol and SHA-1
5 Authentication Protocol.
- 6 • Section 9 MAC Layer Tests: This section includes test setups, procedures, and
7 minimum requirements for the Control Channel MAC Protocol, Access Channel
8 MAC Protocol, Forward Traffic Channel MAC Protocol, and Reverse Traffic Channel
9 MAC Protocol.
- 10 • Section 10 Physical Layer Tests: This section includes test setups, procedures, and
11 minimum requirements for testing conformance of the physical layer
12 transmissions.
- 13 • Section 11 BCMCS Tests: This section includes test setups, procedures, and
14 minimum requirements for access terminal registration procedure for Broadcast
15 and Multicast services.
- 16 • Section 12 Figures: This section includes various figures used in the document.

17 **1.4 Abbreviations, Acronyms and Terms**

18 **Access Network (AN).** The network equipment providing data connectivity between a
19 packet switched data network (typically the Internet) and the access terminals.

20 **ASP.** Active Set Pilot.

21 **Access Terminal (AT).** A device providing data connectivity to a user. An access terminal
22 may be connected to a computing device such as a laptop personal computer or it may be a
23 self-contained data device such as a personal digital assistant.

24 **BCMCS.** Broadcast and Multicast services.

25 **CDMA.** Code Division Multiple Access.

26 **CDMA System Time in Slots.** An integer value s such that: $s = \lfloor t \times 600 \rfloor$, where t
27 represents CDMA System Time in seconds. Whenever the document refers to the CDMA
28 System Time in slots, it is referring to the value s .

29 **CDMA System Time.** The time reference used by the system. CDMA System Time is
30 synchronous to UTC time except for leap seconds and uses the same time origin as GPS
31 time. Access terminals use the same CDMA System Time, offset by the propagation delay
32 from the access network to the access terminal.

33 **Channel.** The set of channels transmitted between the access network and the access
34 terminals within a given frequency assignment. A Channel consists of a Forward Link and
35 a Reverse Link.

36 **DH.** Diffie Hellman.

37 **DRC.** Data Rate Control.

- 1 **FAC.** Forward Access Channel.
- 2 **Forward Channel.** The portion of the Channel consisting of those Physical Layer Channels
3 transmitted from the access network to the access terminal.
- 4 **Forward Control Channel.** The channel that carries data to be received by all access
5 terminals monitoring the Forward Channel.
- 6 **Forward MAC Channel.** The portion of the Forward Channel dedicated to Medium Access
7 Control activities. The Forward MAC Channel consists of the RPC, DRCLock, and RA
8 Channels.
- 9 **Forward MAC Reverse Activity (RA) Channel.** The portion of the Forward MAC Channel
10 that indicates activity level on the Reverse Channel.
- 11 **Forward MAC Reverse Power Control (RPC) Channel.** The portion of the Forward MAC
12 Channel that controls the power of the Reverse Channel for one particular access
13 terminal.
- 14 **Forward Pilot Channel.** The portion of the Forward Channel that carries the pilot.
- 15 **Forward Traffic Channel.** The portion of the Forward Channel that carries information for
16 a specific access terminal. The Forward Traffic Channel can be used as either a Dedicated
17 Resource or a non-Dedicated Resource. Prior to successful access terminal authentication,
18 the Forward Traffic Channel serves as a non-Dedicated Resource. Only after successful
19 access terminal authentication can the Forward Traffic Channel be used as a Dedicated
20 Resource for the specific access terminal.
- 21 **FTP.** File Transfer Protocol.
- 22 **Frame.** The duration of time specified by 16 slots or 26.66... ms.
- 23 **GAUP.** Generic Attribute Update Protocol.
- 24 **Global Positioning System (GPS).** A US government satellite system that provides location
25 and time information to users. See Navstar GPS Space Segment/Navigation User
26 Interfaces ICD-GPS-200 for specifications.
- 27 **H-ARQ Bit.** Hybrid-ARQ bit. The bit sent on ARQ channel in response to the 1st, 2nd, and 3rd
28 sub-packet of a reverse-link physical packet to support physical layer ARQ.
- 29 **L-ARQ Bit.** Last ARQ bit. The bit sent on ARQ channel in response to the last sub-packet of
30 a reverse-link physical packet to support MAC layer ARQ.
- 31 **MAC Layer.** The MAC Layer defines the procedures used to receive and to transmit over
32 the Physical Layer.
- 33 **Multi-User packet.** A single physical layer packet composed of one or more security layer
34 packets addressed to one or more access terminals.
- 35 **NA.** Not Applicable.
- 36 **Physical Layer Protocol.** The Physical Layer Protocol provides the channel structure,
37 frequency, power output, modulation, and encoding specifications for the forward and
38 reverse links.

1 **P-ARQ.** Packet-ARQ bit. The bit sent on the ARQ channel in response to a reverse-link
2 physical layer packet to support MAC layer ARQ.

3 **RATI.** Random Access Terminal Identifier.

4 **Reservation.** Air interface resources set up by the access network to carry a higher layer
5 flow. A Reservation is identified by its ReservationLabel. ReservationLabels are bound to
6 RLP Flows that carry higher layer flows. A Reservation can be either in the Open or Close
7 state.

8 **Reverse Access Channel.** The portion of the Reverse Channel that is used by access
9 terminals to communicate with the access network when they do not have a traffic
10 channel assigned. There is a separate Reverse Access Channel for each sector of the
11 access network.

12 **Reverse Access Data Channel.** The portion of the Access Channel that carries data.

13 **Reverse Access Pilot Channel.** The portion of the Access Channel that carries the pilot.

14 **Reverse Channel.** The portion of the Channel consisting of those Physical Layer Channels
15 transmitted from the access terminal to the access network.

16 **Reverse Traffic Ack Channel.** The portion of the Reverse Traffic Channel that indicates
17 the success or failure of the Forward Traffic Channel reception.

18 **Reverse Traffic Channel.** The portion of the Reverse Channel that carries information
19 from a specific access terminal to the access network. The Reverse Traffic Channel can be
20 used as either a Dedicated Resource or a non-Dedicated Resource. Prior to successful
21 access terminal authentication, the Reverse Traffic Channel serves as a non-Dedicated
22 Resource. Only after successful access terminal authentication can the Reverse Traffic
23 Channel be used as a Dedicated Resource for the specific access terminal.

24 **Reverse Traffic Data Channel.** The portion of the Reverse Traffic Channel that carries
25 user data.

26 **Reverse Traffic MAC Channel.** The portion of the Reverse Traffic Channel dedicated to
27 Medium Access Control activities. The Reverse Traffic MAC Channel consists of the RRI
28 and DRC Channels.

29 **Reverse Traffic MAC Data Rate Control (DRC) Channel.** The portion of the Reverse
30 Traffic Channel that indicates the rate at which the access terminal can receive the
31 Forward Traffic Channel and the sector from which the access terminal wishes to receive
32 the Forward Traffic Channel.

33 **Reverse Traffic MAC Data Source Control (DSC) Channel.** The portion of the Reverse
34 Traffic Channel that indicates the data source from which the access terminal wishes to
35 receive the Forward Traffic Channel.

36 **Reverse Traffic MAC Reverse Rate Indicator (RRI) Channel.** The portion of the Reverse
37 Traffic Channel that indicates the rate of the Reverse Traffic Data Channel.

38 **Reverse Traffic Pilot Channel.** The portion of the Reverse Traffic Channel that carries
39 the pilot.

- 1 **Reverse Traffic Auxiliary Pilot Channel.** The portion of the Reverse Traffic Channel that
2 carries the auxiliary pilot.
- 3 **RLP.** Radio Link Protocol provides retransmission and duplicate detection for an octet-
4 aligned data stream.
- 5 **Rx.** Receive.
- 6 **Sector.** The part of the access network that is identified by (SectorID, CDMA Channel).
- 7 **Security Layer.** The Security Layer provides authentication and encryption services. The
8 Security Layer is defined in Chapter 9 of [1].
- 9 **Session Layer.** The Session Layer provides protocol negotiation, protocol configuration, and
10 state maintenance services. The Session Layer is defined in Chapter 7 of [1].
- 11 **Single User packet.** A single physical layer packet consisting of one or more security layer
12 packets addressed to one access terminal.
- 13 **Slot.** A duration of time specified by 1.66... ms.
- 14 **SLP.** Signaling Link Protocol provides best-effort and reliable-delivery mechanisms for
15 signaling messages. SLP is defined in [1].
- 16 **SNP.** Signaling Network Protocol provides message transmission services for signaling
17 messages. The protocols that control each layer use SNP to deliver their messages to their
18 peer protocols.
- 19 **Stream Layer.** The Stream Layer provides multiplexing of distinct streams. Stream 0 is
20 dedicated to signaling and defaults to the default signaling stream (SNP / SLP). Stream 1,
21 Stream 2, and Stream 3 are not used by default. The Stream Layer is defined in Chapter 6
22 of [1].
- 23 **Sub-Frame.** A sub-frame is a group of four contiguous slots. The start of a sub-frame is
24 specified by $(T - \text{FrameOffset}) \bmod 4 = 0$, where T is the CDMA System Time in slots.
- 25 **Sub-packet.** A sub-packet is the smallest unit of a Reverse Traffic Channel transmission
26 that can be acknowledged at the physical layer by the access network. A sub-packet is
27 transmitted over four contiguous slots.
- 28 **Subnet Mask (of length n).** A 128-bit value whose binary representation consists of n
29 consecutive '1's followed by 128- n consecutive '0's.
- 30 **Tx.** Transmit.
- 31 **TxT2P.** Transmitted Traffic Channel to Pilot Channel transmit power ratio.
- 32 **T2P.** Traffic Channel to Pilot Channel transmit power ratio.
- 33 **UATI.** Unicast Access Terminal Identifier.
- 34 **Universal Coordinated Time (UTC).** An internationally agreed-upon time scale
35 maintained by the Bureau International de l'Heure (BIH) used as the time reference by
36 nearly all commonly available time and frequency distribution systems.
- 37 **UTC.** Universal Temps Coordine. See Universal Coordinated Time.

1 **ms.** Millisecond

2 **s.** Second

3 **1.5 Notation**

4 $\lfloor x \rfloor$ Indicates the largest integer less than or equal to x:

5 $\lfloor 1.1 \rfloor = 1, \lfloor 1.0 \rfloor = 1.$

6 **x mod y** Indicates the remainder after dividing x by y:

7 $x \text{ mod } y = x - (y \times \lfloor x/y \rfloor).$

2 DEFAULT SIGNALING APPLICATION TESTS

This section includes tests for the Signaling Network Protocol (SNP) and the Signaling Link Protocol (SLP) of the Default Signaling Application.

2.1 Default Signaling Link Protocol Tests

2.1.1 Access Network Tests

2.1.1.1 SLP Initialization Test

2.1.1.1.1 Definition

This test verifies that upon protocol initialization, the access network sets the reliable-delivery SLP-D packet sequence number equal to 0.

2.1.1.1.2 Traceability

See section 2.6.4.2.3.2 of [1].

2.1.1.1.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network. Begin recording at the access terminal SLP-D packets received from the access network.
- b. Verify that the SequenceNumber field in the SLP-D packet sent by the access network meets the minimum standard as per 2.1.1.1.4.

2.1.1.1.4 Minimum Standard

The SequenceNumber field in the first reliable-delivery SLP-D packet sent by the access network during connection establishment shall be 0.

2.1.1.2 SLP-D Sequence Number Increment Tests

2.1.1.2.1 Definition

This test verifies that the access network increments the sequence number by 1 for each new reliable-delivery SLP-D packet sent to the access terminal and this sequence number wraps around to 0 after reaching 7.

2.1.1.2.2 Traceability

See section 2.6.4.2.3.3 and 13.7 of [1].

2.1.1.2.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network and record at the access terminal the SLP-D packets received from the access network.
- b. Instruct the access terminal to send a Default Signaling Application *ConfigurationRequest* message.

- 1 c. Record the reliable delivery SLP-D packets associated with the Default Signaling
2 Application *ConfigurationResponse* message from the access network.
- 3 d. Repeat steps b and c, nine times.
- 4 e. Verify that consecutive reliable-delivery SLP-D packets sent by the access network
5 meet the minimum standard as per 2.1.1.2.4.

6 2.1.1.2.4 Minimum Standard

7 The access network shall increment the SequenceNumber field in the header of
8 consecutive reliable-delivery SLP-D packets by 1 mod 8 as defined in 14.6 of [1].

9 2.1.1.3 Reliable-Delivery SLP-D Packet Acknowledgment Test

10 2.1.1.3.1 Definition

11 This test verifies that the access network acknowledges a reliable -delivery SLP-D packet
12 that has been received.

13 2.1.1.3.2 Traceability

14 See section 2.6.4.2.3.3 and 13.7 of [1].

15 2.1.1.3.3 Test Procedure

- 16 a. Instruct the access terminal to set up a connection with the access network and
17 record at the access terminal the SLP-D packets received from the access network.
- 18 b. Instruct the access terminal to send a Default Signaling Application
19 *ConfigurationRequest* message.
- 20 c. Wait for a Default Signaling Application *ConfigurationResponse* message from the
21 access network.
- 22 d. Verify that the access network meets the minimum standard as per 2.1.1.3.4.

23 2.1.1.3.4 Minimum Standard

24 The access network shall acknowledge each individual reliable -delivery SLP-D packet.

25 2.1.1.4 Retransmission of Unacknowledged Reliable-Delivery SLP-D Packet Test

26 2.1.1.4.1 Definition

27 This test verifies that the access network sends a reliable -delivery SLP-D packet exactly
28 $N_{SLPAttempt} (=3)$ times if it never receives an acknowledgment.

29 2.1.1.4.2 Traceability

30 See section 2.6.4.2.3.3 and 13.7 of [1].

1 2.1.1.4.3 Test Procedure

- 2 a. Instruct the access terminal to set up a connection with the access network and
3 record at the access terminal the SLP-D packets received from the access network.
- 4 b. Instruct the access terminal to send a Default Signaling Application
5 *ConfigurationRequest* message.
- 6 c. When a reliable-delivery SLP-D packet containing a Default Signaling Application
7 *ConfigurationResponse* message is received from the access network, instruct the
8 access terminal to not acknowledge it on the Reverse Traffic Channel.
- 9 d. Verify that the access network meets the minimum standard as per 2.1.1.4.4.

10 2.1.1.4.4 Minimum Standard

11 The access network shall send a reliable-delivery SLP-D packet containing a Default
12 Signaling Application *ConfigurationResponse* message exactly $N_{SLPAttempt}$ (=3) times if it does
13 not receive any acknowledgment from the access terminal.

14 2.1.1.5 Successful Reassembly of SLP-F Packets Sent on the Access Channel Test

15 2.1.1.5.1 Definition

16 This test verifies that a signaling message carried in multiple SLP-F packets sent on the
17 Access Channel is successfully reassembled in the access network.

18 2.1.1.5.2 Traceability

19 See section 2.6.4.3.5 of [1].

20 2.1.1.5.3 Test Procedure

- 21 a. Instruct the access terminal to transmit a *ConnectionRequest* message, and a
22 *RouteUpdate* message fragmented into two parts, on the Access Channel. Ensure
23 that the *RouteUpdate* message is fragmented such that all the Pilot information is
24 included in the second fragment. Begin recording at the access terminal the SLP-D
25 packets sent to and received from the access network.
- 26 b. Verify that the access network meets the minimum standard as per 2.1.1.5.4.

27 2.1.1.5.4 Minimum Standard

28 The access network shall successfully reassemble the signaling message carried in
29 multiple SLP-F packets sent on the Access Channel and respond by sending a
30 *TrafficChannelAssignment* message to the access terminal.

1 2.1.1.6 Successful Reassembly of SLP-F Packets Sent on the Reverse Traffic Channel Test

2 2.1.1.6.1 Definition

3 This test verifies that reliable-delivery signaling messages carried in multiple SLP-F
4 packets sent on the Reverse Traffic Channel are successfully reassembled in the access
5 network.

6 2.1.1.6.2 Traceability

7 See section 2.6.4.3.5 and 13.7 of [1].

8 2.1.1.6.3 Test Procedure

- 9 a. Configure the access terminal to fragment all Session Configuration Protocol
10 *ConfigurationRequest* messages sent on the Reverse Traffic Channel.
- 11 b. Instruct the access terminal to set up a connection with the access network and
12 begin recording at the access terminal the SLP-D packets sent to and received from
13 the access network.
- 14 c. Instruct the access terminal to send a Session Configuration Protocol
15 *ConfigurationRequest* message.
- 16 d. Verify that the access network meets the minimum standard as per 2.1.1.6.4.

17 2.1.1.6.4 Minimum Standard

18 The access network shall successfully reassemble reliable-delivery SLP-D packets that
19 were fragmented at the access terminal, and then send a Session Configuration Protocol
20 *ConfigurationResponse* message to the access terminal.

21 2.1.2 Access Terminal Tests

22 2.1.2.1 SLP Initialization Tests

23 2.1.2.1.1 Definition

24 This test verifies that upon protocol initialization, the access terminal sets the reliable-
25 delivery SLP-D packet sequence number equal to 0.

26 2.1.2.1.2 Traceability

27 See section 2.6.4.2.3.2 of [1].

28 2.1.2.1.3 Test Procedure

- 29 a. Instruct the access terminal to set up a connection with the access network. Begin
30 recording at the access network SLP-D packets received from the access terminal.
- 31 b. Verify that the access terminal meets the minimum standard as per 2.1.2.1.4.

1 2.1.2.1.4 Minimum Standard

2 The SequenceNumber field in the first reliable-delivery SLP-D packet sent by the access
3 terminal shall be 0.

4 2.1.2.2 SLP Reset Test

5 2.1.2.2.1 Definition

6 This test verifies that the access terminal responds to a *Reset* message with a *ResetAck*
7 message, resets the packet sequence number (SequenceNumber field) included in the
8 first reliable-delivery SLP-D packet to 0 and also resets the receive vector **Rx** to 0.

9 2.1.2.2.2 Traceability

10 See section 2.6.4.1 of [1].

11 2.1.2.2.3 Test Procedure

- 12 a. Instruct the access terminal to set up a connection with the access network and
13 record at the access network SLP-D packets received from the access terminal.
- 14 b. Instruct the access network to send the Signaling Link Protocol (SLP) *Reset*
15 message to the access terminal.
- 16 c. Verify that the access terminal meets the minimum standard as per bullet 1 in
17 2.1.2.2.4.
- 18 d. Instruct the access network to send a new *TrafficChannelAssignment* message to the
19 access terminal.
- 20 e. Verify that the access terminal meets the minimum standard as per bullet 2 in
21 2.1.2.2.4. This implicitly verifies that the access terminal resets the receive vector
22 Rx[i] to 0, for $i = 0..2^s-1$ ($s = 3$) after an SLP reset.
- 23 f. Verify that following step b, the access terminal meets the minimum standard as
24 per bullet 3 in 2.1.2.2.4.

25 2.1.2.2.4 Minimum Standard

- 26 1. The access terminal shall respond to an SLP *Reset* message with an SLP *ResetAck*
27 message
- 28 2. The access terminal shall respond to *TrafficChannelAssignment* message sent in
29 step d with a *TrafficChannelComplete* message.
- 30 3. After an SLP reset, the access terminal shall set the SequenceNumber field in SLP-
31 D header of the first reliable-delivery SLP-D packet (i.e. *TrafficChannelComplete*
32 message) equal to 0.

1 2.1.2.3 SLP-D Sequence Number Increment Test

2 2.1.2.3.1 Definition

3 This test verifies that the access terminal increments the sequence number by 1 for each
4 new reliable-delivery SLP-D packet sent to the access network and this sequence number
5 wraps around to 0 after reaching 7.

6 2.1.2.3.2 Traceability

7 See section 2.6.4.2.3.3 of [1].

8 2.1.2.3.3 Test Procedure

- 9 a. Instruct the access terminal to set up a connection with the access network and
10 record at the access network the SLP-D packets received from the access terminal.
- 11 b. Instruct the access network to send a new Route Update Protocol
12 *TrafficChannelAssignment* message.
- 13 c. Wait for a Route Update Protocol *TrafficChannelComplete* message.
- 14 d. Repeat steps b and c 9 times.
- 15 e. Verify that in the consecutive reliable-delivery SLP-D packets sent by the access
16 terminal, the SequenceNumber field in the SLP-D header meets the minimum
17 standard as per 2.1.2.3.4.

18 2.1.2.3.4 Minimum Standard

19 The SequenceNumber field in the header of the consecutive reliable-delivery SLP-D
20 packets received from the access terminal shall increment by 1 mod 8 as defined in 14.6 of
21 [1].

22 2.1.2.4 Reliable-Delivery SLP-D Packet Acknowledgement Test

23 2.1.2.4.1 Definition

24 This test verifies that the access terminal acknowledges an arriving reliable-delivery SLP-
25 D packet.

26 2.1.2.4.2 Traceability

27 See section 2.6.4.2.3.3 of [1].

28 2.1.2.4.3 Test Procedure

- 29 a. Instruct the access terminal to set up a connection with the access network and
30 record at the access network the SLP-D packets received from the access terminal.
- 31 b. Instruct the access network to send a new Route Update Protocol
32 *TrafficChannelAssignment* message.
- 33 c. Wait for a Route Update Protocol *TrafficChannelComplete* message.

1 d. Verify that the access terminal meets the minimum standard as per 2.1.2.4.4.

2 2.1.2.4.4 Minimum Standard

3 The access terminal shall acknowledge each individual reliable -delivery SLP-D packet that
4 it receives.

5 2.1.2.5 Retransmission of Unacknowledged Reliable -Delivery SLP-D Packet Test

6 2.1.2.5.1 Definition

7 This test verifies that the access terminal sends a reliable -delivery signaling message
8 exactly $N_{\text{SLPAttempt}}$ (= 3) times if it never receives an acknowledgment.

9 2.1.2.5.2 Traceability

10 See section 2.6.4.2.3.3 of [1].

11 2.1.2.5.3 Test Procedure

12 a. Instruct the access terminal to set up a connection with the access network and
13 record at the access network the SLP-D packets received from the access terminal.

14 b. Instruct the access network to send a new *TrafficChannelAssignment* message.

15 c. When a reliable -delivery SLP-D packet containing Route Update Protocol
16 *TrafficChannelComplete* message is sent by the access terminal, instruct the access
17 network to never acknowledge it on the Forward Traffic Channel.

18 d. Verify that the access terminal meets the minimum standard as per 2.1.2.5.4.

19 2.1.2.5.4 Minimum Standard

20 The access terminal shall send a reliable -delivery SLP-D packet containing Route Update
21 Protocol *TrafficChannelComplete* message exactly $N_{\text{SLPAttempt}}$ (=3) times if it never receives an
22 acknowledgment.

23 2.1.2.6 Successful Reassembly of SLP-F Packets Sent on the Forward Traffic Channel Test

24 2.1.2.6.1 Definition

25 This test verifies that a signaling message carried in multiple SLP-F packets sent on the
26 Forward Traffic Channel is successfully reassembled in the access terminal.

27 2.1.2.6.2 Traceability

28 See section 2.6.4.3.5 of [1].

29 2.1.2.6.3 Test Procedure

30 a. Instruct the access terminal to set up a connection with the access network and
31 begin recording at the access network the SLP-D packets sent to and received from
32 the access terminal.

- 1 b. Instruct the access network to send a new fragmented Route Update Protocol
- 2 *TrafficChannelAssignment* message on the Forward Traffic Channel.
- 3 c. Verify that the access terminal meets the minimum standard as per 2.1.2.6.4.

4 2.1.2.6.4 Minimum Standard

5 The access terminal shall successfully reassemble reliable -delivery SLP-D packets sent on
6 the Forward Traffic Channel that were fragmented at the access network and shall send a
7 Route Update Protocol *TrafficChannelComplete* message to the access network.

8 2.1.2.7 Successful Reassembly of Fragmented Broadcast Messages on the Control Channel 9 Test

10 2.1.2.7.1 Definition

11 This test verifies that a broadcast signaling message carried in multiple SLP-F packets
12 sent on the Control Channel is successfully reassembled in the access terminal.

13 2.1.2.7.2 Traceability

14 See section 2.6.4.3.5 of [1].

15 2.1.2.7.3 Test Procedure

- 16 a. Instruct the access network to send a new fragmented *SectorParameters* message
- 17 once every 1.28 s up to 5 times. Change the SectorID in each new *SectorParameters*
- 18 message such that the subnet changes from the previous one.
- 19 b. Verify that the access terminal meets the minimum standard as per 2.1.2.7.4.

20 2.1.2.7.4 Minimum Standard

21 The access terminal shall successfully reassemble fragmented broadcast signaling
22 messages sent on the Control Channel that were fragmented at the access network and
23 shall respond by sending a *UATIRequest* message.

24 2.1.2.8 Successful Reassembly of Fragmented Unicast Messages on the Control Channel 25 Test

26 2.1.2.8.1 Definition

27 This test verifies that a unicast signaling message carried in multiple SLP-F packets sent
28 on the Control Channel is successfully reassembled in the access terminal.

29 2.1.2.8.2 Traceability

30 See section 2.6.4.3.5 of [1].

1 2.1.2.8.3 Test Procedure

- 2 a. Instruct the access network to send a fragmented *SectorParameters* message
3 interleaved with a fragmented *TrafficChannelAssignment* message on the Control
4 Channel.
- 5 b. Verify that the access terminal meets the minimum standard as per 2.1.2.8.4.

6 2.1.2.8.4 Minimum Standard

7 The access terminal shall successfully reassemble fragmented unicast signaling
8 messages sent on the Control Channel from the access network and shall set up a
9 connection with the access network.

10

1 No Text.

1 **3 DEFAULT PACKET APPLICATION TESTS**

2 This section includes tests for the Radio Link Protocol, Location Update Protocol, and the
3 Flow Control Protocol.

4 **3.1 Radio Link Protocol Tests**

5 The tests in this section assume that the access terminal and the access network support
6 the Default Packet Application.

7 3.1.1 Access Network RLP Tests

8 3.1.1.1 RLP Initialization Test

9 3.1.1.1.1 Definition

10 This test verifies that upon protocol initialization, the access network sets the RLP
11 sequence number of the first RLP Packet transmitted on the Forward Traffic Channel
12 equal to zero. The test procedure utilizes the fact that when a connection is opened by the
13 access terminal or the access network, the RLP instance of the Packet Application bound
14 to the service access network will undergo initialization.

15 3.1.1.1.2 Traceability

16 See section 3.4.4.1.1 of [1].

17 3.1.1.1.3 Test Procedure

- 18 a. Configure the access terminal to negotiate the use of the Default Packet
19 Application bound to the service access network (app type = 0x0002) during session
20 configuration. Instruct the access terminal to transmit a *SessionClose* message to
21 the access network. Instruct the access terminal to start a new session with the
22 access network.
- 23 b. Instruct the access terminal to set up a connection and establish a data call with
24 the access network.
- 25 c. Initiate downloading of a file from the service access network and record the SEQ
26 field in the first RLP packet received at the access terminal.
- 27 d. Verify that the SEQ field in the first Forward Traffic Channel RLP packet meets the
28 minimum standard as per 3.1.1.1.4.

29 3.1.1.1.4 Minimum Standard

30 The SEQ field in the first Forward Traffic Channel RLP packet received from the access
31 network after connection establishment shall be set equal to zero.

1 3.1.1.2 RLP Sequence Number Increment Test

2 3.1.1.2.1 Definition

3 This test verifies that the basic RLP sequence number increment procedure in the access
4 network works correctly.

5 3.1.1.2.2 Traceability

6 See section 3.4.4.1.2.1 of [1].

7 3.1.1.2.3 Test Procedure

8 a. Configure the access terminal to negotiate the use of the Default Packet
9 Application bound to the service access network (app type = 0x0002) during session
10 configuration. Instruct the access terminal to transmit a *SessionClose* message to
11 the access network. Instruct the access terminal to start a new session with the
12 access network.

13 b. Instruct the access terminal to set up a connection and establish a data call with
14 the access network.

15 c. Initiate downloading of a file from the service access network via FTP. Record two
16 consecutive Forward Traffic Channel RLP packets sent by the access network.

17 d. Verify that the access network meets the minimum standard as per 3.1.1.2.4.

18 3.1.1.2.4 Minimum Standard

19 The RLP Sequence number (SEQ) in each first time transmitted RLP packet shall be set
20 equal to the sequence number of the immediately preceding first time transmitted RLP
21 packet plus the number of octets excluding the SEQ field included in that packet.

22 3.1.1.3 RLP Reset Test

23 3.1.1.3.1 Definition

24 This test verifies that the access network upon receiving an RLP *Reset* message sends an
25 RLP *ResetAck* message to the access terminal, and the RLP sequence number in the first
26 Forward Traffic Channel RLP packet is initialized to zero. It also verifies that the RLP
27 receiver at the access network performs the initialization procedure and resets V(R) and
28 V(N) to zero after receiving the *Reset* message.

29 3.1.1.3.2 Traceability

30 See section 3.4.4.1.1.1 and 3.4.4.1.1.2 of [1].

31 3.1.1.3.3 Test Procedure

32 a. Configure the access terminal to negotiate the use of the Default Packet
33 Application bound to the service access network (app type = 0x0002) during session
34 configuration. Instruct the access terminal to transmit a *SessionClose* message to

- 1 the access network. Instruct the access terminal to start a new session with the
2 access network.
- 3 b. Instruct the access terminal to set up a connection and establish a data call with
4 the access network.
- 5 c. Initiate downloading of a file from the service access network.
- 6 d. While the file download is in progress, instruct the access terminal to send an RLP
7 *Reset* message to the access network.
- 8 e. Verify that the access network meets the minimum standard as per bullet 1 in
9 3.1.1.3.4.
- 10 f. Record the SEQ field in the first RLP packet received from the access network
11 following the RLP *Reset*.
- 12 g. Verify that the SEQ field in the first Forward Traffic Channel RLP packet meets the
13 minimum standard as per bullet 2 in 3.1.1.3.4.
- 14 h. Verify that the access network meets the minimum standard as per bullet 3 in
15 3.1.1.3.4.

16 3.1.1.3.4 Minimum Standard

- 17 1. The access network shall send an RLP *ResetAck* message in response to an RLP
18 *Reset* message.
- 19 2. The access network shall initialize the RLP sequence number for the first RLP
20 packet equal to zero following the RLP reset.
- 21 3. The access network shall not send an RLP *Nak* message or an RLP *Reset* message
22 for the first RLP packet received after an RLP reset. This implicitly verifies that the
23 access network initializes the receive variables V(R) and V(N) to zero after an RLP
24 reset.

25 3.1.1.4 RLP NAK Test

26 3.1.1.4.1 Definition

27 This test verifies that the access network sends RLP *Nak* messages on the Forward Traffic
28 Channel, when the access terminal does not send selected RLP octets in an octet stream
29 on the Reverse Traffic Channel.

30 3.1.1.4.2 Traceability

31 See section 3.4.4.1.2.2 of [1].

32 3.1.1.4.3 Test Procedure

- 33 a. Configure the access terminal to negotiate the use of the Default Packet
34 Application bound to the service access network (app type = 0x0002) during session
35 configuration. Instruct the access terminal to transmit a *SessionClose* message to

1 the access network. Instruct the access terminal to start a new session with the
2 access network.

3 b. Instruct the access terminal to set up a connection and establish a data call with
4 the access network.

5 c. Initiate uploading of a file to the service access network. Record at the access
6 terminal any Reverse Traffic Channel RLP packets dropped and any Forward Traffic
7 Channel RLP *Nak* messages sent by the access network.

8 d. Drop one Reverse Traffic Channel RLP packet with sequence number in the range
9 [0,500].

10 e. Verify that the access network meets the minimum standard as per 3.1.1.4.4.

11 3.1.1.4.4 Minimum Standard

12 The access network shall send an RLP *Nak* message to request selected RLP octets in an
13 octet stream that were not transmitted by the access terminal on the Reverse Traffic
14 Channel.

15 3.1.1.5 RLP Synchronization Loss Detection Test

16 3.1.1.5.1 Definition

17 This test verifies that when the access terminal *Naks* an RLP sequence number that has
18 never been sent by the access network on the Forward Traffic Channel, then the access
19 network initiates an RLP reset procedure.

20 3.1.1.5.2 Traceability

21 See section 3.4.4.1.2.1 and 3.4.4.1.1.2 of [1].

22 3.1.1.5.3 Test Procedure

23 a. Configure the access terminal to negotiate the use of the Default Packet
24 Application bound to the service access network (app type = 0x0002) during session
25 configuration. Instruct the access terminal to transmit a *SessionClose* message to
26 the access network. Instruct the access terminal to start a new session with the
27 access network.

28 b. Instruct the access terminal to set up a connection and establish a data call with
29 the access network.

30 c. Instruct the access terminal to send an RLP *Nak* message requesting an RLP octet
31 with sequence number 2^{20} .

32 d. Verify that the access network meets the minimum standard as per 3.1.1.5.4.

33 3.1.1.5.4 Minimum Standard

34 The access network shall send an RLP *Reset* message when an RLP *Nak* message on the
35 Reverse Traffic Channel requests an RLP octet with sequence number x in the range $[V(S),$

1 $V(S) + 2^{(22-1)} - 1]$, where $V(S)$ is the sequence number of the next RLP data octet to be sent
2 by the access network.

3 3.1.1.6 Basic File Transfer Test

4 3.1.1.6.1 Definition

5 This test verifies that the access network implementation of the RLP supports basic file
6 transfer functionality on the Forward Traffic Channel.

7 3.1.1.6.2 Traceability

8 See section 3.4.1 of [1].

9 3.1.1.6.3 Test Procedure

- 10 a. Configure the access terminal to negotiate the use of the Default Packet
11 Application bound to the service access network (app type = 0x0002) during session
12 configuration. Instruct the access terminal to transmit a *SessionClose* message to
13 the access network. Instruct the access terminal to start a new session with the
14 access network.
- 15 b. Configure the access terminal so that the effective Forward Traffic Channel packet
16 error rate seen by the RLP is $1\% \pm 0.25\%$.
- 17 c. Instruct the access terminal to set up a connection and establish a data call with
18 the access network.
- 19 d. Initiate downloading of a 200 kbytes file from the service network via FTP. A
20 representative data file is RAND200.BIN defined in ANNEX D of [2].
- 21 e. Verify that the access network meets the minimum standard as per bullets 1 and 2
22 in 3.1.1.6.4.

23 3.1.1.6.4 Minimum Standard

- 24 1. The file shall be successfully transferred using the Forward Traffic Channel.
- 25 2. The received file shall be complete and identical in content to the original file.

26 3.1.2 Access Terminal RLP Tests

27 3.1.2.1 RLP Initialization Test

28 3.1.2.1.1 Definition

29 This test verifies that upon protocol initialization, the access terminal sets the RLP
30 sequence number of the first RLP packet transmitted on the Reverse Traffic Channel
31 equal to zero. The test procedure utilizes the fact that when a connection is opened by the
32 access terminal or the access network, the RLP instance of the Packet Application bound
33 to the service access network will undergo initialization.

1 3.1.2.1.2 Traceability

2 See section 3.4.4.1.1 of [1].

3 3.1.2.1.3 Test Procedure

- 4 a. Configure the access terminal to negotiate the use of the Default Packet
5 Application bound to the service access network (app type = 0x0002) during session
6 configuration. Instruct the access terminal to transmit a *SessionClose* message to
7 the access network. Instruct the access terminal to start a new session with the
8 access network.
- 9 b. Instruct the access terminal to set up a connection and establish a data call with
10 the access network.
- 11 c. Initiate uploading of a file from the access terminal to the service access network
12 and record the SEQ field in the first RLP packet received at the access network.
- 13 d. Verify that the SEQ field in the first Reverse Traffic Channel RLP packet meets the
14 minimum standard as per 3.1.2.1.4.

15 3.1.2.1.4 Minimum Standard

16 The SEQ field in the first Reverse Traffic Channel RLP packet received from the access
17 terminal after connection establishment shall be set equal to zero.

18 3.1.2.2 RLP Sequence Number Increment Test

19 3.1.2.2.1 Definition

20 This test verifies that the basic sequence number increment procedure in the access
21 terminal works correctly.

22 3.1.2.2.2 Traceability

23 See section 3.4.4.1.2.1 of [1].

24 3.1.2.2.3 Test Procedure

- 25 a. Configure the access terminal to negotiate the use of the Default Packet
26 Application bound to the service access network (app type = 0x0002) during session
27 configuration. Instruct the access terminal to transmit a *SessionClose* message to
28 the access network. Instruct the access terminal to start a new session with the
29 access network.
- 30 b. Instruct the access terminal to set up a connection and establish a data call with
31 the access network.
- 32 c. Initiate uploading of a file from the access terminal to the service access network.
33 Record two consecutive Reverse Traffic Channel RLP packets sent by the access
34 terminal.
- 35 d. Verify that the test meets the minimum standard as per 3.1.2.2.4.

1 3.1.2.2.4 Minimum Standard

2 The RLP Sequence number (SEQ) in each new first time transmitted RLP packet shall be
3 set equal to the sequence number of the immediately preceding first-time transmitted RLP
4 packet plus the number of octets excluding the SEQ field included in that packet (not
5 counting the first octet).

6 3.1.2.3 RLP Reset Test

7 3.1.2.3.1 Definition

8 This test verifies that the access terminal upon receiving an RLP *Reset* message sends an
9 RLP *ResetAck* message to the access network, and the RLP sequence number in the first
10 Reverse Traffic Channel RLP packet is initialized to zero. It also verifies that the RLP
11 receiver at the access terminal performs the initialization procedure and resets V(R) and
12 V(N) to zero after receiving the *Reset* message.

13 3.1.2.3.2 Traceability

14 See section 3.4.4.1.1.1 and 3.4.4.1.1.2 of [1].

15 3.1.2.3.3 Test Procedure

- 16 a. Configure the access terminal to negotiate the use of the Default Packet
17 Application bound to the service access network (app type = 0x0002) during session
18 configuration. Instruct the access terminal to transmit a *SessionClose* message to
19 the access network. Instruct the access terminal to start a new session with the
20 access network.
- 21 b. Instruct the access terminal to set up a connection and establish a data call with
22 the access network.
- 23 c. Instruct the access network to initiate uploading of a file from the access terminal.
- 24 d. While the file upload is in progress, instruct the access network to send an RLP
25 *Reset* message to the access terminal.
- 26 e. Verify that the access terminal meets the minimum standard as per bullet 1 in
27 3.1.2.3.4.
- 28 f. Record the SEQ field in the first RLP packet received from the access terminal
29 following the RLP *Reset*.
- 30 g. Verify that the SEQ field in the first Reverse Traffic Channel RLP packet meets the
31 minimum standard as per bullet 2 in 3.1.2.3.4.
- 32 h. Verify that the access terminal meets the minimum standard as per bullet 3 in
33 3.1.2.3.4.

34 3.1.2.3.4 Minimum Standard

- 35 1. The access terminal shall send an RLP *ResetAck* message to the access network in
36 response to an RLP *Reset* message.

- 1 2. The access terminal shall initialize the sequence number (SEQ) in the Reverse
2 Traffic Channel RLP packet equal to zero following the RLP reset.
- 3 3. The access terminal shall not send an RLP *Nak* message or an RLP *Reset* message
4 upon receiving the first RLP packet following the RLP reset. This implicitly verifies
5 that access terminal correctly initializes the receive variables V(R) and V(N) equal
6 to zero.

7 3.1.2.4 RLP NAK Test

8 3.1.2.4.1 Definition

9 This test verifies that the access terminal sends RLP *Nak* messages on the Reverse Traffic
10 Channel when the access network does not send selected RLP octets in an octet stream on
11 the Forward Traffic Channel.

12 3.1.2.4.2 Traceability

13 See section 3.4.4.1.2.2 of [1].

14 3.1.2.4.3 Test Procedure

- 15 a. Configure the access terminal to negotiate the use of the Default Packet
16 Application bound to the service access network (app type = 0x0002) during session
17 configuration. Instruct the access terminal to transmit a *SessionClose* message to
18 the access network. Instruct the access terminal to start a new session with the
19 access network.
- 20 b. Instruct the access terminal to set up a connection and establish a data call with
21 the access network.
- 22 c. Initiate downloading of a file from the service access network. Begin recording at
23 the access network any Forward Traffic Channel RLP packets dropped and any RLP
24 *Nak* messages sent by the access terminal.
- 25 d. Drop one Forward Traffic Channel RLP packet at the access network with sequence
26 number in the range [0, 500].
- 27 e. Verify that at least one RLP *Nak* message corresponding to the dropped RLP octets is
28 received from the access terminal as per the minimum standard 3.1.2.4.4.

29 3.1.2.4.4 Minimum Standard

30 The access terminal shall send RLP *Nak* messages on the Reverse Traffic Channel to
31 request select RLP octets in an octet stream that were not transmitted by the access
32 network.

1 3.1.2.5 RLP Synchronization Loss Detection Test

2 3.1.2.5.1 Definition

3 This test verifies that when the access network *Naks* an RLP sequence number that has
4 never been sent by the access terminal on the Reverse Traffic Channel, the access
5 terminal initiates an RLP reset procedure.

6 3.1.2.5.2 Traceability

7 See section 3.4.4.1.2.1 and 3.4.4.1.1.2 of [1].

8 3.1.2.5.3 Test Procedure

- 9 a. Configure the access terminal to negotiate the use of Default Packet Application
10 bound to the service access network (app type = 0x0002) during session
11 configuration. Instruct the access terminal to transmit a *SessionClose* message to
12 the access network. Instruct the access terminal to start a new session with the
13 access network.
- 14 b. Instruct the access terminal to set up a connection and establish a data call with
15 the access network.
- 16 c. Instruct the access network to send an RLP *Nak* message requesting an RLP octet
17 with sequence number 2^{20} .
- 18 d. Verify that the access terminal meets the minimum standard as per 3.1.2.5.4.

19 3.1.2.5.4 Minimum Standard

20 The access terminal shall send an RLP *Reset* message, when an RLP *Nak* message on the
21 Forward Traffic Channel requests an RLP octet with sequence number x in the range $[V(S),$
22 $V(S) + 2^{(22-1)} - 1]$, where $V(S)$ is the sequence number of the next RLP data octet to be sent by
23 the access terminal.

24 3.1.2.6 Basic File Transfer Test

25 3.1.2.6.1 Definition

26 This test verifies that access terminal implementation of the RLP supports basic file
27 transfer functionality on the Reverse Traffic Channel.

28 3.1.2.6.2 Traceability

29 See section 3.4.1 of [1].

30 3.1.2.6.3 Test Procedure

- 31 a. Configure the access terminal to negotiate the use of the Default Packet
32 Application bound to the service access network (app type = 0x0002) during session
33 configuration. Instruct the access terminal to transmit a *SessionClose* message to

- 1 the access network. Instruct the access terminal to start a new session with the
2 access network.
- 3 b. Configure the access network so that the effective Reverse Traffic Channel packet
4 error rate seen by the RLP in the access network is $1\% \pm 0.25\%$.
- 5 c. Instruct the access terminal to set up a connection and establish a data call with
6 the access terminal.
- 7 d. Initiate uploading of a 200 kbytes file from the access terminal to the service
8 access network. A representative data file is RAND200.BIN defined in ANNEX D of
9 [2].
- 10 e. Verify that the access terminal meets the minimum standard as per bullets 1 and
11 2 in 3.1.2.6.4.

12 3.1.2.6.4 Minimum Standard

- 13 1. The file shall be successfully transferred using the Reverse Traffic Channel.
- 14 2. The received file shall be complete and identical in content to the original file.

15 **3.2 Location Update Protocol Tests**

16 These tests are applicable if the access terminal supports the Default Packet Application.

17 3.2.1 Access Network Tests

18 None

19 3.2.2 Access Terminal Tests

20 3.2.2.1 LocationRequest Message Response Test

21 3.2.2.1.1 Definition

22 This test verifies that the access terminal responds to a *LocationRequest* message with a
23 *LocationNotification* message and to a *LocationAssignment* message with a *LocationComplete*
24 message.

25 3.2.2.1.2 Traceability

26 See section 3.5.4.1.2 of [1].

27 3.2.2.1.3 Test Procedure

- 28 a. Configure the access terminal to negotiate the use of the Default Packet
29 Application bound to the service access network (app type = 0x0002) during session
30 configuration. Cause the access terminal to open a connection with the access
31 network. Instruct the access terminal to transmit a *SessionClose* message to the
32 access network. Instruct the access terminal to start a new session with the
33 access network.

- 1 b. After the access network receives a *ConnectionClose* message from the access
2 terminal, instruct the access network to assign a non-NULL location value to the
3 access terminal via a *LocationAssignment* message.
- 4 c. Verify that the access terminal meets the minimum standard as per bullet 1 in
5 3.2.2.1.4.
- 6 d. Instruct the access network to send a *LocationRequest* message.
- 7 e. Verify that the access terminal meets the minimum standard as per bullet 2 in
8 3.2.2.1.4.
- 9 f. Instruct the access network to send a *LocationAssignment* message with
10 *LocationType* field set equal to '00'.
- 11 g. Wait for a *LocationComplete* message from the access terminal.
- 12 h. Instruct the access network to send a *LocationRequest* message.
- 13 i. Verify that the access terminal meets the minimum standard as per bullet in
14 3.2.2.1.4.

15 3.2.2.1.4 Minimum Standard

- 16 1. The access terminal shall respond to a *LocationAssignment* message with a
17 *LocationComplete* message.
- 18 2. The access terminal shall respond to a *LocationRequest* message with a
19 *LocationNotification* message and the *LocationNotification* message contains
20 *LocationValue*, which is identical to that assigned in step b.
- 21 3. The access terminal shall not include *LocationLength* and *LocationValue* fields in
22 the *LocationNotification* message.

23 3.3 Flow Control Protocol Tests

24 The tests in this section assume that the access terminal and the access network support
25 the Default Packet Application.

26 3.3.1 Access Network Tests

27 3.3.1.1 XonRequest and XoffRequest Message Response Test

28 3.3.1.1.1 Definition

29 This test verifies that the access network responds to a *XonRequest* message with a
30 *XonResponse* message and to a *XoffRequest* message with a *XoffResponse* message.

31 3.3.1.1.2 Traceability

32 See section 3.6.4.1.2.2 of [1].

1 3.3.1.1.3 Test Procedure

- 2 a. Configure the access terminal to negotiate the use of Default Packet Application
3 bound to the service access network (app subtype = 0x0002) during session
4 configuration. Instruct the access terminal to transmit a *SessionClose* message to
5 the access network. Instruct the access terminal to start a new session with the
6 access network.
- 7 b. Instruct the access terminal to set up a connection and establish a data call with
8 the access network. Initiate downloading of a file from the service network. A
9 representative data file is RAND200.BIN defined in ANNEX D of [2].
- 10 c. While the file download is in progress, instruct the access terminal to send a
11 *XoffRequest* message to the access network and cease transmission of RLP packets
12 on the Reverse Traffic Channel.
- 13 d. Verify that the access network meets the minimum standard as per bullet 1 in
14 3.3.1.1.4.
- 15 e. Instruct the access terminal to send a *XonRequest* message to the access network.
- 16 f. Verify that the access network meets the minimum standard as per bullet 2 in
17 3.3.1.1.4.
- 18 g. While the file download is in progress, instruct the access terminal to send a
19 *XoffRequest* message to the access network and cease transmission of RLP packets
20 on the Reverse Traffic Channel.
- 21 h. Instruct the access terminal to send an RLP packet to the access network.
- 22 i. Verify that the access network meets the minimum standard as per bullet 3 in
23 3.3.1.1.4.

24 3.3.1.1.4 Minimum Standard

- 25 1. The access network shall respond to a *XoffRequest* message from the access
26 terminal with a *XoffResponse* message and shall stop the flow of RLP packets.
- 27 2. The access network shall respond to a *XonRequest* message from the access
28 terminal with a *XonResponse* message and shall resume the flow of RLP packets.
- 29 3. The access network shall respond to an RLP packet from the access terminal by
30 resuming the flow of RLP packets on the Forward link.

31 3.3.2 Access Terminal Tests

32 3.3.2.1 DataReady Message Response Test

33 3.3.2.1.1 Definition

34 This test verifies that the access terminal responds to a *DataReady* message with a
35 *DataReadyAck* message.

1 3.3.2.1.2 Traceability

2 See section 3.6.4.1.2.1 of [1].

3 3.3.2.1.3 Test Procedure

4 a. Configure the access terminal to negotiate the use of Default Packet Application
5 bound to the service access network (app subtype = 0x0002) during session
6 configuration. Instruct the access terminal to transmit a *SessionClose* message to
7 the access network. Instruct the access terminal to start a new session with the
8 access network.

9 b. Instruct the access terminal to set up a connection and establish a data call with
10 the access network.

11 c. Instruct the access network to send a *DataReady* message to the access terminal.

12 d. Verify that the access terminal meets the minimum standard as per 3.3.2.1.4.

13 3.3.2.1.4 Minimum Standard

14 The access terminal shall respond to a *DataReady* message with a *DataReadyAck* message.
15

- 1 No Text.

1 **4 MULTI-FLOW APPLICATION PROTOCOL TESTS**

2 The tests in this section assume that the access terminal and the access network support
3 the Multi-Flow Packet Application. In this chapter the test procedure does not specify the
4 actual value NN for the RLP flow that is to be used for the test. Any RLP flow can be used for
5 the purpose of tests in this chapter. However, the same flow should be used for a test.

6 **4.1 Radio Link Protocol Tests**

7 4.1.1 Access Network RLP Tests

8 4.1.1.1 RLP Initialization Test

9 4.1.1.1.1 Definition

10 This test verifies that upon protocol initialization, the access network sets the RLP
11 sequence number of the first RLP Packet transmitted on the Forward Traffic Channel
12 equal to zero. The test procedure utilizes the fact that when a connection is opened by the
13 access terminal or the access network, the active RLP instance of the Packet Application
14 bound to the service access network will undergo initialization.

15 4.1.1.1.2 Traceability

16 See section 4.4.4.1.1 of [1].

17 4.1.1.1.3 Test Procedure

- 18 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
19 Application bound to the service access network (app type = 0x0005).
- 20 b. Set the active parameter of the attribute FlowMMidentificationFwd and
21 FlowMMidentificationRev to 0x01.
- 22 c. Instruct the access terminal to set up a connection and establish a data call with
23 the access network.
- 24 d. Initiate downloading of a file from the service access network and record the SEQ
25 field in the first RLP packet received at the access terminal.
- 26 e. Verify that the SEQ field in the first Forward Traffic Channel RLP packet meets the
27 minimum standard as per 4.1.1.1.4.

28 4.1.1.1.4 Minimum Standard

29 The SEQ field in the first Forward Traffic Channel RLP packet received from the access
30 network after connection establishment shall be set equal to zero.

1 4.1.1.2 RLP Sequence Number Increment Test

2 4.1.1.2.1 Definition

3 This test verifies that the basic RLP sequence number increment procedure in the access
4 network works correctly.

5 4.1.1.2.2 Traceability

6 See section 4.4.4.1.2 of [1].

7 4.1.1.2.3 Test Procedure

- 8 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
9 Application bound to the service access network (app type = 0x0005).
- 10 b. Set the active parameter of the attribute *FlowNMidentificationFwd* and
11 *FlowNMidentificationRev* to 0x01.
- 12 c. Instruct the access terminal to set up a connection and establish a data call with
13 the access network.
- 14 d. Initiate downloading of a file from the service access network via FTP. Record two
15 consecutive Forward Traffic Channel RLP packets sent by the access network.
- 16 e. Verify that the access network meets the minimum standard as per 4.1.1.2.4.

17 4.1.1.2.4 Minimum Standard

18 The RLP Sequence number (SEQ) in each first time transmitted RLP packet shall be set
19 equal to the sequence number of the immediately preceding first time transmitted RLP
20 packet plus the number of octets excluding the SEQ field included in that packet.

21 4.1.1.3 RLP Reset Test

22 4.1.1.3.1 Definition

23 This test verifies that the access network upon receiving an RLP *ResetRxIndication*
24 message sends an RLP *ResetRxComplete* message to the access terminal, and the RLP
25 sequence number in the first Forward Traffic Channel RLP packet is initialized to zero.

26 4.1.1.3.2 Traceability

27 See section 4.4.4.1.1.2.2 and 4.4.4.1.1.2.4 of [1].

28 4.1.1.3.3 Test Procedure

- 29 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
30 Application bound to the service access network (app type = 0x0005).
- 31 b. Set the active parameter of the attribute *FlowNMidentificationFwd* and
32 *FlowNMidentificationRev* to 0x01.

- 1 c. Instruct the access terminal to set up a connection and establish a data call with
2 the access network.
- 3 d. Initiate downloading of a file from the service access network.
- 4 e. While the file download is in progress, instruct the access terminal to send an RLP
5 *ResetRxIndication* message to the access network.
- 6 f. Verify that the access network meets the minimum standard as per bullet 1 in
7 4.1.1.3.4.
- 8 g. Record the SEQ field in the first RLP packet received from the access network
9 following the RLP Reset.
- 10 h. Verify that the SEQ field in the first Forward Traffic Channel RLP packet meets the
11 minimum standard as per bullet 2 in 4.1.1.3.4.

12 4.1.1.3.4 Minimum Standard

- 13 1. The access network shall send an RLP *ResetRxComplete* message in response to an
14 RLP *ResetRxIndication* message.
- 15 2. The access network shall initialize the RLP sequence number for the first RLP
16 packet equal to zero following the RLP reset.

17 4.1.1.4 RLP NAK Test

18 4.1.1.4.1 Definition

19 This test verifies that the access network sends RLP *Nak* messages on the Forward Traffic
20 Channel, when the access terminal does not send selected RLP octets in an octet stream
21 on the Reverse Traffic Channel.

22 4.1.1.4.2 Traceability

23 See section 4.4.4.1.3 of [1].

24 4.1.1.4.3 Test Procedure

- 25 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
26 Application bound to the service access network (app type = 0x0005).
- 27 b. Set the active parameter of the attribute *FlowNMIdentificationFwd* and
28 *FlowNMIdentificationRev* to 0x01.
- 29 c. Enable RLP *Nak* based retransmissions by setting the attribute
30 *FlowNMNakEnableRev* to 0x01 and disable Physical layer nak based retransmissions
31 by setting *FlowNNPhysicalLayerNakEnableRev* to 0x00.
- 32 d. Instruct the access terminal to set up a connection and establish a data call with
33 the access network.

- e. Initiate uploading of a file to the service access network. Record at the access terminal any Reverse Traffic Channel RLP packets dropped and any Forward Traffic Channel RLP *Nak* messages sent by the access network.
- f. At the access network, drop one Reverse Traffic Channel RLP packet with sequence number in the range [0,500].
- g. Verify that the access network meets the minimum standard as per 4.1.1.4.4.

4.1.1.4.4 Minimum Standard

The access network shall send an RLP *Nak* message to request selected RLP octets in an octet stream that were not transmitted by the access terminal on the Reverse Traffic Channel.

4.1.1.5 RLP Synchronization Loss Detection Test

4.1.1.5.1 Definition

This test verifies that when the access terminal *Naks* an RLP sequence number that has never been sent by the access network on the Forward Traffic Channel, then the access network initiates an RLP reset procedure.

4.1.1.5.2 Traceability

See section 4.4.4.1.2, 4.4.4.1.1.2.1 and 4.4.4.1.1.2.3 of [1].

4.1.1.5.3 Test Procedure

- a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet Application bound to the service access network (app type = 0x0005).
- b. Set the active parameter of the attribute *FlowNMidentificationFwd* and *FlowNMidentificationRev* to 0x01.
- c. Instruct the access terminal to set up a connection and establish a data call with the access network.
- d. Instruct the access terminal to send an RLP *Nak* message requesting an RLP octet with sequence number 2^{20} .
- e. Verify that the access network meets the minimum standard as per bullet 1 of 4.1.1.5.4.
- f. Verify that when the access network receives a *ResetTxIndicationAck* message from the access terminal it meets the minimum standard as per bullet 2 of 4.1.1.5.4

4.1.1.5.4 Minimum Standard

1. The access network shall send an RLP *ResetTxIndication* message when an RLP *Nak* message on the Reverse Traffic Channel requests an RLP octet with sequence number x in the range $[V(S), V(S) + 2^{(22-1)} - 1]$, where $V(S)$ is the sequence number of the next RLP data octet to be sent by the access network.

- 1 2. The access network shall send an RLP *ResetTxComplete* message when it receives
2 an RLP *ResetTxIndicationAck* message.

3 4.1.1.6 Basic File Transfer Test

4 4.1.1.6.1 Definition

5 This test verifies that the access network implementation of the RLP supports basic file
6 transfer functionality on the Forward Traffic Channel.

7 4.1.1.6.2 Traceability

8 See section 4.4.1 of [1].

9 4.1.1.6.3 Test Procedure

- 10 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
11 Application bound to the service access network (app type = 0x0005).
- 12 b. Set the active parameter of the attribute *FlowNMIentificationFwd* and
13 *FlowNMIentificationRev* to 0x01.
- 14 c. Configure the access terminal so that the effective Forward Traffic Channel packe t
15 error rate seen by the RLP is $1\% \pm 0.25\%$.
- 16 d. Instruct the access terminal to set up a connection and establish a data call with
17 the access network.
- 18 e. Initiate downloading of a 200 kbytes file from the service network via FTP. A
19 representative data file is *RAND200.BIN* defined in ANNEX D of [2].
- 20 f. Verify that the access network meets the minimum standard as per bullets 1 and 2
21 in 4.1.1.6.4.

22 4.1.1.6.4 Minimum Standard

- 23 1. The file shall be successfully transferred using the Forward Traffic Channel.
- 24 2. The received file shall be complete and identical in content to the original file.

25 4.1.2 Access Terminal RLP Tests

26 4.1.2.1 RLP Physical Layer NAK based Retransmission test

27 4.1.2.1.1 Definition

28 This test verifies that if an RLP belonging to Multi-Flow Packet Application at an access
29 terminal supporting Subtype 3 RTC MAC protocol receives a *ReverseTrafficPacketsMissed*
30 indication, then it shall retransmit the octets from the lost sub-packet if it is configured
31 with parameter *FlowNMPysicalLayerNakEnableRev* set to 0x01, subject to the constraints
32 that the lost octets are available for retransmission and have not been retransmitted. The
33 test utilizes the fact that when RLP *Nak* based retransmissions are turned off, an access

1 terminal can retransmit data only if `FlowNMPHysicalLayerNakEnableRev` is set to `0x01`, i.e.,
2 enabled.

3 4.1.2.1.2 Traceability

4 See section 4.4.4.2.1 of [1].

5 4.1.2.1.3 Test Procedure

- 6 a. Connect the sector to the access terminal antenna connector.
- 7 b. Set `Power` to `-75 dBm`.
- 8 c. Set `ReverseLinkSilenceDuration` to `'00'`.
- 9 d. Fix the RAB transmitted by the access network to `'0'` (unloaded) for the entire test
10 duration.
- 11 e. Instruct the access terminal to negotiate the use of Multi-Flow packet Application
12 bound to the service access network (app type = `0x0005`).
- 13 f. Set the active parameter of the attribute `FlowNMIdentificationFwd` and
14 `FlowNMIdentificationRev` to `0x01`.
- 15 g. Set the values for the MAC Flow to defaults for flow with `MACFlowID` equal to one as
16 specified in [1].
- 17 h. Enable MAC layer ARQ based retransmissions by setting
18 `FlowNMPHysicalLayerNakEnableRev` to `0x01`. During session configuration the
19 access network should propose attribute values `0x01` and `0x00` for
20 `FlowNMPHysicalLayerNakEnableRev` and ensure that the access terminal accepts
21 the value `0x01`.
- 22 i. Disable RLP *Nak* based retransmissions by setting `FlowNMNakEnableRev` to `0x00`.
- 23 j. After the connection has been established, configure the access network to always
24 set the H-ARQ, L-ARQ and P-ARQ bits to NAK.
- 25 k. At the access terminal log the number of bytes transmitted through RLP
26 retransmissions.
- 27 l. Instruct the access terminal to send a Ping packet directed to the access network.
- 28 m. Verify that the access terminal meets the minimum standard as per bullet 1 of
29 section 4.1.2.1.4.
- 30 n. Repeat steps a through g.
- 31 o. For the Multi-Flow Packet Application RLP, set the
32 `FlowNMPHysicalLayerNakEnableRev` to `0x00`.
- 33 p. Repeat steps i through l.
- 34 q. Verify that the access terminal meets the minimum standard as per bullet 2 of
35 section 4.1.2.1.4.

1 4.1.2.1.4 Minimum Standard

- 2 1. The number of bytes that the access terminal transmits through RLP
3 retransmissions should be greater than zero.
- 4 2. The number of bytes that the access terminal transmits through RLP
5 retransmissions should be equal to zero.

6 4.1.2.2 RLP Initialization Test

7 4.1.2.2.1 Definition

8 This test verifies that upon protocol initialization, the access terminal sets the RLP
9 sequence number of the first RLP packet transmitted on the Reverse Traffic Channel
10 equal to zero. The test procedure utilizes the fact that when a connection is opened by the
11 access terminal or the access network, the active RLP instance of the Packet Application
12 bound to the service access network will undergo initialization.

13 4.1.2.2.2 Traceability

14 See section 4.4.4.1.1 of [1].

15 4.1.2.2.3 Test Procedure

- 16 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
17 Application bound to the service access network (app type = 0x0005).
- 18 b. Set the active parameter of the attribute FlowNMidentificationFwd and
19 FlowNMidentificationRev to 0x01.
- 20 c. Instruct the access terminal to set up a connection and establish a data call with
21 the access network.
- 22 d. Initiate uploading of a file from the access terminal to the service access network
23 and record the SEQ field in the first RLP packet received at the access network.
- 24 e. Verify that the SEQ field in the first Reverse Traffic Channel RLP packet meets the
25 minimum standard as per 4.1.2.2.4.

26 4.1.2.2.4 Minimum Standard

27 The SEQ field in the first Reverse Traffic Channel RLP packet received from the access
28 terminal after connection establishment shall be set equal to zero.

29 4.1.2.3 RLP Sequence Number Increment Test

30 4.1.2.3.1 Definition

31 This test verifies that the basic sequence number increment procedure in the access
32 terminal works correctly.

1 4.1.2.3.2 Traceability

2 See section 4.4.4..2.1 of [1].

3 4.1.2.3.3 Test Procedure

- 4 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
5 Application bound to the service access network (app type = 0x0005).
- 6 b. Set the active parameter of the attribute *FlowMMidentificationFwd* and
7 *FlowMMidentificationRev* to 0x01.
- 8 c. Instruct the access terminal to set up a connection and establish a data call with
9 the access network.
- 10 d. Initiate uploading of a file from the access terminal to the service access network.
11 Record two consecutive Reverse Traffic Channel RLP packets sent by the access
12 terminal.
- 13 e. Verify that the test meets the minimum standard as per 4.1.2.3.4.

14 4.1.2.3.4 Minimum Standard

15 The RLP Sequence number (SEQ) in each new first time transmitted RLP packet shall be
16 set equal to the sequence number of the immediately preceding first-time transmitted RLP
17 packet plus the number of octets excluding the SEQ field included in that packet.

18 4.1.2.4 RLP Reset Test

19 4.1.2.4.1 Definition

20 This test verifies that the access terminal upon receiving an RLP *ResetRxIndication*
21 message sends an RLP *ResetRxIndicationAck* message to the access network, and the RLP
22 sequence number in the first Reverse Traffic Channel RLP packet is initialized to zero.

23 4.1.2.4.2 Traceability

24 See section 4.4.4.1.1.2.2 and 4.4.4.1.1.2.4 of [1].

25 4.1.2.4.3 Test Procedure

- 26 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
27 Application bound to the service access network (app type = 0x0005).
- 28 b. Set the active parameter of the attribute *FlowMMidentificationFwd* and
29 *FlowMMidentificationRev* to 0x01.
- 30 c. Instruct the access terminal to set up a connection and establish a data call with
31 the access network.
- 32 d. Initiate uploading of a file from the access terminal to the service access network.
- 33 e. While the file upload is in progress, instruct the access network to send an RLP
34 *ResetRxIndication* message to the access terminal.

- 1 f. Verify that the access terminal meets the minimum standard as per bullet 1 in
2 4.1.2.4.4.
- 3 g. Record the SEQ field in the first RLP packet received from the access terminal
4 following the RLP Reset.
- 5 h. Verify that the SEQ field in the first Reverse Traffic Channel RLP packet meets the
6 minimum standard as per bullet 2 in 4.1.2.4.4.

7 4.1.2.4.4 Minimum Standard

- 8 1. The access terminal shall send an RLP *ResetRxComplete* message to the access
9 network in response to an RLP *ResetRxIndication* message.
- 10 2. The access terminal shall initialize the sequence number (SEQ) in the Reverse
11 Traffic Channel RLP packet equal to zero following the RLP reset.

12 4.1.2.5 RLP NAK Test

13 4.1.2.5.1 Definition

14 This test verifies that the access terminal sends RLP *Nak* messages on the Reverse Traffic
15 Channel when the access network does not send selected RLP octets in an octet stream on
16 the Forward Traffic Channel.

17 4.1.2.5.2 Traceability

18 See section 4.4.4.2.2 of [1].

19 4.1.2.5.3 Test Procedure

- 20 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
21 Application bound to the service access network (app type = 0x0005).
- 22 b. Set the active parameter of the attribute *FlowMMidentificationFwd* and
23 *FlowMMidentificationRev* to 0x01.
- 24 c. Instruct the access terminal to set up a connection and establish a data call with
25 the access network.
- 26 d. Initiate downloading of a file from the service access network. Begin recording at
27 the access network any Forward Traffic Channel RLP packets dropped and any RLP
28 *Nak* messages sent by the access terminal.
- 29 e. Drop one Forward Traffic Channel RLP packet at the access network with sequence
30 number in the range [0, 500].
- 31 f. Verify that at least one RLP *Nak* message corresponding to the dropped RLP octets is
32 received from the access terminal as per the minimum standard 4.1.2.5.4.

1 4.1.2.5.4 Minimum Standard

2 The access terminal shall send RLP *Nak* messages on the Reverse Traffic Channel to
3 request select RLP octets in an octet stream that were not transmitted by the access
4 network.

5 4.1.2.6 RLP Synchronization Loss Detection Test

6 4.1.2.6.1 Definition

7 This test verifies that when the access network *Naks* an RLP sequence number that has
8 never been sent by the access terminal on the Reverse Traffic Channel, the access
9 terminal initiates an RLP reset procedure.

10 4.1.2.6.2 Traceability

11 See section 4.4.4.1.1.2.1, 4.4.4.1.1.2.2, 4.4.4.1.1.2.3 and 4.4.4.1.1.2.5 of [1].

12 4.1.2.6.3 Test Procedure

- 13 a. Instruct the access terminal to negotiate the use of Multi-Flow Packet Application
14 bound to the service access network (app type = 0x0005).
- 15 b. Set the active parameter of the attribute *FlowNMidentificationFwd* and
16 *FlowNMidentificationRev* to 0x01.
- 17 c. Instruct the access terminal to set up a connection and establish a data call with
18 the access network.
- 19 d. Instruct the access network to send an RLP *Nak* message requesting an RLP octet
20 with sequence number 2^{20} .
- 21 e. Verify that the access terminal meets the minimum standard as per bullet 1 of
22 4.1.2.6.4.
- 23 f. Verify that when the access terminal receives the RLP *ResetTxIndicationAck*
24 message it meets the minimum standard as per bullet 2 of 4.1.2.6.4.

25 4.1.2.6.4 Minimum Standard

- 26 1. The access terminal shall send an RLP *ResetTxIndication* message, when an RLP
27 *Nak* message on the Forward Traffic Channel requests an RLP octet with sequence
28 number x in the range $[V(S), V(S) + 2^{(22-1)} - 1]$, where $V(S)$ is the sequence number of
29 the next RLP data octet to be sent by the access terminal.
- 30 2. The access terminal shall send an RLP *ResetTxComplete* message when it receives
31 an RLP *ResetTxIndicationAck* message.

1 4.1.2.7 Basic File Transfer Test

2 4.1.2.7.1 Definition

3 This test verifies that access terminal implementation of the RLP supports basic file
4 transfer functionality on the Reverse Traffic Channel.

5 4.1.2.7.2 Traceability

6 See section 4.4.1 of [1].

7 4.1.2.7.3 Test Procedure

- 8 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
9 Application bound to the service access network (app type = 0x0005).
- 10 b. Set the active parameter of the attribute *FlowNMidentificationFwd* and
11 *FlowNMidentificationRev* to 0x01.
- 12 c. Configure the access terminal so that the effective Reverse Traffic Channel packet
13 error rate seen by the RLP in the access network is $1\% \pm 0.25\%$.
- 14 d. Instruct the access terminal to set up a connection and establish a data call with
15 the access network.
- 16 e. Initiate uploading of a 200 kbytes file from the access terminal to the service
17 access network. A representative data file is RAND200.BIN defined in ANNEX D of
18 [2].
- 19 f. Verify that the access terminal meets the minimum standard as per bullets 1 and
20 2 in 4.1.2.7.4.

21 4.1.2.7.4 Minimum Standard

- 22 1. The file shall be successfully transferred using the Reverse Traffic Channel.
- 23 2. The received file shall be complete and identical in content to the original file.

24 **4.2 Data Over Signaling Protocol Tests**

25 4.2.1 Access Network Tests

26 4.2.1.1 Data Over Signaling Initialization Test

27 4.2.1.1.1 Definition

28 This test verifies the functionality of the Data Over Signaling Protocol when access
29 network is the transmitter and the access terminal is the receiver. This test assumes
30 that the data arriving at the access network and access terminal can be transmitted using
31 the Data Over Signaling Protocol. Specifically, test verifies that after initialization, the
32 access network transmits the first *DataOverSignaling* message with *MessageSequence*
33 field set to 0.

1 4.2.1.1.2 Traceability

2 See section 4.5 of [1] and [5].

3 4.2.1.1.3 Test Procedure

- 4 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
- 5 Application bound to the service access network (app type = 0x0005).
- 6 b. Set the ProtocolIdentifier field of the FlowNMMHigherLayerProtocolFwd to HDLC
- 7 framing.
- 8 c. During Session Configuration, set the Active parameter of FlowNMIdentificationFwd
- 9 attribute to 0x01.
- 10 d. Set the ReservationLabel for FlowNMReservationFwd to High Priority Signaling. Set
- 11 FlowNMDataOverSignalingAllowedRev to 0x01.
- 12 e. Instruct the access terminal to send a *ReservationOn* message for the flow whose
- 13 data is to be carried using *DataOverSignaling* message to the access network and
- 14 ensure that the access network responds with a *ReservationAccept* message.
- 15 f. Close the connection and make sure that the data arriving at the access network
- 16 for reservation label High Priority Signaling can be sent using the Data Over
- 17 Signaling protocol.
- 18 g. Transmit a zero byte ping packet from the access network directed to the access
- 19 terminal using the Data Over Signaling Protocol and setting the AckRequired field
- 20 of the *DataOverSignaling* message to 1 and Reset field set to 0. Note, any higher
- 21 layer source that generates a *DataOverSignaling* message can be used instead of
- 22 ping.
- 23 h. Verify that the *DataOverSignaling* message transmitted by the access network
- 24 meets the minimum standard as per 4.2.1.1.4.

25 4.2.1.1.4 Minimum Standard

26 The MessageSequenceNumber field in the *DataOverSignaling* message sent by the access

27 network is 0.

28 4.2.1.2 Data Over Signaling Message Transmission and Response Test

29 4.2.1.2.1 Definition

30 This test verifies the functionality of the Data Over Signaling Protocol when access

31 terminal is the transmitter and the access network is the receiver. This test assumes

32 that the data arriving at the access network and access terminal can be transmitted using

33 the Data Over Signaling Protocol. The first sub-test verifies that the access network

34 responds to the first *DataOverSignaling* message received from the access terminal with a

35 *DataOverSignalingAck* message with AckSequence field set to 0. The second sub-test

36 verifies that the access network increments the MessageSequence correctly. The third

1 sub-test verifies that the access network discards *DataOverSignaling* messages that have
2 incorrect MessageSequence number.

3 4.2.1.2.2 Traceability

4 See section 4.5 and 4.8.1 of [1] and [5].

5 4.2.1.2.3 Test Procedure

- 6 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
7 Application bound to the service access network (app type = 0x0005).
- 8 b. Set the ProtocolIdentifier field of the FlowNMHigherLayerProtocolRev to HDLC
9 framing.
- 10 c. During Session Configuration, set the active parameter of the
11 FlowNMIdentificationRev attribute to 0x01.
- 12 d. Set the ReservationLabel for the FlowNMReservationRev to High Priority Signaling.
13 Set FlowNMDataOverSignalingAllowedRev to 0x01.
- 14 e. Instruct the access terminal to send a *ReservationOn* message for the flow whose
15 data is to be carried using *DataOverSignaling* message to the access network and
16 ensure that the access network responds with a *ReservationAccept* message.
- 17 f. Close the connection and make sure that the data arriving at the access terminal
18 for high priority can be sent using the Data Over Signaling protocol.
- 19 g. Transmit a zero byte ping packet from the access terminal directed to the access
20 network using the Data Over Signaling Protocol and setting the AckRequired field of
21 the *DataOverSignaling* message to '1'. Note, any higher layer source that generates
22 a *DataOverSignaling* message can be used instead of ping, as long as the delivery to
23 the higher layers at the access network can be verified.
- 24 h. Verify that the access network meets the minimum standard as specified in the
25 bullet 1 of 4.2.1.2.4.
- 26 i. Repeat step g.
- 27 j. Verify that access network meets the minimum standards as per bullet 2 of
28 4.2.1.2.4.
- 29 k. Repeat step g, with the exception that MessageSequence field of the
30 *DataOverSignaling* message is set to zero.
- 31 l. Verify that that the access network meets the minimum standard as per bullet 3 of
32 4.2.1.2.4

33 4.2.1.2.4 Minimum Standard

- 34 1. Upon receiving the *DataOverSignaling* message with MessageSequence field set to
35 zero, access network responds with a *DataOverSignalingAck* message with

1 AckSequence field set to zero and the payload of the *DataOverSignaling* message is
2 delivered to the higher layer protocol.

3 2. Upon receiving the *DataOverSignaling* message with MessageSequence field set to
4 one, access network responds with a *DataOverSignalingAck* message with
5 AckSequence field set to one and the payload of the *DataOverSignaling* message is
6 delivered to the higher layer protocol.

7 3. Upon receiving the second *DataOverSignaling* message with sequence field set to
8 zero, the access network discards the message and the payload carried by the
9 *DataOverSignaling* message is not delivered to the higher layer protocol.

10 4.2.2 Access Terminal Tests

11 4.2.2.1 Data Over Signaling Initialization Test

12 4.2.2.1.1 Definition

13 This test verifies the functionality of the Data Over Signaling Protocol when access
14 terminal is the transmitter and the access network is the receiver. This test assumes
15 that the data arriving at the access network and access terminal can be transmitted using
16 the Data Over Signaling Protocol. Specifically, test verifies that after initialization, the
17 access terminal transmits the first *DataOverSignaling* message with MessageSequence
18 field set to 0.

19 4.2.2.1.2 Traceability

20 See section 4.5 and 4.8.1 of [1] and [5].

21 4.2.2.1.3 Test Procedure

- 22 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
23 Application bound to the service access network (app type = 0x0005).
- 24 b. Set the ProtocolIdentifier field of the FlowNMHigherLayerProtocolRev to HDLC
25 framing.
- 26 c. During Session Configuration, set the active parameter of the
27 FlowNMIdentificationRev attribute to 0x01.
- 28 d. Set the ReservationLabel for the FlowNMReservationRev to High Priority Signaling.
29 Set FlowNMDataOverSignalingAllowedRev to 0x01.
- 30 e. Instruct the access terminal to send a *ReservationOn* message for the flow whose
31 data is to be carried using *DataOverSignaling* message to the access network and
32 ensure that the access network responds with a *ReservationAccept* message.
- 33 f. Close the connection and make sure that the data arriving at the access terminal
34 for high priority can be sent using the Data Over Signaling protocol.
- 35 g. Transmit a zero byte ping packetaccess terminal directed to the access network
36 using the Data Over Signaling Protocol and setting the AckRequired field of the

1 *DataOverSignaling* message to '1'. Note, any higher layer source that generates a
2 *DataOverSignaling* message can be used instead of ping.

3 h. Verify that the *DataOverSignaling* message transmitted by the access terminal
4 meets the minimum standard as per 4.2.2.1.4.

5 4.2.2.1.4 Minimum Standard

6 The MessageSequenceNumber field in the *DataOverSignaling* message sent by the access
7 terminal is zero.

8 4.2.2.2 Data Over Signaling Message Transmission and Response Test

9 4.2.2.2.1 Definition

10 This test verifies the functionality of the Data Over Signaling Protocol when access
11 network is the transmitter and the access terminal is the receiver. This test assumes
12 that the data arriving at the access network and access terminal can be transmitted using
13 the Data Over Signaling Protocol. The first sub-test verifies that the access terminal
14 responds to the first *DataOverSignaling* message received from the access network with a
15 *DataOverSignalingAck* with AckSequence field set to zero. The second sub-test verifies that
16 the access terminal increments the MessageSequence correctly. The third sub-test
17 verifies that the access terminal discards *DataOverSignaling* messages that have incorrect
18 MessageSequence number. The fourth sub-test verifies that the access terminal responds
19 to a *DataOverSignaling* message with Reset field set to '1', with a *DataOverSignalingAck*
20 message with AckSequence field set to zero.

21 4.2.2.2.2 Traceability

22 See section 4.5 of [1] and [5].

23 4.2.2.2.3 Test Procedure

24 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
25 Application bound to the service access network (app type = 0x0005).

26 b. Set the ProtocolIdentifier field of the FlowNMHigherLayerProtocolFwd to HDLC
27 framing.

28 c. During Session Configuration, set the Active parameter of FlowNMidentificationFwd
29 attribute to 0x01.

30 d. Set the ReservationLabel for FlowNMReservationFwd to High Priority Signaling. Set
31 FlowNMDataOverSignalingAllowedRev to 0x01.

32 e. Instruct the access terminal to send a *ReservationOn* message for the flow whose
33 data is to be carried using *DataOverSignaling* message to the access network and
34 ensure that the access network responds with a *ReservationAccept* message.

35 f. Close the connection and make sure that the data arriving at the access network
36 for reservation label High Priority Signaling can be sent using the Data Over
37 Signaling protocol.

- 1 g. Transmit a 0 byte ping packet from the access network directed to the access
2 terminal using the Data Over Signaling Protocol and setting the AckRequired field
3 of the *DataOverSignaling* message to '1' and reset field set to '0'. Note, any higher
4 layer source that generates DataOverSignaling message can be used instead of a
5 ping packet, as long as the delivery to the higher layers at the access terminal can
6 be verified.
- 7 h. Verify that the access terminal meets the minimum standard as specified in the
8 bullet 1 of 4.2.2.2.4.
- 9 i. Repeat step g.
- 10 j. Verify that access terminal meets the minimum standards as per bullet 2 of
11 4.2.2.2.4.
- 12 k. Repeat step g, with the exception that MessageSequence field of the
13 *DataOverSignaling* message is set to zero.
- 14 l. Verify that that the access terminal meets the minimum standard as per bullet 3 of
15 4.2.2.2.4.
- 16 m. Repeat step l, with the exception that the reset field of the *DataOverSignaling*
17 message is set to '1'.
- 18 n. Verify that that the access terminal meets the minimum standard as per bullet 4 of
19 4.2.2.2.4.

20 4.2.2.2.4 Minimum Standard

- 21 1. Upon receiving the *DataOverSignaling* message with MessageSequence field zero,
22 the access terminal responds with a *DataOverSignalingAck* message with
23 AckSequence field set to zero and the payload of the *DataOverSignaling* message is
24 delivered to the higher layer protocol.
- 25 2. Upon receiving the *DataOverSignaling* message with MessageSequence field one,
26 the access terminal responds with a *DataOverSignalingAck* message with
27 AckSequence field set to one and the payload of the *DataOverSignaling* message is
28 delivered to the higher layer protocol.
- 29 3. Upon receiving the second *DataOverSignaling* message with sequence field set to
30 zero, the access terminal shall discard it and the payload of the *DataOverSignaling*
31 message is not delivered to the higher layer protocol.
- 32 4. Upon receiving the *DataOverSignaling* message with Reset field set to '1', the access
33 terminal responds with a *DataOverSignalingAck* message with AckSequence field
34 set to zero and the payload carried in the *DataOverSingaling* message is delivered to
35 the higher layer protocol.

36 **4.3 Location Update Protocol Tests**

37 These tests are applicable if the access terminal supports the Multi-Flow Packet
38 Application.

1 4.3.1 Access Network Tests

2 None

3 4.3.2 Access Terminal Tests

4 4.3.2.1 LocationRequest Message Response Test

5 4.3.2.1.1 Definition

6 This test verifies that the access terminal responds to a *LocationRequest* message with a
7 *LocationNotification* message and to a *LocationAssignment* message with a *LocationComplete*
8 message.

9 4.3.2.1.2 Traceability

10 See section 4.6.4.1.2 of [1].

11 4.3.2.1.3 Test Procedure

- 12 a. Instruct the access terminal to negotiate the use of the Multi-Flow Packet
13 Application bound to the service access network (app type = 0x0005). Cause the
14 access terminal to open a connection with the access network.
- 15 b. After the access network receives a *ConnectionClose* message from the access
16 terminal, instruct the access network to assign a non-NULL location value to the
17 access terminal via a *LocationAssignment* message.
- 18 c. Verify that the access terminal meets the minimum standard as per bullet 1 in
19 4.3.2.1.4.
- 20 d. Instruct the access network to send a *LocationRequest* message.
- 21 e. Verify that the access terminal meets the minimum standard as per bullet 2 in
22 4.3.2.1.4.
- 23 f. Instruct the access network to send a *LocationAssignment* message with
24 LocationType field set equal to '00'.
- 25 g. Wait for a *LocationComplete* message from the access terminal.
- 26 h. Instruct the access network to send a *LocationRequest* message.
- 27 i. Verify that the access terminal meets the minimum standard as per bullet 3 in
28 4.3.2.1.4.

29 4.3.2.1.4 Minimum Standard

- 30 1. The access terminal shall respond to a *LocationAssignment* message with a
31 *LocationComplete* message.
- 32 2. The access terminal shall respond to a *LocationRequest* message with a
33 *LocationNotification* message and the *LocationNotification* message contains
34 LocationValue, which is identical to that assigned in step b.

- 1 3. The access terminal shall not include *LocationLength* and *LocationValue* fields in
2 the *LocationNotification* message.

3 4.3.2.2 *StorageBLOBRequestServiceNetworkIDrequest* and *StorageBLOBNotification*
4 *ServiceNetworkIDAssignment* message Response Test

5 4.3.2.2.1 Definition

6 This test verifies that the access terminal responds to a *StorageBLOBRequest* message with
7 a *StorageBLOBNotification* message and to a *StorageBLOBAssignment* message with a
8 *StorageBLOBComplete* message.

9 4.3.2.2.2 Traceability

10 See section 4.6.4.1.2 of [1].

11 4.3.2.2.3 Test Procedure

- 12 a. Instruct the access network to negotiate the use of the Multi-Flow Packet
13 Application bound to the service access network (app type = 0x0005).
- 14 b. Instruct the access network to assign a non-NULL value of *StorageBLOB*,
15 *StorageBLOBType*, and *StorageBLOBLength* to the access terminal via a
16 *StorageBLOBAssignment* message. Ensure that the *StorageBLOBLength* is equal to
17 the length of *StorageBLOB* in octets.
- 18 c. Verify that the access terminal meets the minimum standard as per bullet 1 in
19 4.3.2.2.4
- 20 d. Instruct the access network to send a *StorageBLOBRequest* message.
- 21 e. Verify that the access terminal meets the minimum standard as per bullet 2 in
22 4.3.2.1.4.
- 23 f. Instruct the access network to assign a NULL value of *StorageBLOB* to the access
24 terminal via a *StorageBLOBAssignment* message. Ensure that the *StorageBLOBType*
25 and *StorageBLOBLength* are set to zero and the *StorageBLOB* field is omitted in the
26 *StorageBLOBAssignment* message.
- 27 g. Wait for a *StorageBLOBComplete* message from the access terminal.
- 28 h. Instruct the access network to send a *StorageBLOBRequest* message.
- 29 i. Verify that the access terminal meets the minimum standard as per bullet 3 in
30 4.3.2.2.4.

31 4.3.2.2.4 Minimum Standard

- 32 1. The access terminal shall respond to the *StorageBLOBAssignment* message with a
33 *StorageBLOBComplete* message.
- 34 2. The access terminal shall respond to the *StorageBLOBRequest* message with a
35 *StorageBLOBNotification* message and the *StorageBLOBNotification* message contains

1 StorageBLOB, StorageBLOBType, and StorageBLOBLength values that are identical
2 to that assigned in step b of 4.3.2.2.2.

3 3. The access terminal shall respond to the *StorageBLOBRequest* message with a
4 *StorageBLOBNotification* message and shall set the StorageBLOBLength field to zero
5 and omit the StorageBLOB field in the *StorageBLOBNotification* message.

6 **4.4 Flow Control Protocol Tests**

7 The tests in this section assume that the access terminal and the access network support
8 the Multi-Flow Packet Application.

9 4.4.1 Access Network Tests

10 4.4.1.1 XonRequest and XoffRequest Message Response Test

11 4.4.1.1.1 Definition

12 This test verifies that the access network responds to an *XonRequest* message with an
13 *XonResponse* message and to an *XoffRequest* message with an *XoffResponse* message.

14 4.4.1.1.2 Traceability

15 See section 4.7.4.1.3.2 of [1].

16 4.4.1.1.3 Test Procedure

- 17 a. Instruct the access terminal to negotiate the use of Multi-Flow Packet Application
18 bound to the service access network (app subtype = 0x0005).
- 19 b. Instruct the access terminal to set up a connection and establish a data call with
20 the access network. Initiate downloading of a file from the service network. A
21 representative data file is RAND200.BIN defined in ANNEX D of [2].
- 22 c. While the file download is in progress, instruct the access terminal to send an
23 *XoffRequest* message to the access network and cease transmission of RLP packets
24 on the Reverse Traffic Channel.
- 25 d. Verify that the access network meets the minimum standard as per bullet 1 in
26 4.4.1.1.4.
- 27 e. Instruct the access terminal to send an *XonRequest* message to the access network.
- 28 f. Verify that the access network meets the minimum standard as per bullet 2 in
29 4.4.1.1.4.
- 30 g. While the file download is in progress, instruct the access terminal to send an
31 *XoffRequest* message to the access network and cease transmission of RLP packets
32 on the Reverse Traffic Channel.
- 33 h. Instruct the access terminal to send an RLP packet to the access network.

- 1 i. Verify that the access network meets the minimum standard as per bullet 3 in
2 4.4.1.1.4.

3 4.4.1.1.4 Minimum Standard

- 4 1. The access network shall respond to an *XoffRequest* message from the access
5 terminal with an *XoffResponse* message and shall stop the flow of RLP packets.
6 2. The access network shall respond to an *XonRequest* message from the access
7 terminal with an *XonResponse* message and shall resume the flow of RLP packets.
8 3. The access network shall respond to an RLP packet from the access terminal by
9 resuming the flow of RLP packets on the Forward link.

10 4.4.2 Access Terminal Tests

11 4.4.2.1 DataReady Message Response Test

12 4.4.2.1.1 Definition

13 This test verifies that the access terminal responds to a *DataReady* message with a
14 *DataReadyAck* message.

15 4.4.2.1.2 Traceability

16 See section 4.7.4.1.1 of [1].

17 4.4.2.1.3 Test Procedure

- 18 a. Instruct the access terminal to negotiate the use of Multi-Flow Packet Application
19 bound to the service access network (app subtype = 0x0005).
20 b. Instruct the access terminal to set up a connection and establish a data call with
21 the access network.
22 c. Instruct the access network to send a *DataReady* message to the access terminal.
23 d. Verify that the access terminal meets the minimum standard as per 4.4.2.1.4

24 4.4.2.1.4 Minimum Standard

25 The access terminal shall respond to a *DataReady* message with a *DataReadyAck* message.
26
27
28
29
30
31

1 **5 STREAM LAYER PROTOCOL TESTS**

2 This section includes tests for the Default Stream Protocol.

3 **5.1 Default Stream Protocol Tests**

4 5.1.1 Access Network Tests

5 5.1.1.1 ConfigurationRequest Message Response Test

6 5.1.1.1.1 Definition

7 This test verifies that the access network responds to a Stream Protocol
8 *ConfigurationRequest* message with a Stream Protocol *ConfigurationResponse* message.

9 5.1.1.1.2 Traceability

10 See section 13.7 of [1].

11 5.1.1.1.3 Test Procedure

- 12 a. Instruct the access terminal to set up a connection with the access network.
- 13 b. Instruct the access terminal to send a Stream Protocol *ConfigurationRequest*
14 message.
- 15 c. Verify that the access network meets the minimum standard as per 5.1.1.1.4.

16 5.1.1.1.4 Minimum Standard

17 The access network shall respond to a Stream Protocol *ConfigurationRequest* message with
18 a Stream Protocol *ConfigurationResponse* message.

19 5.1.2 Access Terminal Tests

20 5.1.2.1 ConfigurationRequest Message Response Test

21 5.1.2.1.1 Definition

22 This test verifies that the access terminal responds to a Stream Protocol
23 *ConfigurationRequest* message with a Stream Protocol *ConfigurationResponse* message.

24 5.1.2.1.2 Traceability

25 See section 13.7 of [1].

26 5.1.2.1.3 Test Procedure

- 27 a. Instruct the access terminal to set up a connection with the access network.
- 28 b. Instruct the access network to send a Session Configuration Protocol
29 *ConfigurationStart* message.

1 c. After the receipt of a Session Configuration Protocol *ConfigurationComplete* message
2 from the access terminal, instruct the access network to send a Stream Protocol
3 *ConfigurationRequest* message.

4 d. Verify that the access terminal meets the minimum standard as per 5.1.2.1.4.

5 5.1.2.1.4 Minimum Standard

6 The access terminal shall respond to a Stream Protocol *ConfigurationRequest* message with
7 a Stream Protocol *ConfigurationResponse* message.

1 **6 SESSION LAYER TESTS**

2 This section includes tests for Session Layer of [1].

3 **6.1 Default Session Management Protocol Tests**

4 6.1.1 Access Network Tests

5 6.1.1.1 KeepAliveRequest Message Response Test

6 6.1.1.1.1 Definition

7 This test verifies that the access network responds to a *KeepAliveRequest* message from
8 the access terminal with a *KeepAliveResponse* message.

9 6.1.1.1.2 Traceability

10 See section 6.2.6.1.6.1 of [1].

11 6.1.1.1.3 Test Procedure

- 12 a. Instruct the access terminal to send a *KeepAliveRequest* message to the access
13 network.
- 14 b. Verify that the access network meets the minimum standard as per 6.1.1.1.4.

15 6.1.1.1.4 Minimum Standard

16 The access network shall respond to a *KeepAliveRequest* message from the access terminal
17 with a *KeepAliveResponse* message.

18 6.1.1.2 ConfigurationRequest Message Response Test

19 6.1.1.2.1 Definition

20 This test verifies that the access network responds to a Session Management Protocol
21 *ConfigurationRequest* message with a Session Management Protocol *ConfigurationResponse*
22 message.

23 6.1.1.2.2 Traceability

24 See section 6.2.5 and 13.7 of [1].

25 6.1.1.2.3 Test Procedure

- 26 a. Instruct the access terminal to set up a connection with the access network.
- 27 b. Instruct the access terminal to send a Session Management Protocol
28 *ConfigurationRequest* message.
- 29 c. Verify that the access network meets the minimum standard as per 6.1.1.2.4.

1 6.1.1.2.4 Minimum Standard

2 The access network shall respond to a Session Management Protocol *ConfigurationRequest*
3 message with a Session Management Protocol *ConfigurationResponse* message.

4 6.1.1.3 Routing of UATI Assignment Message

5 6.1.1.3.1 Definition

6 This section verifies the access network processing of the *UATIRequest* message.

7 In Test 1, the two sectors in the test belong to the same subnet. This test verifies that the
8 two sectors reply to the *UATIRequest* message by sending a *UATIAssignment* message.

9 In Test 2, the two sectors in the test belong to different subnets. This test verifies that at
10 least the sector belonging to the subnet that the access terminal simulator is currently
11 monitoring replies to the *UATIRequest* message by sending a *UATIAssignment* message.

12 6.1.1.3.2 Traceability

13 See section 6.3.7.1.5.2 and 8.8.6.1.5.1 of [1].

14 6.1.1.3.3 Test Procedure

- 15 a. Configure the two sectors under test and an access terminal simulator as shown in
16 Figure 12.5.
- 17 b. The access terminal simulator shall not be in an active session at the beginning of
18 the test.
- 19 c. Adjust the forward link attenuators so that the received signal strength, at the
20 access terminal simulator, from Sector 1 and Sector 2 are approximately the same
21 (± 0.5 dB). Both sectors shall be visible for the access terminal simulator.
- 22 d. Configure Sector 1 and Sector 2 so that they belong to the same subnet.
- 23 e. Set the access terminal simulator to initiate a connection. Since the access
24 terminal simulator does not have an active session, it shall send a *UATIRequest*
25 message in the Access Channel to get a UATI address.
- 26 f. Record the content of the *RouteUpdate* message sent by the access terminal
27 simulator in the Access Channel.
- 28 g. Monitor the message transmissions from Sector 1 and Sector 2 and verify that the
29 access network meets the minimum standard as per bullet 1 of section 6.1.1.3.4.
- 30 h. Release the previous session at the access terminal simulator.
- 31 i. Configure Sector 1 and Sector 2 so that they belong to different subnets.
- 32 j. Set the access terminal simulator to initiate a connection. Since the access
33 terminal simulator does not have any active session, it shall send a *UATIRequest*
34 message in the Access Channel to get a UATI address.

1 k. Record the content of the *RouteUpdate* message sent by the access terminal
2 simulator in the Access Channel.

3 1. Monitor the message transmissions from Sector 1 and Sector 2 and verify that the
4 access network meets the minimum standard as per bullet 2 of section 6.1.1.3.4.

5 6.1.1.3.4 Minimum Standard

6 1. Both sectors listed in the *RouteUpdate* message that the access terminal simulator
7 sent on the Access Channel shall transmit a *UATIAssignment* message as a
8 response to the *UATIRequest* message sent by the access terminal simulator. Both
9 sectors shall transmit the message at least once in the same synchronous or sub-
10 synchronous capsule.

11 2. Sector 1 shall transmit a *UATIAssignment* message as a response to the *UATIRequest*
12 message sent by the access terminal simulator.

13 Note: The *UATIRequest* message and the *RouteUpdate* message are included in the same
14 Access Channel transmission.

15 6.1.1.4 Invalid UATI processing

16 6.1.1.4.1 Definition

17 This section verifies the behavior of the access network when there is an access terminal
18 with an unrecognizable UATI.

19 6.1.1.4.2 Traceability

20 See section 6.2.6.1.7 and 9.4.8 of [1].

21 6.1.1.4.3 Test Procedure

22 Refer to Figure 12.4 for a functional block diagram of the test setup.

23 a. Configure the sectors under test and an access terminal simulator.

24 b. The access network and the access terminal simulator shall be in an active
25 session at the beginning of the test.

26 c. Set the access terminal simulator to change its UATI address and Color Code.

27 d. Page the access terminal simulator.

28 e. Monitor the access network behavior and verify that the access network meets the
29 minimum standard as per section 6.1.1.4.4.

30 6.1.1.4.4 Minimum Standard

31 The access network shall send a *SessionClose* message in response to the access terminal
32 simulator probe. The access network should send the *SessionClose* message within 1.2
33 seconds of the reception of the access terminal simulator probe.

1 6.1.2 Access Terminal Tests

2 6.1.2.1 KeepAliveRequest Message Response Test

3 6.1.2.1.1 Definition

4 This test verifies that the access terminal responds to a *KeepAliveRequest* message from
5 the access network with a *KeepAliveResponse* message.

6 6.1.2.1.2 Traceability

7 See section 6.2.6.1.6.1 of [1].

8 6.1.2.1.3 Test Procedure

- 9 a. Instruct the access terminal to open a connection with the access network.
- 10 b. After the access network has received the *Connectionclose* message, instruct the
11 access network to send a *KeepAliveRequest* message to the access terminal.
- 12 c. Verify that the access terminal meets the minimum standard as per 6.1.2.1.4.

13 6.1.2.1.4 Minimum Standard

14 The access terminal shall respond to a *KeepAliveRequest* message from the access network
15 with a *KeepAliveResponse* message.

16 6.1.2.2 SessionClose Message Response Test

17 6.1.2.2.1 Definition

18 This test verifies that the access terminal responds to a *SessionClose* message from the
19 access network with a *SessionClose* message.

20 6.1.2.2.2 Traceability

21 See section 6.2.6.1.2 of [1].

22 6.1.2.2.3 Test Procedure

- 23 a. Instruct the access terminal to set up a session with the access network. Instruct
24 the access terminal to open a connection with the access network.
- 25 b. After the access network has received the *Connectionclose* message, instruct the
26 access network to send a *SessionClose* message.
- 27 c. Verify that the access terminal meets the minimum standard as per 6.1.2.2.4.

28 6.1.2.2.4 Minimum Standard

29 The access terminal shall respond with a *SessionClose* message.

6.1.2.3 ConfigurationRequest Message Response Test

6.1.2.3.1 Definition

This test verifies that the access terminal responds to a Session Management Protocol *ConfigurationRequest* message with a Session Management Protocol *ConfigurationResponse* message.

6.1.2.3.2 Traceability

See section 6.2.5 and 13.7 of [1].

6.1.2.3.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network.
- b. Instruct the access network to send a Session Configuration Protocol *ConfigurationStart* message.
- c. When the access network receives a Session Configuration Protocol *ConfigurationComplete* message, instruct the access network to send a Session Management Protocol *ConfigurationRequest* message to the access terminal.
- d. Verify that the access terminal meets the minimum standard as per 6.1.2.3.4.

6.1.2.3.4 Minimum Standard

The access terminal shall respond to a Session Management Protocol *ConfigurationRequest* message with a Session Management Protocol *ConfigurationResponse* message.

6.2 Default Address Management Protocol Tests

6.2.1 Access Network Tests

6.2.1.1 Recognition of Dual Addresses during Address Assignment Test

6.2.1.1.1 Definition

This test verifies that the access network recognizes dual addresses while a new UATI assignment is in progress.

6.2.1.1.2 Traceability

See section 6.3.7.1.6.2 of [1].

6.2.1.1.3 Test Procedure

- a. Instruct the access terminal to send a *UATIRequest* message.
- b. Instruct the access terminal to ignore the *UATIAssignment* message and send a *KeepAliveRequest* message using the address that was assigned prior to the current *UATIAssignment* message.

- 1 c. Verify that the access network meets the minimum standard as per bullet 1 in
2 6.2.1.1.4.
- 3 d. If re-transmitting of the *UATIAssignment* message is not supported by the access
4 network, instruct the access terminal to send the *UATIRequest* message.
- 5 e. Upon receipt of the second valid *UATIAssignment* message, instruct the access
6 terminal to send a *KeepAliveRequest* message using the address that was assigned
7 in the latest *UATIAssignment* message.
- 8 f. Verify that the access network meets the minimum standard as per bullet 2 in
9 6.2.1.1.4.

10 6.2.1.1.4 Minimum Standard

- 11 1. The access network shall recognize the last UATI assigned prior to the latest UATI
12 assignment and send a *KeepAliveResponse* message addressed to the access
13 terminal using the old UATI.
- 14 2. The access network shall recognize the latest UATI and send a *KeepAliveResponse*
15 message addressed to the access terminal using the latest UATI.

16 6.2.1.2 ConfigurationRequest Message Response Test

17 6.2.1.2.1 Definition

18 This test verifies that the access network responds to a Default Address Management
19 Protocol *ConfigurationRequest* message with a corresponding Address Management Protocol
20 *ConfigurationResponse* message.

21 6.2.1.2.2 Traceability

22 See section 6.3.6.1 and 13.7 of [1].

23 6.2.1.2.3 Test Procedure

- 24 a. Instruct the access terminal to set up a connection with the access network.
- 25 b. Instruct the access terminal to send a Default Address Management Protocol
26 *ConfigurationRequest* message.
- 27 c. Verify that the access network meets the minimum standard as per 6.2.1.2.4.

28 6.2.1.2.4 Minimum Standard

29 The access network shall respond to a Default Address Management Protocol
30 *ConfigurationRequest* message with a Default Address Management Protocol
31 *ConfigurationResponse* message.

1 6.2.2 Access Terminal Tests

2 6.2.2.1 Purging of RATI after Session Establishment Test

3 6.2.2.1.1 Definition

4 This test verifies that after the access terminal establishes a new session, it stops
5 responding to *Page* messages addressed by its RATI.

6 6.2.2.1.2 Traceability

7 See section 6.3.7.1.5.1 of [1].

8 6.2.2.1.3 Test Procedure

- 9 a. Instruct the access terminal to establish a session with the access network.
- 10 b. After the access network receives an Address Management Protocol *UATIComplete*
11 message, send a *UATIAssignment* message to the access terminal addressed by the
12 RATI used during session establishment.
- 13 c. Verify that the access terminal ignores the *UATIAssignment* message addressed by
14 its RATI and meets the minimum standard as per 6.2.2.1.4.

15 6.2.2.1.4 Minimum Standard

16 The access terminal shall set its RATI to NULL after it has been assigned a UATI during
17 new session setup.

18 6.2.2.2 Idle State Response to Subnet/Sector Change Test

19 6.2.2.2.1 Definition

20 This test verifies that the access terminal sends a *UATIRequest* message upon entering a
21 new subnet while in the Idle State of the Default Air-Link Management protocol.

22 6.2.2.2.2 Traceability

23 See section 6.3.7.1.6.1 and 7.9.6.2.2 of [1].

24 6.2.2.2.3 Test Procedure

- 25 a. Configure two neighboring sectors in the access network with different subnets.
- 26 b. Adjust the forward link attenuators so that the received signal strength, at the
27 access terminal, from Sector 1 and Sector 2 are such that only sector 1 is visible to
28 the access terminal.
- 29 c. Instruct the access terminal to set up a new session and establish a data call with
30 the sector 1 access network.

- 1 d. Adjust the forward link attenuators so that the received signal strength, at the
2 access terminal, from Sector 1 and Sector 2 are such that only sector 2 is visible to
3 the access terminal.
- 4 e. Instruct the access network to release the connection.
- 5 f. Verify that the access terminal meets the minimum standard as per bullet 1 in
6 6.2.2.2.4.
- 7 g. Instruct the access network to respond to a *UATIRequest* message with a
8 *UATIAssignment* message.
- 9 h. Wait until the access terminal sends a *UATIComplete* message.
- 10 i. Configure two neighboring sectors in the access network with different
11 SubnetMask values in the *SectorParameters* message.
- 12 j. Adjust the forward link attenuators so that the received signal strength, at the
13 access terminal, from Sector 1 and Sector 2 are such that only sector 1 is visible to
14 the access terminal.
- 15 k. Instruct the access terminal to set up a new session and establish a data call with
16 the sector 1 access network. Ensure that the access network either assigns the
17 same UATISubnetMask as brocast in the *SectorParameters* message or does not
18 include this field in the *UATIAssignment* message.
- 19 l. Allow the connection to become idle.
- 20 m. Adjust the forward link attenuators so that the received signal strength, at the
21 access terminal, from Sector 1 and Sector 2 are such that only sector 2 is visible to
22 the access terminal.
- 23 n. Verify that the access terminal meets the minimum standard as per bullet 2 in
24 6.2.2.2.4.

25 6.2.2.2.4 Minimum Standard

- 26 1. The access terminal shall send a *UATIRequest* message if the subnet associated
27 with UATI and the current subnet are different, and SupportSecondaryColorCodes is
28 set to 0x00 or UATIColorCode is different from all of the SecondaryColorCode values
29 provided as public data by the Overhead Messages Protocol
- 30 2. The access terminal shall send a *UATIRequest* message if the UATISubnetMask is
31 not equal to the SubnetMask of the sector it is monitoring and
32 SupportSecondaryColorCodes is set to 0x00 or UATIColorCode is different from all of
33 the SecondaryColorCode values provided as public data by the Overhead Messages
34 Protocol.

6.2.2.3 Access Terminal Response to a Change in the Serving Sector Test

6.2.2.3.1 Definition

This test verifies the response of the access terminal to a serving sector change in the Open State of the Default Address Management Protocol. The access terminal purges the old session when it notices a change in the serving sector with respect to the sector that assigned the UATI.

6.2.2.3.2 Traceability

See section 6.3.7.1.5.1 of [1].

6.2.2.3.3 Test Procedure

- a. Instruct the access terminal to establish a session. After receiving a *UATISessionComplete* and *ConnectionClose* messages from the access terminal, instruct the access network to turn off the transmitter for 25 seconds.
- b. Change the SectorID field in the *SectorParameters* message such that the Subnet changes. Turn on the access network transmitter.
- c. Verify that the access terminal meets the minimum standard as per bullet 1 in 6.2.2.3.4.
- d. After reception of a *UATISessionComplete* message, and subsequent *ConnectionRequest* and *ConnectionClose* messages from the access terminal, instruct the access network to transmit a *ConnectionClose* message to the access terminal.
- e. Ensure that the access terminal does not have an open connection with the access network and instruct the access network to page the access terminal using the UATI assigned in step a. Verify the access terminal meets the minimum standard as per bullet 2 in 6.2.2.3.4.

6.2.2.3.4 Minimum Standard

1. The access terminal should purge the old session. The access terminal shall send a *UATISessionRequest* message with *ATISessionType* = '11'.
2. If the access terminal has purged the old session, the access terminal shall ignore the UATI associated with the previous session and shall not send a connection request in response to the *Page* message.

6.2.2.4 Idle State UATIAssignment Message Response Test

6.2.2.4.1 Definition

This test verifies that the access terminal responds to a valid *UATIAssignment* message in the Idle State of the Default Air-Link Management Protocol by sending a corresponding *UATISessionComplete* message.

1 6.2.2.4.2 Traceability

2 See section 6.3.7.1.6.1 and 13.6 of [1].

3 6.2.2.4.3 Test Procedure

- 4 a. Configure two neighboring sectors in the access network with different subnets and
5 and some upper bits (bits 24-127) of the SectorID are different.
- 6 b. Adjust the forward link attenuators so that the received signal strength, at the
7 access terminal, from Sector 1 and Sector 2 are such that only sector 1 is visible to
8 the access terminal.
- 9 c. Instruct the access terminal to set up a new session and establish a data call with
10 the sector 1 access network. Instruct the access network to send a *UATIAssignment*
11 message with SubnetIncluded field set equal to '1'.
- 12 d. Verify that the access terminal meets the minimum standard as per bullet 1 of
13 6.2.2.4.4.
- 14 e. Adjust the forward link attenuators so that the received signal strength, at the
15 access terminal, from Sector 1 and Sector 2 are such that only sector 2 is visible to
16 the access terminal.
- 17 f. Wait for a *UATIRequest* message from the access terminal.
- 18 g. Configure the access network, so that upon receiving a *UATIRequest* message, it
19 sends a new *UATIAssignment* message that includes SubnetIncluded field set equal
20 to '1' and the UATI field set with some upper bits (bits 24-127) different from those
21 in step c, and the UpperOldUATILength field set equal to 0xD.
- 22 h. Wait for a *UATISuccess* message from the access terminal and verify that it meets
23 the minimum standard as per bullet 2 in 6.2.2.4.4.
- 24 i. Instruct the access network to resend the *UATIAssignment* message in step a
25 without altering the *MessageSequence* field.
- 26 j. Verify that the access terminal meets the minimum standard as per bullet 3 in
27 6.2.2.4.4.
- 28 k. Instruct the access network to send a new *UATIAssignment* message with the
29 following changes: Set the *MessageSequence* field to be 1 higher than in step g; Set
30 the SubnetIncluded field equal to '0'; Set the *UATIColorCode* field to be different
31 than the *ColorCode* field value broadcast in the *QuickConfig* message.
- 32 l. Verify that the access terminal meets the minimum standard as per bullet 4 of
33 6.2.2.4.4.

34 6.2.2.4.4 Minimum Standard

- 35 1. The access terminal shall respond to a valid *UATIAssignment* message with a
36 *UATISuccess* message.

- 1 2. The access terminal shall include UpperOldUATILength least significant octets of
2 OldUATI(127:24) in the *UATISuccess* message, which were requested in the
3 *UATIAssignment* message. The upper bits of the old UATI correspond to the UATI that
4 was assigned in step a.
- 5 3. The access terminal shall discard the *UATIAssignment* message.
- 6 4. The access terminal shall discard a *UATIAssignment* message that is not “fresh” and
7 does not send a *UATISuccess* message nor does it respond to a *Page* message
8 addressed to the ATI corresponding to “non fresh” *UATIAssignment* message in step
9 k.

10 6.2.2.5 Connected State UATIAssignment Message Response Test

11 6.2.2.5.1 Definition

12 This test verifies that the access terminal responds to a “fresh” *UATIAssignment* message
13 in the Connected State of the Default Air-Link Management Protocol by sending a
14 *UATISuccess* message.

15 6.2.2.5.2 Traceability

16 See section 6.3.7.1.6.1 of [1].

17 6.2.2.5.3 Test Procedure

- 18 a. Instruct the access terminal to set up a connection and establish a data call with
19 the access network.
- 20 b. Instruct the access network to send a *UATIAssignment* message with
21 SubnetIncluded field set equal to ‘1’ and the UpperOldUATILength field set equal to
22 0xD.
- 23 c. Verify that the access terminal meets the minimum standard as per bullet 1 of
24 6.2.2.5.4.
- 25 d. Allow the connection to become dormant.
- 26 e. Instruct the access network to transmit a *Page* message to the access terminal
27 using the new UATI.
- 28 f. Verify that the access terminal meets the minimum standard as per bullet 2 of
29 6.2.2.5.4.

30 6.2.2.5.4 Minimum Standard

- 31 1. The access terminal shall respond to a valid *UATIAssignment* message with a
32 *UATISuccess* message.
- 33 2. The access terminal shall establish a connection with the access network.

1 6.2.2.6 HardwareIDRequest Message Response Test

2 6.2.2.6.1 Definition

3 This test verifies that the access terminal responds to an Address Management Protocol
4 *HardwareIDRequest* message with an Address Management Protocol *HardwareIDResponse*
5 message.

6 6.2.2.6.2 Traceability

7 See section 6.3.7.1.3 of [1].

8 6.2.2.6.3 Test Procedure

9 a. Instruct the access network to send an Address Management Protocol
10 *HardwareIDRequest* message.

11 b. Verify that the access terminal meets the minimum standard as per 6.2.2.6.4.

12 6.2.2.6.4 Minimum Standard

13 The access terminal shall respond to an Address Management Protocol *HardwareIDRequest*
14 message with an Address Management Protocol *HardwareIDResponse* message.

15 6.2.2.7 Access Terminal Idle State Address Timer Operation Test

16 6.2.2.7.1 Definition

17 This test verifies that while the Address timer $T_{\text{ADMPAddress}}$ is active, the access terminal
18 recognizes both the new UATI included in the latest *UATIAssignment* message and the old
19 UATI. After the expiration of the Address timer, the access terminal recognizes only the
20 new UATI assigned to it.

21 6.2.2.7.2 Traceability

22 See section 6.3.7.1.6.1 and 6.3.9 of [1].

23 6.2.2.7.3 Test Procedure

24 a. Instruct the access terminal to set-up a connection and establish a data call with
25 the access network. Instruct the access network to transmit a *ConnectionClose*
26 message to the access terminal.

27 b. Instruct the access network to send a *UATIAssignment* message with
28 SubnetIncluded field set equal to '1'.

29 c. After receiving a *UATIComplete* message from the access terminal, instruct the
30 access network to send a *HardwareIDRequest* message to the access terminal using
31 the old UATI assigned in step b.

32 d. Verify that the access terminal meets the minimum standard as per bullet 1 in
33 6.2.2.7.4.

- 1 e. Approximately 200s \pm 10s after the receipt of the *UATIDComplete* message in step c,
2 instruct the access network to send a *HardwareIDRequest* message using the old
3 UATI assigned in step b.
- 4 f. Verify that the access terminal meets the minimum standard as per bullet 2 in
5 6.2.2.7.4.
- 6 g. Instruct the access network to send a *HardwareIDRequest* message to the access
7 terminal using the new UATI assigned in step b.
- 8 h. Verify that the access terminal meets the minimum standard as per bullet 2 in
9 6.2.2.7.4.

10 6.2.2.7.4 Minimum Standard

- 11 1. While the Address timer is active, the access terminal shall respond to a
12 *HardwareIDRequest* message carrying the old UATI assigned prior to the latest UATI
13 assignment with a *HardwareIDResponse* message.
- 14 2. While the Address timer is disabled, the access terminal shall only respond to a
15 *HardwareIDRequest* message carrying the new UATI assigned by the latest
16 *UATIAssignment* message with a *HardwareIDResponse* message.

17 6.2.2.8 ConfigurationRequest Message Response Test

18 6.2.2.8.1 Definition

19 This test verifies that the access terminal responds to a Default Address Management
20 Protocol *ConfigurationRequest* message with a corresponding Address Management Protocol
21 *ConfigurationResponse* message.

22 6.2.2.8.2 Traceability

23 See section 13.7 of [1].

24 6.2.2.8.3 Test Procedure

- 25 a. Instruct the access terminal to set up a connection with the access network.
- 26 b. Instruct the access network to send a Session Configuration Protocol
27 *ConfigurationStart* message.
- 28 c. When the access network receives a Session Configuration Protocol
29 *ConfigurationComplete* message, instruct the access network to send a Default
30 Address Management Protocol *ConfigurationRequest* message to the access terminal.
- 31 d. Verify that the access terminal meets the minimum standard as per 6.2.2.8.4.

32 6.2.2.8.4 Minimum Standard

33 The access terminal shall respond to a Default Address Management Protocol
34 *ConfigurationRequest* message with a corresponding Address Management Protocol
35 *ConfigurationResponse* message.

6.3 Default Session Configuration Protocol Tests

6.3.1 Access Network Tests

6.3.1.1 ConfigurationRequest Message Response Test

6.3.1.1.1 Definition

This test verifies that the access network responds to a Session Configuration Protocol *ConfigurationRequest* message with a Session Configuration Protocol *ConfigurationResponse* message.

6.3.1.1.2 Traceability

See section 13.7 of [1].

6.3.1.1.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network.
- b. Instruct the access terminal to send a Session Configuration Protocol *ConfigurationRequest* message.
- c. Verify that the access network meets the minimum standard as per 6.3.1.1.4.

6.3.1.1.4 Minimum Standard

The access network shall respond to a Session Configuration Protocol *ConfigurationRequest* message with a corresponding Session Configuration Protocol *ConfigurationResponse* message.

6.3.1.2 ConfigurationComplete Message Response Test

6.3.1.2.1 Definition

This test verifies that the access network responds to a Session Configuration Protocol *ConfigurationComplete* message with either a *ConfigurationRequest* message or a *ConfigurationComplete* message.

6.3.1.2.2 Traceability

See section 13.7 of [1].

6.3.1.2.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network.
- b. Instruct the access terminal to send a Session Configuration Protocol *ConfigurationRequest* message.
- c. Upon receiving a Session Configuration Protocol *ConfigurationResponse* message from the access network, instruct the access terminal to send a Session

1 Configuration Protocol *ConfigurationComplete* message on the Reverse Traffic
2 Channel.

3 d. Verify that the access network meets the minimum standard as per 6.3.1.2.4.

4 6.3.1.2.4 Minimum Standard

5 The access network shall respond to a Session Configuration Protocol
6 *ConfigurationComplete* message with either a Session Configuration Protocol
7 *ConfigurationRequest* message or a Session Configuration Protocol *ConfigurationComplete*
8 message.

9 6.3.2 Access Terminal Tests

10 6.3.2.1 ConfigurationRequest Message Response Test

11 6.3.2.1.1 Definition

12 This test verifies that the access terminal responds to a Session Configuration Protocol
13 *ConfigurationRequest* message with a Session Configuration Protocol *ConfigurationResponse*
14 message.

15 6.3.2.1.2 Traceability

16 See section 13.7 of [1].

17 6.3.2.1.3 Test Procedure

18 a. Instruct the access terminal to set up a connection and establish a data call with
19 the access network.

20 b. Instruct the access network to send a Session Configuration Protocol
21 *ConfigurationStart* message.

22 c. Wait for the receipt of Session Configuration Protocol *ConfigurationComplete*
23 message from the access terminal.

24 d. Instruct the access network to send a Session Configuration Protocol
25 *ConfigurationRequest* message.

26 e. Verify that the access terminal meets the minimum standard as per 6.3.2.1.4.

27 6.3.2.1.4 Minimum Standard

28 The access terminal shall respond to a Session Configuration Protocol *ConfigurationRequest*
29 message with a corresponding Session Configuration Protocol *ConfigurationResponse*
30 message.

1 6.3.2.2 ConfigurationComplete Message Response Test

2 6.3.2.2.1 Definition

3 This test verifies that at the end of the access network initiated session reconfiguration,
4 the access terminal responds to the Session Configuration Protocol *ConfigurationComplete*
5 message by closing the connection.

6 6.3.2.2.2 Traceability

7 See section 7.4.6.1.6.1 and 13.7 of [1].

8 6.3.2.2.3 Test Procedure

- 9 a. Instruct the access terminal to set up a connection and establish a data call with
10 the access network.
- 11 b. Instruct the access network to send a Session Configuration Protocol
12 *ConfigurationStart* message.
- 13 c. Wait for the receipt of Session Configuration Protocol *ConfigurationComplete*
14 message from the access terminal.
- 15 d. Instruct the access network to send a Session Configuration Protocol
16 *ConfigurationRequest* message on the Forward Traffic Channel.
- 17 e. Wait for the receipt of the Session Configuration Protocol *ConfigurationResponse*
18 message from the access terminal.
- 19 f. Instruct the access network to send the Session Configuration Protocol
20 *ConfigurationComplete* message.
- 21 g. Ensure that the access network does not send a *ConnectionClose* message.
- 22 h. Verify that the access terminal meets the minimum standard as per 6.3.2.2.4.

23 6.3.2.2.4 Minimum Standard

24 The access terminal shall respond to a Session Configuration Protocol
25 *ConfigurationComplete* message from the access network by sending a *ConnectionClose*
26 message with CloseReason field set equal to 000 (= Normal Close).

27 6.3.2.3 Multiple Personality Negotiation

28 6.3.2.3.1 Definition

29 This test verifies that the access terminal can negotiate multiple personalities with the
30 access network.

31 6.3.2.3.2 Traceability

32 See sections 6.4.6 and 6.4.2.4 of [1].

1 6.3.2.3.3 Test Procedure

- 2 a. If the access terminal has an open session with the access network, instruct the
3 access network to transmit a *SessionClose* message to the access terminal.
- 4 b. Configure the access network to negotiate 4 personalities with the access
5 terminal.
- 6 c. Cause the access terminal to start a session negotiation with the access network.
- 7 d. Verify that the access terminal meets the minimum standard as per bullet 1 of
8 6.3.2.3.4.
- 9 e. Ensure that the access network transmits a *ConfigurationResponse* (SCP) message
10 to the access terminal accepting the protocol Subtypes for the access terminal
11 personality.
- 12 f. Verify that the access terminal meets the minimum standard as per bullet 2 of
13 6.3.2.3.4.
- 14 g. Ensure that the access network transmits a *ConfigurationResponse* (Stream
15 Protocol) message to the access terminal accepting the stream to application
16 bindings proposed by the access terminal.
- 17 h. Verify that the access terminal meets the minimum standard as per bullet 3 of
18 6.3.2.3.4. Note the access terminal may transmit other *ConfigurationRequest*
19 messages before transmitting the *ConfigurationComplete* message.
- 20 i. Ensure that the access network transmits a *SoftConfigurationComplete* message to
21 the access terminal with *PersonalityIndexStore* field set to 0 and *Continue* set to 1,
22 if more personalities need to be negotiated, or set to 0 if personality configuration is
23 complete.
- 24 j. Repeat steps d-h.
- 25 k. Ensure that the access network transmits a *SoftConfigurationComplete* message to
26 the access terminal with *PersonalityIndexStore* field set to 1 and *Continue* set to 1.
- 27 l. Repeat steps d-h.
- 28 m. Ensure that the access network transmits a *SoftConfigurationComplete* message to
29 the access terminal with *PersonalityIndexStore* field set to 2 and *Continue* set to 1.
- 30 n. Repeat steps d-h.
- 31 o. Ensure that the access network transmits a *SoftConfigurationComplete* message to
32 the access terminal with *PersonalityIndexStore* field set to 3 and *Continue* set to 0.
- 33 p. Verify that the access terminal meets the minimum standard as per bullet 4 of
34 6.3.2.3.4.
- 35 q. Repeat the following steps for a value of 0x0-0x3 for
36 *SessionConfigurationToken4MSB*.

- 1 r. Cause the access terminal to transmit a *ConnectionRequest* message to the access
2 network.
- 3 s. If the four MSB of SessionConfigurationToken used by the access terminal in the
4 MAC layer header are not equal to SessionConfigurationToken4MSB, instruct the
5 access network to transmit an *AttributeUpdateRequest* message changing the
6 SessionConfigurationToken such that the four MSB have a value equal to
7 SessionConfigurationToken4MSB.
- 8 t. Allow the connection to become dormant.
- 9 u. Cause the access terminal to transmit a *ConnectionRequest* message to the access
10 network.
- 11 v. Verify that the access terminal meets the minimum standard as per bullet 5 of
12 6.3.2.3.4.

13 6.3.2.3.4 Minimum Standard

- 14 1. Verify that the access terminal transmits a *ConfigurationRequest* message (SCP)
15 listing the protocol Subtypes in order of preference.
- 16 2. Verify that the access terminal transmits a *ConfigurationRequest* message (Stream
17 Protocol) listing all stream to application bindings available for this personality.
- 18 3. Verify that the access terminal transmits a *ConfigurationComplete* message to the
19 access network.
- 20 4. Verify that the access terminal transmits a *ConnectionClose* message to the access
21 network.
- 22 5. Verify that the access terminal uses a SessionConfigurationToken with four MSB
23 of SessionConfigurationToken in the MAC layer header equal to
24 SessionConfigurationToken4MSB.

25 6.3.2.4 Personality Deletion Test

26 6.3.2.4.1 Definition

27 This test verifies that the access terminal can delete a personality.

28 6.3.2.4.2 Traceability

29 See sections 6.4.6, 6.4.2.4, 7.4.6.2.1 and 7.4.6.2.2 of [1].

30 6.3.2.4.3 Test Procedure

- 31 a. If the access terminal has an open session with the access network, instruct the
32 access network to transmit a *SessionClose* message to the access terminal.
- 33 b. Configure the access network to negotiate 4 personalities with the access terminal
34 and to establish a data call.

- 1 c. After the negotiation of the personalities is complete, ensure that the access
2 terminal transmits a *ConnectionClose* message to the access network.
- 3 d. Cause the access terminal to transmit a *ConnectionRequest* message to the access
4 network.
- 5 e. If the access terminal is using personality stored with PersonalityIndex value of
6 0x3, cause the access terminal to change its in-use personality.
- 7 f. While the access terminal has an open connection with the access network,
8 instruct the access network to transmit a *DeletePersonality* message to the access
9 terminal with PersonalityCount set to 0x1 and PersonalityIndex set to 0x3.
- 10 g. Verify that the access terminal meets the minimum standard as per bullet 1 of
11 6.3.2.3.4.
- 12 h. Instruct the access network to transmit a *ConfigurationStart* message to the access
13 terminal. Ensure that the personality negotiated in this step has at least one
14 protocol subtype that is different than the deleted personality. For example a
15 different RTCMAC subtype may be negotiated.
- 16 i. Verify that the access terminal meets the minimum standard as per bullet 2 of
17 6.3.2.3.4.
- 18 j. Instruct the access network to transmit a *ConfigurationComplete* message to the
19 access terminal with a SessionConfigurationToken value of 0x3.
- 20 k. Allow the connection to become dormant.
- 21 l. Cause the access terminal to establish a connection with the access network.
- 22 m. If the access terminal does not use a SessionConfigurationToken value of 0x3,
23 instruct the access network to transmit an *AttributeUpdateRequest* message to the
24 access terminal with a SessionConfigurationToken value with four MSB set to 0x3.
- 25 n. Verify that the access terminal meets the minimum standard as per bullet 3 of
26 6.3.2.3.4.

27 6.3.2.4.4 Minimum Standard

- 28 1. Verify that the access terminal transmits a *DeletePersonalityAck* message in
29 response to the *DeletePersonality* message.
- 30 2. Verify that the access terminal transmits a *ConfigurationComplete* message to the
31 access network.
- 32 3. Verify that the access terminal starts using a SessionConfigurationToken value
33 with 4 MSB set to 0x3 and starts using the new personality.
- 34

1 No Text.

2

7 CONNECTION LAYER TESTS

This section includes tests for the Connection Layer of [1].

7.1 Default Air-Link Management Protocol Tests

7.1.1 Access Network Tests

7.1.1.1 ConfigurationRequest Message Response Test

7.1.1.1.1 Definition

This test verifies that the access network responds to the Default Air-Link Management Protocol *ConfigurationRequest* message with a Default Air-Link Management Protocol *ConfigurationResponse* message.

7.1.1.1.2 Traceability

See section 13.7 of [1].

7.1.1.1.3 Test Procedure

- a. Instruct the access terminal to set up a connection with the access network.
- b. Instruct the access terminal to send a Default Air-Link Management Protocol *ConfigurationRequest* message.
- c. Verify that the access network meets the minimum standard as per 7.1.1.1.4.

7.1.1.1.4 Minimum Standard

The access network shall respond to Default Air-Link Management Protocol *ConfigurationRequest* message with a corresponding Air-Link Management Protocol *ConfigurationResponse* message.

7.1.1.2 Routing of TrafficChannelAssignment Message

7.1.1.2.1 Definition

This section verifies that all the sectors listed in the *RouteUpdate* message, sent by the access terminal in the connection request, respond by sending a *TrafficChannelAssignment* message.

7.1.1.2.2 Traceability

See section 7.8.6.1.5.1, 7.5.8 and 7.5.6.1.6.2 of [1].

7.1.1.2.3 Test Procedure

Configure the two sectors under test and an access terminal simulator as shown in Figure 12.5.

- 1 a. Adjust the forward link attenuators so that the received signal strength, at the
2 access terminal simulator, from Sector 1 and Sector 2 are approximately the same
3 (± 0.5 dB). Both sectors shall be visible for the access terminal simulator.
- 4 b. Set Sector 1 to page the access terminal simulator.
- 5 c. Configure the access terminal to send a *RouteUpdate* message and a
6 *ConnectionRequest* message to the access network.
- 7 d. Record the content of the *RouteUpdate* message sent by the access terminal
8 simulator in the Access Channel.
- 9 e. Monitor the message transmissions from Sector 1 and Sector 2 and verify that the
10 access network meets the minimum standard as per section 7.1.1.2.4.

11 7.1.1.2.4 Minimum Standard

12 All the sectors listed in the *RouteUpdate* message that the access terminal simulator sent
13 on the Access Channel should transmit a *TrafficChannelAssignment* message in response
14 to the *ConnectionRequest* message. If the *TrafficChannelAssignment* is sent in a synchronous
15 or sub-synchronous capsule, then all of these sectors should transmit the message
16 simultaneously at least once.

17 The transmission times of the Control Channel capsules containing the
18 *TrafficChannelAssignment* messages shall be within 1 second from the reception of the
19 *ConnectionRequest* message at the sector at which it was directed.

20 Note: the *ConnectionRequest* message and the *RouteUpdate* message are included in the
21 same Access Channel transmission.

22 7.1.1.3 Connection Setup Time

23 7.1.1.3.1 Definition

24 This section verifies the time to set up a Connection.

25 7.1.1.3.2 Traceability

26 See section 7.5.6.1.6.2 and 7.5.8 of [1].

27 7.1.1.3.3 Test Procedure

28 Refer to Figure 12.4 for a functional block diagram of the test setup.

- 29 a. Configure the sector under test and an access terminal simulator as shown in
30 Figure 12.4.
- 31 b. The AWGN generators are not applicable in this test.
- 32 c. *Page* the access terminal simulator.
- 33 d. Monitor the message transmissions from the sector and verify that the access
34 network meets the minimum standard as per section 7.1.1.3.4.

1 7.1.1.3.4 Minimum Standard

2 The sector shall transmit the *TrafficChannelAssignment* message within 1 second from the
3 reception of the *ConnectionRequest* message.

4 7.1.2 Access Terminal Tests

5 7.1.2.1 *Redirect* Message Test

6 7.1.2.1.1 Definition

7 This test verifies that upon receiving a *Redirect* message with channel field information,
8 an access terminal in the Idle State or the Connected State of the Default Air-Link
9 Management Protocol tunes to operate on the new channel.

10 7.1.2.1.2 Traceability

11 See section 7.2.6.1.3.1.1, 7.2.6.1.4.1.1 and 7.2.6.2.1 of [1].

12 7.1.2.1.3 Test Procedure

- 13 a. Configure the access network to operate on two CDMA channels.
- 14 b. Instruct the access terminal to set up a connection and establish a data call with
15 the access network on the first CDMA channel.
- 16 c. Instruct the access network to send a *Redirect* message to the access terminal
17 instructing it to tune to the second CDMA channel.
- 18 d. Send a page on the second CDMA channel to the access terminal.
- 19 e. Verify that the access terminal meets the minimum standard as per bullet 1 in
20 7.1.2.1.4.
- 21 f. Instruct the access network to withhold sending a *TrafficChannelAssignment*
22 message in response to step e.
- 23 g. Instruct the access network to send a *Redirect* message on the Control Channel
24 instructing the access terminal to tune to the first CDMA channel.
- 25 h. Send a page on the first CDMA Channel to the access terminal.
- 26 i. Verify that the access terminal meets the minimum standard as per bullet 2 in
27 7.1.2.1.4.

28 7.1.2.1.4 Minimum Standard

- 29 1. The access terminal shall respond to the *Page* message sent on the second CDMA
30 channel provided in the *Redirect* message (sent in the Connected State of the
31 Default Air-Link Management Protocol) with a *ConnectionRequest* message.
- 32 2. The access terminal shall respond to the *Page* message sent on the first CDMA
33 channel provided in the *Redirect* message (sent in the Idle State of the Default Air-
34 Link Management Protocol) with a *ConnectionRequest* message.

1 7.1.2.2 ConfigurationRequest Message Response Test

2 7.1.2.2.1 Definition

3 This test verifies that the access terminal responds to a Default Air-Link Management
4 Protocol *ConfigurationRequest* message with a Default Air-Link Management Protocol
5 *ConfigurationResponse* message.

6 7.1.2.2.2 Traceability

7 See section 13.7 of [1].

8 7.1.2.2.3 Test Procedure

- 9 a. Instruct the access terminal to set up a connection and establish a data call with
10 the access network.
- 11 b. Instruct the access network to send a Session Configuration Protocol
12 *ConfigurationStart* message.
- 13 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
14 message from the access terminal.
- 15 d. Instruct the access network to send a Default Air-Link Management Protocol
16 *ConfigurationRequest* message to the access terminal.
- 17 e. Verify that the access terminal meets the minimum standard as per 7.1.2.2.4.

18 7.1.2.2.4 Minimum Standard

19 The access terminal shall respond to a Default Air-Link Management Protocol
20 *ConfigurationRequest* message with a corresponding Default Air-Link Management Protocol
21 *ConfigurationResponse* message.

22 **7.2 Default Initialization State Protocol Tests**

23 7.2.1 Access Network Tests

24 7.2.1.1 *Sync* Message Transmission Test

25 7.2.1.1.1 Definition

26 This test verifies that the access network periodically transmits the *Sync* message on the
27 Synchronous Control Channel.

28 7.2.1.1.2 Traceability

29 See section 7.3.6.1 of [1].

30 7.2.1.1.3 Test Procedure

- 31 a. Monitor the *Sync* messages being sent on the Control Channel.
- 32 b. Verify that the access network meets the minimum standard as per 7.2.1.1.4.

1 7.2.1.1.4 Minimum Requirement

2 The access network shall transmit a *Sync* message at least once every 1.28 s.

3 7.2.1.2 ConfigurationRequest Message Response Test

4 7.2.1.2.1 Definition

5 This test verifies that the access network responds to the Default Initialization State
6 Protocol *ConfigurationRequest* message with a Default Initialization State Protocol
7 *ConfigurationResponse* message.

8 7.2.1.2.2 Traceability

9 See section 13.7 of [1].

10 7.2.1.2.3 Test Procedure

- 11 a. Instruct the access terminal to set up a connection with the access network.
12 b. Instruct the access terminal to send a Default Initialization State Protocol
13 *ConfigurationRequest* message.
14 c. Verify that the access network meets the minimum standard as per 7.2.1.2.4.

15 7.2.1.2.4 Minimum Standard

16 The access network shall respond to Default Initialization State Protocol
17 *ConfigurationRequest* message with a corresponding Initialization State Protocol
18 *ConfigurationResponse* message.

19 7.2.2 Access Terminal Tests

20 7.2.2.1 Access Terminal Processing of MinimumRevision and MaximumRevision Fields in
21 the *Sync* message Test

22 7.2.2.1.1 Definition

23 This test verifies that if the Revision Number of the access terminal is less than the
24 MinimumRevision field or greater than MaximumRevision field in the *Sync* message, then
25 the access terminal does not attempt to send any messages on the Access Channel.

26 7.2.2.1.2 Traceability

27 See section 7.3.6.1.5 and 1.15 of [1].

28 7.2.2.1.3 Test Procedure

- 29 a. Configure the access network to broadcast the *Sync* message with
30 MinimumRevision field set to a value greater than or equal to 0x02 and less than or
31 equal to 0xFF and MaximumRevision field set to a value greater than or equal to

1 MinimumRevision and less than or equal to 0xFF. Instruct the access network to
2 send a *Page* message to the access terminal.

3 b. Verify that the access terminal² meets the minimum standard as per bullet 1 in
4 7.2.2.1.4.

5 c. Configure the access network to broadcast the *Sync* message with
6 MinimumRevision field set equal to 0x00 and MaximumRevision field set equal to
7 0x00. Instruct the access network to send a *Page* message to the access terminal.

8 d. Verify that the access terminal meets the minimum standard as per bullet 2 in
9 7.2.2.1.4.

10 e. Configure the access network to broadcast the *Sync* message with
11 MinimumRevision field set equal to 0x01 and MaximumRevision field set equal to
12 0x01. Instruct the access network to send a *Page* message to the access terminal.

13 f. Verify that the access terminal meets the minimum standard as per bullet 3 in
14 7.2.2.1.4.

15 7.2.2.1.4 Minimum Standard

16 1. The access terminal shall not send any messages on the Access Channel if the
17 revision number of the access terminal is less than the MinimumRevision field in
18 the *Sync* message.

19 2. The access terminal shall not send any messages on the Access Channel if the
20 revision number of the access terminal is greater than MaximumRevision field in
21 the *Sync* message.

22 3. The access terminal shall send a *ConnectionRequest* message on the Access
23 Channel if the revision number of the access terminal is greater than or equal to
24 MinimumRevision field and less than or equal to and MaximumRevision field in
25 the *Sync* message.

26 7.2.2.2 ConfigurationRequest Message Response Test

27 7.2.2.2.1 Definition

28 This test verifies that the access terminal responds to a Default Initialization State
29 Protocol *ConfigurationRequest* message with a Default Initialization State Protocol
30 *ConfigurationResponse* message.

31 7.2.2.2.2 Traceability

32 See section 13.7 of [1].

² This test assumes that the revision number of the access terminal is 0x01.

1 7.2.2.2.3 Test Procedure

- 2 a. Instruct the access terminal to set up a connection with the access network.
- 3 b. Instruct the access network to send a Session Configuration Protocol
4 *ConfigurationStart* message.
- 5 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
6 message from the access terminal.
- 7 d. Instruct the access network to send a Default Initialization State Protocol
8 *ConfigurationRequest* message to the access terminal.
- 9 e. Verify that the access terminal meets the minimum standard as per 7.2.2.2.4.

10 7.2.2.2.4 Minimum Standard

11 The access terminal shall respond to a Default Initialization State Protocol
12 *ConfigurationRequest* message with a corresponding Default Initialization State Protocol
13 *ConfigurationResponse* message.

14 **7.3 Default Idle State Protocol Tests**

15 7.3.1 Access Network Tests

16 7.3.1.1 *Page* Message Transmissions to an Access Terminal Operating in Slotted Mode
17 Test

18 7.3.1.1.1 Definition

19 This test verifies that the access network sends *Page* messages to an access terminal
20 operating in slotted mode in the designated slots.

21 7.3.1.1.2 Traceability

22 See section 7.4.6.1.4 of [1].

23 7.3.1.1.3 Test Procedure

- 24 a. Instruct the access terminal to negotiate the use of the Default Packet Application
25 bound to the service access network (app type = 0x0002). After successful
26 negotiation instruct the access terminal to close the connection by sending a
27 *ConnectionClose* message with *SuspendEnable* field set equal to '0'.
- 28 b. Instruct the access network to send a Ping directed to the access terminal.
- 29 c. Record at the access terminal the *Page* message received and the Control Channel
30 cycle during which the *Page* message was received. Verify that the access network
31 meets the minimum standard as per 7.3.1.1.4.

1 7.3.1.1.4 Minimum Standard

2 The access network shall send *Page* messages to the access terminal that has R set to
3 equal the PreferredControlChannelCycle, in the Control Channel cycle C that satisfies the
4 following constraint: $(C+R) \bmod 12 = 0$, where C is the number of Control Channel cycles
5 since the start of system time and R is the offset in units of Control Channel cycle as per
6 [1].

7 7.3.1.2 ConfigurationRequest Message Response Test

8 7.3.1.2.1 Definition

9 This test verifies that the access network responds to the Default Idle State Protocol
10 *ConfigurationRequest* message with a Default Idle State Protocol *ConfigurationResponse*
11 message.

12 7.3.1.2.2 Traceability

13 See section 13.7 of [1].

14 7.3.1.2.3 Test Procedure

- 15 a. Instruct the access terminal to set up a connection with the access network.
- 16 b. Instruct the access terminal to send a Default Idle State Protocol
17 *ConfigurationRequest* message.
- 18 c. Verify that the access network meets the minimum standard as per 7.3.1.2.4.

19 7.3.1.2.4 Minimum Standard

20 The access network shall respond to the Default Idle State Protocol *ConfigurationRequest*
21 message with a corresponding Default Idle State Protocol *ConfigurationResponse* message.

22 7.3.2 Access Terminal Tests

23 7.3.2.1 Access Terminal Slotted Mode Operation Test

24 7.3.2.1.1 Definition

25 This test verifies that the access terminal listens to *Page* messages transmitted in the
26 designated slots while operating in slotted mode.

27 7.3.2.1.2 Traceability

28 See section 7.4.6.1.4 of [1].

29 7.3.2.1.3 Test Procedure

- 30 a. Instruct the access network to send a *Page* message to the access terminal in slots
31 in the beginning of the Control Channel cycle C that satisfies the constraint: $(C+R)$
32 $\bmod 12 = 0$, where C is the number of Control Channel cycles since the start of

1 system time and R is the offset in units of Control Channel cycle computed as per
2 [1].

3 b. Verify that the access terminal meets the minimum standard as per 7.3.2.1.4.

4 7.3.2.1.4 Minimum Standard

5 The access terminal shall respond to *Page* messages transmitted in the designated slots
6 with a *ConnectionRequest* message while operating in slotted mode.

7 7.3.2.2 Access Terminal Monitor State CDMA Channel Selection Test

8 7.3.2.2.1 Definition

9 This test verifies that in the Monitor State of this protocol, the access terminal selects the
10 correct CDMA Channel from the list of channels in the *SectorParameters* message.

11 7.3.2.2.2 Traceability

12 See section 7.4.6.1.5.1.1 of [1].

13 7.3.2.2.3 Test Procedure

- 14 a. Configure the access network to operate on two CDMA channels and modify the
15 *SectorParameters* message broadcast on the two CDMA channels to indicate the
16 channels being supported.
- 17 b. Instruct the access network to use the *SessionSeed* provided by the access
18 terminal during the session and data call setup to determine the CDMA channel
19 that the access terminal will be monitoring, by using the hash function described
20 in 10.4 of [1] with *Decorrelate* parameter set equal to 0.
- 21 c. Instruct the access network to send a *Page* message to the access terminal on the
22 CDMA Channel determined in step b.
- 23 d. Verify that the access terminal meets the minimum standard as per 7.3.2.2.4 and
24 responds to the *Page* message with a *ConnectionRequest* message.
- 25 e. Instruct the access network to send a *TrafficChannelAssignment* message to the
26 access terminal directing it to the other CDMA Channel being supported by the
27 access network.
- 28 f. After access terminal acquires the other CDMA channel, instruct the access
29 network to close the connection by sending a *ConnectionClose* message.
- 30 g. Instruct the access network to send a *Page* message to the access terminal on the
31 CDMA Channel determined in step b.
- 32 h. Verify that the access terminal meets the minimum standard as per 7.3.2.2.4.

1 7.3.2.2.4 Minimum Standard

2 In the Monitor State of this protocol, the access terminal shall select the correct CDMA
3 Channel from the list of channels in the *SectorParameters* message and respond to the *Page*
4 message with a *ConnectionRequest* message.

5 7.3.2.3 Access Network Initiated Fast Connection Setup Test

6 7.3.2.3.1 Definition

7 This test verifies that the access terminal supports accelerated connection setup when
8 the access network directly sends a *TrafficChannelAssignment* message by eliminating the
9 *Page* and *ConnectionRequest* message exchange.

10 7.3.2.3.2 Traceability

11 See section 7.4.6.1.6.1 of [1].

12 7.3.2.3.3 Test Procedure

- 13 a. Instruct the access terminal to set up a connection and establish a data call with
14 the access network.
- 15 b. Instruct the access network to close the connection by sending a *ConnectionClose*
16 message.
- 17 c. Instruct the access network to send a *TrafficChannelAssignment* message to the
18 access terminal on the Control Channel with contents identical to that in step a.
- 19 d. Verify that the access terminal sets up the connection successfully and meets the
20 minimum standard as per 7.3.2.3.4.

21 7.3.2.3.4 Minimum Standard

22 When the access network bypasses the paging process and directly sends
23 *TrafficChannelAssignment* message, the access terminal shall respond by sending a
24 *TrafficChannelComplete* message.

25 7.3.2.4 ConfigurationRequest Message Response Test

26 7.3.2.4.1 Definition

27 This test verifies that the access terminal responds to a Default Idle State Protocol
28 *ConfigurationRequest* message with a Default Idle State Protocol *ConfigurationResponse*
29 message.

30 7.3.2.4.2 Traceability

31 See section 13.7 of [1].

32 7.3.2.4.3 Test Procedure

- 33 a. Instruct the access terminal to set up a connection with the access network.

- 1 b. Instruct the access network to send an Idle State Protocol *ConfigurationRequest*
- 2 message.
- 3 c. Verify that the access terminal meets the minimum standard as per 7.3.2.4.4.

4 7.3.2.4.4 Minimum Standard

5 The access terminal shall respond to a Default Idle State Protocol *ConfigurationRequest*
6 message with a corresponding Idle State Protocol *ConfigurationResponse* message.

7 **7.4 Enhanced Idle State Protocol Tests**

8 7.4.1 Access Network Tests

9 7.4.1.1 *Page* Message Transmissions to an Access Terminal Operating in Slotted Mode 10 Test

11 7.4.1.1.1 Definition

12 This test verifies that the access network sends *Page* messages to an access terminal
13 operating in slotted mode in the designated slots. The value of the three sleep periods
14 tested depends on the value chosen for SlotCycle1, SlotCycle2 and SlotCycle3 fields of the
15 SlottedMode attribute.

16 7.4.1.1.2 Traceability

17 See section 7.5.6.1.4 and 7.5.6.1.3 of [1].

18 7.4.1.1.3 Test Procedure

- 19 a. Instruct the access terminal to negotiate the use of the Enhanced Idle State
20 protocol. If the access terminal supports a value of SlotCycle1 that is less than
21 0x06, set SlotCycle1 to a value less than 0x06 in the SlottedMode Attribute of the
22 Enhanced Idle State Protocol. Otherwise, set SlotCycle1 to a value greater than or
23 equal to 0x06 in the SlottedMode Attribute of the Enhanced Idle State Protocol.
- 24 a. After a successful negotiation, instruct the access terminal to set up a connection
25 and establish a data call with the access network.
- 26 b. After the connection has been established, instruct the access network to close the
27 connection by transmitting a *ConnectionClose* message.
- 28 c. Before T12 instruct the access network to transmit a *Page* to the access terminal
29 by sending a Ping from the access network directed to the access terminal.
- 30 d. Record at the access network the CDMA System Time in slots when the *Page*
31 message was transmitted. Verify that the access network meets the minimum
32 standard as per 7.4.1.1.4.
- 33 e. After the access terminal responds to the *Page* message with a *ConnectionRequest*
34 message, instruct the access network to send a *TrafficChannelAssignment* message
35 to the access terminal.

- 1 f. Instruct the access network to close the connection by sending a *ConnectionClose*
2 message.
- 3 g. After T12 and before T23 instruct the access network to transmit a *Page* to the
4 access terminal by sending a Ping from the access network directed to the access
5 terminal.
- 6 h. Record at the access network the CDMA System Time in slots when the *Page*
7 message was transmitted to the access terminal. Verify that the access network
8 meets the minimum standard as per 7.4.1.1.4.
- 9 i. After the access terminal responds to the *Page* message with a *ConnectionRequest*
10 message, instruct the access network to send a *TrafficChannelAssignment* message
11 to the access terminal.
- 12 j. Instruct the access network to close the connection by sending a *ConnectionClose*.
- 13 k. After T23, instruct the access network to transmit a *Page* to the access terminal by
14 sending a Ping from the access network directed to the access terminal.
- 15 l. Record at the access terminal the *Page* message received and the Period during
16 which the *Page* message was received. Verify that the access network meets the
17 minimum standard as per 7.4.1.1.4.

18 7.4.1.1.4 Minimum Standard

19 Upon receiving the Ping packet, the access network shall send *Page* messages to the
20 access terminal that has R set to equal the PreferredControlChannelCycle, in sub-
21 synchronous capsules or synchronous capsules at time T that satisfies the following
22 constraint: $(T+256 \times R) \bmod \text{Period} = \text{Offset}$, where T is the CDMA System Time in slots,
23 Offset is public data of the Control Channel MAC Protocol as per [1], and Period is computed
24 as specified in [1].

25 7.4.1.2 ConfigurationRequest Message Response Test

26 7.4.1.2.1 Definition

27 This test verifies that the access network responds to the Enhanced Idle State Protocol
28 *ConfigurationRequest* message with an Enhanced Idle State *ConfigurationResponse* message.

29 7.4.1.2.2 Traceability

30 See section 13.7 of [1].

31 7.4.1.2.3 Test Procedure

- 32 a. Instruct the access terminal to set up a connection with the access network and
33 negotiate the use of Enhanced Idle State protocol.
- 34 b. Instruct the access terminal to send an Enhanced Idle State Protocol
35 *ConfigurationRequest* message.
- 36 c. Verify that the access network meets the minimum standard as per 7.4.1.2.4.

1 7.4.1.2.4 Minimum Standard

2 The access network shall respond to the Enhanced Idle State Protocol *ConfigurationRequest*
3 message with a corresponding Enhanced Idle State Protocol *ConfigurationResponse*
4 message.

5 7.4.2 Access Terminal Tests

6 7.4.2.1 Access Terminal Slotted Mode Operation Test

7 7.4.2.1.1 Definition

8 This test verifies that the access terminal listens to *Page* messages transmitted in the
9 designated slots while operating in slotted mode. The value of the three sleep periods
10 tested depends on the value chosen for SlotCycle1, SlotCycle2 and SlotCycle3 fields of the
11 SlottedMode attribute.

12 7.4.2.1.2 Traceability

13 See section 7.5.6.1.4 of [1].

14 7.4.2.1.3 Test Procedure

- 15 b. Instruct the access terminal to negotiate the use of Enhanced Idle State protocol. If
16 the access terminal supports a value of SlotCycle1 that is less than 0x06, set
17 SlotCycle1 to a value less than 0x06 in the SlottedMode Attribute of the Enhanced
18 Idle State Protocol. Otherwise, set SlotCycle1 to a value greater than or equal to
19 0x06 in the SlottedMode Attribute of the Enhanced Idle State Protocol.
- 20 c. After a successful negotiation, instruct the access terminal to set up a connection
21 and establish a data call with the access network.
- 22 d. After the connection has been established, instruct the access network to close the
23 connection by transmitting a *ConnectionClose* message.
- 24 e. Before T12, instruct the access network to transmit a *Page* to the access terminal
25 by sending a Ping from the access network directed to the access terminal.
- 26 f. Verify that the access terminal meets the minimum standard as per 7.4.2.1.4.
- 27 g. After the access terminal responds to the *Page* message with a *ConnectionRequest*
28 message, instruct the access network to send a *TrafficChannelAssignment* message
29 to the access terminal.
- 30 h. Instruct the access network to close the connection by sending a *ConnectionClose*
31 message.
- 32 i. After T12 and before T23, instruct the access network to transmit a *Page* to the
33 access terminal by sending a Ping from the access network directed to the access
34 terminal.
- 35 j. Verify that the access terminal meets the minimum standard as per 7.4.2.1.4.

- 1 k. After the access terminal responds to the *Page* message with a *ConnectionRequest*
2 message, instruct the access network to send a *TrafficChannelAssignment* message
3 to the access terminal.
- 4 l. Instruct the access network to close the connection by sending a *ConnectionClose*
5 message.
- 6 m. After T23, instruct the access network to transmit a *Page* to the access terminal by
7 sending a Ping from the access network directed to the access terminal.
- 8 n. Verify that the access terminal meets the minimum standard as per 7.4.2.1.4.

9 7.4.2.1.4 Minimum Standard

10 The access terminal shall respond to *Page* messages transmitted in the designated slots
11 with a *ConnectionRequest* message while operating in slotted mode.

12 7.4.2.2 Access Terminal Monitor State CDMA Channel Selection Test

13 7.4.2.2.1 Definition

14 This test verifies that in the Monitor State of this protocol, the access terminal selects the
15 correct CDMA Channel from the list of channels in the *SectorParameters* message.

16 7.4.2.2.2 Traceability

17 See section 7.5.6.1.6.1.1 of [1].

18 7.4.2.2.3 Test Procedure

- 19 a. Configure the access network to operate on two CDMA channels and modify the
20 *SectorParameters* message broadcast on the two CDMA channels to indicate the
21 channels being supported.
- 22 b. Instruct the access terminal to set up a session and establish a data call with the
23 access network and to negotiate the use of Enhanced Idle State protocol.
- 24 c. Instruct the access network to use the *SessionSeed* provided by the access
25 terminal during the session setup to determine the CDMA channel that the access
26 terminal will be monitoring, by using the hash function described in 15.4 of [1] with
27 *Decorrelate* parameter set equal to 0.
- 28 d. Instruct the access network to send a *Page* message to the access terminal on the
29 CDMA Channel determined in step b.
- 30 e. Verify that the access terminal meets the minimum standard as per 7.4.2.2.4 and
31 responds to the *Page* message with a *ConnectionRequest* message.
- 32 f. Instruct the access network to send a *TrafficChannelAssignment* message to the
33 access terminal directing it to the other CDMA Channel being supported by the
34 access network.

- 1 g. Instruct the access terminal to close the connection by sending a *ConnectionClose*
2 message.
- 3 h. Instruct the access network to send a *Page* message to the access terminal on the
4 CDMA Channel determined in step b.
- 5 i. Verify that the access terminal meets the minimum standard as per 7.4.2.2.4.

6 7.4.2.2.4 Minimum Standard

7 In the Monitor State of this protocol, the access terminal shall select the correct CDMA
8 Channel from the list of channels in the *SectorParameters* message and respond to the *Page*
9 message with a *ConnectionRequest* message.

10 7.4.2.3 Access Network Initiated Fast Connection Setup Test

11 7.4.2.3.1 Definition

12 This test verifies that the access terminal supports accelerated connection setup when
13 the access network directly sends a *TrafficChannelAssignment* message by eliminating the
14 *Page* and *ConnectionRequest* message.

15 7.4.2.3.2 Traceability

16 See section 7.5.6.1.6.1 of [1].

17 7.4.2.3.3 Test Procedure

- 18 a. Instruct the access terminal to set up a session with the access network and
19 negotiate the use of Enhanced Idle State protocol.
- 20 b. Instruct the access terminal to set up a connection and establish a data call with
21 the access network.
- 22 c. Instruct the access network to close the connection by sending a *ConnectionClose*
23 message.
- 24 d. Instruct the access network to send a *TrafficChannelAssignment* message to the
25 access terminal on the Control Channel with contents identical to that in step a.
- 26 e. Verify that the access terminal sets up the connection successfully and meets the
27 minimum standard as per 7.4.2.3.4.

28 7.4.2.3.4 Minimum Standard

29 When the access network bypasses the paging process and directly sends
30 *TrafficChannelAssignment* message with the same contents as the previous
31 *TrafficChannelAssignment* message, the access terminal shall respond by sending a
32 *TrafficChannelComplete* message.

1 7.4.2.4 ConfigurationRequest Message Response Test

2 7.4.2.4.1 Definition

3 This test verifies that the access terminal responds to an Enhanced Idle State Protocol
4 *ConfigurationRequest* message with an Enhanced Idle State Protocol *ConfigurationResponse*
5 message.

6 7.4.2.4.2 Traceability

7 See section 13.7 of [1].

8 7.4.2.4.3 Test Procedure

- 9 a. Instruct the access terminal to set up a connection with the access network.
10 b. Instruct the access network to send an Enhanced Idle State Protocol
11 *ConfigurationRequest* message.
12 c. Verify that the access terminal meets the minimum standard as per 7.4.2.4.4.

13 7.4.2.4.4 Minimum Standard

14 The access terminal shall respond to an Enhanced Idle State Protocol *ConfigurationRequest*
15 message with a corresponding Enhanced Idle State *ConfigurationResponse* message.

16 **7.5 Default Connected State Protocol Tests**

17 7.5.1 Access Network Tests

18 7.5.1.1 ConfigurationRequest Message Response Test

19 7.5.1.1.1 Definition

20 This test verifies that the access network responds to a Default Connected State Protocol
21 *ConfigurationRequest* message with a Default Connected State Protocol
22 *ConfigurationResponse* message.

23 7.5.1.1.2 Traceability

24 See section 13.7 of [1].

25 7.5.1.1.3 Test Procedure

- 26 a. Instruct the access terminal to set up a connection with the access terminal.
27 b. Instruct the access terminal to send a Connected State Protocol
28 *ConfigurationRequest* message to the access network.
29 c. Verify that the access network meets the minimum standard as per 7.5.1.1.4.

1 7.5.1.1.4 Minimum Standard

2 The access network shall respond to a Default Connected State Protocol
3 *ConfigurationRequest* message with a Connected State Protocol *ConfigurationResponse*
4 message.

5 7.5.2 Access Terminal Tests

6 7.5.2.1 *ConnectionClose* Message Response Test

7 7.5.2.1.1 Definition

8 This test verifies that the access terminal responds to a *ConnectionClose* message from the
9 access network with a *ConnectionClose* message.

10 7.5.2.1.2 Traceability

11 See section 7.7.6.1.1.3 of [1].

12 7.5.2.1.3 Test Procedure

- 13 a. Instruct the access terminal to set up a connection and establish a data call with
14 the access network.
- 15 b. Instruct the access network to send a *ConnectionClose* message with CloseReason
16 field set equal to 000 (Normal Close).
- 17 c. Verify that the access terminal meets the minimum standard as per 7.5.2.1.4.

18 7.5.2.1.4 Minimum Standard

19 The access terminal shall respond to a *ConnectionClose* message with CloseReason field set
20 equal to 000 (Normal Close from the access network) with a *ConnectionClose* message with
21 CloseReason field set equal to 001 (Close Reply).

22 7.5.2.2 *ConfigurationRequest* Message Response Test

23 7.5.2.2.1 Definition

24 This test verifies that the access terminal responds to a Default Connected State Protocol
25 *ConfigurationRequest* message with a Default Connected State Protocol
26 *ConfigurationResponse* message.

27 7.5.2.2.2 Traceability

28 See section 13.7 of [1].

29 7.5.2.2.3 Test Procedure

- 30 a. Instruct the access terminal to set up a connection and establish a data call with
31 the access network.

- 1 b. Instruct the access network to send a Session Configuration Protocol
2 *ConfigurationStart* message.
- 3 c. Wait until the access network receives a Session Configuration Protocol
4 *ConfigurationComplete* message,
- 5 d. Instruct the access network to send a Connected State Protocol
6 *ConfigurationRequest* message to the access terminal.
- 7 e. Verify that the access terminal meets the minimum standard as per 7.5.2.2.4.

8 7.5.2.2.4 Minimum Standard

9 The access terminal shall respond to a Connected State Protocol *ConfigurationRequest*
10 message (in the access network Initiated State of the Session Configuration Protocol) with
11 a Connected State Protocol *ConfigurationResponse* message.

12 **7.6 Default Route Update Protocol Tests**

13 7.6.1 Access Network Tests

14 7.6.1.1 ConfigurationRequest Message Response Test

15 7.6.1.1.1 Definition

16 This test verifies that the access network responds to a Route Update Protocol
17 *ConfigurationRequest* message with a Route Update Protocol *ConfigurationResponse* message.

18 7.6.1.1.2 Traceability

19 See section 13.7 of [1].

20 7.6.1.1.3 Test Procedure

- 21 a. Instruct the access terminal to set up a connection with the access network.
- 22 b. Instruct the access terminal to send a Route Update Protocol *ConfigurationRequest*
23 message to the access network.
- 24 c. Verify that the access network meets the minimum standard as per 7.6.1.1.4.

25 7.6.1.1.4 Minimum Standard

26 The access network shall respond to a Route Update Protocol *ConfigurationRequest* message
27 from the access terminal with a Route Update Protocol *ConfigurationResponse* message.

7.6.2 Access Terminal Tests

7.6.2.1 Access Terminal Idle State Distance Based Route Update Message Test

7.6.2.1.1 Definition

This test verifies that if the access terminal does not support the setting of `SupportRouteUpdateEnhancements` to non-default value, the access terminal sends a *RouteUpdate* message whenever the distance from the sector where the access terminal last sent a *RouteUpdate* message is greater than the `RouteUpdateRadiusOverhead` field specified in the *SectorParameters* message and if the value of `RouteUpdateRadiusOverhead` specified in the *SectorParameters* message sent by the sector in which the access terminal sent a *RouteUpdate* message is not zero. If the access terminal supports the setting of `SupportRouteUpdateEnhancements` to non-default value, then the access terminal sends a *RouteUpdate* message whenever the distance from the sector where the access terminal last sent a *RouteUpdate* message is greater than $\max(0, r_m \times r_o + r_a)$, where r_o is the `RouteUpdateRadiusOverhead` field specified in the *SectorParameters* message, r_m is the `RouteUpdateRadiusMultiply` attribute and r_a is the `RouteUpdateRadiusAdd` attribute and if the value of `RouteUpdateRadiusOverhead` specified in the *SectorParameters* message sent by the sector in which the access terminal sent a *RouteUpdate* message is not zero.

7.6.2.1.2 Traceability

See section 7.8.6.1.5.4 and 7.8.7 of [1].

7.6.2.1.3 Test Procedure

- a. Configure the access network to ensure that `SupportRouteUpdateEnhancements` is set to its default value of 0x00. Instruct the access terminal to set up a connection and establish a data call with the access network. Allow the connection to become dormant.
- b. Configure the access network to support two sectors. Instruct the first sector to broadcast *SectorParameters* message with Latitude and Longitude field set equal to 0 and `RouteUpdateRadiusOverhead` set equal to 5. Instruct the second sector to broadcast *SectorParameters* message with Latitude and Longitude field set equal to 100 and `RouteUpdateRadiusOverhead` field set equal to 5.
- c. Configure the test so that the active set pilot for the access terminal in the Idle State of the Default Air-Link Management protocol is set to the first sector. Instruct the access network to send a *KeepAliveRequest* message on the Control Channel of the first sector. Wait until a *KeepAliveResponse* message is received from the access terminal.
- d. Weaken the first sector and strengthen the second sector causing the access terminal to acquire the second sector.
- e. Verify that the access terminal meets the minimum standard as per bullet 1 7.6.2.1.4.

- 1 f. If the access terminal supports the setting of `SupportRouteUpdateEnhancements` to
2 a non-default value, configure the access network to negotiate
3 `SupportRouteUpdateEnhancements` to `0x01` or `0x02` or `0x03`,
4 `RouteUpdateRadiusMultiply` attribute to `0x0a` and `RouteUpdateRadiusAdd` attribute
5 to `0x00`.
- 6 g. Repeat steps b through d.
- 7 h. Verify that the access terminal meets the minimum standard as per bullet 1
8 7.6.2.1.4.
- 9 i. If the access terminal supports the setting of `SupportRouteUpdateEnhancements` to
10 a non-default value, configure the access network to negotiate
11 `SupportRouteUpdateEnhancements` to `0x01` or `0x02` or `0x03`,
12 `RouteUpdateRadiusMultiply` attribute to `0x42` and `RouteUpdateRadiusAdd` attribute
13 to `0x00`.
- 14 j. Repeat the steps b through d.
- 15 k. Verify that the access terminal meets the minimum standard as per bullet 2
16 7.6.2.1.4.

17 7.6.2.1.4 Minimum Standard

- 18 1. The access terminal shall send a *RouteUpdate* message whenever the distance
19 from the last sector where the access terminal last sent a *RouteUpdate* message
20 exceeds the `RouteUpdateRadiusOverhead` field in the *SectorParameters* message.
- 21 2. The access terminal shall not send a *RouteUpdate* message.

22 7.6.2.2 *RouteUpdateRequest* Message Response Test

23 7.6.2.2.1 Definition

24 This test verifies that the access terminal responds to a Route Update Protocol
25 *RouteUpdateRequest* message with a Route Update Protocol *RouteUpdate* message. This test
26 is applicable only to access terminals that support a non default value of
27 `SupportRouteUpdateEnhancements` attribute.

28 7.6.2.2.2 Traceability

29 See section 7.8.6.1.5.4 of [1].

30 7.6.2.2.3 Test Procedure

- 31 a. Instruct the access terminal to set up a connection and establish a data call with
32 the access network.
- 33 b. If supported by the access terminal, configure the access network to negotiate a
34 value of `0x01` for `SupportRouteUpdateEnhancements`.
- 35 c. Instruct the access network to send a Route Update Protocol *RouteUpdateRequest*
36 message to the access terminal.

- 1 d. Verify that the access terminal meets the minimum standard as per 7.6.2.2.4.
- 2 e. If supported by the access terminal, configure the access network to negotiate a
- 3 value of 0x02 for SupportRouteUpdateEnhancements.
- 4 f. Instruct the access network to send a Route Update Protocol *RouteUpdateRequest*
- 5 message to the access terminal.
- 6 g. Verify that the access terminal meets the minimum standard as 7.6.2.2.4.
- 7 h. If supported by the access terminal, configure the access network to negotiate a
- 8 value of 0x03 for SupportRouteUpdateEnhancements.
- 9 i. Instruct the access network to send a Route Update Protocol *RouteUpdateRequest*
- 10 message to the access terminal.
- 11 j. Verify that the access terminal meets the minimum standard as 7.6.2.2.4.

12 7.6.2.2.4 Minimum Standard

13 The access terminal shall respond to a Route Update Protocol *RouteUpdateRequest*
14 message from the access network with a Route Update Protocol *RouteUpdate* message.

15 7.6.2.3 TrafficChannelAssignment Message Response Test

16 7.6.2.3.1 Definition

17 This test verifies that in the Connected State of the Default Air-Link Management
18 Protocol, the access terminal responds only to a valid *TrafficChannelAssignment* message
19 with a *TrafficChannelComplete* message.

20 7.6.2.3.2 Traceability

21 See section 7.8.6.1.6.6 of [1].

22 7.6.2.3.3 Test Procedure

- 23 a. Instruct the access terminal to set up a connection and establish a data call with
- 24 the access network with the access network and at the access network store the
- 25 contents of the *TrafficChannelAssignment* message.
- 26 b. Instruct the access network to send a *TrafficChannelAssignment* message whose
- 27 content is identical to that in step a with the exception of the MessageSequence
- 28 field which is one higher than in step a.
- 29 c. Verify that the access terminal meets the minimum standard as per bullet 1 of
- 30 7.6.2.3.4.
- 31 d. Instruct the access network to send a *TrafficChannelAssignment* message whose
- 32 content is identical to that sent in step a (with the same MessageSequence field as
- 33 in step a).
- 34 e. Verify that the access terminal meets the minimum standard as per bullet 2 in
- 35 7.6.2.3.4.

1 7.6.2.3.4 Minimum Standard

- 2 1. The access terminal shall respond to a valid *TrafficChannelAssignment* message
3 with a *TrafficChannelComplete* message.
- 4 2. The access terminal shall validate the *TrafficChannelAssignment* message using the
5 procedure defined in 10.6 of [1]. The access terminal shall discard the message and
6 not send a corresponding *TrafficChannelComplete* message.

7 7.6.2.4 ConfigurationRequest Message Response Test

8 7.6.2.4.1 Definition

9 This test verifies that the access terminal responds to a Route Update Protocol
10 *ConfigurationRequest* message with a Route Update Protocol *ConfigurationResponse* message.

11 7.6.2.4.2 Traceability

12 See section 13.7 of [1].

13 7.6.2.4.3 Test Procedure

- 14 a. Instruct the access terminal to set up a connection with the access network.
- 15 b. Instruct the access network to send a Session Configuration Protocol
16 *ConfigurationStart* message.
- 17 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
18 message from the access terminal.
- 19 d. Instruct the access network to send a Route Update Protocol *ConfigurationRequest*
20 message to the access terminal.
- 21 e. Verify that the access terminal meets the minimum standard as per 7.6.2.4.4.

22 7.6.2.4.4 Minimum Standard

23 The access terminal shall respond to a Route Update Protocol *ConfigurationRequest* message
24 (in the access network Initiated State of the Session Configuration Protocol) with a Route
25 Update Protocol *ConfigurationResponse* message.

26 **7.7 MC Route Update Protocol Tests**

27 7.7.1 Access Network Tests

28 7.7.1.1 ConfigurationRequest Message Response Test

29 7.7.1.1.1 Definition

30 This test verifies that the access network responds to a MultiCarrier Route Update Protocol
31 *ConfigurationRequest* message with a MultiCarrier Route Update Protocol
32 *ConfigurationResponse* message.

1 7.7.1.1.2 Traceability

2 See section 13.7 of [1].

3 7.7.1.1.3 Test Procedure

- 4 d. Instruct the access terminal to set up a connection and establish a data call with
- 5 the access network.
- 6 e. Instruct the access terminal to send a MultiCarrier Route Update Protocol
- 7 *ConfigurationRequest* message to the access network.
- 8 f. Verify that the access network meets the minimum standard as per 7.7.1.1.4.

9 7.7.1.1.4 Minimum Standard

10 The access network shall respond to a MultiCarrier Route Update Protocol
11 *ConfigurationRequest* message from the access terminal with a MultiCarrier Route Update
12 Protocol *ConfigurationResponse* message.

13 7.7.2 Access Terminal Tests

14 Test cases 7.6.2.1-7.6.2.3 of the Default Route Update Protocol are applicable to
15 MultiCarrier Route Update Protocol. In addition to these test cases, the following test cases
16 should be executed for MultiCarrier Route Update Protocol.

17 7.7.2.1 ConfigurationRequest Message Response Test

18 7.7.2.1.1 Definition

19 This test verifies that the access terminal responds to a MultiCarrier Route Update
20 Protocol *ConfigurationRequest* message with a MultiCarrier Route Update Protocol
21 *ConfigurationResponse* message.

22 7.7.2.1.2 Traceability

23 See section 13.7 of [1].

24 7.7.2.1.3 Test Procedure

- 25 a. Instruct the access terminal to set up a connection with the access network.
- 26 b. Instruct the access network to send a Session Configuration Protocol
- 27 *ConfigurationStart* message.
- 28 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
- 29 message from the access terminal.
- 30 d. Instruct the access network to send a MultiCarrier Route Update Protocol
- 31 *ConfigurationRequest* message to the access terminal.
- 32 e. Verify that the access terminal meets the minimum standard as per 7.7.2.2.4.

1 7.7.2.1.4 Minimum Standard

2 The access terminal shall respond to a MultiCarrier Route Update Protocol
3 *ConfigurationRequest* message (in the access network Initiated State of the Session
4 Configuration Protocol) with a MultiCarrier Route Update Protocol *ConfigurationResponse*
5 message.

6 7.7.2.2 ATTotalPilotTransmission field in Route Update Message

7 7.7.2.2.1 Definition

8 This test verifies that the access terminal includes the ATTotalPilotTransmission field in
9 the *RouteUpdate* message when the message is transmitted over the traffic channel.
10 Otherwise, the access terminal shall not include this field.

11 7.7.2.2.2 Traceability

12 See section 7.9.6.2.1 of [1].

13 7.7.2.2.3 Test Procedure

- 14 a. Configure the access network to support two sectors.
- 15 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 16 c. If the access terminal is not using MC-RUP, instruct the access network to
17 terminate the existing session and negotiate a new session. Ensure that the access
18 terminal and the access network negotiate the use of MC-RUP.
- 19 d. Allow the connection to go dormant.
- 20 e. Cause the access terminal to open a connection with the access network.
- 21 f. Verify that the access terminal meets the minimum standard as per bullet 1 of
22 7.7.2.4.4.
- 23 g. While the access terminal is connected with the access network, cause the access
24 terminal to transmit a *RouteUpdate* message. This can be achieved by changing the
25 strength of the pilot of the second sector.
- 26 h. Verify that the access terminal meets the minimum standard as per bullet 2 of
27 7.7.2.4.4.

1 7.7.2.2.4 Minimum Standard

- 2 1. The access terminal shall not include the ATTotalPilotTransmission feild in the
3 *RouteUpdate* message transmitted on the Access Channel.
- 4 2. The access terminal shall include the ATTotalPilotTransmission field in the
5 *RouteUpdate* message transmitted on the Reverse Traffic Channel.

6 7.7.2.3 ReferencePilotChannel field in Route Update Message

7 7.7.2.3.1 Definition

8 This test verifies that if the ReferencePilotChannel is the FDD-paired forward CDMA
9 channel associated with the reverse CDMA channel on which the *RouteUpdate* message is
10 being sent, then the access terminal shall not include ReferencePilotChannel in the
11 *RouteUpdate* message. Otherwise, the access terminal shall include the
12 ReferencePilotChannel field in the *RouteUpdate* message. Note, the steps f and h can be
13 executed in any order.

14 7.7.2.3.2 Traceability

15 See section 7.9.6.2.1of [1].

16 7.7.2.3.3 Test Procedure

- 17 a. Configure the access network to support atleast 2 channels and 2 sectors.
- 18 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 19 c. If the access terminal is not using MC-RUP, instruct the access network to
20 terminate the existing session and negotiate a new session Ensure that the access
21 terminal and the access network negotiate the use of MC-RUP.
- 22 d. Allow the connection to go dormant.
- 23 e. Cause the access terminal to open a connection with the access network.
- 24 f. While the access terminal is connected with the access network, cause the access
25 terminal to transmit a *RouteUpdate* message on the reverse channel that is not the
26 FDD-paired reverse cdma channel associated with the reference pilot channel. The
27 *RouteUpdate* message can be generated by changing the strength of the pilot of the
28 second sector.
- 29 g. Verify that the access terminal meets the minimum standard as per bullet 1 of
30 7.7.2.3.4.
- 31 h. While the access terminal is connected with the access network, cause the access
32 terminal to transmit a *RouteUpdate* message on the FDD-paired reverse cdma
33 channel associated with the reference pilot channel.
- 34 i. Verify that the access terminal meets the minimum standard as per bullet 2 of
35 7.7.2.3.4.

1 7.7.2.3.4 Minimum Standard

- 2 1. The access terminal shall include the ReferencePilotChannel field in the
3 *RouteUpdate* message transmitted on the Reverse Traffic Channel.
- 4 2. The access terminal shall not include the ReferencePilotChannel feild in the
5 *RouteUpdate* message transmitted on the Reverse Traffic Channel.

6 7.7.2.4 Route Update for pilots with same Pilot Group

7 7.7.2.4.1 Definition

8 This test verifies that the access terminal does not include pilots with the same pilot
9 group having the same <PNoffset, PilotGroupID>) in the *RouteUpdate* message.

10 7.7.2.4.2 Traceability

11 See section 7.9.6.1.6.5 of [1].

12 7.7.2.4.3 Test Procedure

- 13 a. Configure the access network to support 2 channels and 2 sectors (sector 1 and
14 sector 2). For all pilots, configure the access network to transmit *SectorParamters*
15 message advertising only the neighbors in the same sub-active set. Configure the
16 pilots in the same geographic sector to have identical PN offset. Note, sector 1 and
17 sector 2 will have different PN offset. Configure the PilotGroupID for all pilots to 0.
18 Configure the channel conditions such that the access terminal is able receive
19 pilots from sector 1 but not from from sector 2.
- 20 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 21 c. If the access terminal is not using MC-RUP, instruct the access network to
22 terminate the existing session and negotiate a new session Ensure that the access
23 terminal and the access network negotiate the use of MC-RUP. Ensure that the
24 access terminal negotiates a value greater than 0x01 for MaxNumberofFLSupported
25 MaxNumberofRLSupported attributes of the MC-RUP protocol.
- 26 d. Allow the connection to go dormant.
- 27 e. Cause the access terminal to open a connection with the access network.
- 28 f. Verify that the access terminal meets the minimum standard as per bullet 1 of
29 7.6.2.3.4.
- 30 g. Ensure that the access network transmits a *TrafficChannelAssignment* message
31 with multiple carriers assigned to the access terminal.
- 32 h. Verify that the access terminal meets the minimum standard as per bullet 2 of
33 7.7.2.4.4.
- 34 i. Cause the access terminal to transmit a *RouteUpdate* message by changing the
35 receive strength of the pilots from sector 2.

- 1 j. Verify that the access terminal meets the minimum standard as per bullet 3 of
2 7.7.2.4.4.

3 7.7.2.4.4 Minimum Standard

- 4 1. The access terminal includes only 1 pilot from a pilot group in the *RouteUpdate*
5 message.
- 6 2. The access terminal transmits *TrafficChannelComplete* message and is able to
7 receive and transmit data on the allocated carriers.
- 8 3. The access terminal includes only 1 pilot from each pilot group in the *RouteUpdate*
9 message, i.e., *RouteUpdate* message contains report for 2 pilots, one from each
10 sector.

11 7.7.2.5 Route Update for pilots with different Pilot Group

12 7.7.2.5.1 Definition

13 This test verifies that the access terminal includes pilots with different pilot group (having
14 different <PNoffset, PilotGroupID>) in the *RouteUpdate* message.

15 7.7.2.5.2 Traceability

16 See section 7.9.6.1.6.5 of [1].

17 7.7.2.5.3 Test Procedure

- 18 a. Configure the access network to support 2 channels and 2 sectors (sector 1 and
19 sector 2). For all pilots, configure the access network to transmit *SectorParameters*
20 message advertising neighbors in the same sub-active set as well as the neighbors
21 on other channels supported on the sector. Configure pilots to have different PN
22 offset. Configure the PilotGroupID for all pilots to 0. Configure the access network to
23 transmit the ChannelRecord and PilotGroupID for the neighbors in the
24 *SectorParameters* message. Configure the channel conditions such that the access
25 terminal is able receive pilots from sector 1 but not from from sector 2.
- 26 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 27 c. If the access terminal is not using MC-RUP, instruct the access network to
28 terminate the existing session and negotiate a new session Ensure that the access
29 terminal and the access network negotiate the use of MC-RUP. Ensure that the
30 access terminal negotiates a value greater than 0x01 for MaxNumberofFLSupported
31 MaxNumberofRLSupported attributes of the MC-RUP protocol.
- 32 d. Allow the connection to go dormant.
- 33 e. Cause the access terminal to open a connection with the access network.
- 34 f. Verify that the access terminal meets the minimum standard as per bullet 1 of
35 7.7.2.5.4.

- 1 g. Ensure that the access network transmits a *TrafficChannelAssignment* message
2 with multiple carriers assigned to the access terminal.
- 3 h. Verify that the access terminal meets the minimum standard as per bullet 2 of
4 7.7.2.5.4.
- 5 i. Cause the access terminal to transmit a *RouteUpdate* message by changing the
6 receive strength of the pilots from sector 2.
- 7 j. Verify that the access terminal meets the minimum standard as per bullet 3 of
8 7.7.2.5.4.
- 9 k. Repeat the test with the following changes to the configuration. Configure the pilots
10 in the same geographic sector to have identical PN offset. Note, sector 1 and sector
11 2 will have different PN offset. Configure the PilotGroupID for all pilots to be
12 different.

13 7.7.2.5.4 Minimum Standard

- 14 1. The access terminal includes a report for each pilot channel on the sector 1 in the
15 *RouteUpdate* message.
- 16 2. The access terminal transmits *TrafficChannelComplete* message and is able to
17 receive and transmit data on the allocated carriers.
- 18 3. The access terminal includes a report for each pilot channel on the sector 1 and
19 sector 2 in the *RouteUpdate* message.

20 7.7.2.6 RouteUpdate transmission when ThisSubActiveSetNotReportable is true

21 7.7.2.6.1 Definition

22 This test verifies that the access terminal does not include pilots from a SubActive set if
23 the access network sets the ThisSubActiveSetNotReportable to true for this SubActive set
24 in the *TrafficChannelAssignment* message.

25 7.7.2.6.2 Traceability

26 See section 7.9.6.1.2.9, 7.9.6.1.2.10, 7.9.6.2.2 of [1].

27 7.7.2.6.3 Test Procedure

- 28 a. Configure the access network to support 2 or channels. Configure the channel
29 conditions such that the access terminal is able receive pilots from the sector.
- 30 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 31 c. If the access terminal is not using MC-RUP, instruct the access network to
32 terminate the existing session and negotiate a new session. Ensure that the access
33 terminal and the access network negotiate the use of MC-RUP. Ensure that the
34 access terminal negotiates a value greater than 0x01 for MaxNumberofFLSupported
35 MaxNumberofRLSupported attributes of the MC-RUP protocol.

- 1 d. Allow the connection to go dormant.
- 2 e. Cause the access terminal to open a connection with the access network.
- 3 f. Instruct the access network to transmit the *TrafficChannelAssignment* message
- 4 with *ThisSubactiveSetNotReportable* set to true for all remaining SubActive-Sets
- 5 other than the SubActive-Set carrying the ReferencePilot one of the carriers
- 6 having a lower value than the ReferencePilotChannel.
- 7 g. Ensure that the access terminal receives the *TrafficChannelAssignment* message
- 8 and transmits a *TrafficChannelComplete* message.
- 9 h. While the access network is connected to the access network, cause the access
- 10 terminal to transmit a *RouteUpdate* message to the access network.
- 11 i. Verify that the access terminal meets the minimum standard as per 7.7.2.6.4.
- 12 j. Allow the connection to become dormant.
- 13 k. Cause the access terminal to open a connection with the access network.
- 14 l. Verify that the access terminal meets the minimum standard as per 7.7.2.6.4.

15 7.7.2.6.4 Minimum Standard

16 The access terminal transmits a *RouteUpdate* message and does not include a report for
 17 any pilot belonging to any the sub-active set for which the access network had set
 18 *ThisSubactiveSetNotReportable* set to true in the *TrafficChannelAssignment* message.

19 **7.8 Overhead Messages Protocol Tests**

20 7.8.1 Access Network Tests

21 7.8.1.1 *QuickConfig* Message Transmission Test

22 7.8.1.1.1 Definition

23 This test verifies that the access network periodically transmits the *QuickConfig* message
 24 on the Control Channel Synchronous Sleep State capsule.

25 7.8.1.1.2 Traceability

26 See section 7.11.6.1.5 of [1].

27 7.8.1.1.3 Test Procedure

- 28 a. Instruct the access terminal to record the messages received in every Control
- 29 Channel Synchronous Sleep State capsule.
- 30 b. Verify that the access network meets the minimum standard as per 7.8.1.1.4.

1 7.8.1.1.4 Minimum Standard

2 The access network shall transmit a *QuickConfig* message in every Control Channel
3 Synchronous Sleep State capsule once every 426.67 ms.

4 7.8.1.2 *SectorParameters* Message Transmission Test

5 7.8.1.2.1 Definition

6 This test verifies that the access network periodically transmits the *SectorParameters*
7 message in a Control Channel Synchronous capsule.

8 7.8.1.2.2 Traceability

9 See section 7.11.6.1.5 of [1].

10 7.8.1.2.3 Test Procedure

- 11 a. Instruct the access terminal to record the messages received in every Control
12 Channel Synchronous capsule.
- 13 b. Verify that the access network meets the minimum standard as per 7.8.1.2.4.

14 7.8.1.2.4 Minimum Standard

15 The access network shall transmit a *SectorParameters* message in a Control Channel
16 Synchronous capsule at least once every 5.12 s.

17 7.8.1.3 *ConfigurationRequest* Message Response Test

18 7.8.1.3.1 Definition

19 This test verifies that the access network responds to the Overhead Messages Protocol
20 *ConfigurationRequest* message with an Overhead Messages Protocol *ConfigurationResponse*
21 message.

22 7.8.1.3.2 Traceability

23 See section 13.7 of [1].

24 7.8.1.3.3 Test Procedure

- 25 a. Instruct the access terminal to set up a connection with the access network.
- 26 b. Instruct the access terminal to send the Overhead Messages Protocol
27 *ConfigurationRequest* message to the access network.
- 28 c. Verify that the access network meets the minimum standard as per 7.8.1.3.4.

29 7.8.1.3.4 Minimum Standard

30 The access network shall send an Overhead Messages Protocol *ConfigurationResponse*
31 message.

1 7.8.2 Access Terminal Tests

2 7.8.2.1 ConfigurationRequest Message Response Test

3 7.8.2.1.1 Definition

4 This test verifies that the access terminal responds to the Overhead Messages Protocol
5 *ConfigurationRequest* message with Overhead Messages Protocol *ConfigurationResponse*
6 message.

7 7.8.2.1.2 Traceability

8 See section 13.7 of [1].

9 7.8.2.1.3 Test Procedure

- 10 a. Instruct the access terminal to set up a connection with the access network.
- 11 b. Instruct the access network to send a Session Configuration Protocol
12 *ConfigurationStart* message.
- 13 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
14 message from the access terminal.
- 15 d. Instruct the access network to send the Overhead Messages Protocol
16 *ConfigurationRequest* message to the access terminal.
- 17 e. Verify that the access terminal meets the minimum standard as per 7.8.2.1.4.

18 7.8.2.1.4 Minimum Standard

19 The access terminal shall respond to the Overhead Messages Protocol *ConfigurationRequest*
20 message with an Overhead Messages Protocol *ConfigurationResponse* message.

21

22

- 1 No Text.

1 **8 SECURITY LAYER TESTS**

2 This section includes tests for the Security Layer of [1].

3 **8.1 DH Key Exchange Protocol Tests**

4 8.1.1 Access Network Test

5 8.1.1.1 DH Key Exchange Protocol Negotiation Test

6 This test is applicable if the access network supports the DH Key Exchange Protocol.

7 8.1.1.1.1 Definition

8 This test verifies that the access network supports the negotiation of DH Key Exchange
9 Protocol.

10 8.1.1.1.2 Traceability

11 See section 8.6.5.1.2 of [1].

12 8.1.1.1.3 Test Procedure

- 13 a. Instruct the access terminal to set up a connection and propose the use of DH Key
14 Exchange Protocol by sending a Session Configuration Protocol *ConfigurationRequest*
15 message.
- 16 b. After receiving a Session Configuration Protocol *ConfigurationResponse* message
17 from the access network, verify that the access network meets the minimum
18 standard as per bullet 1 in 8.1.1.1.4.
- 19 c. Verify that the access network meets the minimum standard as per bullet 2 in
20 8.1.1.1.4.
- 21 d. Verify that the KeySignature in the *ANKeyComplete* message sent by the access
22 network meets the minimum standard as per bullet 3 in 8.1.1.1.4.

23 8.1.1.1.4 Minimum Standard

- 24 1. The access network shall initiate the DH Key exchange by sending a DH Key
25 Exchange Protocol *KeyRequest* message.
- 26 2. The access network shall respond to a DH Key Exchange Protocol *KeyResponse*
27 message with a DH Key Exchange Protocol *ANKeyComplete* message.
- 28 3. The KeySignature shall match the signature computed by the access terminal as
29 per [1].

1 8.1.1.2 Default Key Exchange Protocol KeySignature Computation time

2 8.1.1.2.1 Definition

3 The DH Key Exchange Protocol states that upon the reception of the *KeyResponse* message,
4 the access network shall start the computation of the secret key.

5 After the completion of the secret key computation, the access network should send an
6 *ANKeyComplete* message to the access terminal.

7 This test verifies that the computation time for the secret key is within a specified time
8 frame.

9 8.1.1.2.2 Traceability

10 See section 8.6.5.1.2, 8.6.5.3.4, 8.6.5.3.1 and 8.6.8 of [1].

11 8.1.1.2.3 Test Procedure

12 Refer to Figure 12.4 for a functional block diagram of the test setup.

- 13 a. Configure the sector under test and an access terminal simulator as shown in
14 Figure 12.4.
- 15 b. The AWGN generators are not applicable in this test.
- 16 c. Set the access network to initiate the key exchange (by sending a *KeyRequest*
17 message to the access terminal simulator).
- 18 d. Monitor the message transmissions and receptions at the sector under test.
- 19 e. Calculate the time (T_1) from the reception of the *KeyResponse* message to the
20 transmission of the *ANKeyComplete* message at the access network and verify that
21 the access network meets the minimum standard as per section 8.1.1.2.4.

22 8.1.1.2.4 Minimum Standard

23 The sector shall transmit the *ANKeyComplete* message with a valid computed KeySignature
24 within 3 seconds from the reception of the *KeyResponse* message from the access terminal
25 simulator (T_1 shall be less than or equal to 3 seconds).

26 The computed KeySignature is considered to be valid if the access terminal simulator
27 reports a '1' in the Result field of the *ATKeyComplete* message.

28 8.1.2 Access Terminal Test

29 8.1.2.1 DH Key Exchange Protocol Negotiation Test

30 This test is applicable if the access terminal and the access network support the DH Key
31 Exchange Protocol.

1 8.1.2.1.1 Definition

2 This test verifies that the access terminal supports the negotiation of DH Key Exchange
3 Protocol.

4 8.1.2.1.2 Traceability

5 See section 8.6.5.1.1 of [1].

6 8.1.2.1.3 Test Procedure

- 7 a. Instruct the access terminal to set up a connection and send a Session
8 Configuration Protocol *ConfigurationStart* message.
- 9 b. After receiving a Session Configuration Protocol *ConfigurationComplete* message,
10 instruct the access network to propose the use of DH Key Exchange Protocol by
11 sending a Session Configuration Protocol *ConfigurationRequest* message.
- 12 c. After receiving a Session Configuration Protocol *ConfigurationResponse* message
13 from the access terminal, instruct the access network to send the DH Key
14 Exchange Protocol *KeyRequest* message.
- 15 d. Verify that the access terminal meets the minimum standard as per bullet 1 in
16 8.1.2.1.4.
- 17 e. Instruct the access network to send the DH Key Exchange Protocol *ANKeyComplete*
18 message.
- 19 f. Verify that the access terminal meets the minimum standard as per bullet 2 in
20 8.1.2.1.4.

21 8.1.2.1.4 Minimum Standard

- 22 1. The access terminal shall respond to the DH Key Exchange Protocol *KeyRequest*
23 message with a DH Key exchange Protocol *KeyResponse* message.
- 24 2. The access terminal shall respond to the DH Key Exchange Protocol *ANKeyComplete*
25 message with a DH Key Exchange Protocol *ATKeyComplete* message.

26 8.1.2.2 DH Key Exchange Protocol KeySignature Computation time

27 8.1.2.2.1 Definition

28 The Default Key Exchange Protocol described in [1] states that upon transmission of the
29 *KeyResponse* message, the access terminal shall start the computation of the session key.

30 Once the access terminal receives the *ANKeyComplete* message, it has to start verifying
31 the signature.

32 This test verifies the time that the access terminal uses to calculate the key and to verify
33 the signature.

1 8.1.2.2.2 Traceability

2 See section 8.6.5.1.1, 8.6.8 and 8.6.5.3.2 of [1].

3 8.1.2.2.3 Test Procedure

- 4 a. Connect the sector to the access terminal antenna connector as shown in Figure
5 12.2.
- 6 b. Set the access network to initiate the key exchange by sending a *KeyRequest*
7 message to the access terminal.
- 8 c. Monitor the message transmissions and receptions at the access terminal under
9 test.
- 10 d. Calculate the time (T_1) from the reception of the *ANKeyComplete* message to the
11 transmission of the *ATKeyComplete* message at the access terminal and verify that
12 the access terminal meets the minimum requirements as per 8.1.2.2.4.

13 8.1.2.2.4 Minimum Standard

14 The access terminal shall transmit the *ATKeyComplete* message with a Result field value
15 equal to '1' within $3 (T_{KEPSigCompAT})$ seconds from the reception of the *ANKeyComplete* message
16 or within $T_{KEPKeyCompAT}$ from the time AT sent the *KeyResponse* Message, whichever occurs
17 later.

18 **8.2 SHA-1 Authentication Protocol Tests**

19 8.2.1 Access Network Test

20 8.2.1.1 SHA-1 Authentication Protocol Negotiation Test

21 This test is applicable if the access network supports the SHA-1 Authentication Protocol.

22 8.2.1.1.1 Definition

23 This test verifies that the access network supports the negotiation of SHA-1
24 Authentication Protocol.

25 8.2.1.1.2 Traceability

26 See section 8.8.6.1.2 of [1].

27 8.2.1.1.3 Test Procedure

- 28 a. Instruct the access terminal to set up a connection and propose the use of Generic
29 Security Protocol by sending a Session Configuration Protocol *ConfigurationRequest*
30 message.
- 31 b. After receiving a Session Configuration Protocol *ConfigurationResponse* message,
32 instruct the access terminal to propose the use of SHA-1 Authentication Protocol by
33 sending a Session Configuration Protocol *ConfigurationRequest* message.

- 1 c. After protocol negotiation is complete, instruct the access terminal to close the
2 connection.
- 3 d. Instruct the access terminal to send a *ConnectionRequest* message. Verify that the
4 access network meets the minimum standard as per bullet 1 in 8.2.1.1.4.
- 5 e. Close the connection set up in step d. Instruct the access terminal to send a
6 *ConnectionRequest* message but alter the ACPAC field in the Access Channel
7 Authentication packet header to a different value than what was computed by the
8 SHA-1 Authentication Protocol.
- 9 f. Verify that the access network meets the minimum standard as per bullet 2 in
10 8.2.1.1.4.
- 11 g. Instruct the access terminal to set up a connection and propose the use of Default
12 Security Protocol by sending a Session Configuration Protocol *ConfigurationRequest*
13 message.
- 14 h. Repeat steps b through f.

15 8.2.1.1.4 Minimum Standard

- 16 1. The access network shall respond to the *ConnectionRequest* message with a
17 *TrafficChannelAssignment* message.
- 18 2. The access network shall discard the Access Channel security layer packet
19 containing the *ConnectionRequest* message if the ACPAC field included in the
20 header field of the authentication packet sent by the access terminal does not
21 match the ACPAC value computed by the access network and shall not send a
22 *TrafficChannelAssignment* message to the access terminal.

23 8.2.2 Access Terminal Test

24 8.2.2.1 SHA-1 Authentication Protocol Negotiation Test

25 This test is applicable if the access terminal and the access network support the SHA-1
26 Authentication Protocol.

27 8.2.2.1.1 Definition

28 This test verifies that the access terminal supports the negotiation of SHA-1
29 Authentication Protocol.

30 8.2.2.1.2 Traceability

31 See section 8.8.6.1.1 of [1].

32 8.2.2.1.3 Test Procedure

- 33 a. Instruct the access terminal to set up a connection and establish a data call and
34 send a Session Configuration Protocol *ConfigurationStart* message.

- 1 b. After receiving a Session Configuration Protocol *ConfigurationComplete* message,
2 instruct the access network to propose the use of Generic Security Protocol by
3 sending a Session Configuration Protocol *ConfigurationRequest* message.
- 4 c. After receiving a Session Configuration Protocol *ConfigurationResponse* message,
5 instruct the access network to propose the use of SHA-1 Authentication Protocol by
6 sending a Session Configuration Protocol *ConfigurationRequest* message.
- 7 d. After protocol negotiation is complete, instruct the access network to close the
8 connection.
- 9 e. Instruct the access network to send a *Page* message to the access terminal.
- 10 f. Verify that the access terminal meets the minimum standard as per 8.2.2.1.4.

11 8.2.2.1.4 Minimum Standard

12 The ACPAC field included in the header field of the authentication packet sent by the
13 access terminal shall match the ACPAC value computed by the access network.

14 **8.3 Security Protocol Tests**

15 8.3.1 Access Network Test

16 8.3.1.1 SecurityLayerFormat Field in the Control Channel MAC Packet Header Test

17 8.3.1.1.1 Definition

18 This test verifies that the access network correctly sets the SecurityLayerFormat field in
19 the header of Control Channel MAC Layer packets.

20 8.3.1.1.2 Traceability

21 See section 9.2.6.2.1 of [1].

22 8.3.1.1.3 Test Procedure

- 23 a. Instruct the access terminal to set up a connection and negotiate the default
24 protocol configuration. Close the connection for the default configuration to take
25 effect.
- 26 b. Instruct the access terminal to send a *KeepAliveRequest* message.
- 27 c. Record at the access terminal the header of the Control Channel MAC Layer Packet
28 containing the *KeepAliveResponse* message from the access network.
- 29 d. Verify that the access network meets the minimum standard as per bullet 1 in
30 8.3.1.1.4. If the access network supports the Generic Security Protocol, then
31 continue with steps e through j; otherwise, terminate the test.
- 32 e. Instruct the access terminal to set up a connection and propose the use of Generic
33 Security Protocol by sending a Session Configuration Protocol *ConfigurationRequest*
34 message.

- 1 f. After receiving a Session Configuration Protocol *ConfigurationResponse* message,
2 instruct the access terminal to send a Session Configuration Protocol
3 *ConfigurationComplete* message.
- 4 g. After receiving a Session Configuration Protocol *ConfigurationComplete* message,
5 instruct the access terminal to close the connection for the negotiated security
6 protocol to take effect.
- 7 h. Instruct the access terminal to send a *KeepAliveRequest* message.
- 8 i. Record at the access terminal the header of the Control Channel MAC Layer Packet
9 containing the *KeepAliveResponse* message from the access network.
- 10 j. Verify that the access network meets the minimum standard as per bullet 2 in
11 8.3.1.1.4.

12 8.3.1.1.4 Minimum Standard

- 13 1. When the Default Security Protocol is ACTIVE, the access network shall set the
14 *SecurityLayerFormat* field in the Header of the CC MAC Layer Packet equal to '0'.
- 15 2. When the Generic Security Protocol is ACTIVE, the access network shall set the
16 *SecurityLayerFormat* field in the Header of the CC MAC Layer Packet equal to '1'.

17 8.3.2 Access Terminal Test

18 8.3.2.1 *SecurityLayerFormat* Field in the Access Channel MAC Packet Header Test

19 8.3.2.1.1 Definition

20 This test verifies that the access terminal correctly sets the *SecurityLayerFormat* field in
21 the header of Access Channel MAC Layer packets.

22 8.3.2.1.2 Traceability

23 See section 9.4.6.2.1 of [1].

24 8.3.2.1.3 Test Procedure

- 25 a. Instruct the access terminal to set up a connection and establish a data call and
26 negotiate default protocol configuration, then close the connection for the default
27 configuration to take effect.
- 28 b. Instruct the access network to send a *KeepAliveRequest* message. Record, at the
29 access network, the header of the Access Channel MAC Layer Packet containing
30 the *KeepAliveResponse* message from the access terminal.
- 31 c. Verify that the access terminal meets the minimum standard as per bullet 1 in
32 8.3.2.1.4. If the access terminal supports the Generic Security Protocol, then
33 continue with steps e through j; otherwise, terminate the test.
- 34 d. Instruct the access terminal to set up a connection. Instruct the access network to
35 send a Session Configuration Protocol *ConfigurationStart* message.

- 1 e. After receiving a Session Configuration Protocol *ConfigurationComplete* message
2 from the access terminal, instruct the access network to propose the use of
3 Generic Security Protocol by sending a Session Configuration Protocol
4 *ConfigurationRequest* message.
- 5 f. After receiving a Session Configuration Protocol *ConfigurationResponse* message,
6 instruct the access network to send a *ConfigurationComplete* message and close the
7 connection for the negotiated security protocol to take effect.
- 8 g. Instruct the access network to send a *KeepAliveRequest* message.
- 9 h. Record, at the access network, the header of the Access Channel MAC Layer
10 Packet containing the *KeepAliveResponse* message from the access terminal.
- 11 i. Verify that the access terminal meets the minimum standard as per bullet 1 in
12 8.3.2.1.4.

13 8.3.2.1.4 Minimum Standard

- 14 1. When the Default Security Protocol is INACTIVE, the access terminal shall set the
15 SecurityLayerFormat field in the Header of the AC MAC Layer Packet equal to '0'.
- 16 2. When the Generic Security Protocol is ACTIVE, the access terminal shall set the
17 SecurityLayerFormat field in the Header of the AC MAC Layer Packet equal to '1'.

1 **9 MAC LAYER TESTS**

2 This section includes tests for Session Layer of [1].

3 **9.1 Default Control Channel MAC Protocol Tests**

4 9.1.1 Access Network Test

5 9.1.1.1 Control Channel Header Fields in Synchronous Capsule Test

6 9.1.1.1.1 Definition

7 This test verifies that the SynchronousCapsule, LastPacket, Offset and FirstPacket fields
8 in the CC Header of the first CC MAC packet in a Synchronous capsule are set correctly.

9 9.1.1.1.2 Traceability

10 See section 9.2.6.1.4.1.2 of [1].

11 9.1.1.1.3 Test Procedure

- 12 a. Instruct the access terminal to record the Synchronous Control Channel MAC layer
13 packets received.
- 14 b. Verify that the SynchronousCapsule field in the Control Channel Header meets the
15 minimum standard as per bullet 1 in 9.1.1.1.4.
- 16 c. Verify that the LastPacket field in the Control Channel Header meets the
17 minimum standard as per bullet 1 in 9.1.1.1.4.
- 18 d. Verify that the Offset field in the Control Channel Header for the first CC MAC
19 Packet meets the minimum standard as per bullet 2 in 9.1.1.1.4.
- 20 e. Verify that the FirstPacket field in the Control Channel Header meets the
21 minimum standard as per bullet 3 in 9.1.1.1.4.

22 9.1.1.1.4 Minimum Standard

- 23 1. The access network shall set the SynchronousCapsule field, in the CC Header of
24 the CC MAC packets in a Synchronous Control Channel capsule, equal to '1'.
- 25 2. The access network shall set the LastPacket field, in the CC Header of the Last CC
26 MAC packet in a Synchronous Control Channel capsule, equal to '1'; otherwise, the
27 LastPacket field shall be set equal to '0'. "Last CC MAC Packet" is defined as the
28 packet such that no other Synchronous Control Channel MAC packet is received
29 until the next Control Channel cycle.
- 30 3. The access network shall set the Offset field, in the CC Header of the First CC MAC
31 packet in a Synchronous Control Channel capsule, equal to the value
32 corresponding to the number of slots by which the start of the Synchronous Capsule
33 is offset with respect to the start of the Control Channel cycle.

- 1 4. The access network shall set the FirstPacket field, in the CC Header of the first CC
2 MAC packet in a Synchronous Control Channel capsule, equal to '1'.

3 9.1.1.2 ConfigurationRequest Message Response Test

4 9.1.1.2.1 Definition

5 This test verifies that the access network responds to a Default Control Channel MAC
6 Protocol *ConfigurationRequest* message with a Default Control Channel MAC Protocol
7 *ConfigurationResponse* message.

8 9.1.1.2.2 Traceability

9 See section 13.7 of [1].

10 9.1.1.2.3 Test Procedure

- 11 a. Instruct the access terminal to set up a connection with the access network.
12 b. Instruct the access terminal to send a Control Channel MAC Protocol
13 *ConfigurationRequest* message.
14 c. Verify that the access network meets the minimum standard as per 9.1.1.2.4.

15 9.1.1.2.4 Minimum Standard

16 The access network shall respond to a Default Control Channel MAC Protocol
17 *ConfigurationRequest* message with a corresponding Default Control Channel MAC Protocol
18 *ConfigurationResponse* message.

19 9.1.2 Access Terminal Test

20 9.1.2.1 *ConfigurationRequest* Message Response Test

21 9.1.2.1.1 Definition

22 This test verifies that the access terminal responds to a Default Control Channel MAC
23 Protocol *ConfigurationRequest* message with a Default Control Channel MAC Protocol
24 *ConfigurationResponse* message while in the access network Initiated State of the Session
25 Configuration Protocol.

26 9.1.2.1.2 Traceability

27 See section 13.7 of [1].

28 9.1.2.1.3 Test Procedure

- 29 a. Instruct the access terminal to set up a connection with the access network.
30 b. Instruct the access network to send a Session Configuration Protocol
31 *ConfigurationStart* message.

- 1 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
- 2 message from the access terminal.
- 3 d. Instruct the access network to send a Default Control Channel MAC Protocol
- 4 *ConfigurationRequest* message to the access terminal.
- 5 e. Verify that the access terminal meets the minimum standard as per 9.1.2.1.4.

6 9.1.2.1.4 Minimum Standard

7 The access terminal shall respond to the Default Control Channel MAC Protocol
8 *ConfigurationRequest* message with a corresponding Default Control Channel MAC Protocol
9 *ConfigurationResponse* message.

10 **9.2 Enhanced Control Channel MAC Protocol Tests**

11 9.2.1 Access Network Test

12 9.2.1.1 Control Channel Header Fields in Synchronous Capsule Test

13 9.2.1.1.1 Definition

14 This test verifies that the SynchronousCapsule, LastPacket, Offset and FirstPacket fields
15 in the CC Header of the first CC MAC packet in a Synchronous capsule are set correctly.

16 9.2.1.1.2 Traceability

17 See section 9.2.6.1.4.1.2 and 9.3.7.1.4.1.2 of [1].

18 9.2.1.1.3 Test Procedure

- 19 a. Instruct the access terminal to record the Synchronous Control Channel MAC layer
- 20 packets received.
- 21 b. Verify that the SynchronousCapsule field in the Control Channel Header meets the
- 22 minimum standard as per bullet 1 in 9.2.1.1.4.
- 23 c. Verify that the LastPacket field in the Control Channel Header meets the
- 24 minimum standard as per bullet 1 in 9.2.1.1.4.
- 25 d. Verify that the Offset field in the Control Channel Header for the first CC MAC
- 26 Packet meets the minimum standard as per bullet 2 in 9.2.1.1.4.
- 27 e. Verify that the FirstPacket field in the Control Channel Header meets the
- 28 minimum standard as per bullet 3 in 9.2.1.1.4.

29 9.2.1.1.4 Minimum Standard

- 30 1. The access network shall set the SynchronousCapsule field, in the CC Header of
- 31 the CC MAC packets in a Synchronous Control Channel capsule, equal to '1'.
- 32 2. The access network shall set the LastPacket field, in the CC Header of the Last CC
- 33 MAC packet in a Synchronous Control Channel capsule, equal to '1'; otherwise, the

1 LastPacket field shall be set equal to '0'. "Last CC MAC Packet" is defined as the
2 packet such that no other Synchronous Control Channel MAC packet is received
3 until the next Control Channel cycle.

4 3. The access network shall set the Offset field, in the CC Header of the First CC MAC
5 packet in a Synchronous Control Channel capsule, equal to the value
6 corresponding to the number of slots by which the start of the Synchronous Capsule
7 is offset with respect to the start of the Control Channel cycle.

8 4. The access network shall set the FirstPacket field, in the CC Header of the first CC
9 MAC packet in a Synchronous Control Channel capsule, equal to '1'.

10 9.2.1.2 Control Channel Header Fields in Sub-Synchronous Capsule Test

11 9.2.1.2.1 Definition

12 This test verifies that the SynchronousCapsule, LastPacket, Offset and FirstPacket fields
13 in the CC Header of the first CC MAC packet in a Sub-Synchronous capsule are set
14 correctly.

15 9.2.1.2.2 Traceability

16 See section 9.3.7.1.4.1.4 of [1].

17 9.2.1.2.3 Test Procedure

- 18 a. Instruct the access terminal to negotiate the use of the either Multi-Flow Packet
19 Application bound to the service network (app type = 0x0005) or or Enhanced Multi-
20 Flow Packet Application bound to the service access network (app type = 0x0009) or
21 Multi-Link Multi-Flow Packet Application bound to the service access network (app
22 type = 0x000D). During session configuration set
23 PreferredControlChannelCycleEnabled to 1. If the access terminal supports a value
24 of SlotCycle1 that is less than 0x06, set SlotCycle1 to a value less than 0x06 in the
25 SlottedMode Attribute of the Enhanced Idle State Protocol. After a successful
26 negotiation, instruct the access terminal to close the connection by sending a
27 *ConnectionClose* message with SuspendEnable field set equal to '0'.
- 28 b. Instruct the access terminal to record the Sub-Synchronous Control Channel MAC
29 layer and Synchronous Control Channel MAC layer packets received.
- 30 c. Instruct the access network to send a Ping directed to the access terminal during
31 Period1.
- 32 d. If a packet is received in the Sub-Synchronous Control Channel, verify that the
33 SynchronousCapsule field in the Control Channel Header meets the minimum
34 standard as per bullet 1 in 9.2.1.2.4.
- 35 e. Verify that the LastPacket field in the Control Channel Header meets the
36 minimum standard as per bullet 1 in 9.2.1.2.4.

- 1 f. Verify that the Offset field in the Control Channel Header for the first CC MAC
2 Packet meets the minimum standard as per bullet 2 in 9.2.1.2.4.
- 3 g. Verify that the FirstPacket field in the Control Channel Header meets the
4 minimum standard as per bullet 3 in 9.2.1.2.4.

5 9.2.1.2.4 Minimum Standard

- 6 1. The access network shall set the SynchronousCapsule field, in the CC Header of
7 the CC MAC packets in a Sub-Synchronous Control Channel capsule, equal to '0'.
- 8 2. The access network shall set the LastPacket field in a Sub-Synchronous Control
9 Channel capsule to '1'.
- 10 3. The access network shall set the Offset field in a Sub-Synchronous Control
11 Channel capsule to '0'.
- 12 4. The access network shall set the FirstPacket field in a Sub-Synchronous Control
13 Channel capsule to '1'.

14 9.2.1.3 ConfigurationRequest Message Response Test

15 9.2.1.3.1 Definition

16 This test verifies that the access network responds to an Enhanced Control Channel MAC
17 Protocol *ConfigurationRequest* message with an Enhanced Control Channel MAC Protocol
18 *ConfigurationResponse* message.

19 9.2.1.3.2 Traceability

20 See section 8.3.5.3 and 13.7 of [1].

21 9.2.1.3.3 Test Procedure

- 22 a. Instruct the access terminal to set up a connection with the access network.
- 23 b. Instruct the access terminal to send a Control Channel MAC Protocol
24 *ConfigurationRequest* message.
- 25 c. Verify that the access network meets the minimum standard as per 9.2.1.3.4.

26 9.2.1.3.4 Minimum Standard

27 The access network shall respond to an Enhanced Control Channel MAC Protocol
28 *ConfigurationRequest* message with a corresponding Enhanced Control Channel MAC
29 Protocol *ConfigurationResponse* message.

1 9.2.2 Access Terminal Test

2 9.2.2.1 ConfigurationRequest Message Response Test

3 9.2.2.1.1 Definition

4 This test verifies that the access terminal responds to an Enhanced Control Channel MAC
5 Protocol *ConfigurationRequest* message with an Enhanced Control Channel MAC Protocol
6 *ConfigurationResponse* message while in the access network Initiated State of the Session
7 Configuration Protocol.

8 9.2.2.1.2 Traceability

9 See section 8.3.5.3 and 13.7 of [1].

10 9.2.2.1.3 Test Procedure

- 11 a. Instruct the access terminal to set up a connection with the access terminal.
- 12 b. Instruct the access network to send a Session Configuration Protocol
13 *ConfigurationStart* message.
- 14 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
15 message from the access terminal.
- 16 d. Instruct the access network to send an Enhanced Control Channel MAC Protocol
17 *ConfigurationRequest* message to the access terminal.
- 18 e. Verify that the access terminal meets the minimum standard as per 9.2.2.1.4.

19 9.2.2.1.4 Minimum Standard

20 The access terminal shall respond to the Enhanced Control Channel MAC Protocol
21 *ConfigurationRequest* message with a corresponding Enhanced Control Channel MAC
22 Protocol *ConfigurationResponse* message.

23 **9.3 Default Access Channel MAC Protocol Tests**

24 9.3.1 Access Network Tests

25 9.3.1.1 *AccessParameters* Message Transmission Test

26 9.3.1.1.1 Definition

27 This test verifies that the access network periodically transmits the *AccessParameters*
28 message on the Control Channel.

29 9.3.1.1.2 Traceability

30 See section 9.4.6.2.6 of [1].

1 9.3.1.1.3 Test Procedure

- 2 a. Instruct the access terminal to record the messages received on the Control
3 Channel.
- 4 b. Verify that the access network meets the minimum standard as per 9.3.1.1.4.

5 9.3.1.1.4 Minimum Standard

6 The access network shall transmit an *AccessParameters* message on the Control Channel
7 at least once every $\text{Min}(N_{\text{ACMPAccessParameters}}, 5.12 \text{ seconds})$.

8 9.3.1.2 *ConfigurationRequest* Message Response Test

9 9.3.1.2.1 Definition

10 This test verifies that the access network responds to a Default Access Channel MAC
11 Protocol *ConfigurationRequest* message with a Default Access Channel MAC Protocol
12 *ConfigurationResponse* message.

13 9.3.1.2.2 Traceability

14 See section 13.7 of [1].

15 9.3.1.2.3 Test Procedure

- 16 a. Instruct the access terminal to set up a connection with the access network.
- 17 b. Instruct the access terminal to send an Access Channel MAC Protocol
18 *ConfigurationRequest* message.
- 19 c. Verify that the access network meets the minimum standard as per 9.3.1.2.4.

20 9.3.1.2.4 Minimum Standard

21 The access network shall respond to a Default Access Channel MAC Protocol
22 *ConfigurationRequest* message with a corresponding Default Access Channel MAC Protocol
23 *ConfigurationResponse* message.

24 9.3.2 Access Terminal Tests

25 9.3.2.1 *ConfigurationRequest* Message Response Test

26 9.3.2.1.1 Definition

27 This test verifies that if the access terminal receives a Default Access Channel MAC
28 Protocol *ConfigurationRequest* message while in the access network Initiated State of the
29 Session Configuration Protocol, then it responds with a Default Access Channel MAC
30 Protocol *ConfigurationResponse* message.

31 9.3.2.1.2 Traceability

32 See section 13.7 of [1].

1 9.3.2.1.3 Test Procedure

- 2 a. Instruct the access terminal to set up a connection with the access terminal.
- 3 b. Instruct the access network to send a Session Configuration Protocol
4 *ConfigurationStart* message.
- 5 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
6 message from the access terminal.
- 7 d. Instruct the access network to send a Default Access Channel MAC Protocol
8 *ConfigurationRequest* message to the access terminal.
- 9 e. Verify that the access terminal meets the minimum standard as per 9.3.2.1.4.

10 9.3.2.1.4 Minimum Standard

11 The access terminal shall respond to a Default Access Channel MAC Protocol
12 *ConfigurationRequest* message with a corresponding Default Access Channel MAC Protocol
13 *ConfigurationResponse* message.

14 **9.4 Enhanced Access Channel MAC Protocol Tests**

15 9.4.1 Access Network Tests

16 9.4.1.1 AccessParameters Message Transmission Test

17 9.4.1.1.1 Definition

18 This test verifies that the access network periodically transmits the *AccessParameters*
19 message on the Control Channel. It is applicable only to access network supporting
20 Enhanced Access Channel MAC protocol.

21 9.4.1.1.2 Traceability

22 See section 9.5.6.1.4.2 of [1].

23 9.4.1.1.3 Test Procedure

- 24 a. Instruct the access terminal to record the messages received on the Control
25 Channel.
- 26 b. Verify that the access network meets the minimum standard as per 9.4.1.1.4.

27 9.4.1.1.4 Minimum Standard

28 The access network shall transmit an *AccessParameters* message on the Control Channel
29 at least once every $\text{Min}(N_{\text{ACMPAccessParameters}}, 5.12 \text{ seconds})$.

1 9.4.1.2 ConfigurationRequest Message Response Test

2 9.4.1.2.1 Definition

3 This test verifies that the access network responds to an Enhanced Access Channel MAC
4 Protocol *ConfigurationRequest* message with an Enhanced Access Channel MAC Protocol
5 *ConfigurationResponse* message. It is applicable only to access network supporting
6 Enhanced Access Channel MAC protocol.

7 9.4.1.2.2 Traceability

8 See section 8.5.5.3 and 13.7 of [1].

9 9.4.1.2.3 Test Procedure

- 10 a. Instruct the access terminal to set up a connection with the access network.
11 b. Instruct the access terminal to send an Access Channel MAC Protocol
12 *ConfigurationRequest* message.
13 c. Verify that the access network meets the minimum standard as per 9.4.1.2.4.

14 9.4.1.2.4 Minimum Standard

15 The access network shall respond to an Enhanced Access Channel MAC Protocol
16 *ConfigurationRequest* message with a corresponding Enhanced Access Channel MAC
17 Protocol *ConfigurationResponse* message.

18 9.4.2 Access Terminal Tests

19 9.4.2.1 ConfigurationRequest Message Response Test

20 9.4.2.1.1 Definition

21 This test verifies that if the access terminal receives an Enhanced Access Channel MAC
22 Protocol *ConfigurationRequest* message while in the access network Initiated State of the
23 Session Configuration Protocol, then it responds with an Enhanced Access Channel MAC
24 Protocol *ConfigurationResponse* message.

25 9.4.2.1.2 Traceability

26 See section 8.5.5.3 and 13.7 of [1].

27 9.4.2.1.3 Test Procedure

- 28 a. Instruct the access terminal to set up a connection with the access terminal.
29 b. Instruct the access network to send a Session Configuration Protocol
30 *ConfigurationStart* message.
31 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
32 message from the access terminal.

- 1 d. Instruct the access network to send an Enhanced Access Channel MAC Protocol
2 *ConfigurationRequest* message to the access terminal.
- 3 e. Verify that the access terminal meets the minimum standard as per 9.4.2.1.4.

4 9.4.2.1.4 Minimum Standard

5 The access terminal shall respond to an Enhanced Access Channel MAC Protocol
6 *ConfigurationRequest* message with a corresponding Enhanced Access Channel MAC
7 Protocol *ConfigurationResponse* message.

8 **9.5 Default Forward Traffic Channel MAC Protocol Tests**

9 9.5.1 Access Network Tests

10 9.5.1.1 FixedModeEnable Message Response Test

11 9.5.1.1.1 Definition

12 This test verifies that the access network responds to the receipt of a *FixedModeEnable*
13 message from the access terminal by going to the Fixed Rate State and transmitting
14 packets at the fixed rate requested in the *FixedModeEnable* message. After the expiration
15 of the EndTime value indicated in the *FixedModeEnable* message, the access network
16 transitions to the Variable Rate State.

17 9.5.1.1.2 Traceability

18 See section 9.6.6.1.4 and 9.6.6.1.5 of [1].

19 9.5.1.1.3 Test Procedure

- 20 a. Instruct the access terminal to negotiate the use of the Default Packet Application
21 bound to the service access network (app type = 0x0002).
- 22 b. Instruct the access terminal to set up a connection and establish a data call with
23 the access network.
- 24 c. Initiate downloading of a file from the service access network. A representative
25 data file is RAND200.BIN defined in ANNEX D of [2].
- 26 d. Instruct the access terminal to go into the Fixed Rate State by covering its DRC
27 with a null cover and send a *FixedModeEnable* message with DRCCover (serving
28 sector), RequestedRateDRCValue, and EndTime fields set appropriately. The
29 RequestedRateDRCValue should be lower than any of the variable data rates
30 recorded recently.
- 31 e. Verify that the access network meets the minimum standard as per bullet 1 in
32 9.5.1.1.4.
- 33 f. After the expiration of the EndTime associated with the Fixed Rate State, instruct
34 the access terminal to set the DRC equal to a fixed value higher than the
35 RequestedRateDRCValue in step c.

- 1 g. Verify that the access network meets the minimum standard as per bullet 1 in
2 9.5.1.1.4.

3 9.5.1.1.4 Minimum Standard

- 4 1. Before the expiration of the EndTime associated with the Fixed Rate State, the
5 access network shall transmit Fixed Rate Packets at the rate requested in a
6 *FixedModeEnable* message.
- 7 2. After the expiration of the EndTime associated with the Fixed Rate State, the
8 access network shall transition to Variable Rate State by transmitting Variable
9 Rate Packets at the rate requested on the DRC channel in step e.

10 9.5.1.2 RABOffset Support Test

11 9.5.1.2.1 Definition

12 This section verifies that the access network supports all possible values of RABOffset. As
13 specified in [1], the range of RABOffset is from 0 (RABOffset = 000) to 7 (RABOffset = 111)
14 slots.

15 9.5.1.2.2 Traceability

16 See section 7.8.6.2.2 and 10.4.1.3.2.2.3 of [1].

17 9.5.1.2.3 Test Procedure

- 18 a. Instruct the access terminal to set up a connection and establish a data call with
19 the access terminal.
- 20 b. Instruct the access network to send a *TrafficChannelAssignment* message with
21 RABLength set to 8 slots and RABOffset set to '000'.
- 22 c. Instruct the access network to send an alternating pattern of one '1' RAB followed by
23 one '0' RAB.
- 24 d. Instruct the Access terminal to close the connection.
- 25 e. Repeat the steps a through d with other values of RABOffset ranging from '001' to
26 '111' sent in the *TrafficChannelAssignment* message.
- 27 f. Verify that the access network meets the minimum standard as 9.5.1.2.4.

28 9.5.1.2.4 Minimum Standard

29 The RAB transition shall start in a slot that satisfies $T \bmod \text{RABLength} = \text{RABOffset}$
30 where T is the CDMA System Time in slots.

1 9.5.1.3 ConfigurationRequest Message Response Test

2 9.5.1.3.1 Definition

3 This test verifies that the access network responds to a Default Forward Traffic Channel
4 MAC Protocol *ConfigurationRequest* message with a Default Forward Traffic Channel MAC
5 Protocol *ConfigurationResponse* message.

6 9.5.1.3.2 Traceability

7 See section 13.7 of [1].

8 9.5.1.3.3 Test Procedure

- 9 a. Instruct the access terminal to set up a connection with the access network.
10 b. Instruct the access terminal to send a Default Forward Traffic Channel MAC
11 Protocol *ConfigurationRequest* message.
12 c. Verify that the access network meets the minimum standard as per 9.5.1.3.4.

13 9.5.1.3.4 Minimum Standard

14 The access network shall respond to a Default Forward Traffic Channel MAC Protocol
15 *ConfigurationRequest* message with a corresponding Default Forward Traffic Channel MAC
16 Protocol *ConfigurationResponse* message.

17 9.5.2 Access Terminal Tests

18 9.5.2.1 ConfigurationRequest Message Response Test

19 9.5.2.1.1 Definition

20 This test verifies that if the access terminal receives a Default Forward Traffic Channel
21 MAC Protocol *ConfigurationRequest* message while in the access network Initiated State of
22 the Session Configuration Protocol, then it responds with a Default Forward Traffic
23 Channel MAC Protocol *ConfigurationResponse* message.

24 9.5.2.1.2 Traceability

25 See section 13.7 of [1].

26 9.5.2.1.3 Test Procedure

- 27 a. Instruct the access terminal to set up a connection with the access network.
28 b. Instruct the access network to send a Session Configuration Protocol
29 *ConfigurationStart* message.
30 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
31 message from the access terminal.

- 1 d. Instruct the access network to send a Forward Traffic Channel MAC Protocol
2 *ConfigurationRequest* message to the access terminal.
- 3 e. Verify that the access terminal meets the minimum standard as per 9.5.2.1.4.

4 9.5.2.1.4 Minimum Standard

5 The access terminal shall respond to a Default Forward Traffic Channel MAC Protocol
6 *ConfigurationRequest* message with a corresponding Default Forward Traffic Channel MAC
7 Protocol *ConfigurationResponse* message.

8 **9.6 Enhanced Forward Traffic Channel MAC Protocol Tests**

9 9.6.1 Access Network Tests

10 9.6.1.1 *FixedModeEnable* Message Response Test

11 9.6.1.1.1 Definition

12 This test verifies that the access network responds to the receipt of a *FixedModeEnable*
13 message from the access terminal by going to the Fixed Rate State and transmitting
14 packets at the fixed rate requested in the *FixedModeEnable* message. After the expiration
15 of the *EndTime* value indicated in the *FixedModeEnable* message, the access network
16 transitions to the Variable Rate State.

17 9.6.1.1.2 Traceability

18 See section 9.7.6.1.8.1.2 of [1].

19 9.6.1.1.3 Test Procedure

- 20 a. Instruct the access terminal to negotiate the use of either Multi-Flow Packet
21 Application bound to the service access network (app type = 0x0005) or Enhanced
22 Multi-Flow Packet Application bound to the service access network (app type =
23 0x0009) or Multi-Link Multi-Flow Packet Application bound to the service access
24 network (app type = 0x000D).
- 25 b. Instruct the access terminal to set up a connection and establish a data call with
26 the access network.
- 27 c. Initiate downloading of a file from the service access network. A representative
28 data file is RAND200.BIN defined in ANNEX D of [2].
- 29 d. Instruct the access terminal to go into the Fixed Rate State by covering its DRC
30 with a null cover and send a *FixedModeEnable* message with *DRCCover* (serving
31 sector), *RequestedRateDRCValue*, and *EndTime* fields set appropriately. The
32 *RequestedRateDRCValue* should be lower than any of the variable data rates
33 recorded recently.
- 34 e. Verify that the access network meets the minimum standard as per bullet 1 in
35 9.6.1.1.4.

- 1 f. After the expiration of the *EndTime* associated with the Fixed Rate State, instruct
2 the access terminal to set the DRC equal to a fixed value higher than the
3 *RequestedRateDRCValue* in step c.
- 4 g. Verify that the access network meets the minimum standard as per bullet 1 in
5 9.6.1.1.4.

6 9.6.1.1.4 Minimum Standard

- 7 1. Before the expiration of the *EndTime* associated with the Fixed Rate State, the
8 access network shall transmit Fixed Rate Packets at the rate requested in a
9 *FixedModeEnable* message.
- 10 2. After the expiration of the *EndTime* associated with the Fixed Rate State, the
11 access network shall transition to Variable Rate State by transmitting Variable
12 Rate Packets at the rate requested on the DRC channel in step e.

13 9.6.1.2 *ConfigurationRequest* Message Response Test

14 9.6.1.2.1 Definition

15 This test verifies that the access network responds to an Enhanced Forward Traffic
16 Channel MAC Protocol *ConfigurationRequest* message with an Enhanced Forward Traffic
17 Channel MAC Protocol *ConfigurationResponse* message.

18 9.6.1.2.2 Traceability

19 See section 13.7 of [1].

20 9.6.1.2.3 Test Procedure

- 21 a. Instruct the access terminal to set up a connection with the access network.
- 22 b. Instruct the access terminal to send an Enhanced Forward Traffic Channel MAC
23 Protocol *ConfigurationRequest* message.
- 24 c. Verify that the access network meets the minimum standard as per 9.6.1.2.4.

25 9.6.1.2.4 Minimum Standard

26 The access network shall respond to an Enhanced Forward Traffic Channel MAC Protocol
27 *ConfigurationRequest* message with a corresponding Enhanced Forward Traffic Channel
28 MAC Protocol *ConfigurationResponse* message.

29 9.6.2 Access Terminal Tests

30 9.6.2.1 *ConfigurationRequest* Message Response Test

31 9.6.2.1.1 Definition

32 This test verifies that if the access terminal receives an Enhanced Forward Traffic
33 Channel MAC Protocol *ConfigurationRequest* message while in the access network Initiated

1 State of the Session Configuration Protocol, then it responds with an Enhanced Forward
2 Traffic Channel MAC Protocol *ConfigurationResponse* message.

3 9.6.2.1.2 Traceability

4 See section 13.7 of [1].

5 9.6.2.1.3 Test Procedure

- 6 a. Instruct the access terminal to set up a connection with the access terminal.
- 7 b. Instruct the access network to send a Session Configuration Protocol
8 *ConfigurationStart* message.
- 9 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
10 message from the access terminal.
- 11 d. Instruct the access network to send an Enhanced Forward Traffic Channel MAC
12 Protocol *ConfigurationRequest* message to the access terminal.
- 13 e. Verify that the access terminal meets the minimum standard as per 9.6.2.1.4.

14 9.6.2.1.4 Minimum Standard

15 The access terminal shall respond to an Enhanced Forward Traffic Channel MAC Protocol
16 *ConfigurationRequest* message with a corresponding Enhanced Forward Traffic Channel
17 MAC Protocol *ConfigurationResponse* message.

18 9.6.2.2 Parsing of Multi-User MAC Packets

19 9.6.2.2.1 Definition

20 Multi-User MAC packets have been introduced in [1]. Multi-User MAC packets carry one or
21 more Security Layer packets addressed to one or more access terminals. This test verifies
22 that if access terminal is able to decode a physical layer packet containing a Multi-User
23 MAC packet, then it parses the contents of the Multi-User packet and obtains any security
24 layer packet addressed to it.

25 9.6.2.2.2 Traceability

26 See section 9.7.6.1.1 and 9.7.6.1.5 of [1].

27 9.6.2.2.3 Test Procedure

- 28 a. Instruct the access terminal to negotiate the use of either Multi-Flow Packet
29 Application bound to the service access network (app type = 0x0005) or Enhanced
30 Multi-Flow Packet Application bound to the service access network (app type =
31 0x0009) or Multi-Link Multi-Flow Packet Application bound to the service access
32 network (app type = 0x000D).
- 33 b. Instruct the access terminal to set up a connection with the access network.

- 1 c. Use access network initiated GAUP *AttributeUpdateRequest* message to set the
- 2 MultiUserPacketsEnabled attribute to 0x01.
- 3 d. Instruct the access network to transmit a MultiUser MAC Packet to the access
- 4 terminal.
- 5 e. Repeat step d until the access network receives a positive Hybrid ARQ from the
- 6 access terminal.
- 7 f. Verify that the access terminal meets the minimum standard as specified in
- 8 9.6.2.2.4.

9 9.6.2.2.4 Minimum Standard

10 The access terminal shall parse the contents of Security Layer packet in the MultiUser
11 MAC packet.

12 **9.7 Default Reverse Traffic Channel MAC Protocol Tests**

13 9.7.1 Access Network Tests

14 9.7.1.1 *ConfigurationRequest* Message Response Test

15 9.7.1.1.1 Definition

16 This test verifies that the access network responds to a Default Reverse Traffic Channel
17 MAC Protocol *ConfigurationRequest* message with a Default Reverse Traffic Channel MAC
18 Protocol *ConfigurationResponse* message.

19 9.7.1.1.2 Traceability

20 See section 13.7 of [1].

21 9.7.1.1.3 Test Procedure

- 22 a. Instruct the access terminal to set up a connection with the access network.
- 23 b. Instruct the access terminal to send a Reverse Traffic Channel MAC Protocol
- 24 *ConfigurationRequest* message.
- 25 c. Verify that the access network meets the minimum standard as per 9.7.1.1.4.

26 9.7.1.1.4 Minimum Standard

27 The access network shall respond to a Default Reverse Traffic Channel MAC Protocol
28 *ConfigurationRequest* message with a Default Reverse Traffic Channel MAC Protocol
29 *ConfigurationResponse* message.

1 9.7.1.2 Reception of Reverse Traffic Channel with Different Frame Offsets

2 9.7.1.2.1 Definition

3 The access terminal shall delay the Reverse Data Channel and Reverse Rate Indicator
4 Channel by FrameOffset slots with respect to the system-time-aligned frame boundary.

5 9.7.1.2.2 Traceability

6 See section 9.9.6.1.5.1 and 7.8.6.2.2 of [1].

7 9.7.1.2.3 Test Procedure

- 8 a. Instruct the access terminal to set up a connection with the access network.
- 9 b. Note the value of FrameOffset generated by the access network and assigned in the
10 *TrafficChannelAssignment* message and increment N(value) by one.
- 11 c. Instruct the access terminal to send a *ConnectionClose* message with
12 SuspendEnable set to '0'.
- 13 d. Repeat steps a through c 512 times.
- 14 e. Compute $D^2 = \sum_i (N_i - 32)^2 / 32$.
- 15 f. Verify that the access network meets the requirement as specified in 9.7.1.2.4

16 9.7.1.2.4 Minimum Standard

17 The value of D^2 should be less than 30.58.

18 9.7.2 Access Terminal Tests

19 9.7.2.1 *ConfigurationRequest* Message Response Test

20 9.7.2.1.1 Definition

21 This test verifies that if the access terminal receives a Reverse Traffic Channel MAC
22 Protocol *ConfigurationRequest* message while in the access network Initiated State of the
23 Session Configuration Protocol, then it responds with a Reverse Traffic Channel MAC
24 Protocol *ConfigurationResponse* message.

25 9.7.2.1.2 Traceability

26 See section 13.7 of [1].

27 9.7.2.1.3 Test Procedure

- 28 a. Instruct the access terminal to set up a connection with the access terminal.
- 29 b. Instruct the access network to send a Session Configuration Protocol
30 *ConfigurationStart* message.
- 31 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
32 message from the access terminal.

- 1 d. Instruct the access network to send a Reverse Traffic Channel MAC Protocol
2 *ConfigurationRequest* message to the access terminal.
- 3 e. Verify that the access terminal meets the minimum standard as per 9.7.2.1.4.

4 9.7.2.1.4 Minimum Standard

5 The access terminal shall respond to a Default Reverse Traffic Channel MAC Protocol
6 *ConfigurationRequest* message with a Reverse Traffic Channel MAC Protocol
7 *ConfigurationResponse* message.

8 **9.8 Subtype 3 Reverse Traffic Channel MAC Protocol**

9 9.8.1 Access Network Tests

10 None.

11 9.8.2 Access terminal Tests

12 9.8.2.1 TxT2P Ramping with Variable Allocation Test

13 9.8.2.1.1 Definition

14 This test verifies that the access terminal supporting Subtype 3 or MultiCarrier RTC MAC
15 protocol will transmit at a payload high enough without violating RTC MAC algorithm. In
16 this test, slot 0 refers to the first slot that the access terminal starts to transmit a non-
17 zero payload from MACFlow with MACFlowID equal to one.

18 In this test, the access terminal perceived network loading is controlled by setting the
19 RAB. When the RAB value of '0' is transmitted the access terminal may be able to increase
20 its transmission rate. The rate at which the physical layer transmissions rate will
21 increase is primarily dependent on the design of the T2PInflow parameter. T2PInflow is a
22 function of the perceived sector loading, i.e., FRAB. The T2PInflow parameter for MACFlow
23 with MACFlowID equal to one is configured such that the T2PInflow allocation reacts to the
24 loading in the access network, i.e. is affected by value of FRAB and QRAB. Thus, when the
25 RAB is set to '0', the access terminal is able to ramp up its transmission rate. Similarly,
26 when the RAB bit is set to '1', the access terminal ramps its rate down. The rate of
27 ramping up and down is dependent T2PInflow values. Further, due to the configuration of
28 various parameters, ramping up and ramping down results in oscillation between any two
29 Packet Sizes followed by a period of transmission at the higher Packet Size. For example,
30 say at a certain point the rate is oscillating between 1024 bits and 1536 bits. Then, the
31 transmitted Packet Size will stabilize at 1536 bits for a period and then oscillate between
32 the next higher rates of 1536 and 2048. The number of slots between F_{2048} (the first
33 occurrence of PS 2048) and L_{1536} (the last occurrence of PS 1536) should be close to an
34 expected value within margin of error. The length of this period where the Packet Size
35 oscillates between two rates is imposed as a minimum standard in Table 9.8.2.1.4-2 and
36 Table 9.8.2.1.4-3. Similar oscillatory behavior will hold for ramping down of rates when the
37 RAB bit is set to '1'. The number of slots that the Packet Size oscillates between two rates
38 is imposed as a minimum standard in Table 9.8.2.1.4-2 and Table 9.8.2.1.4-3. These tables

1 allow for $\pm 40\%$ margin of error from the expected results. Table 9.8.2.1.4-1 imposes a $\pm 10\%$
2 margin of error for the end-to-end ramping up and ramping down rate.

3 9.8.2.1.2 Traceability

4 See section 9.12.6.1.6.1.1 and 9.12.7 of [1] and [4].

5 9.8.2.1.3 Test Procedure

- 6 a. Connect the sector to the access terminal antenna connector.
- 7 b. Set I_{or} to -75 dBm.
- 8 c. Disable the occurrence of Reverse Link Silence Interval by setting
9 ReverseLinkSilenceDuration to 0x00.
- 10 d. Configure the access network to transmit an RAB value of '0' (unloaded) for 180
11 seconds and followed by an RAB value of '1' (loaded) for next 20 seconds. Log the
12 value of RAB transmitted by access network at each slot.
- 13 e. Map the RETAP to MACFlowID one. If value for any parameter is not specified, use
14 defaults from [1].
- 15 f. For RTC MAC, configure the MACFlow with MACFlowID equal to one transmission
16 mode to be High Capacity, BucketLevelMaxNV (NV = 0x01) to 0x00, and
17 HiCapTerminationTargetPS is 0x3 (4 sub-frames) for all packet size PS and ensure
18 that the access terminal is initially not transmitting any data on the Reverse
19 Traffic Channel.
- 20 g. Set up a Test Application session. Using SCP, in the TxT2PMax Attribute of the
21 Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values
22 specified in table 9.8.2.1.3-1.
- 23 h. Using SCP, negotiate TransmissionMode NV (NV = 0x00) to 0x01 (LoLat), FRABLow to
24 0x04 (-1), MergeThreshold to 0x05 (infinity), and MergeThresholdNV (NV = 0x01) to
25 0x06 (infinity). This ensures that signaling flow's data does not interfere with the
26 mac flow's data.
- 27 i. Open a connection. Configure the access network to transmit
28 RChannelGainIncluded set to '1' and RChannelGain set to '00' in the
29 *TrafficChannelAssignment* message.
- 30 j. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
31 PayloadThresh attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol to
32 0x03.

Table 9.8.2.1.3-1 T2PMaxPilotStrength

Field	Value (Hexadecimal)
NumPilotStrengthAxisValues	0x1 (1)
PilotStrengthAxis PilotStrengthAxis0	0x28 (-10 dB)
TxT2PmaxPilotStrengthAxis TxT2PmaxPilotStrengthAxis0	0x26 (19 dB)

- k. Using access network initiated GAUP *AttributeUpdateRequest* message, in the BucketFactor*NV* (*NV* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the fields to the values specified in table 9.8.2.1.3-2.

Table 9.8.2.1.3-2 BucketFactor

Field	Value (Hexadecimal)
NumT2PAxisValues	0x0 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis T2PAxis00	0x0 (0 dB)
FRABAxis FRABAxis0	0x8 (-1)
BucketFactorT2PAxisFRABAxis BucketFactorT2PAxis00FRABAxis0	0x0C (1.5)

- l. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PInflowRange*NV* (*NV* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to values specified in table 9.8.2.1.3-3.

Table 9.8.2.1.3-3 T2PInflowRange

Field	Value (Hexadecimal)
T2PInflowmin	0x23 (8.75 dB)
T2PInflowmax	0x78 (30 dB)

- m. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PTransitionFunction*NN* (*NN* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values specified in table 9.8.2.1.3-4.

1

Table 9.8.2.1.3-4 T2PUp and T2PDn

Field	Value (Hexadecimal)
NumT2PAxisValues	0x3 (3)
NumFRABAxisValues	0x0 (0)
T2PAxis	
T2PAxis00	0xf (3.75 dB)
T2PAxis01	0x28 (10 dB)
T2PAxis02	0x3a (14.5 dB)
T2PAxis03	0x4c (19 dB)
FRABAxis	
FRABAxis0	0x8 (-1)
T2PUpT2PAxisFRABAxis	
T2PUpT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PUpT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PUpT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PUpT2PAxis03FRABAxis0	0xd0 (-12 dB)
T2PDnT2PAxisFRABAxis	
T2PDnT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PDnT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PDnT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PDnT2PAxis03FRABAxis0	0xd0 (-12 dB)

- 2 n. In RETAP, set the BurstSize field of the BurstSizeMode parameter to 0xFFFF and
3 BurstPeriod field of the BurstPeriodMode parameter to 0xFFFF.
- 4 o. After the configuration of RETAP and RTC MAC parameters is complete, instruct
5 the access network to always positively acknowledge the transmission of a packet
6 on each sub-frame of the reverse link through the H-ARQ and P-ARQ bits.
- 7 p. Wait for RETAP to start generation of packets. Using access network initiated GAUP
8 *AttributeUpdateRequest* message, set the BucketLevelMaxNW (NW = 0x01) to 0x6C.
9 Ensure that the access terminal receives this message such that the RAB value
10 transmitted by the access network is '0' for at least the next 20 seconds.
- 11 q. Monitor the sequence of transmit payload on the Reverse Traffic Channel till RAB
12 value of '1' has been transmitted by the access network for 20 seconds. Note the
13 value of the slot number when the access terminal first transmits a payload size of
14 PS 6144 bits while the access network is transmitting an RAB value of '1' (referred
15 to 'R' in the minimum standard). Slot number should be noted with slot zero

1 referring to the first instance when the access terminal transmits a payload for
2 MACFlow with MACFlowID equal to one.

3 9.8.2.1.4 Minimum Standard

4 The access terminal shall transmit the payloads (data rates) during the time intervals as
5 specified in 9.8.2.1.4-1, Table 9.8.2.1.4-2 and Table 9.8.2.1.4-3. In Table 9.8.2.1.4-3, R
6 refers to the first slot when the access terminal transmits a payload size of 6144 bits while
7 the access network is transmitting an RAB value of '1' (loaded), Note slot 0 is the first slot
8 when the access terminal transmits payload from MACFlow with MACFlowID equal to one.³
9 FPS refers to the first slot in the given time interval where the access terminal transmits
10 at with a Payload Size PS. Similarly, L_{PS} refers to the last slot in the given time interval
11 where the access terminal transmits at with a Payload Size PS.

12 **Table 9.8.2.1.4-1 End to End Minimum Standard**

Time t (slots)	Payload (Nominal Data Rate)
$0 < t < (4220 * 0.9)$	6144 bits (230.4 kbps) or below
$(5340 * 1.1) \leq t < 6000$	8192 bits (307.2 kbps)
$R < t \leq R + (4640 * 0.9)$	1536 (57.6 kbps) or higher
$t \geq R + (4912 * 1.1)$	1024 bits (38.4 kbps) or lower

13

14

³ Before transmission from MAC Flow with MACFlowID equal to one, there will be LoLatency transmission on the reserse link due to data from signaling flow. This transmission does not indicate slot zero.

1

Table 9.8.2.1.4-2 Minimum Requirement for TxT2P Ramping Up

Lower Rate	Higher Rate	First Occurrence of higher rate before $t < 6000$	Last occurrence of lower rate before $t < 6000$	Expected number of slots for Rate Transition	Allowed Slots for Rate Transition (B)
768	1024	F_{1024}	L_{768}	112	$112 * 0.5$ $\leq L_{768} - F_{1024} \leq$ $112 * 1.5$
1024	1536	F_{1536}	L_{1024}	300	$300 * 0.6$ $\leq L_{1024} - F_{1536} \leq$ $300 * 1.4$
1536	2048	F_{2048}	L_{1536}	372	$372 * 0.6$ $\leq L_{1536} - F_{2048} \leq$ $372 * 1.4$
2048	3072	F_{3072}	L_{2048}	456	$456 * 0.6$ $\leq L_{2048} - F_{3072} \leq$ $456 * 1.4$
3072	4096	F_{4096}	L_{3072}	492	$492 * 0.6$ $\leq L_{3072} - F_{4096} \leq$ $492 * 1.4$
4096	6144	F_{6144}	L_{4096}	776	$776 * 0.6$ $\leq L_{4096} - F_{6144} \leq$ $776 * 1.4$
6144	8192	F_{8192}	L_{6144}	1120	$1120 * 0.6$ $\leq L_{6144} - F_{8192} \leq$ $1120 * 1.4$

2

3

4

5

6

1

2

Table 9.8.2.1.4-3 Minimum Requirement for TxT2P Ramping Down

Lower Rate	Higher Rate	First Occurrence of lower rate after slot t > 6000	Last occurrence of higher rate after slot t > 6000	Expected number of slots for Rate Transition	Allowed Slots for Rate Transition (B)
6144	8192	F_{6144}	L_{8192}	1072	$1072 * 0.6$ $\leq L_{8192} - F_{6144} \leq$ $1072 * 1.4$
4096	6144	F_{4096}	L_{6144}	784	$784 * 0.6$ $\leq L_{6144} - F_{4096} \leq$ $784 * 1.4$
3072	4096	F_{3072}	L_{4096}	452	$452 * 0.6$ $\leq L_{4096} - F_{3072} \leq$ $452 * 1.4$
2048	3072	F_{2048}	L_{3072}	456	$456 * 0.6$ $\leq L_{3072} - F_{2048} \leq$ $456 * 1.4$
1536	2048	F_{1536}	L_{2048}	352	$352 * 0.6$ $\leq L_{1536} - F_{2048} \leq$ $352 * 1.4$
1024	1536	F_{1024}	L_{1536}	272	$272 * 0.6$ $\leq L_{1536} - F_{1024} \leq$ $272 * 1.4$
768	1024	F_{768}	L_{1024}	100	$100 * 0.5$ $\leq L_{1024} - F_{768} \leq$ $100 * 1.5$

9.8.2.2 TxT2P Ramping with Fixed Allocation Test

9.8.2.2.1 Definition

This test verifies that the access terminal supporting Subtype 3 or MultiCarrier RTC MAC protocol will transmit at a payload high enough without violating RTC MAC algorithm. In this test, slot 0 refers to the first slot that the access terminal starts to transmit a non-zero payload from MACFlow with MACFlowID equal to one.

In this test, the access terminal perceived network loading is controlled by setting the RAB. When the RAB value of '0' is transmitted the access terminal may be able to increase its transmission rate. The rate at which the physical layer transmissions rate will increase is primarily dependent on the design of the T2PInflow parameter. Typically, T2PInflow is a function of the perceived sector loading, i.e. FRAB. However, in this test the T2PInflow parameters are made independent of loading. Here, the T2PInflow is designed in such a way that the access terminal is able to transmit 2048 or 1536 bits regardless of the sector loading.

9.8.2.2.2 Traceability

See section 9.12.6.1.6.1.1 and 9.12.7 of [1] and [4].

9.8.2.2.3 Test Procedure

- a. Connect the sector to the access terminal antenna connector.
- b. Set \bar{I}_or to -75 dBm.
- c. Disable the occurrence of Reverse Link Silence Interval by setting ReverseLinkSilenceDuration to 0x00.
- d. Configure the access network to transmit an RAB value of '0' (unloaded) for 180 seconds and followed by an RAB value of '1' (loaded) for next 20 seconds. Log the value of RAB transmitted by access network at each slot.
- e. Map the RETAP to MACFlow with MACFlowID equal to one. If value for any parameter is not specified, use defaults from [1].
- f. For RTC MAC, configure the MACFlow with MACFlowID equal to one transmission mode to be High Capacity, BucketLevelMaxNV (NV = 0x01) to 0x00, and HiCapTerminationTargetPS is 0x3 (4 sub-frames) for all packet size PS and ensure that the access terminal is initially not transmitting any data on the Reverse Traffic Channel.
- g. Set up a Test Application session. Using SCP, in the TxT2PMax Attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values specified in table 9.8.2.1.3-1.
- h. Open a connection. Configure the access network to transmit RACHannelGainIncluded set to 1 and RACHannelGain set to '00' in the *TrafficChannelAssignment* message.

- 1 i. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
 2 PayloadThresh attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol to
 3 0x03.
- 4 j. Using access network initiated GAUP *AttributeUpdateRequest* message, in the
 5 T2PInflowRange Attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol,
 6 set the attributes to the values specified in table 9.8.2.2.3-1.

7
 8
 9 **Table 9.8.2.2.3-1 T2PInflowRange**

Field	Value (Hexadecimal)
T2PInflowmin	0x23 (8.75 dB)
T2PInflowmax	0x34 (13 dB)

- 10 k. Using access network initiated GAUP *AttributeUpdateRequest* message, in the
 11 BucketFactor*NN* (*NN* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel
 12 MAC Protocol, set the fields to the values specified in table 9.8.2.2.3-2.

13 **Table 9.8.2.2.3-2 BucketFactor**

Field	Value (Hexadecimal)
NumT2PAxisValues	0x0 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis T2PAxis00	0x0 (0 dB)
FRABAxis FRABAxis0	0x8 (-1)
BucketFactorT2PAxisFRABAxis BucketFactorT2PAxis00FRABAxis0	0x09 (1.125)

- 14 l. Using access network initiated GAUP *AttributeUpdateRequest* message, in the
 15 T2PTransitionFunction*NN* (*NN* = 0x01) Attribute of the Subtype 3 Reverse Traffic
 16 Channel MAC Protocol, set the attributes to the values specified in table 9.8.2.2.3-3.

17
 18
 19
 20
 21

1
2
3
4
5
6
7
8
9
10

Table 9.8.2.2.3-3 T2Pup and T2PDn

Field	Value (Hexadecimal)
NumT2PAxisValues	0x2 (2)
NumFRABAxisValues	0x0 (0)
T2PAxis	
T2PAxis00	0x0 (0 dB)
T2PAxis01	0x34 (13 dB)
T2PAxis02	0x36 (13.5 dB)
FRABAxis	
FRABAxis0	0x8 (-1)
T2PUpT2PAxisFRABAxis	
T2PUpT2PAxis00FRABAxis0	0x34 (13 dB)
T2PUpT2PAxis01FRABAxis0	0x34 (13 dB)
T2PUpT2PAxis02FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxisFRABAxis	
T2PDnT2PAxis00FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxis01FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxis02FRABAxis0	0x88 (-30 dB)

- 11 m. In RETAP, set the BurstSize field of the BurstSizeMode parameter to 0xFFFF and
12 BurstPeriod field of the BurstPeriodMode parameter to 0xFFFF.
- 13 n. After the configuration of RETAP and RTC MAC parameters is complete, instruct
14 the access network to always positively acknowledge the transmission of a packet
15 on each sub-frame of the reverse link through the H-ARQ and P-ARQ bits.

- 1 o. Wait for RETAP to start generation of packets. Using access network initiated GAUP
 2 *AttributeUpdateRequest* message, set the *BucketLevelMaxNV* (*NV* = 0x01) to 0x63
 3 (24.75 dB). Ensure that the access terminal receives this message such that the
 4 RAB value transmitted by the access network is '0' for at least the next 20 seconds.
- 5 p. Monitor the sequence of transmit payload on the Reverse Traffic Channel till RAB
 6 value of '1' has been transmitted by the access network for 20 seconds.
- 7 q. Verify that the access terminal meets the minimum standard as per 9.8.2.2.4.

8 9.8.2.2.4 Minimum Standard

9 The access terminal shall transmit the payloads (data rates) during the time intervals as
 10 specified in table 9.8.2.2.4-1.

11
12
13
14 **Table 9.8.2.2.4-1 Minimum Requirement for Fixed Allocation TxT2P Ramping**

Time <i>t</i> (slots)	Payload (Nominal Data Rate)
120 ≤ <i>t</i> < 10880	2048 bits (76.8 kbps) or 1536 bits (57.6 kbps)

15 9.8.2.3 Rate Transition between sub-frames

16 This test is applicable only to access terminals that support Subtype 3 or *MultiCarrier*
 17 *Reverse Traffic Channel MAC* protocol.

18 9.8.2.3.1 Definition

19 The RTC payload that an access terminal can transmit in a sub-frame is limited by, among
 20 other constraints, the payload transmitted in the previous packets. This test will verify
 21 that, in the absence of other constraints, the access terminal will ramp up its RTC payload
 22 as allowed by *PermittedPayload*.

23 9.8.2.3.2 Traceability

24 See section 9.12.6.1.6.1.1 of [1] and [4].

25 9.8.2.3.3 Test Procedure

- 26 a. Connect the sector to the access terminal antenna connector.
- 27 b. Set *Ior* to -75 dBm.
- 28 c. Disable the occurrence of Reverse Link Silence Interval by setting
 29 *ReverseLinkSilenceDuration* to 0x0.
- 30 d. Configure the access network to transmit an RAB value of '0' (unloaded) for the
 31 duration of the test.

- 1 e. Map the RETAP to MACFlowID 0x01. If value for any parameter is not specified, use
2 defaults from [1].
- 3 f. For RTC MAC, configure the MACFlow with MACFlowID equal to one transmission
4 mode to be High Capacity, BucketLevelMax*NN* (*NN* = 0x01) to 0x00, and
5 HiCapTerminationTargetPS is 0x3 (4 sub-frames) for all packet size PS and ensure
6 that the access terminal is initially not transmitting any data on the Reverse
7 Traffic Channel.
- 8 g. Set up a Test Application session. Open a connection. Configure the access
9 network to transmit RChannelGainIncluded set to 1 and RChannelGain set to
10 '00' in the *TrafficChannelAssignment* message.
- 11 h. Using access network initiated GAUP *AttributeUpdateRequest* message, set all fields
12 in the PermittedPayload attribute in the RTC MAC protocol to their default values.
13 These values can be found in section 10.11.7.2.5 of [1].
- 14 i. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
15 T2PInflowRange*NN* (*NN* = 0x01) attribute of the Reverse Traffic Channel MAC
16 Protocol to the values specified in table 9.8.2.3.3-1.

Table 9.8.2.3.3-1 T2PInflowRange

Parameter	Value (Hexadecimal)
T2PInflowmin	0x80 (32 dB)
T2PInflowmax	0x80 (32 dB)

- 18 j. After the configuration of RETAP and RTC MAC parameters is complete, instruct
19 the access network to always positively acknowledge the transmission of a packet
20 on each sub-frame of the reverse link through the H-ARQ and P-ARQ bits.
- 21 k. Wait for RETAP to start generation of packets. Using access network initiated GAUP
22 *AttributeUpdateRequest* message, set the BucketLevelMax*NN* (*NN* = 0x01) to 0x6C.
- 23 l. Monitor the sequence of transmit data rate on the Reverse Data Channel as the
24 access terminal ramps up to the 8192-bit payload (307.2 kbps).
- 25 m. Verify that the access terminal meets the minimum standard as per 9.8.2.3.4.

26 9.8.2.3.4 Minimum Standard

27 The access terminal shall increase its RTC payload as allowed by PermittedPayloadPS_k.
28 The access terminal shall increase its transmit payload size every 3 to 5 sub-frames from
29 0 to 8192 bits in the following sequence: 0, 1024 bits, 2048 bits, 4096 bits and 8192 bits, as
30 shown in Figure 12.1. In the figure, the counting of sub-frames for each rate transition
31 begins when the RTC MAC transmits data for the first time from MACFlow with MACFlowID
32 equal to one.

1 9.8.2.4 Data based T2PInflow Decay test

2 9.8.2.4.1 Definition

3 This test verifies that the access terminal supporting Subtype 3 or MultiCarrier RTC MAC
 4 protocol will decay a flows' T2PInflow at every sub-frame on which it is not transmitting any
 5 data for the flow. The test assumes that the access terminal is receiving the Forward
 6 Channel for the entire duration of the test. After a period of transmission the access
 7 terminal runs out of data to transmit leading to a period of no transmission. The access
 8 terminal will decay the T2PInflow during this period.

9 9.8.2.4.2 Traceability

10 See section 9.12.6.1.6.1 of [1] and [4].

11 9.8.2.4.3 Test Procedure

- 12 a. Connect the sector to the access terminal antenna connector.
- 13 b. Ior to -75 dBm.
- 14 c. Disable the occurrence of Reverse Link Silence Interval by setting
 15 ReverseLinkSilenceDuration to 0x0.
- 16 d. Fix the RAB transmitted by the access network to '0' (unloaded) for the entire test
 17 duration.
- 18 e. Map the RETAP to MACFlowID 0x01. If value for any parameter is not specified, use
 19 defaults from [1].
- 20 f. For RTC MAC, configure PermittedPayloadPS_k to 0xC for all k and all PS.
- 21 g. For RTC MAC, configure the MACFlow with MACFlowID equal to one transmission
 22 mode to be High Capacity (TransmissionModeNV (NV = 0x01) = 0x00),
 23 BucketLevelMaxNV (NV = 0x01) to 0x00, and HiCapTerminationTargetPS to 0x3 (4
 24 sub-frames) for all packet size PS.
- 25 h. Set up a Test Application session. Using SCP, in the TxT2PMax Attribute of the
 26 Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values
 27 specified in table 9.8.2.4.3-1.
- 28 i. Open a connection. Configure the access network to transmit
 29 RACHannelGainIncluded set to 1 and RACHannelGain set to '00' in the
 30 *TrafficChannelAssignment* message.
- 31 j. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
 32 T2PFilterTCNV (NV = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC
 33 Protocol to 0x02 (128 slots).
- 34 k. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
 35 PayloadThresh attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol to
 36 0x03 (infinity).

Table 9.8.2.4.3-1 T2PMaxPilotStrength

Field	Value (Hexadecimal)
NumPilotStrengthValues	0x1 (1)
PilotStrengthAxis PilotStrengthAxis0	0x28 (-10 dB)
TxT2PmaxPilotStrengthAxis TxT2PmaxPilotStrengthAxis0	0x26 (19 dB)

1. Using access network initiated GAUP *AttributeUpdateRequest* message, in the BucketFactor*NN* (*NN* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the fields to the values specified in table 9.8.2.4.3-2.

Table 9.8.2.4.3-2 BucketFactor

Field	Value (Hexadecimal)
NumT2PAxisValues	0x0 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis T2PAxis00	0x0 (0 dB)
FRABAxis FRABAxis0	0x8 (-1)
BucketFactorT2PAxisFRABAxis BucketFactorT2PAxis00FRABAxis0	0x1A (3.25)

- m. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PInflowRange*NN* (*NN* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to values specified in table 9.8.2.4.3-3.

Table 9.8.2.4.3-2 T2PInflowRange

Field	Value (Hexadecimal)
T2PInflowmin	0xf (3.75 dB)
T2PInflowmax	0x78 (30 dB)

- n. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PTransitionFunction*NN* (*NN* = 0x01) Attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values specified in table 9.8.2.4.3-3.

1
2
3**Table 9.8.2.4.3-3 T2PUp and T2PDn**

Field	Value (Hexadecimal)
NumT2PAxisValues	0x3 (3)
NumFRABAxisValues	0x0 (0)
T2PAxis	
T2PAxis00	0xf (3.75 dB)
T2PAxis01	0x28 (10 dB)
T2PAxis02	0x3a (14.5 dB)
T2PAxis03	0x4c (19 dB)
FRABAxis	
FRABAxis0	0x8 (-1)
T2PUpT2PAxisFRABAxis	
T2PUpT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PUpT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PUpT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PUpT2PAxis03FRABAxis0	0xd0 (-12 dB)
T2PDnT2PAxisFRABAxis	
T2PDnT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PDnT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PDnT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PDnT2PAxis03FRABAxis0	0xd0 (-12 dB)

- 4 o. Configure the access terminal for 16 slot termination of each sub-packet by
5 instructing the access network to always negatively acknowledge the first three
6 transmissions of a sub-packet on the reverse link by transmitting a NAK in the H-
7 ARQ, and positively acknowledge the transmission of the last sub-packet through
8 the L-ARQ and P-ARQ bits.
- 9 p. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
10 BucketLevelMaxNV (NV = 0x01) to 0x6C. In RETAP, set the BurstSize field of the
11 BurstSizeMode parameter to 0x00C6 and BurstPeriod field of the BurstPeriodMode
12 parameter to 0x000C and ensure that the RETAP starts transmitting packets
13 within 100 slots of transmission of GAUP *AttributeUpdateRequest* message.
- 14 q. Monitor the sequence of transmit payload on the Reverse Traffic Channel.

- 1 r. Verify that the access terminal meets the minimum standard as per section
2 9.8.2.4.4.

3 9.8.2.4.4 Minimum Standard

4 The access terminal shall transmit the payloads (data rates) during the time intervals as
5 specified in table 9.8.2.4.4-1. In this test, slot 0 refers to the first slot used for the
6 transmission of data arriving at the access terminal during 2nd BurstPeriod.

7 **Table 9.8.2.4.4-1 Minimum Requirement for T2PInflow Decay**

Time t (slots)	Payload (Nominal Data Rate)
$t < 100$	1024 bits (38.4 kbps) or below
$100 \leq t < 252$	1536 bits (57.6 kbps) or below
$252 \leq t < 700$	2048 bits (76.8 kbps) or lower

8 9.8.2.5 Reverse Link Silence Interval based T2PInflow Decay test

9 9.8.2.5.1 Definition

10 This test verifies that the access terminal supporting Subtype 3 or MultiCarrier RTC MAC
11 protocol will decay a flows' T2PInflow during reverse link silence interval. The test
12 assumes that the access terminal is receiving the Forward Channel for the entire
13 duration of the test. In the test, after a period of transmission, the access terminal is
14 unable to transmit data due to occurrence of reverse link silence interval resulting in
15 T2PInflow decay.

16 9.8.2.5.2 Traceability

17 See section 9.10.6.1.6.1 of [1] and [4].

18 9.8.2.5.3 Test Procedure

- 19 a. Connect the sector to the access terminal antenna connector.
20 b. I_{or} to -75 dBm.
21 c. Set ReverseLinkSilenceDuration to 0x3 (48 slots).
22 d. Set ReverseLinkSilencePeriod to 0x0 (54.6 seconds).
23 e. Fix the RAB transmitted by the access network to '0' (unloaded) for the entire test
24 duration.
25 f. Map the RETAP to MACFlowID 0x01. If value for any parameter is not specified, use
26 defaults from [1].
27 g. For RTC MAC, configure PermittedPayloadPS_k to 0xC for all k and all PS.
28 h. For RTC MAC, configure the MACFlow with MACFlowID equal to one transmission
29 mode to be High Capacity (TransmissionMode NV (NV = 0x01) = 0x00),

- 1 BucketLevelMaxNN (NN = 0x01) to 0x00, and HiCapTerminationTargetPS to 0x3 (4
 2 sub-frames) for all packet size PS.
- 3 i. Set up a Test Application session. Using SCP, in the TxT2PMax Attribute of the
 4 Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values
 5 specified in table 9.8.2.5.3-1. Using SCP set T2PNoTxFilterTC to 0x0 (64 slots).
- 6 j. Open a connection. Configure the access network to transmit
 7 RACHannelGainIncluded set to 1 and RACHannelGain set to '00' in the
 8 *TrafficChannelAssignment* message.
- 9 k. Using access network initiated GAUP *AttributeUpdateRequest* message, set
 10 T2PFilterTCNN (NN = 0x01) to 0x0 (64 slots).
- 11 l. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
 12 PayloadThresh attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol to
 13 0x03 (infinity).

14 **Table 9.8.2.5.3-1 T2PMaxPilotStrength**

Field	Value (Hexadecimal)
NumPilotStrengthValues	0x1 (1)
PilotStrengthAxis PilotStrengthAxis0	0x28 (-10 dB)
TxT2PmaxPilotStrengthAxis TxT2PmaxPilotStrengthAxis0	0x26 (19 dB)

- 15 m. Using access network initiated GAUP *AttributeUpdateRequest* message, in the
 16 BucketFactorNN (NN = 0x01) attribute of the Subtype 3 Reverse Traffic Channel
 17 MAC Protocol, set the fields to the values specified in table 9.8.2.5.3-2

Table 9.8.2.5.3-2 BucketFactor

Field	Value (Hexadecimal)
NumT2PAxisValues	0x0 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis T2PAxis00	0x0 (0 dB)
FRABAxis FRABAxis0	0x8 (-1)
BucketFactorT2PAxisFRABAxis BucketFactorT2PAxis00FRABAxis0	0x1A (3.25)

- n. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PInflowRange*NV* (*NV* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to values specified in table 9.8.2.5.3-3.

Table 9.8.2.5.3-3 T2PInflowRange

Field	Value (Hexadecimal)
T2PInflowmin	0xf (3.75 dB)
T2PInflowmax	0x78 (30 dB)

- o. Using access network initiated GAUP *AttributeUpdateRequest* message, in the T2PTransitionFunction*NV* (*NV* = 0x01) Attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values specified in table 9.8.2.5.3-4.

1

Table 9.8.2.5.3-4 T2PUp and T2PDn

Field	Value (Hexadecimal)
NumT2PAxisValues	0x3 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis	
T2PAxis00	0xf (3.75 dB)
T2PAxis01	0x28 (10 dB)
T2PAxis02	0x3a (14.5 dB)
T2PAxis03	0x4c (19 dB)
FRABAxis	
FRABAxis0	0x8 (-1)
T2PUpT2PAxisFRABAxis	
T2PUpT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PUpT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PUpT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PUpT2PAxis03FRABAxis0	0xd0 (-12 dB)
T2PDnT2PAxisFRABAxis	
T2PDnT2PAxis00FRABAxis0	0xfa (-1.5 dB)
T2PDnT2PAxis01FRABAxis0	0xc4 (-15 dB)
T2PDnT2PAxis02FRABAxis0	0xcc (-13 dB)
T2PDnT2PAxis03FRABAxis0	0xd0 (-12 dB)

- 2 p. Configure the access terminal for 16 slot termination of each sub-packet by
3 instructing the access network to always negatively acknowledge the first three
4 transmissions of a sub-packet on the reverse link by transmitting a NAK in the H-
5 ARQ, and positively acknowledge the transmission of the last sub-packet through
6 the L-ARQ and P-ARQ bits.
- 7 q. Using access network initiated GAUP *AttributeUpdateRequest* message, set the
8 BucketLevelMaxNV (NV = 0x01) to 0x6C. In RETAP, set the BurstSize field of the
9 BurstSizeMode parameter to 0xFFFF and BurstPeriod field of the BurstPeriodMode
10 parameter to 0xFFFF.
- 11 r. Monitor the sequence of transmit payload on the Reverse Traffic Channel.
- 12 s. Verify that the access terminal meets the minimum standard as specified in
13 section 9.8.2.5.4.

1 9.8.2.5.4 Minimum Standard

2 The access terminal shall transmit the payloads (data rates) during the time intervals as
 3 specified in table 9.8.2.5.4-1. In this test, slot 0 refers to the first slot used for transmission
 4 by the access terminal after the occurrence of second silence interval.

5 **Table 9.8.2.5.4-1 Minimum Requirement for T2PInflow Decay**

Time t (slots)	Payload (Nominal Data Rate)
$0 \leq t < 300$	4096 bits (153.6 kbps) or below
$300 \leq t < 600$	6144 bits (230.4 kbps) or below

6 9.8.2.6 Signaling Flow merging test

7 This test is applicable only to access terminals supporting Subtype 3 or MultiCarrier
 8 Reverse Traffic Channel MAC protocol.

9 9.8.2.6.1 Definition

10 This test verifies that the access terminal supporting Subtype 3 or MultiCarrier RTC MAC
 11 protocol allows MACFlow with MACFlowID equal to zero (signaling flow) to merge its data
 12 with existing LowLatency transmissions under three scenarios: if $FRAB < FRAB_{Low}$
 13 (default value is -0.8), if $SumQOutflow$ is greater than or equal to $MergeThreshold$, or if the
 14 $QOutflow$ for the signaling flow is greater than or equal to $MergeThreshold_{NN}$ for the
 15 signaling flow. If all three conditions are not met, the access terminal does not merge the
 16 signaling flow's data with a LowLatency transmission.

17 9.8.2.6.2 Traceability

18 See section 8.8.6.1.2, 9.12.6.1.6.1.1 and 9.12.7 of [1].

19 9.8.2.6.3 Test Procedure

- 20 a. Connect the sector to the access terminal antenna connector.
- 21 b. Set I_{or} to -75 dBm.
- 22 c. Map the RETAP to MACFlowID one. If value for any parameter is not specified, use
 23 defaults from [1].
- 24 d. Using SCP, in the TxT2PMax Attribute of the Subtype 3 Reverse Traffic Channel
 25 MAC Protocol set the PilotStrength and TxT2PmaxPilotStrengthAxis to the values
 26 specified in table 9.8.2.6.3-1.
- 27 e. Instruct the access terminal to set up a connection and establish a TAP call with
 28 the access network. Note, if the attributes in the following steps are negotiated
 29 using SCP, then the call should be established after the configuration is complete.

Table 9.8.2.6.3-1 T2PMaxPilotStrength

Field	Value (Hexadecimal)
NumPilotStrengthValues	0x1 (1)
PilotStrengthAxis PilotStrengthAxis0	0x28 (-10 dB)
TxT2PmaxPilotStrengthAxis TxT2PmaxPilotStrengthAxis0	0x0F (7.5 dB)

- f. Using access network initiated GAUP *AttributeUpdateRequest* message or using SCP, in the BucketFactor*NN* (*NN* = 0x01) attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the fields to the values specified in table 9.8.2.6.3-2.

Table 9.8.2.6.3-2 BucketFactor

Field	Value (Hexadecimal)
NumT2PAxisValues	0x0 (0)
NumFRABAxisValues	0x0 (0)
T2PAxis T2PAxis00	0x0 (0 dB)
FRABAxis FRABAxis0	0x8 (-1)
BucketFactorT2PAxisFRABAxis BucketFactorT2PAxis00FRABAxis0	0x09 (1.125)

- g. Using access network initiated GAUP *AttributeUpdateRequest* message or using SCP, in the T2PTransitionFunction*NN* (*NN* = 0x01) Attribute of the Subtype 3 Reverse Traffic Channel MAC Protocol, set the attributes to the values specified in the following table 9.8.2.6.3-3.

1

Table 9.8.2.6.3-3 T2PUp and T2PDn

Field	Value (Hexadecimal)
NumT2PAxisValues	0x2 (2)
NumFRABAxisValues	0x0 (0)
T2PAxis	
T2PAxis00	0x0 (0 dB)
T2PAxis01	0x34 (13 dB)
T2PAxis02	0x36 (13.5 dB)
FRABAxis	
FRABAxis0	0x8 (-1)
T2PUpT2PAxisFRABAxis	
T2PUpT2PAxis00FRABAxis0	0x34 (13 dB)
T2PUpT2PAxis01FRABAxis0	0x34 (13 dB)
T2PUpT2PAxis02FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxisFRABAxis	
T2PDnT2PAxis00FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxis01FRABAxis0	0x88 (-30 dB)
T2PDnT2PAxis02FRABAxis0	0x88 (-30 dB)

- 2 h. Using access network initiated GAUP *AttributeUpdateRequest* message or using SCP,
3 set the TransmissionMode to Low Latency (TransmissionMode *NV* (*NV* = 0x01) =
4 0x01) ensure that access terminal is not transmitting any data on the Reverse
5 Data Channel.
- 6 i. Fix the RAB transmitted by the access network to '0' (unloaded).
- 7 j. In RETAP, set the BurstSize field of the BurstSizeMode parameter to 0xFFFF and
8 BurstPeriod field of the BurstPeriodMode parameter to 0xFFFF.
- 9 k. Using access network initiated GAUP *AttributeUpdateRequest* message or using SCP,
10 negotiate MergeThreshold to 0x05 (infinity).
- 11 l. While access terminal is transmitting data for MACFlow with MACFlowID equal to
12 one and the FRAB has settled to a value close to -1, instruct the access network to
13 send a *TrafficChannelAssignment* message to the access terminal. The content of
14 the all *TrafficChannelAssignment* messages is identical to t the previous message
15 with the exception of the MessageSequence field which is incremented by one for
16 each TCA transmission.
- 17 m. Verify that the access terminal meets the minimum standard as per bullet 1 of
18 9.8.2.6.4.
- 19 n. Instruct the access network close the session and start a new session.

- 1 o. Using SCP, negotiate MergeThreshold to 0x00 (0) and set FRABLow to 0x04 (-1).
- 2 p. Repeat steps c-j.
- 3 q. Repeat steps l-m.
- 4 r. Using access network initiated GAUP *AttributeUpdateRequest* message, negotiate
- 5 MergeThreshold to 0x05 (infinity) and MergeThresholdNN (NN= 0x00) to 0.
- 6 s. Repeat steps l-m.

7 9.8.2.6.4 Minimum Standard

- 8 1. The access terminal shall transmit a *TrafficChannelComplete* message in response
- 9 to the *TrafficChannelAssignment* message received by the access terminal. The
- 10 access terminal should transmit the *TrafficChannelComplete* message within 400
- 11 slots of receiving the *TrafficChannelAssignment* message.

12 **9.9 MultiCarrier Reverse Traffic Channel MAC Protocol**

13 9.9.1 Access Network Tests

14 None.

15 9.9.2 Access terminal Tests

16 Tests 9.9.2.1-9.9.2.6 of this section are similar to those in section 9.8.2. For these tests,
 17 the access terminal and access network negotiate the use of MultiCarrier Reverse Traffic
 18 Channel MAC protocol and the access network assigns a single carrier to the access
 19 terminal. All variables, attributes and measured values specified in section 9.8.2 are
 20 applicable to the carrier assigned to the access terminal for the tests 9.9.2.1-9.9.2.6.
 21 Further, RMCTAP may be used instead of RETAP for these tests.

22 9.9.2.1 TxT2P Ramping with Variable Allocation Test

23 Please refer to section 9.8.2.1 for test details.

24 9.9.2.2 TxT2P Ramping with Fixed Allocation Test

25 Please refer to section 9.8.2.2 for test details.

26 9.9.2.3 Rate Transition between sub-frames

27 Please refer to section 9.8.2.3 for test details.

28 9.9.2.4 Data based T2PInflow Decay test

29 Please refer to section 9.8.2.4 for test details.

30 9.9.2.5 Reverse Link Silence Interval based T2PInflow Decay test

31 Please refer to section 9.8.2.5 for test details.

1 9.9.2.6 Signaling Flow merging test

2 Please refer to section 9.8.2.6 for test details.

3 9.9.2.7 ReverseChannelDroppingRank

4 9.9.2.7.1 Definition

5 The Access Network includes the dropping rank of the assigned channels in the
6 *TrafficChannelAssignment* message. The access terminal uses these ranks in dropping the
7 carriers due to PA headroom limitation.

8 9.9.2.7.2 Traceability

9 See sections 7.9.6.2.2, and 9.13.6.1.6.1.3.2 of [1].

10 9.9.2.7.3 Test Procedure

- 11 a. Configure the access network to support 2 or more channels. Configure the
12 channel conditions such that the access terminal is able to receive pilots from the
13 sector.
- 14 b. Configure the access terminal to negotiate MC-RUP with the access network.
- 15 c. If the access terminal is not using MC-RUP, instruct the access network to
16 terminate the existing session and negotiate a new session. Ensure that the access
17 terminal and the access network negotiate the use of MC-RUP. Ensure that the
18 access terminal negotiates a value greater than 0x01 for MaxNumberofFLSupported
19 and MaxNumberofRLSupported attributes of the MC-RUP protocol.
- 20 d. Allow the connection to go dormant.
- 21 e. Cause the access terminal to open a connection with the access network.
- 22 f. Instruct the access network to transmit the *TrafficChannelAssignment* message
23 with ReverseChannelDroppingRank for one of the carriers having a lower value
24 than the other carriers. Note, the access network should not assign the lowest
25 rank to the channel that carries the forward link control channel messages for the
26 access terminal.
- 27 g. Ensure that the access terminal receives the *TrafficChannelAssignment* message
28 and starts transmitting data on all the assigned carriers.
- 29 h. Vary the channel conditions such that the access terminal becomes PA headroom
30 limited such that the access terminal starts dropping carriers.
- 31 i. Verify that the access terminal meets the minimum standard as per bullet 1 of
32 9.9.2.7.4.
- 33 j. Vary the channel conditions such that the access terminal is no longer PA
34 headroom limited.
- 35 k. Verify that the access terminal meets the minimum standard as per bullet 2 of
36 9.9.2.7.4.

1 9.9.2.7.4 Minimum Standard

- 2 2. Verify that the access terminal transmits stops transmitting on the reverse
3 channel(s) with the lowest ReverseChannelDroppingRank value and transmits a
4 *ReverseCDMAChannelDropped* message to the access network.
- 5 3. Verify that the access terminal does not start transmitting data on the channel(s)
6 that were included in the *ReverseCDMAChannelDropped* message unless it receives
7 a *TrafficChannelAssignment* message re-assigning the dropped channel(s).

8

9

1 No Text.

2

10 PHYSICAL LAYER TESTS

This section includes tests for Physical Layer of [1].

10.1 Transmitter Tests

10.1.1 Access Network Tests

10.1.1.1 Forward Traffic Channel Response to ACK Channel

10.1.1.1.1 Definition

The Forward Traffic Channel Physical Layer packets can be transmitted in 1 to 16 slots. When more than one slot is allocated, the slots transmitted shall use a 4-slot interlacing, i.e., the slots of a packet shall be separated by four slots, and other packets shall be transmitted between the interlaced slots.

If a positive acknowledgement is received on the reverse link ACK Channel informing that the Physical Layer packet has been received before all of the allocated slots have been transmitted, the remaining slots shall not be transmitted and the next allocated slot shall be used for the first slot of the next Physical Layer packet transmission.

These tests verify that the sector transmits the slots of the Forward Traffic Channel packets using 4-slot interlacing for those rates whose packets are more than one slot long. In addition, these tests verify that the sector stops the transmission of the slots of the Forward Traffic Channel packet being transmitted upon reception of a positive acknowledgement through the ACK Channel.

10.1.1.1.2 Traceability

See section 10.3.1.3.1, 11.3.1.3.1 and 12.3.1.3.1 of [1].

10.1.1.1.3 Test Procedure

Refer to Figure 12.4 for a functional block diagram of the test setup.

- a. Configure the sector under test and an access terminal simulator as shown in Figure 12.4.
- b. Disable the AWGN generators (set their output powers to zero) so that the forward and reverse link error rates are negligible. The AWGN generator is not applicable for this test.
- c. For each band class that the sector supports, configure the sector to operate in that band class and perform steps d through e.
- d. Set up a Test Application session. Open a connection and configure the Test Application FTAP so that the ACK and DRC symbols are transmitted at all slots at a known value. Set all possible combinations of DRC and ACK symbols values.

- 1 e. Monitor the sector and access terminal simulator transmissions and receptions
2 and verify that the access network meets the minimum standard as per section
3 10.1.1.1.4.

4 10.1.1.1.4 Minimum Standard

5 For all the tests performed:

- 6 1. The transmit slots of the Forward Traffic Channel packets shall use a 4-slot
7 interlacing for all the Forward Traffic Channel data rates whose packets are more
8 than one slot long.
- 9 2. If ACK = 0 is received at the sector, the remaining slots of the same packet being
10 sent shall not be transmitted and the next allocated slot may be used for the first
11 slot of the next Forward Traffic Channel packet transmission.

12 10.1.2 Access Terminal Tests

13 10.1.2.1 Transmission of Redundant ACK

14 10.1.2.1.1 Definition

15 The access terminal transmits an ACK Channel bit in response to every Forward Traffic
16 Channel slot that is associated with a detected preamble directed to the access terminal.
17 The access terminal transmits one redundant positive ACK in response to a Forward
18 Traffic Channel slot that is detected as a continuation of the Physical Layer packet that
19 has been successfully received. Otherwise, the ACK Channel shall be gated off. The test
20 verifies that only one redundant ACK is transmitted when the preamble of a new packet is
21 not detected and that the redundant ACK is not transmitted if the preamble of a new
22 packet is detected.

23 10.1.2.1.2 Traceability

24 See section 10.3.1.3.3.6, 11.3.1.3.3.5, and 12.3.1.3.3.5 of [1].

25 10.1.2.1.3 Test Procedure

- 26 a. Connect the sector and the AWGN generator to the access terminal antenna
27 connector as shown in Figure 12.2.
- 28 b. Set up a Test Application session. Open a connection and configure the Test
29 Application FTAP so that the Forward Traffic Channel rate corresponds to 76.8 kbps.
- 30 c. Set the test parameters for Test 1 as specified in table 10.1.2.1.3-1.

31
32
33
34

Table 10.1.2.1.3-1 \hat{I}_{or} / I_{oc} and I_{oc}

Parameter	Units	Test 1
\hat{I}_{or} / I_{oc}	dB	-2
I_{oc}	dBm/1.23 MHz	-55

- d. Set the access network to ignore the ACK Channel.
- e. Monitor the access terminal transmissions on the ACK Channel for at least 10 Forward Traffic Channel packets and verify that the access terminal meets the minimum standard as per bullet 1 in section 10.1.2.1.4.
- f. Set \hat{I}_{or} to -75 dBm/1.23 MHz for Test 2. The AWGN generator is not applicable for this test.
- g. The access network shall be in normal operation (i.e. the ACK Channel is no longer ignored).
- h. Count the number of packet errors (through the Test Application FTAP) for at least 10 Forward Traffic Channel packet transmissions and verify the access terminal meets the minimum standard as per bullet 2 in section 10.1.2.1.4.

10.1.2.1.4 Minimum Standard

- The access terminal transmissions on the ACK Channel for each Physical Layer packet transmitted by the access network shall be as follows:
 - A positive ACK acknowledging the successful reception of one packet, followed by at most one redundant positive ACK.
- The number of ACKs transmitted shall be 10.

10.1.2.2 Reverse Traffic Channel Response to ARQ Channel

This test only applies to access terminals that support Subtype 2 Physical Layer.

10.1.2.2.1 Definition

The Reverse Traffic Channel Physical Layer packets can be transmitted in 1 to 4 sub-packets. The access terminal shall use a 12-slot interlacing when transmitting packets containing more than one sub-packet. That is, the transmit sub-packets of a packet shall be separated by 8 slots, and sub-packets of other packets may be transmitted in the sub-frames between those transmit sub-packets.

Associated with each Reverse Traffic Channel Physical Layer sub-packet transmission is an RRI symbol. The RRI symbol carries the payload size and subpacket ID information.

If a positive acknowledgement is received on the ARQ Channel from any sector in the access terminal's active set informing that the Physical Layer packet has been received before all of the sub-packets have been transmitted, the remaining untransmitted sub-

1 packets shall not be transmitted and the next allocated sub-packet may be used for the
2 first slot of the next Physical Layer packet transmission.

3 These tests verify that the access terminal transmits the sub-packets of the Reverse
4 Traffic Channel packets using 12-slot interlacing. In addition, these tests verify that the
5 access terminal stops the transmission of the remaining sub-packets of the Reverse
6 Traffic Channel packet being transmitted upon reception of a positive acknowledgement
7 through the ARQ Channel from any sector in its active set. Conversely, if a negative
8 acknowledgement is received, the access terminal shall continue the transmission of the
9 remaining sub-packets.

10 10.1.2.2.2 Traceability

11 See section 11.3.2.4 and 12.3.2.4 of [1].

12 10.1.2.2.3 Test Procedure

- 13 a. Configure the access terminal under test and 2 sectors as shown in Figure 12.3.
14 The Forward Channel from sector 1 has an arbitrary pilot PN offset index P_1 , and is
15 called Channel 1. The Forward Channel from sector 2 has an arbitrary pilot PN
16 offset index P_2 , and is called Channel 2.
- 17 b. AWGN generator is not applicable to this test.
- 18 c. Send a *TrafficChannelAssignment* message to the access terminal, specifying the
19 pilots specified in table 10.1.2.2.3-1 in the Active Set:

20 **Table 10.1.2.2.3-1 Pilot**

Parameter	Value (Decimal)
PilotPN	P_1
SofterHandoff	0
PilotPN	P_2
SofterHandoff	0 (no combining with P_1)

- 21 d. Set up a Test Application session. Open a connection and configure the Test
22 Application RTAP so that the Transmission Mode is High Capacity. Set the RRI gain
23 to 0 dB.
- 24 e. Set the Reverse Data Channel packet payload to 128 bits and start a new Reverse
25 Data Channel packet every 48 slots (80 ms).
- 26 f. Set ARQMode to 0 (Bi-Polar Keying). Transmit all ACK (positive acknowledgement)
27 symbols on Channel 1 and all NAK (negative acknowledgement) symbols on
28 Channel 2.

- 1 g. Record the RRI symbols with Payload Index 1 and each possible Sub-packet Index
2 and verify that the access terminal meets the minimum standard as per bullet 1 of
3 10.1.2.2.4.
- 4 h. Set ARQMode to 1 (ACK_oriented On-Off Keying). Transmit all NAK symbols on
5 Channel 1 and all ACK symbols on Channel 2.
- 6 i. Record the RRI symbols with Payload Index 1 and each possible Sub-packet Index
7 and verify that the access terminal meets the minimum standard as per bullet 1 of
8 10.1.2.2.4.
- 9 j. Set the Reverse Data Channel packet payload to 12288 bits and start a new Reverse
10 Data Channel packet every 48 slots.
- 11 k. Set ARQMode to 0. Transmit all NAK symbols on both Channels 1 and 2.
- 12 l. Record the RRI symbols with Payload Index 12 and each possible Subpacket Index
13 and verify that the access terminal meets the minimum standard as per bullets 2
14 and 3 of 10.1.2.2.4.

15 10.1.2.2.4 Minimum Standard

- 16 1. The access terminal shall transmit only RRI symbols with subpacket index 0.
- 17 2. The total number of RRI symbols with each sub-packet index 0, 1, 2, and 3 shall be
18 within ± 1 of each other.
- 19 3. The transmit sub-packets of the Reverse Data Channel shall use a 12-slot
20 interlacing.

21 **10.2 Demodulation of the Reverse Activity Channel**

22 10.2.1 Access Network Tests

23 None.

24 10.2.2 Access Terminal Tests

25 10.2.2.1 Demodulation of the Reverse Activity Channel

26 10.2.2.1.1 Definition

27 The Reverse Activity (RA) Channel transmits the Reverse Activity Bit (RAB) stream over
28 the Forward MAC Channel.

29 For Subtypes 0 and 1 RTC MAC, the RA bit is transmitted over RABLength successive slots.
30 The transmission of each RA bit starts in a slot that satisfies

$$31 \quad T \bmod \text{RABLength} = \text{RABOffset}$$

32 where T is the System Time in slots and RABLength and RABOffset are fields in the public
33 data of the *TrafficChannelAssignment* message of the Default Route Update Protocol.

1 The access terminal needs to have a value for the RA bit at all times (CombinedBusyBit). If
 2 the last received RA bit is set to '1' from any sector in the access terminal's active set, the
 3 access terminal sets CombinedBusyBit to '1'. Otherwise, the access terminal sets
 4 CombinedBusyBit to '0'.

5 The tests in this section verify the turn around time of the RA bit and the RA bit
 6 combining rule ("OR of busy").

7 10.2.2.1.2 Traceability

8 See section 10.4.1.3.2.2.3, 11.4.1.3.2.2.3 and 12.4.1.3.2.2.3 of [1].

9 10.2.2.1.3 Test Procedure

- 10 a. Connect two sectors to the access terminal antenna connector as shown in Figure
 11 12.3. The AWGN generator is not applicable in this test. The Forward Channel from
 12 sector 1 has an arbitrary pilot PN offset index P1, and is called Channel 1. The
 13 Forward Channel from sector 2 has an arbitrary pilot PN offset index P2, and is
 14 called Channel 2.

15 If the access terminal supports Subtype 0 or Subtype 1 RTC Mac Protocol, perform steps b to
 16 n.

- 17 b. Send a *UnicastReverseRateLimit* message with the RateLimit value set to '0x5' (153.6
 18 kbps) to the access terminal.
 19 c. Set the test parameters as specified in table 10.2.2.1.3-1.

20 **Table 10.2.2.1.3-1** \hat{I}_{or} / I_{oc} and I_{oc}

Parameter	Units	Value
\hat{I}_{or1}	dBm / 1.23 MHz	-75
\hat{I}_{or2}	dBm / 1.23 MHz	-75

- 21
 22 d. Set up a Test Application session. Open a connection. Configure the Test
 23 Application RTAP so that the Reverse Data Channel rate corresponds to 153.6 kbps.
 24 Configure the Test Application FTAP so that the requested DRC cover corresponds
 25 to the null cover.

- 26 e. Send a *TrafficChannelAssignment* message to the access terminal, specifying
 27 FrameOffset to F0 (even number) and the pilots specified in table 10.2.2.1.3-2 in the
 28 Active Set:

1

Table 10.1.2.2.3-2 Pilot

Parameter	Value
PilotPN	P_1
SofterHandoff	0
RABLength	'00' (8 slots)
RABOffset	$F_0 \bmod \text{RABLength}$ (slots)
PilotPN	P_2
SofterHandoff	1 (Softer Handoff)
RABLength	RABLength_2
RABOffset	RABOffset_2

- 2 f. Send an alternating pattern of one '0' power control bit followed by one '1' power
3 control bit on Channel 1 and Channel 2.
- 4 g. Send an alternating pattern of twenty '0' RAB's followed by twenty '1' RAB's on
5 Channel 1, and a sequence of '0' RAB's on Channel 2.
- 6 h. Monitor the access terminal transmit data rate for at least 10 periods and verify
7 that the access terminal meets the minimum standard as per bullet 1of 10.2.2.1.4.
- 8 i. Send a *TrafficChannelAssignment* message to the access terminal, specifying the
9 same values as the previous *TrafficChannelAssignment* message with the exception
10 of RABOffset for Channel 1 which is set to $(F_0 + \Delta_2) \bmod \text{RABLength}$ slots. Δ_2 can
11 be any integer number different from 0.
- 12 j. Repeat steps g and h verify that the access terminal meets the minimum standard
13 as per bullets 2 of 10.2.2.1.4.
- 14 k. Send a *TrafficChannelAssignment* message to the access terminal, specifying the
15 same values as the previous *TrafficChannelAssignment* message with the exception
16 of the parameters for Channel 1 specified in table 10.2.2.1.3-3.

17

Table 10.1.2.2.3-3 RABOffset and RABLength

Parameter	Value
RABLength	'01' (16 slots)
RABOffset	F_0 (slots)

- 18 l. Repeat steps g and h verify that the access terminal meets the minimum standard
19 as per bullet 3 of 10.2.2.1.4.
- 20 m. Send a *TrafficChannelAssignment* message to the access terminal, specifying the
21 same values as the previous *TrafficChannelAssignment* message with the exception

1 of RABOffset for Channel 1 which is set to $(F0 + \Delta_4) \bmod \text{RABLength}$. Δ_4 can be any
2 even integer number different from 0.

- 3 n. Repeat steps g and h verify that the access terminal meets the minimum standard
4 as per bullet 4 of 10.2.2.1.4.

5 10.2.2.1.4 Minimum Standard

- 6 1. Since RABLength is equal to 8 slots, the test has two possible alignments.
7 Alignment 1 is the alignment where the transition of the RAB's occurs at the
8 Reverse Traffic Channel frame boundaries. Alignment 2 is the alignment where
9 the transition of the RAB's occurs at the midpoint between two Reverse Traffic
10 Channel frame boundaries.

11 For Alignment 1, in each period of the test the access terminal shall perform as
12 follows in sequence:

- 13 a. The access terminal shall start decreasing its transmit rate 16 slots after
14 the beginning of the change (from '0' to '1') in the value of the RA bit.
- 15 b. From the time when the access terminal starts decreasing its transmit
16 rate, the access terminal shall decrease the transmit rate on steps of one
17 rate each subsequent packet transmission until the data rate of 9.6 kbps is
18 achieved.
- 19 c. The access terminal transmit rate shall remain being 9.6 kbps until 16
20 slots after the beginning of the change (from '1' to '0') in the value of the RA
21 bit. At this time, the access terminal shall start increasing its transmit rate
22 in steps of one rate each subsequent packet transmission until the data
23 rate of 153.6 kbps is achieved.

24 For Alignment 2, in each period of the test the access terminal shall perform as
25 follows in sequence:

- 26 d. The access terminal shall start decreasing its transmit rate 8 or 24 slots
27 after the beginning of the change (from '0' to '1') in the value of the RA bit.
- 28 e. From the time when the access terminal starts decreasing its transmit
29 rate, the access terminal shall decrease the transmit rate on steps of one
30 rate each subsequent packet transmission until the data rate of 9.6 kbps is
31 achieved.
- 32 f. The access terminal transmit rate shall remain being 9.6 kbps until 8 or 24
33 slots after the beginning of the change (from '1' to '0') in the value of the RA
34 bit. At this time, the access terminal shall start increasing its transmit rate
35 in steps of one rate each subsequent packet transmission until the data
36 rate of 153.6 kbps is achieved.

- 37 2. Since RABLength is equal to 8 slots, the test has two possible alignments.

38 For Alignment 1, in each period of the test the access terminal shall perform as
39 follows in sequence:

- 1 a. The access terminal shall start decreasing its transmit rate $(8-\Delta_2)$ or $(24-$
2 $\Delta_2)$ slots after the beginning of the change (from '0' to '1') in the value of the
3 RA bit.
- 4 b. From the time when the access terminal starts decreasing its transmit
5 rate, the access terminal shall decrease the transmit rate on steps of one
6 rate each subsequent packet transmission until the data rate of 9.6 kbps is
7 achieved.
- 8 c. The access terminal transmit rate shall remain being 9.6 kbps until $(8-\Delta_2)$
9 or $(24-\Delta_2)$ slots after the beginning of the change (from '1' to '0') in the value
10 of the RA bit. At this time, the access terminal shall start increasing its
11 transmit rate in steps of one rate each subsequent packet transmission
12 until the data rate of 153.6 kbps is achieved.

13 For Alignment 2, in each period of the test the access terminal shall perform as
14 follows in sequence:

- 15 d. The access terminal shall start decreasing its transmit rate $(16-\Delta_2)$ or $(32-$
16 $\Delta_2)$ slots after the beginning of the change (from '0' to '1') in the value of the
17 RA bit.
- 18 e. From the time when the access terminal starts decreasing its transmit
19 rate, the access terminal shall decrease the transmit rate on steps of one
20 rate each subsequent packet transmission until the data rate of 9.6 kbps is
21 achieved.
- 22 f. The access terminal transmit rate shall remain being 9.6 kbps until $(16-$
23 $\Delta_2)$ or $(32-\Delta_2)$ slots after the beginning of the change (from '1' to '0') in the
24 value of the RA bit. At this time, the access terminal shall start increasing
25 its transmit rate in steps of one rate each subsequent packet transmission
26 until the data rate of 153.6 kbps is achieved.

- 27 3. In each period of the test the access terminal shall perform as follows in sequence:
 - 28 a. The access terminal shall start decreasing its transmit rate 16 or 32 slots
29 after the beginning of the change (from '0' to '1') in the value of the RA bit.
 - 30 b. From the time when the access terminal starts decreasing its transmit
31 rate, the access terminal shall decrease the transmit rate on steps of one
32 rate each subsequent packet transmission until the data rate of 9.6 kbps is
33 achieved.
 - 34 c. The access terminal transmit rate shall remain being 9.6 kbps until 16 or
35 32 slots after the beginning of the change (from '1' to '0') in the value of the
36 RA bit. At this time, the access terminal shall start increasing its transmit
37 rate in steps of one rate each subsequent packet transmission until the
38 data rate of 153.6 kbps is achieved.

- 39 4. In each period of the test the access terminal shall perform as follows in sequence:

1
2
3
4
5
6
7
8
9
10
11
12
13

- a. The access terminal shall start decreasing its transmit rate $(16-\Delta_4)$ or $(32-\Delta_4)$ slots after the beginning of the change (from '0' to '1') in the value of the RA bit.
- b. From the time when the access terminal starts decreasing its transmit rate, the access terminal shall decrease the transmit rate on steps of one rate each subsequent packet transmission until the data rate of 9.6 kbps is achieved.
- c. The access terminal transmit rate shall remain being 9.6 kbps until $(16-\Delta_4)$ or $(32-\Delta_4)$ slots after the beginning of the change (from '1' to '0') in the value of the RA bit. At this time, the access terminal shall start increasing its transmit rate in steps of one rate each subsequent packet transmission until the data rate of 153.6 kbps is achieved.

1

2 **11 BROADCAST PROTOCOL TESTS**

3 This section includes tests for [3].

4 **11.1 Generic Broadcast Protocol Tests**

5 11.1.1 Access Network Tests

6 11.1.1.1 ConfigurationRequest Message Response Test

7 11.1.1.1.1 Definition

8 This test verifies that the access network responds to the Generic Broadcast Protocol
9 *ConfigurationRequest* message with a Generic Broadcast Protocol *ConfigurationResponse*
10 message.

11 11.1.1.1.2 Traceability

12 See section 2.4.3.3 of [3].

13 11.1.1.1.3 Test Procedure

- 14 a. Instruct the access terminal to set up a connection with the access network.
- 15 b. Instruct the access terminal to send a Generic Broadcast Protocol
16 *ConfigurationRequest* message.
- 17 c. Verify that the access network meets the minimum standard as per 11.1.1.1.4.

18 11.1.1.1.4 Minimum Standard

19 The access network shall respond to the Generic Broadcast Protocol *ConfigurationRequest*
20 message with a corresponding Generic Broadcast Protocol *ConfigurationResponse* message.

21 11.1.2 Access Terminal Tests

22 11.1.2.1 BCMCS Flow Registration for Paging Test

23 11.1.2.1.1 Definition

24 This test verifies that the access terminal sends *BCMCSFlowRegistration* messages to the
25 access network when timer-based *BCMCS Flow registration* for paging is enabled.

26 11.1.2.1.2 Traceability

27 See section 2.4.4.3.3 of [3].

1 11.1.2.1.3 Test Procedure

- 2 a. Instruct the access terminal to set up a connection and establish a data call with
3 the access network. Enable timer-based BCMCS Flow registration for paging by
4 setting the PagingRegistrationPeriod Attribute of the Generic Broadcast Protocol. If
5 the access terminal supports of PagingRegistrationPeriod less than 0x05, set the
6 value of PagingBroadcastRegistrationPeriod to a value less than 0x05 and greater
7 than or equal to 0x01. Otherwise set PagingRegistrationPeriod to a value greater
8 than or equal to 0x05 and less than or equal to 0xFF. Disable timer-based BCMCS
9 Flow registration for dynamic broadcast by setting the
10 DynamicBroadcastRegistrationPeriod Attribute of the Generic Broadcast Protocol to
11 0x00.
- 12 b. Instruct the access network to set the RegisterForPaging field for at least one
13 BCMCS Flow to '1' in the *BroadcastOverhead* message(s).
- 14 c. Verify that the access terminal meets the minimum standard as per 11.1.2.1.4.

15 11.1.2.1.4 Minimum Standard

16 The access terminal shall send *BCMCSFlowRegistration* messages when the
17 RegistrationTimer reaches a positive integer multiple of PagingRegistrationTimerMax as
18 specified in [3].

19 11.1.2.2 BCMCS Flow Registration for Dynamic Broadcast Test

20 11.1.2.2.1 Definition

21 This test verifies that the access terminal sends *BCMCSFlowRegistration* messages to the
22 access network when timer-based BCMCS Flow registration for dynamic broadcast is
23 enabled.

24 11.1.2.2.2 Traceability

25 See section of 2.4.4.3.3 of [3].

26 11.1.2.2.3 Test Procedure

- 27 a. Instruct the access terminal to set up a connection and establish a data call with
28 the access network. Enable timer-based BCMCS Flow registration for dynamic
29 broadcast by setting the DynamicBroadcastRegistrationPeriod Attribute of the
30 Generic Broadcast Protocol. If the access terminal supports of
31 DynamicBroadcastRegistrationPeriod less than 0x05, set the value of
32 DynamicBroadcastRegistrationPeriod to a value less than 0x05 and greater than or
33 equal to 0x01. Otherwise set DynamicBroadcastRegistrationPeriod to a value
34 greater than or equal to 0x05 and less than or equal to 0xFF. Disable timer-based
35 BCMCS Flow registration for paging by setting the PagingRegistrationPeriod
36 Attribute of the Generic Broadcast Protocol to 0x00.

- 1 b. Instruct the access network to set the ReigsterForDynamicBroadcast field for at
2 least one BCMCS Flow to '1' in the *BroadcastOverhead* message(s).
- 3 c. Verify that the access terminal meets the minimum standard as per 11.1.2.2.4.

4 11.1.2.2.4 Minimum Standard

5 The access terminal shall send *BCMCSFlowRegistration* messages when the
6 RegistrationTimer reaches a positive integer multiple of
7 DynamicBroadcastRegistrationTimerMax as specified in [3].

8 11.1.2.3 ConfigurationRequest Message Response Test

9 11.1.2.3.1 Definition

10 This test verifies that the access terminal responds to the Generic Broadcast Protocol
11 *ConfigurationRequest* message with a Generic Broadcast Protocol *ConfigurationResponse*
12 message.

13 11.1.2.3.2 Traceability

14 See section 2.4.3.3 of [3].

15 11.1.2.3.3 Test Procedure

- 16 a. Instruct the access network to set up a connection with the access terminal.
- 17 b. Instruct the access network to send a Session Configuration Protocol
18 *ConfigurationRequest* message.
- 19 c. Wait for the receipt of a Session Configuration Protocol *ConfigurationComplete*
20 message from the access terminal.
- 21 d. Instruct the access network to send a Generic Broadcast Protocol
22 *ConfigurationRequest* message to the access terminal.
- 23 e. Verify that the access terminal meets the minimum standard as per 11.1.2.3.4.

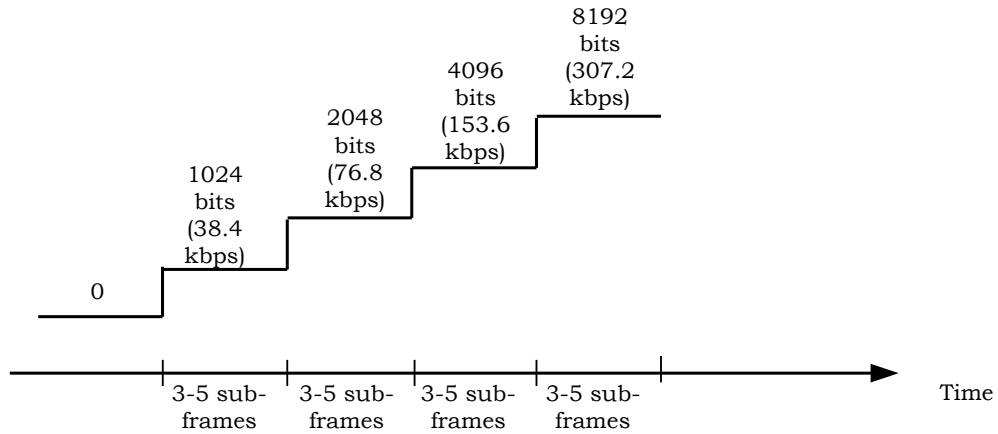
24 11.1.2.3.4 Minimum Standard

25 The access terminal shall respond to a Generic Broadcast Protocol *ConfigurationRequest*
26 message with a corresponding Generic Broadcast Protocol *ConfigurationResponse* message.
27

- 1 No Text.

1

2 **12 FIGURES**

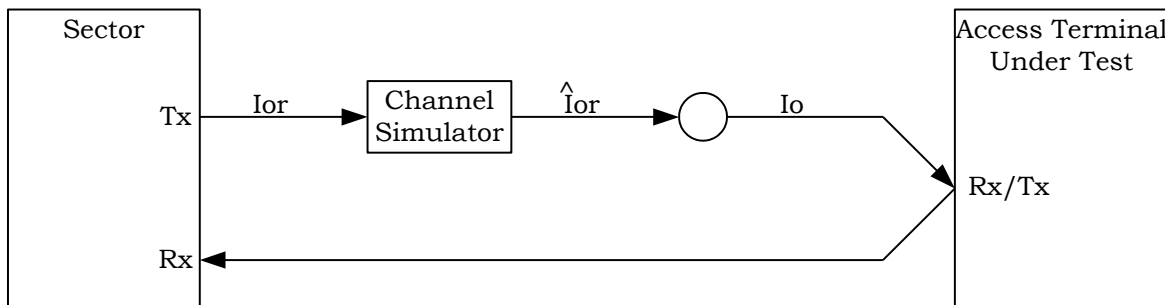


3

4 **Figure 12.1 Conformance Requirements for Testing PermittedPayloadPS_k**

5

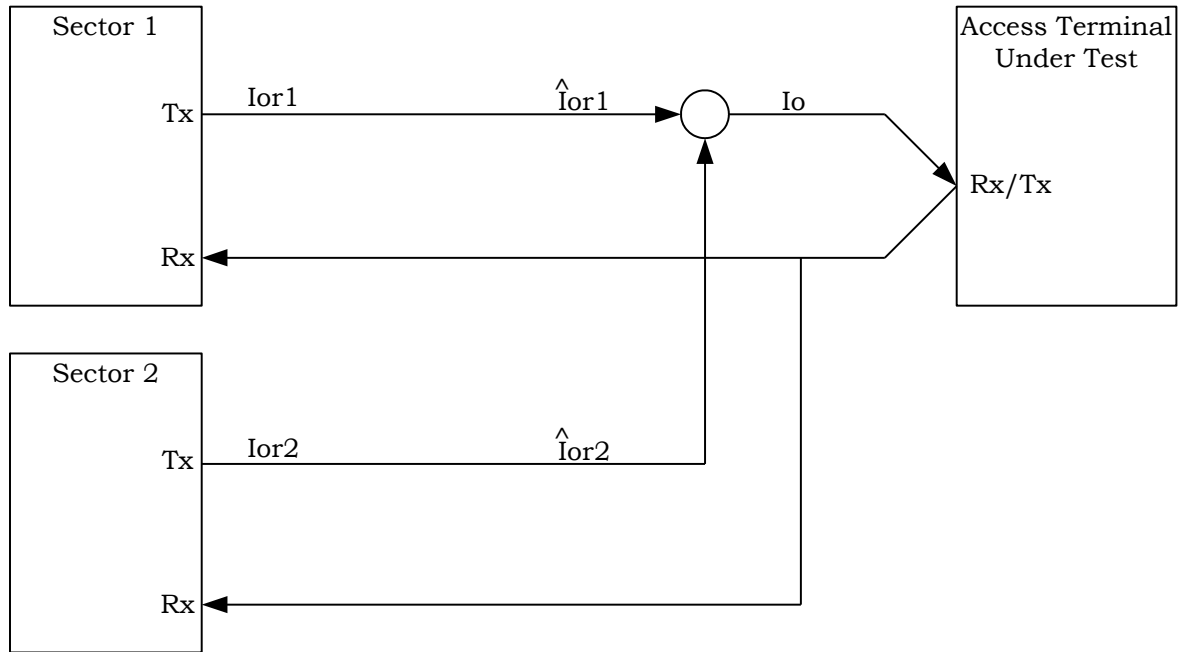
6



7

8 **Figure 12.2 Functional Setup for FTC Redundant ACK**

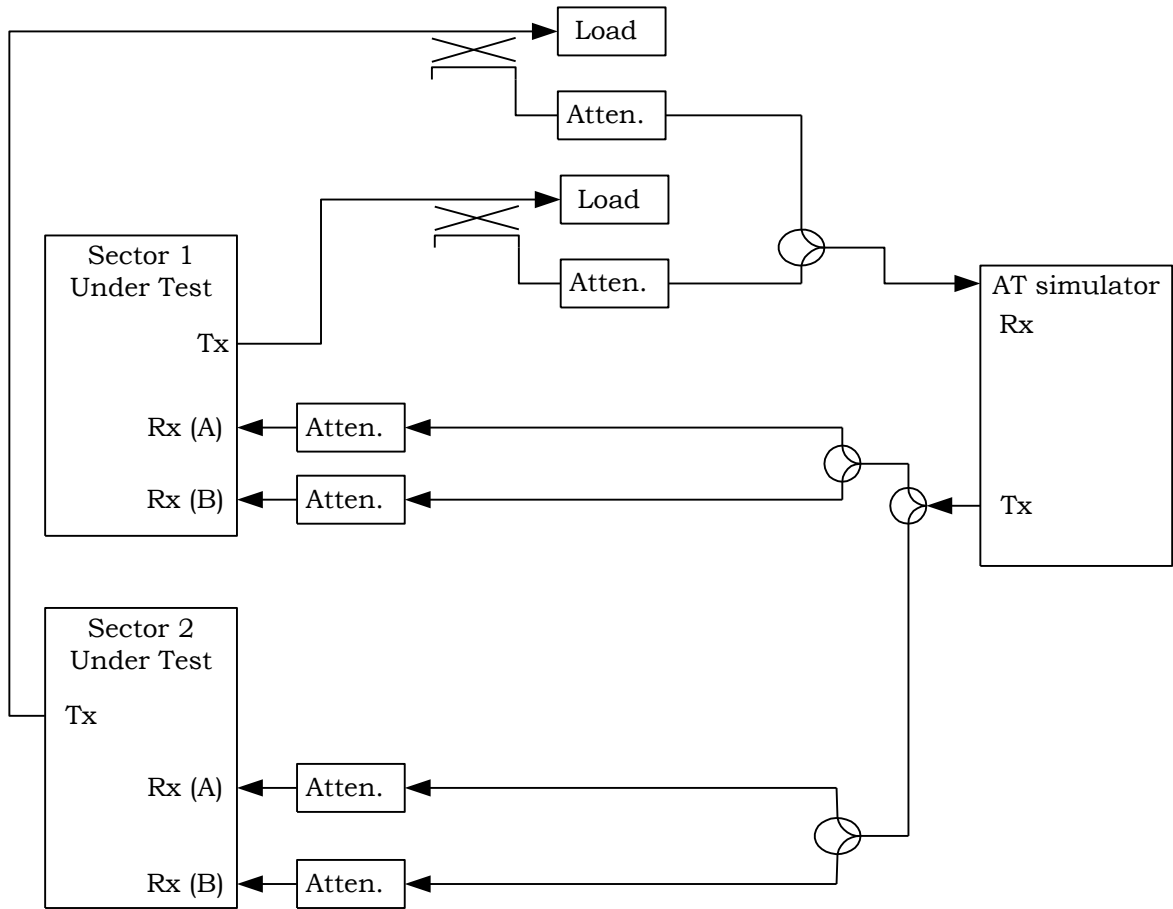
9



1
2 **Figure 12.3 Functional Setup for Reverse Traffic Channel Response to ARQ Channel**
3 **and Demodulation of the Reverse Activity Channel Tests**

4
5 **Error! Objects cannot be created from editing field codes.**

6 **Figure 12.4 Functional Setup for one FTC response to ACK channel and Connection**
7 **Security and Session Layer Tests**



1

2

3

4

Figure 12.5 Functional Setup for Routing of *UATIAssignment* and *TrafficChannelAssignment* Messages Tests

- 1 No Text.

1 **13 ANNEX (INFORMATIVE)**

2

3 This annex classifies the test cases in this document w.r.t. applicability to C.S0024-0,
4 C.S0024-A and C.S0024-B.

5 Chapter 2: Default Signaling Application Tests

6 All tests in this chapter are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

7 Chapter 3: Default Packet Application Tests

8 All tests in this chapter are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

9 Chapter 4: Multi-Flow Application Tests

10 All tests in this chapter are applicable to C.S0024-A and C.S0024-B.

11 Chapter 5: Stream Layer Tests

12 All tests in this chapter are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

13 Chapter 6: Session Layer Tests

14 All tests in this chapter except tests 6.3.2.3 and 6.3.2.4 are applicable to C.S0024-0,
15 C.S0024-A and C.S0024-B. Tests 6.3.2.3 and 6.3.2.4 related to personality negotiaton and
16 deleteion are applicable only to C.S0024-A and C.S0024-B.

17 Chapter 7: Connection Layer Tests

18 Section 7.1 Default Air-Link Management Protocol Tests

19 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

20 Section 7.2 Default Initialization State Protocol Tests

21 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

22 Section 7.3 Default Idle State Protocol Tests

23 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

24 Section 7.4 Enhanced Idle State Protocol Tests

25 All tests in this section are applicable to C.S0024-A and C.S0024-B.

26 Section 7.5 Default Connected State Protocol Tests

27 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

28 Section 7.6 Default Route Update Protocol Tests

29 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

30 Section 7.7 MC Route Update Protocol Tests

31 All tests in this section are applicable to C.S0024-B.

32 Section 7.8 Overhead Messages Protocol Tests

1 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

2 Chapter 8: Security Layer Tests

3 All tests in this chapter are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

4 Chapter 9: MAC Layer Tests

5 Section 9.1 Default Control Channel MAC Protocol Tests

6 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

7 Section 9.2 Enhanced Control Channel MAC Protocol Tests

8 All tests in this section are applicable to C.S0024-A and C.S0024-B.

9 Section 9.3 Default Access Channel MAC Protocol Tests

10 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

11 Section 9.4 Enhanced Access Channel MAC Protocol Tests

12 All tests in this section are applicable to C.S0024-A and C.S0024-B.

13 Section 9.5 Default Forward Traffic Channel MAC Protocol Tests

14 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

15 Section 9.6 Enhanced Forward Traffic Channel MAC Protocol Tests

16 All tests in this section are applicable to C.S0024-A and C.S0024-B.

17 Section 9.7 Default Reverse Traffic Channel MAC Protocol Tests

18 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

19 Section 9.8 Subtype 3 Reverse Traffic Channel MAC Protocol Tests

20 All tests in this section are applicable to C.S0024-A .

21 Section 9.9 MultiCarrier Reverse Traffic Channel MAC Protocol Tests

22 All tests in this section are applicable to C.S0024-B.

23 Chapter 10: Physical Layer Tests

24 Section 10.1 Transmitter Tests

25 All tests in this section except test 10.1.2.2. Reverse Traffic Channel Response to ARQ
26 Channel are applicable to C.S0024-0, C.S0024-A and C.S0024-B. Test 10.1.2.2 Reverse
27 Traffic Channel Response to ARQ Channel is applicable only to C.S0024-A and C.S0024-
28 B.

29 Section 10.1 Demodulation of the Reverse Activity Channel

30 All tests in this section are applicable to C.S0024-0, C.S0024-A and C.S0024-B.

31 Chapter 11: Broadcast Protocol Tests

32 Tests in this chapter are applicable when [3] is supported.