IEEE Std 802.16c™-2002
(Amendment to IEEE Std 802.16™-2001)

IEEE Standards

802.16c™

IEEE Standard for
Local and metropolitan area networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Amendment 1: Detailed System Profiles for 10–66 GHz

IEEE Computer Society
and the
IEEE Microwave Theory and Techniques Society

Sponsored by the
LAN/MAN Standards Committee

Published by
The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

15 January 2003

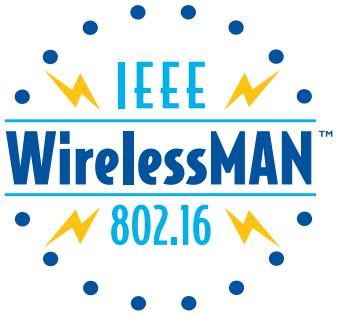
Print: SH95064
PDF: SS95064

IEEE Std 802.16c™-2002
(Amendment to
IEEE Std 802.16™-2001)

IEEE Standard for
Local and metropolitan area networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems—

Amendment 1: Detailed System Profiles for 10–66 GHz



Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

and the
IEEE Microwave Theory and Techniques Society

Approved 11 December 2002

IEEE-SA Standards Board

Abstract: This amendment updates and expands Clause 12 of IEEE Std 802.16-2001, which concerns system profiles that list sets of features and functions to be used in typical implementation cases. Errors and inconsistencies in IEEE Std 802.16-2001 are also corrected. The scope is limited to 10–66 GHz.
Keywords: fixed broadband wireless access networks, metropolitan area network, millimeter waves, microwaves, WirelessMAN™ standards

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Print: ISBN 0-7381-3493-7 SH95064
PDF: ISBN 0-7381-3494-5 SS95064

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

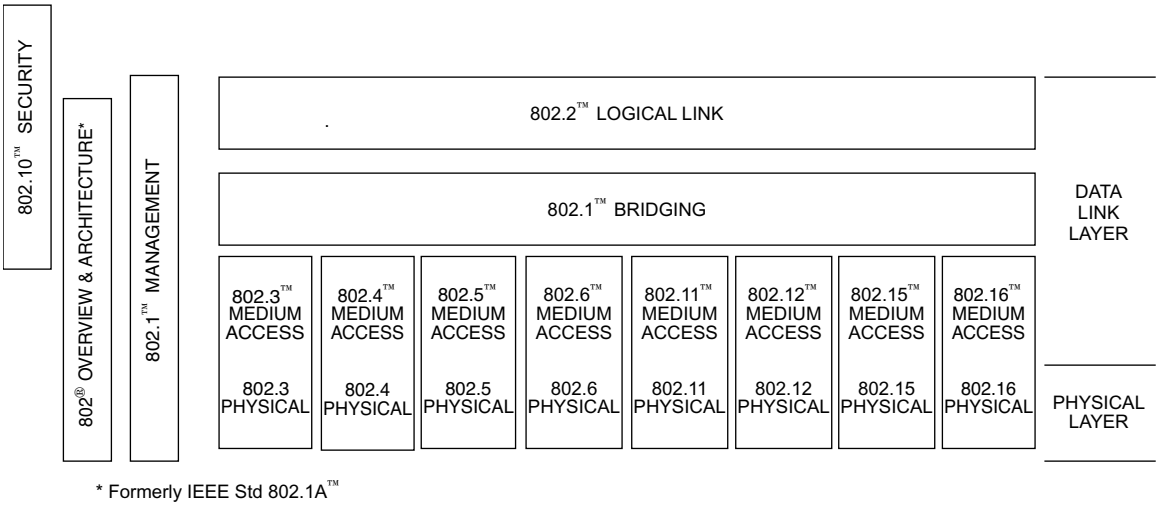
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Introduction

(This introduction is not part of IEEE Std 802.16c-2002, IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems—Amendment 1: Detailed System Profiles for 10–66 GHz.)

This amendment updates and expands Clause 12 of IEEE Std 802.16-2001, which concerns system profiles that list sets of features and functions to be used in typical implementation cases. Errors and inconsistencies in IEEE Std 802.16-2001 are also corrected. The scope is limited to 10–66 GHz.

IEEE Std 802.16 is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard designations.[1])



This family of standards deals with the Physical and Data Link layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1: 1994). The access standards define seven types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the technologies noted above are as follows:

- IEEE Std 802 — *Overview and Architecture*. This standard provides an overview to the family of IEEE 802 Standards.
- IEEE Std 802.1B™ and 802.1k™ [ISO/IEC 15802-2] — *LAN/MAN Management*. Defines an OSI management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- IEEE Std 802.1D™ — *Media Access Control (MAC) Bridges*. Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- IEEE Std 802.1E™ [ISO/IEC 15802-4] — *System Load Protocol*. Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.

[1]The IEEE standards referred to in the above figure and list are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

- IEEE Std 802.1F™ — *Common Definitions and Procedures for IEEE 802 Management Information*.
- IEEE Std 802.1G™ [ISO/IEC 15802-5] — *Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- IEEE Std 802.1H™ [ISO/IEC TR 11802-5] — *Media Access Control (MAC) Bridging of Ethernet V2.0 in Local Area Networks*.
- IEEE Std 802.2 [ISO/IEC 8802-2] — *Logical Link Control*.
- IEEE Std 802.3 — *CSMA/CD Access Method and Physical Layer Specifications*.
- IEEE Std 802.4 [ISO/IEC 8802-4] — *Token Passing Bus Access Method and Physical Layer Specifications*.
- IEEE Std 802.5 [ISO/IEC 8802-5] — *Token Ring Access Method and Physical Layer Specifications*.
- IEEE Std 802.6 [ISO/IEC 8802-6] — *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*.
- IEEE Std 802.10 — *Interoperable LAN/MAN Security.*
- IEEE Std 802.11 [ISO/IEC DIS 8802-11] — *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*.
- IEEE Std 802.12 [ISO/IEC 8802-12] — *Demand Priority Access Method, Physical Layer and Repeater Specifications*.
- IEEE Std 802.15 — *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks*.
- IEEE Std 802.16 — *Air Interface for Fixed Broadband Wireless Access Systems*.

In addition to the family of standards, the following is a recommended practice for a common Physical Layer technology:

- IEEE Std 802.7™ — *IEEE Recommended Practice for Broadband Local Area Networks*.

Participants

This document was developed by the IEEE 802.16 Working Group on Broadband Wireless Access, which is responsible for Wireless Metropolitan Area Network (WirelessMAN™) Standards. The IEEE 802.16 Working Group had the following officers:

Roger B. Marks, *Chair*
Paul F. Struhsaker, *Vice Chair*
Dean Chang, *Secretary*

Primary development was carried out by the Working Group's Task Group c, which had the following officers:

Kenneth Stanwood, *Chair*
Carl Eklund, *Technical Editor*

The following members of the IEEE 802.16 Working Group on Broadband Wireless Access participated in the Working Group Letter Ballot in which the draft of this standard was approved, voting for approval, disapproval, or abstention:

Aditya Agrawal
Song An
Gordon Antonello
Reza Arefi
S. Lek Ariyavisitakul
Jori Arrakoski
Malik Audeh
Eli Avivi
Yvon Belec
Anader Benyamin-Seeyar
Carl Bushue
Baruch Buskila
Yuankai Chang
Dean Chang
David Chauncey
Naftali Chayat
Rémi Chayer
Brian Edmonston
Brian Eidson
Henry Eilts
Carl Eklund
Avraham Freedman
Andrew Garrett
G. Jack Garrison
Marianna Goldhammer
Zion Hadad
Yoav Hebron
Wayne Hunter
David Husson
Hamadi Jamali
Jacob Jorgensen
Tal Kaitz
Mika Kasslin
Phil Kelly
Ofer Kelman
Brian Kiernan
Itzik Kitroser
Thomas Kolze
Jerome Krinock
Jonathan Labs
John Langley
Yigal Leiba
Moshe Levinson
Xiaodong (Alex) Li
John Liebetreu
Heinz Lycklama
Roger B. Marks
Russell McKown
Ronald Meyer
Andrew Middleton
Apurva Mody
Ronald Murias
Robert Nelson
Kim Olszewski
Manish Patel
Kenneth Peirce
Subbu Ponnuswamy
Moshe Ran
Gene Robinson
Shane Rogers
Amir Sarajedini
Octavian Sarca
Durga Satapathy
Yossi Segal
Radu Selea
James Simkins
Manoneet Singh
Sean Sonander
Kenneth Stanwood
Michael Stewart
Paul F. Struhsaker
Jose Tellado
Nico van Waes
Subir Varma
Arthur Wang
Lei Wang
Stanley Wang
Philip Whitehead
Curt Wise
Vladimir Yanover
Heejung Yu

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Gordon Antonello
Gholamreza Arefi-Anbarani
Eladio Arvelo
Morris Balamut
John Barr
Dean Chang
Elizabeth Chesnutt
Keith Chow
Todor Cooklev
Jose M. Costa
Guru Dutt Dhingra
Vern Dubendorf
Sourav Dutta
Carl Eklund
Avraham Freedman
Brian Gieschen
James Gilb
José A. Gutierrez
Zion Hadad
Simon Harrison
Hamadi Jamali
Kevin Karcz
Brian Kiernan
Pi-Cheng Law
Christina Lim
Gregory Luri
Roger B. Marks
Kyle Maus
George Miao
Apurva Mody
Ronald Murias
Robert Nelson
Michael Newman
Charles Ngethe
Paul Nikolich
Subbu Ponnuswamy
Vikram Punj
Jon Rosdahl
Neil Shipp
Kenneth Stanwood
Lei Wang
Stanley Wang
Vladimir Yanover
Jung Yee
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 11 December 2002, it had the following membership:

James T. Carlo, *Chair*
James H. Gurney, *Vice Chair*
Judith Gorman, *Secretary*

Sid Bennett
H. Stephen Berger
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
Julian Forster*
Howard M. Frazier
Toshio Fukuda
Arnold M. Greenspan
Raymond Hapeman
Donald M. Heirman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips
Nader Mehravari
Daleep C. Mohla
William J. Moylan
Malcolm V. Thaden
Geoffrey O. Thompson
Howard L. Wolfman
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Alan Cookson, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Catherine K. N. Berger
IEEE Standards Project Editor

Contents

List of Figures

List of Tables

IEEE Standard for
Local and metropolitan area networks

Part 16: Air Interface for Fixed Broadband Wireless Access Systems—

Amendment 1: Detailed System Profiles for 10–66 GHz

EDITORIAL NOTE—This amendment updates and expands Clause 12 of IEEE Std 802.16™-2001, which concerns system profiles that list sets of features and functions to be used in typical implementation cases. Errors and inconsistencies in IEEE Std 802.16-2001 are also corrected. The scope is limited to 10–66 GHz.

The editing instructions contained in this amendment define how to merge the material contained herein into the existing base standard (IEEE Std 802.16-2001) to form the comprehensive standard.

Editing instructions are shown in ***bold italic***. Three editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed either by using ~~strikethrough~~ (to remove old material) or underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions. ***Replace*** is used to make large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

1.2.1 10–66 GHz licensed bands

Insert the following as paragraph two:

The single-carrier modulation air interface specified herein for 10–66 GHz shall be known as the "WirelessMAN™-SC" air interface.

3. Definitions

Change the definition 3.3 to read:

3.3 Basic Connection: Connection that is established during ~~initial subscriber station registration~~ subscriber station initial ranging and that ~~which~~ is used to transport delay-intolerant MAC management messages.

Change the definition 3.25 and move it to retain alphabetical order:

3.25 Primary ~~m~~Management ~~c~~Connection: A connection that is established during initial subscriber station ~~registration~~ ranging that is used to transport delay-tolerant medium access control management messages.

Delete definition 3.42:

~~**3.42 service flow class:** A grouping of service flow properties to allow higher layer entities and external applications to request service flows with desired quality of service (QoS) parameters in a globally consistent way.~~

Insert the following definition at its correct alphabetical position:

3.43 Secondary Management Connection: A connection that is established during subscriber station registration that is used to transport standards based (SNMP, DHCP, etc.) management messages.

Delete definition 3.44:

~~**3.44 service flow name:** An ASCII string that is used to reference a set of quality of service (QoS) parameters that (partially) define a service flow.~~

6. MAC common part sublayer (CPS)

6.1.1.1.2 Semantics of the service primitive

Change the first paragraph to read:

The parameters of the primitive are as follows:

MAC_CREATE_CONNECTION.request
(
MAC Address
scheduling service type,
convergence sublayer,
service flow parameters,
payload header suppression indicator,
length indicator,
encryption indicator,
Packing on/off indicator,
Fixed-length or variable-length SDU indicator,
SDU length (only needed for fixed-length SDU connections),
CRC request,
ARQ parameters,
sequence number
)

6.1.1.10.4 Effect of receipt

Change the paragraph to read:

The receipt of this primitive causes the MAC entity to process the MAC SDU through the MAC sublayer and to pass the appropriately formatted PDUs to the PHY ~~transmission CS~~ transmission convergence sublayer for transfer to peer MAC sublayer entities, using the CID specified.

6.1.1.11.2 Semantics of service primitive

Change the first paragraph to read:

The parameters of the primitive are as follows:

MAC_DATA.indication
(
Connection ID,
length,
data,
reception status,
~~CS pass through,~~
encryption flag
)

6.2.1 Addressing and connections

Change the first paragraph to read:

Each SS shall have a 48-bit universal MAC address, as defined in IEEE Std 802®-2001. This address uniquely defines the SS from within the set of all possible vendors and equipment types. It is used during the ~~registration~~ initial ranging process to establish the appropriate connections for an SS. It is also used as part of the authentication process by which the BS and SS each verify the identity of each other.

Change the third paragraph to read:

For bearer services, the ~~higher layers of the BS set up~~ BS initiates the set-up of connections based upon the provisioning information distributed to the BS. The registration of an SS, or the modification of the services contracted at an SS, stimulates the higher layers of the BS to initiate the setup of the connections.

6.2.2.1.1 Generic MAC header

Change the second paragraph to read:

The fields of the Generic MAC header are defined in Table 3. Every header is encoded, starting with the HT and encryption control (EC) fields. The coding of these fields is such that the first byte of a MAC header shall never have the value of 0xFX, where 'X' means 'don't care'. This prevents false detection on the stuff byte used in the ~~transmission CS~~ transmission convergence sublayer.

6.2.2.3 MAC Management Messages

Change the first paragraph to read:

A set of MAC Management Messages are defined. These messages shall be carried in the Payload of the MAC PDU. All MAC Management Messages begin with a Management Message Type field and may contain additional fields. MAC Management Messages on the Basic, Broadcast, and Initial Ranging connections shall neither be fragmented nor packed. MAC Management Messages on the Primary Management Connection may be packed and/or fragmented. The format of the Management Message is given in Figure 24. The encoding of the Management Message Type field is given in Table 13. MAC management messages shall not be carried on Transport Connections. MAC management messages that do not contain all required parameters or contain erroneously encoded parameters shall be silently discarded.

Change Table 13, as follows:

21	MCA-REQ	Multicast Assignment Request	~~Basic~~ Primary Management
22	MCA-RSP	Multicast Assignment Response	~~Basic~~ Primary Management

6.2.2.3.3 Uplink Channel Descriptor message

Change the fourth paragraph, as follows:

~~Mini-slot~~ Minislot size
The size *n* of the minislot for this uplink channel in units of Physical Slots. Allowable values are $n = 2^m$, where *m* is an integer ranging from 0 through 7.

6.2.2.3.6 Ranging response (RNG-RSP) message

Change the last two paragraphs to read:

The following parameters shall be included in the RNG-RSP message:

Timing Adjust Information
Power Adjust Information
~~**Frequency Adjust Information**~~
Ranging Status

The following parameters may be included in the RNG-RSP message:

Downlink Frequency Override
Uplink Channel ID Override
Downlink Operational Burst Profile
Basic CID
A required parameter if the RNG-RSP message is being sent on the Initial Ranging CID in response to a RNG-REQ message that was sent on the Initial Ranging CID.
Primary Management CID
A required parameter if the RNG-RSP message is being sent on the Initial Ranging CID in response to a RNG-REQ message that was sent on the Initial Ranging CID.
SS MAC Address (48-bit)
A required parameter when the CID in the MAC header is the Initial Ranging CID.
Frequency Adjust Information

6.2.2.3.7 Registration Request (REG-REQ) message

Change the fourth paragraph to read:

The REG-REQs may contain the following TLV parameters stored in or generated by the SS:

Vendor ID Encoding (of the SS; see 11.4.3)
SS Capabilities Encodings (excluding UL CID support, physical parameters supported, and bandwidth allocation support) (see 11.4.1)
Convergence Sublayer Capabilities (see 11.4.5.1).

6.2.2.3.8 Registration Response (REG-RSP) message

Change the fourth paragraph to read:

The following parameters shall be included in the REG-RSP:

MAC Version (see 11.4.4)
Secondary Management CID
~~**Hashed message authentication code (HMAC)**~~ **Tuple** (see 11.4.10)

Change the last paragraph to read:

The following parameter may be included in the REG-RSP if the REG-REQ contained the Vendor ID Encoding for the SS:

Vendor-specific ~~extensions~~ information (see 11.4.11)

6.2.2.3.9.1 Security Association Add (SA Add) message

Insert the following row to the bottom of Table 26:

Attribute	Contents
HMAC Digest	Keyed secure hash algorithm (SHA) message

Change 6.2.2.3.9.3 to read:

6.2.2.3.9.3 Authorization Reply (Auth Reply) message

Sent by the BS to a client SS in response to an Authorization Request, the Authorization Reply message contains an Authorization Key, the key's lifetime, the key's sequence number, and a list of SA-Descriptors identifying the Primary and Static SAs the requesting SS is authorized to access and their particular properties (e.g., type, cryptographic suite). The Authorization Key shall be encrypted with the SS's public key. The SA-Descriptor list shall include a descriptor for the Basic CID reported to the BS in the corresponding Auth Request. The SA-Descriptor list may include descriptors of Static SAIDs that the SS is authorized to access.

The Auth Reply may also contain PKM configuration settings that override the default timer values.

Code: 5

Attributes are shown in Table 28.

Table 28—Auth Reply attributes

Attribute	Contents
AUTH-Key	Authorization (AUTH) Key, encrypted with the target client SS's public key
Key-Lifetime	Authorization Key's active lifetime
Key-Sequence-Number	Authorization key sequence number
(one or more) SA-Descriptor(s)	Each compound SA-Descriptor Attribute specifies an SAID and additional properties of the SA
PKM Configuration settings (optional)	PKM timer values

6.2.2.3.10 Dynamic Service Addition—Request (DSA-REQ) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall contain the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.11 Dynamic Service Addition—Response (DSA-RSP) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall contain the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.12 Dynamic Service Addition—Acknowledge (DSA-ACK) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall contain the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.13 DSC-REQ—Request (DSC-REQ) message

Change the subclause title to read: "Dynamic Service Change~~DSC~~—Request (DSC-REQ) message".

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall also contain:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.14 Dynamic Service Change—Response (DSC-RSP) message

Change the last paragraph to read:

~~Regardless of success or failure, if Privacy is enabled, the DSA-REQ Message shall contain the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.15 Dynamic Service Change—Acknowledge (DSC-ACK) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall contain the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.16 Dynamic Service Deletion—Request (DSD-REQ) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall include the following:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.17 Dynamic Service Deletion—Response (DSD-RSP) message

Change the last paragraph to read:

~~If Privacy is enabled, the DSA-REQ Message shall include:~~

HMAC Tuple (see 11.4.10)
The HMAC Tuple Attribute contains a keyed Message digest (to authenticate the sender). The HMAC Tuple Attribute shall be the final Attribute in the Dynamic Service Message's Attribute list.

6.2.2.3.24 SS Basic Capability Response (SBC-RSP) message

Change Table 50, as follows:

Table 50—SS SBC-RSP message format

Syntax	Size	Notes
SBC-RSP_Message_Format() {		
Management Message Type = 27	8 bits	
~~**Confirmation Code**~~	~~8 bits~~	
TLV Encoded Attributes	Variable	TLV specific
}		

6.2.6 Bandwidth allocation and request mechanisms

Change the first paragraph to read:

Note that ~~at registration~~during network entry and initialization every SS is assigned three dedicated CIDs for the purpose of sending and receiving control messages. Three connections are used to allow differentiated levels of QoS to be applied to the different connections carrying MAC management traffic. Increasing (or decreasing) bandwidth requirements is necessary for all services except incompressible constant bit rate UGS connections. The needs of incompressible UGS connections do not change between connection establishment and termination. The requirements of compressible UGS connections, such as channelized T1, may increase or decrease depending on traffic. Demand Assigned Multiple Access (DAMA) services are given resources on a demand assignment basis, as the need arises.

6.2.7.2 Framed (burst) FDD

Change the first paragraph to read:

In a framed (burst) FDD system, the uplink and downlink channels are located on separate frequencies and the downlink data can be transmitted in bursts. A fixed duration frame is used for both uplink and downlink transmissions. This facilitates the use of different modulation types. It also allows simultaneous use of both full-duplex subscriber stations (which can transmit and receive simultaneously) and optionally half-duplex subscriber stations (which cannot). If half-duplex subscriber stations are used, the bandwidth controller shall not allocate uplink bandwidth for a half-duplex subscriber station at the same time that it is expected to receive data on the downlink channel, including allowance for the propagation delay, and Tx/Rx and Rx/Tx Transition Gaps.

6.2.7.5 Uplink Map

Change the first paragraph to read:

~~The uplink map (UL-MAP) message defines the usage for the uplink minislots using a series of IEs, which define the usage of each uplink interval~~. The UL-MAP defines the uplink usage in terms of the offset, in units of minislots, of the burst relative to the Allocation Start Time (8.2.6.1.2). ~~The UL-MAP defines the uplink usage in terms of the offset from the previous IE start (the length) in numbers of minislots.~~

6.2.7.5.2 Uplink minislot definition

Change the subclause as follows:

6.2.7.5.2 Uplink ~~minislot definition~~ Minislots

The uplink bandwidth allocation map (UL-MAP) uses units of minislots. The size of the minislot is specified as a ~~number~~ function of PHY slots (PS) and is carried in the Uplink Channel Descriptor for each uplink channel. ~~One mini-slot contains *n* PHY slots (PS), where *n* is an integer ranging from 0 through 255. There is no implication that any MAC PDU can actually be transmitted in a single minislot.~~

6.2.9 Network entry and initialization

Replace the second paragraph with the following:

The procedure can be divided into the following phases:

a) Scan for downlink channel and establish synchronization with the BS
b) Obtain transmit parameters (from UCD message)
c) Perform ranging
d) Negotiate basic capabilities
e) Authorize SS and perform key exchange
f) Perform registration
g) Establish IP connectivity
h) Establish time of day
i) Transfer operational parameters
j) Set up connections

6.2.9.2 Obtain downlink parameters

Replace Figure 46 with the following figure:

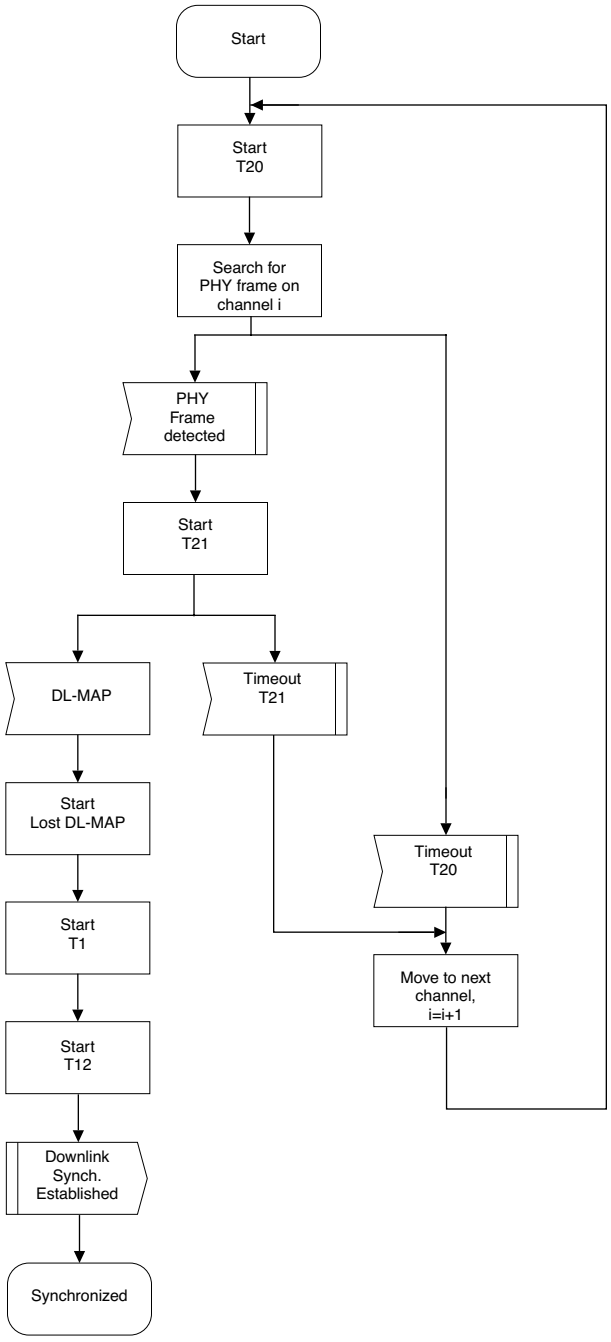


Figure 46—Obtaining downlink synchronization

6.2.9.3 Obtain uplink parameters

Replace Figure 48 with the following figure:

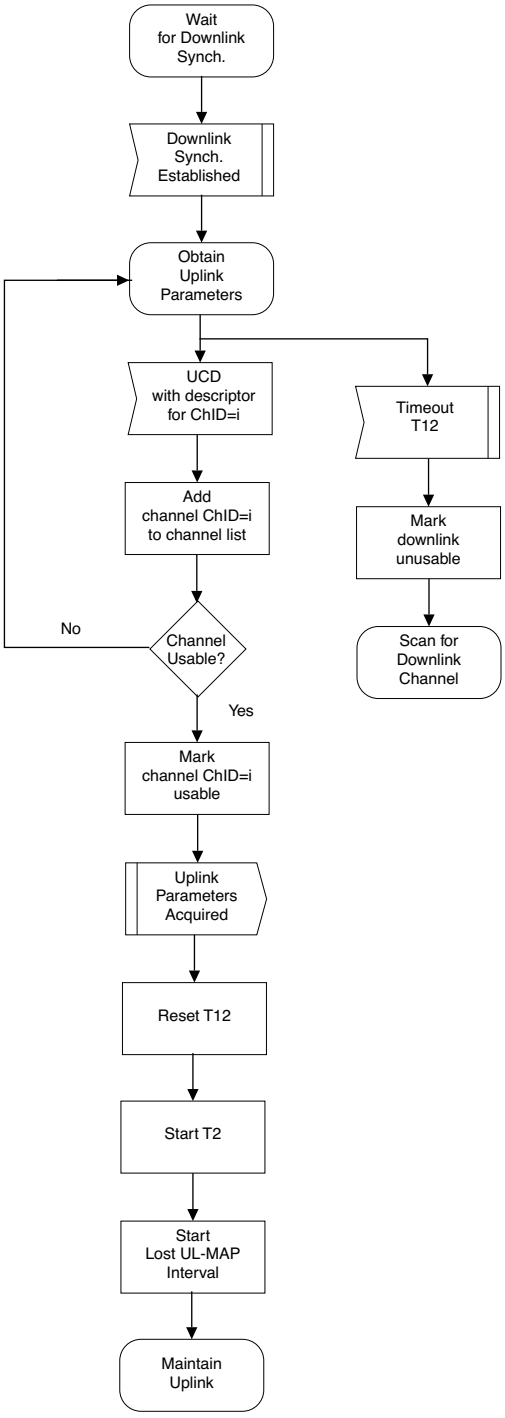


Figure 48—Obtaining uplink parameters

6.2.9.5 Initial ranging and automatic adjustments

Change the seventh paragraph to read:

Once the BS has successfully received the RNG-REQ message, it shall return a RNG-RSP message addressed to the individual SS. Within the RNG-RSP message shall be the Basic and Primary Management CIDs assigned to this SS. The message shall also contain information on RF power level adjustment and offset frequency adjustment as well as any timing offset corrections. At this point the BS shall start using invited Initial Maintenance Intervals addressed to the SS's Basic CID to complete the ranging process.

Replace Figure 50 with Figure 50a and Figure 50b as follows:

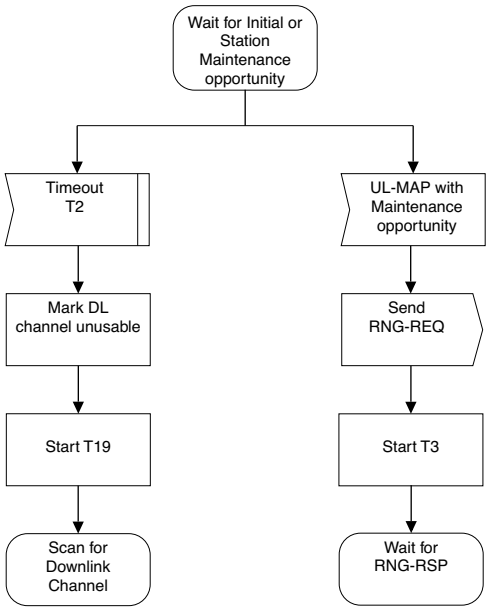
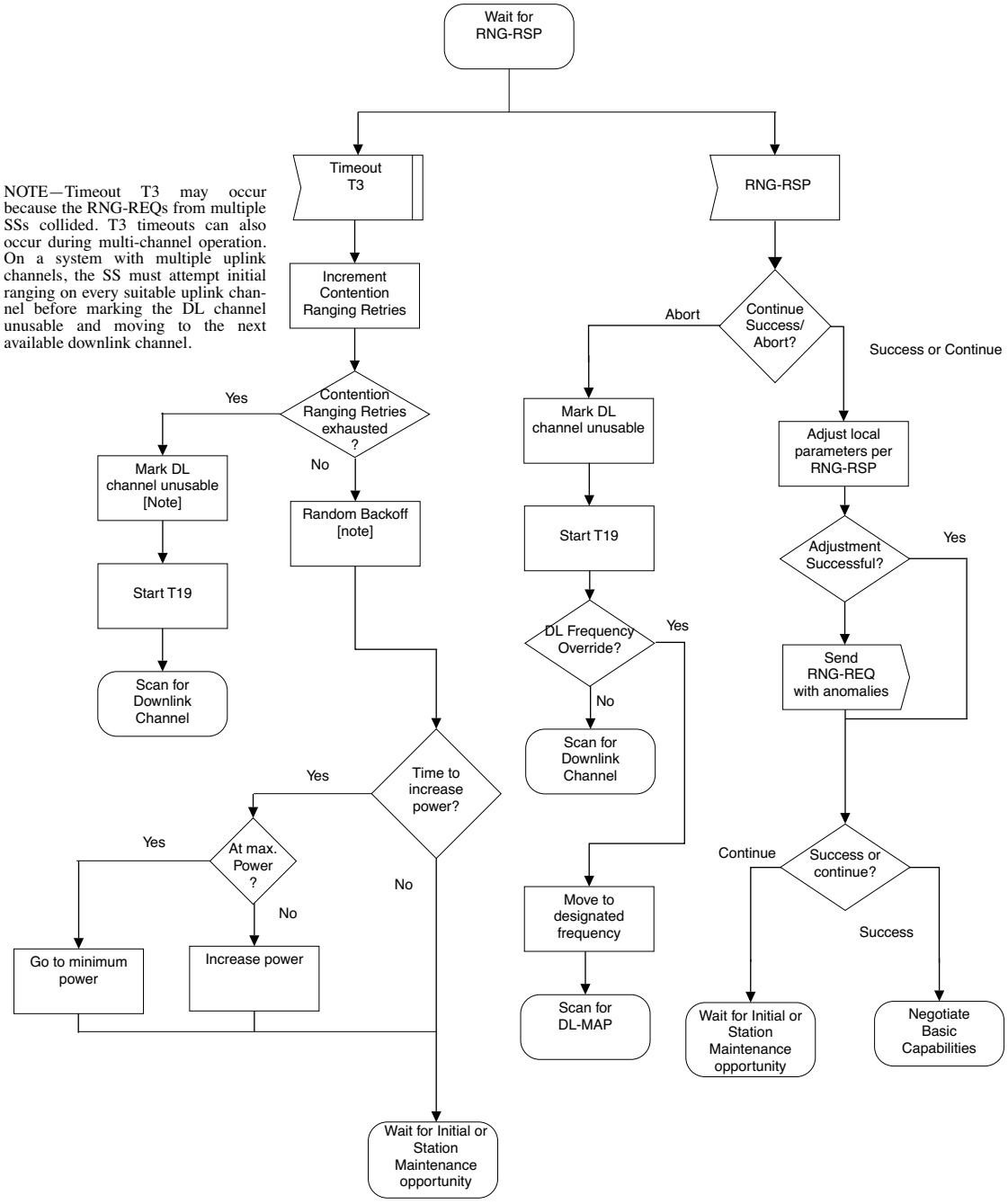


Figure 50a—Initial Ranging—SS (part 1)



NOTE—Timeout T3 may occur because the RNG-REQs from multiple SSs collided. T3 timeouts can also occur during multi-channel operation. On a system with multiple uplink channels, the SS must attempt initial ranging on every suitable uplink channel before marking the DL channel unusable and moving to the next available downlink channel.

Figure 50b—Initial Ranging—SS (part 2)

Replace Figure 51 with Figure 51a and Figure 51b as follows:

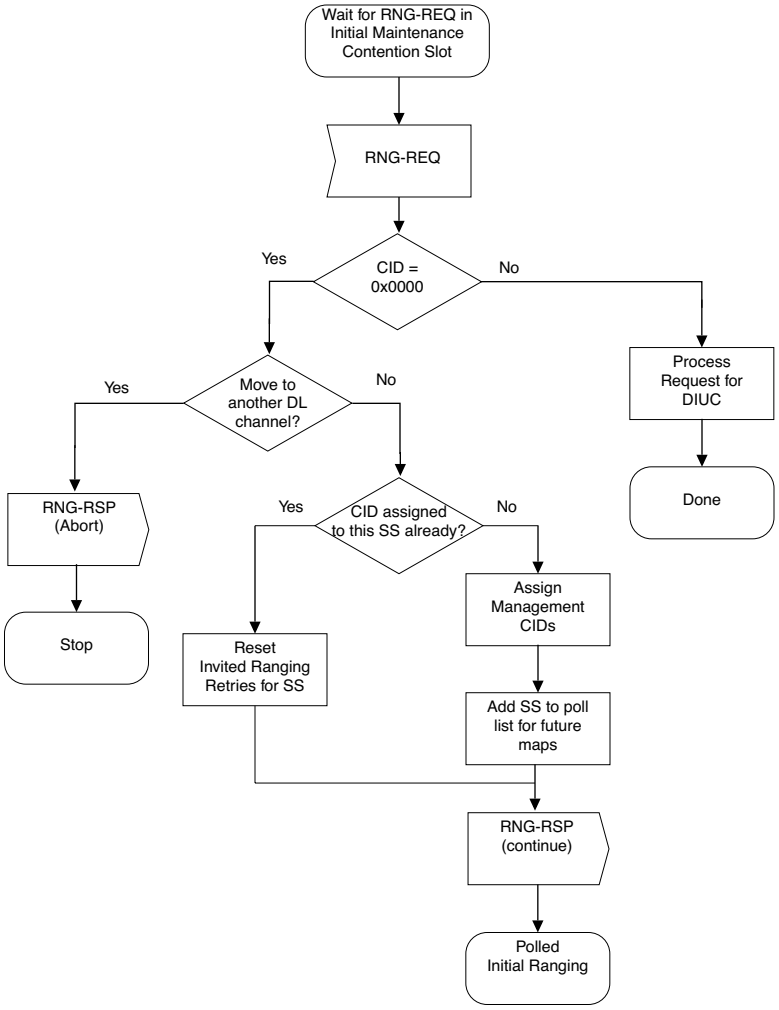
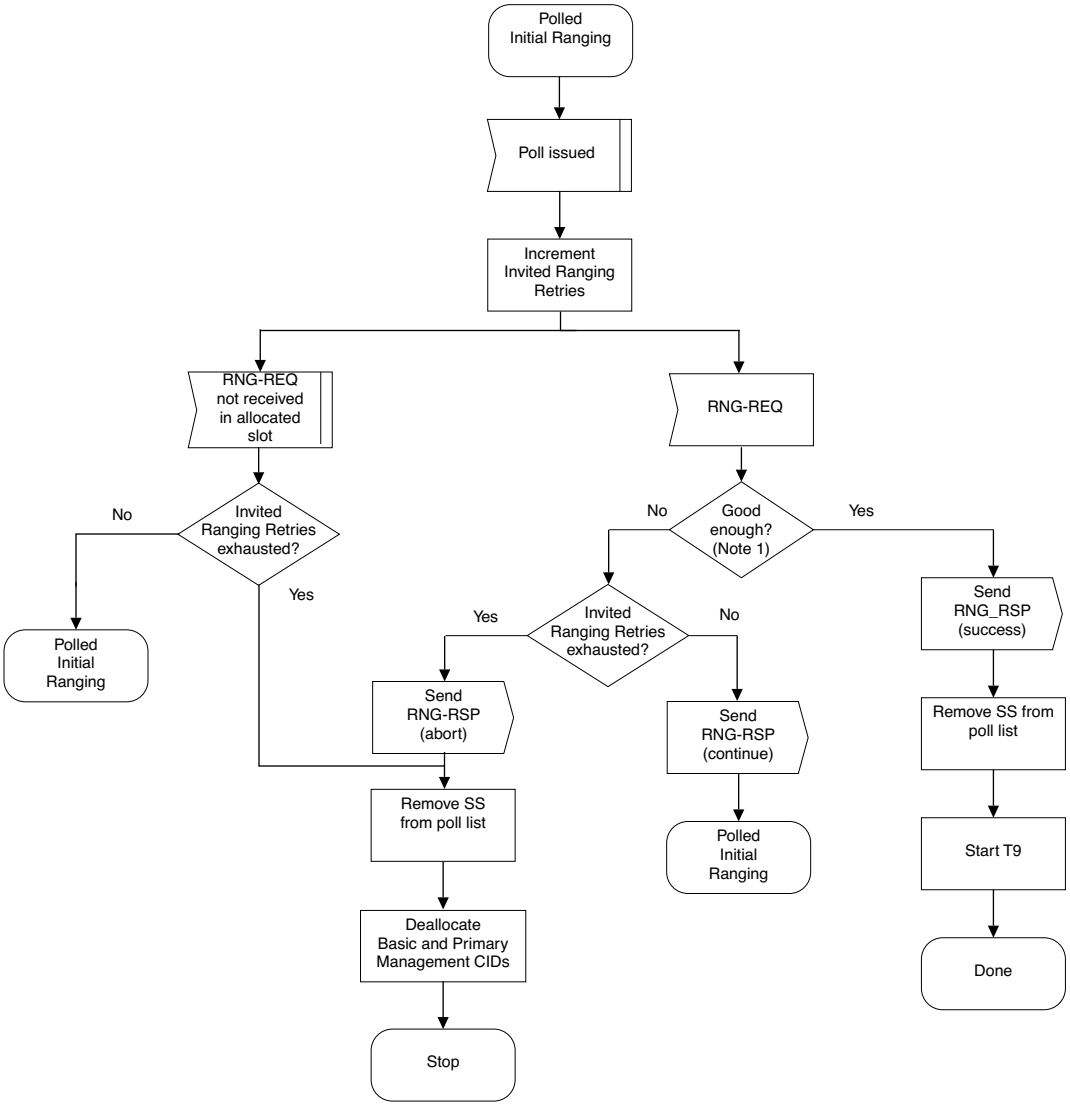


Figure 51a—Initial Ranging—BS



NOTE 1—Means ranging is within the tolerable limits of the BS.

NOTE 2—RNG-REQ pending-until-complete was nonzero, the BS should hold off the station maintenance opportunity accordingly unless needed, for example, to adjust the SS's power level.

Figure 51b—Initial Ranging, Polled Phase–BS

6.2.9.7 Negotiate basic capabilities

Insert Figure Ia, Figure Ib and Figure II as follows:

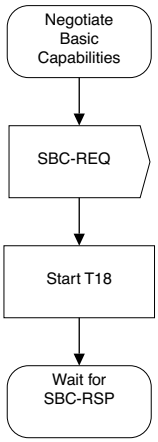


Figure Ia—Negotiate Basic Capabilities—SS

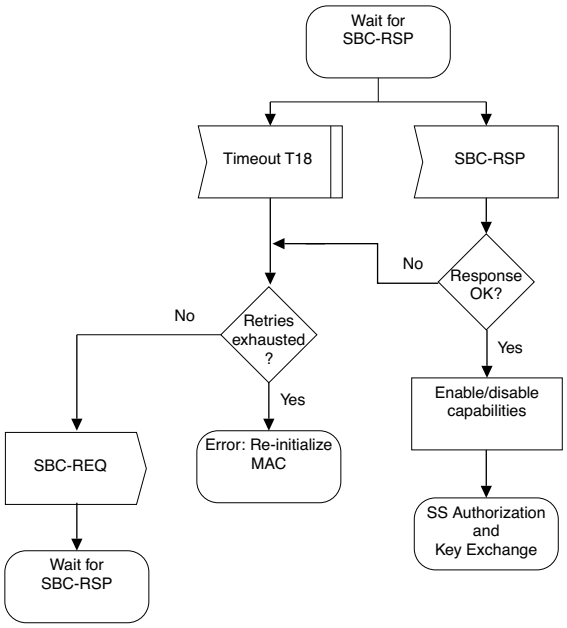


Figure Ib—Wait for SBC-RSP—SS

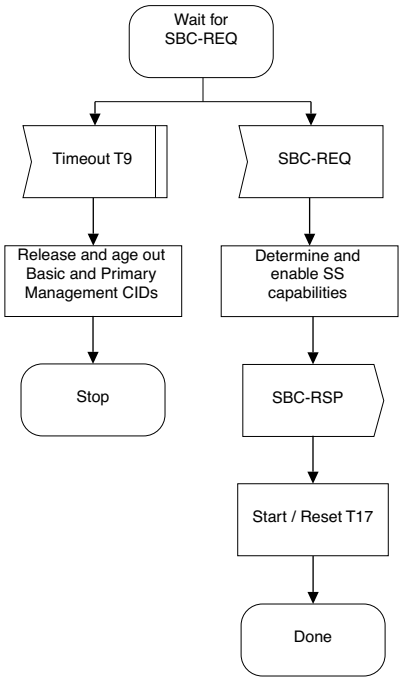


Figure II—Negotiate Basic Capabilities—BS

6.2.9.9 Registration

Replace Figure 52 with the following figure:

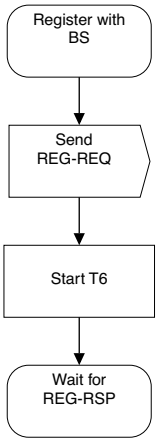


Figure 52—Registration—SS

Replace Figure 53 with the following figure:

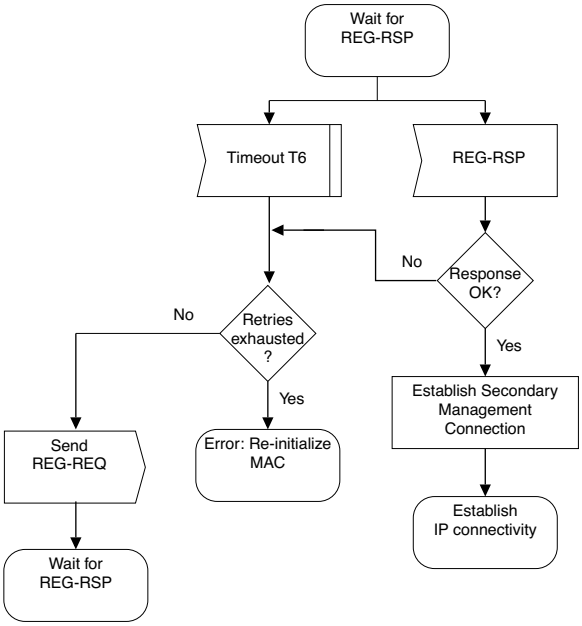


Figure 53—Wait for REG-RSP—SS

Replace Figure 54 with the following figure:

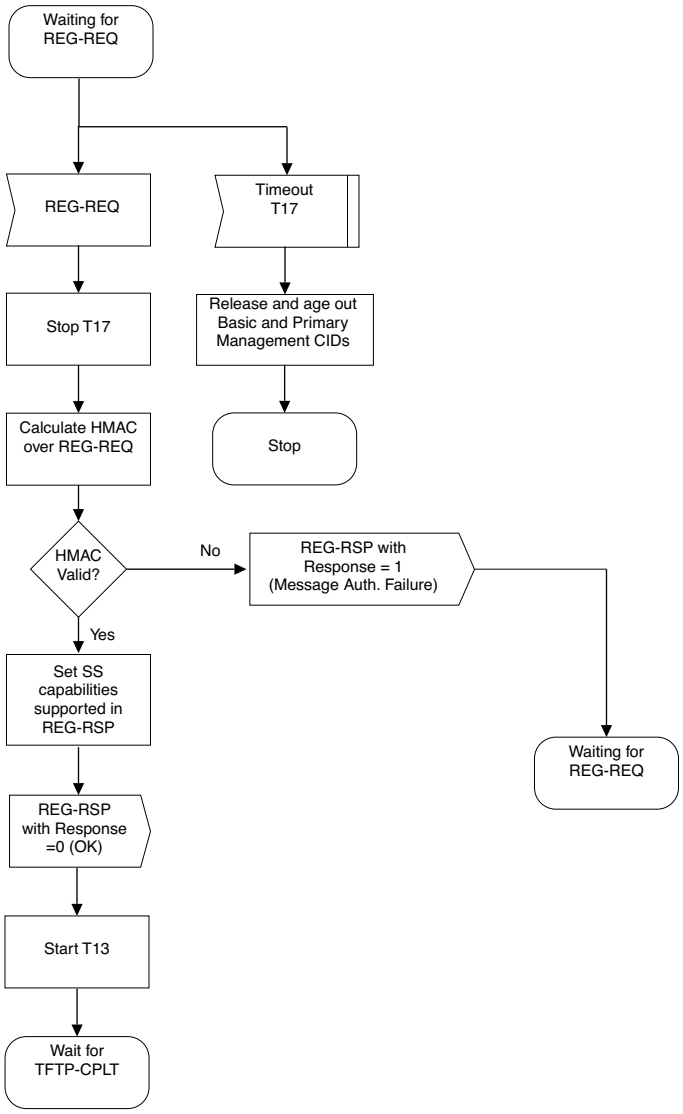


Figure 54—Registration—BS

6.2.9.12 Transfer operational parameters

Change the first paragraph to read:

After DHCP is successful, the SS shall download the SS Configuration File (9.2) using TFTP on the SS's Secondary Management Connection, as shown in ~~Figure 52~~ Table 64. The TFTP Configuration File server is specified by the "siaddr" field of the DHCP response. The SS shall use an adaptive timeout for TFTP based on binary exponential backoff [IETF RFC 1123, IETF RFC 2349].

Insert the following Table 64 into 6.2.9.12:

Then, change the table numbering in the remainder of the document by incrementing them by one.

Table 64—Transfer of Operational Parameters

SS		TFTP Server
Initiate TFTP Get protocol		
	<------TFTP Config File----- >	
		BS
Inform BS of completion		
	---------- TFT-CPLT ------- >	
		Acknowledge completion
	<-------- TFTP-RSP ----------	
		Establish provisioned connections

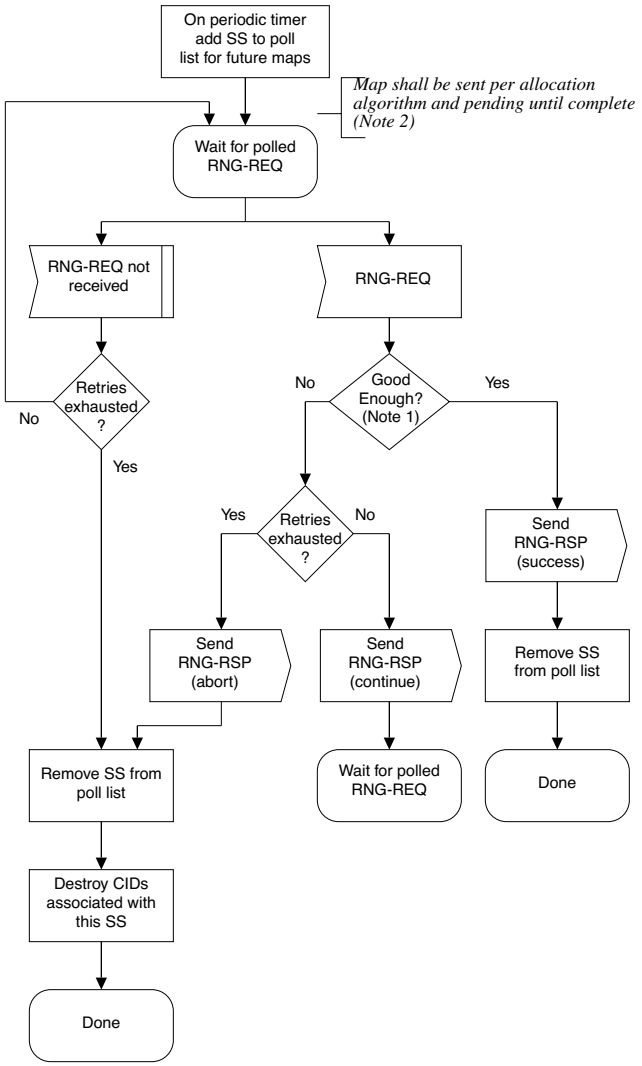
6.2.9.13 Establish provisioned connections

Change the first paragraph to read:

After the transfer of operational parameters, the BS shall send DSA-REQ messages to the ~~BS~~ SS to set up connections for preprovisioned service flows belonging to the SS. The SS responds with DSA-RSP messages. This is described further in 6.2.13.7.1.

6.2.10 Ranging

Replace Figure 55 with the following figure:



NOTES:

1—Means ranging is within the tolerable limits of the BS.

2—If RNG-REQ pending-until-complete was nonzero, the BS should hold off the station maintenance opportunity accordingly unless needed, for example, to adjust the SS's power level.

Figure 55—Periodic Ranging—BS

6.2.13.2 Service Flows

Change the first paragraph to read:

A *service flow* is a MAC-layer transport service that provides unidirectional transport of packets either to uplink packets transmitted by the SS or to downlink packets transmitted by the BS.[1] A service flow is characterized by a set of *QoS Parameters* such as latency, jitter, and throughput assurances. In order to standardize operation between the SS and BS, these attributes include details of how the SS requests uplink ~~mini-slots~~ minislots and the expected behavior of the BS uplink scheduler.

[1]A service flow, as defined here, has no direct relationship to the concept of a "flow" as defined by the IETF Integrated Services (intserv) Working Group [IETF RFC 2212]. An intserv flow is a collection of packets sharing transport-layer endpoints. Multiple intserv flows can be served by a single service flow.

6.2.13.7.1 Static operation

Change the first paragraph to read:

The provisioning of service flows is done via means outside of the scope of this standard, such as the network management system. ~~Configuration of provisioned service flows follows the Registration process.~~ Configuration of connections enabling Service Flows for provisioned services follows the transfer of the operational parameters, as shown in Figure 45. When this is complete, the BS passes service flow encodings to the SS in multiple DSA-REQ messages. The SS replies with DSA-RSP messages to complete service flow initialization.

6.2.13.7.2 Dynamic service flow creation

Change the first paragraph to read:

Service flows may be created by the Dynamic Service Addition (DSA) process as well as through the ~~Registration process outlined above~~ procedure outlined in 6.2.13.7.1. The DSA may be initiated by either the SS or the BS and may create one uplink and/or one downlink dynamic service flow(s). A three-way handshake is used to create service flows.

6.2.13.7.2.2 Dynamic service flow creation—BS initiated

Replace Figure 66 with a new Figure 66 as follows:

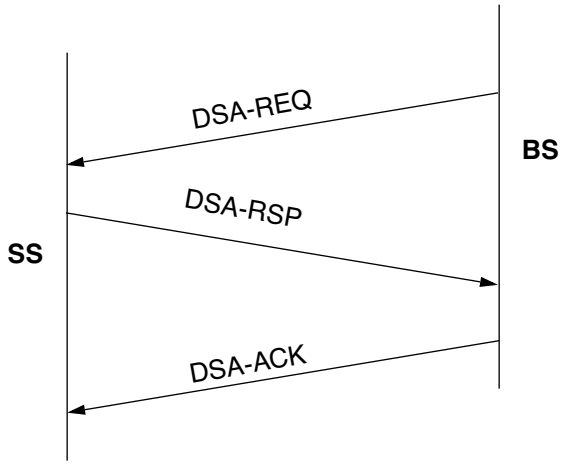


Figure 66—DSA message flow—BS-initiated

6.2.13.8.1 Connection Establishment

Change the second paragraph to read:

The Null state implies that no service flow exists that matches the SFID and/or Transaction ID in a Message. Once the service flow exists, it is operational and has an assigned SFID. In steady state operation, a service flow resides in a Nominal state. When Dynamic Service messaging is occurring, the service flow may transition through other states, but remains operational. Since multiple service flows may exist, there may be multiple state machines active, one for every service flow. Dynamic Service Messages only affect those state machines that match the SFID and/or Transaction ID. ~~If privacy is enabled, b~~ Both the SS and BS shall verify the HMAC digest on all dynamic service Messages before processing them, and discard any Messages that fail.

6.2.13.8.2 DSA state transition diagrams

Replace Figure 76 with a new Figure 76 as follows:

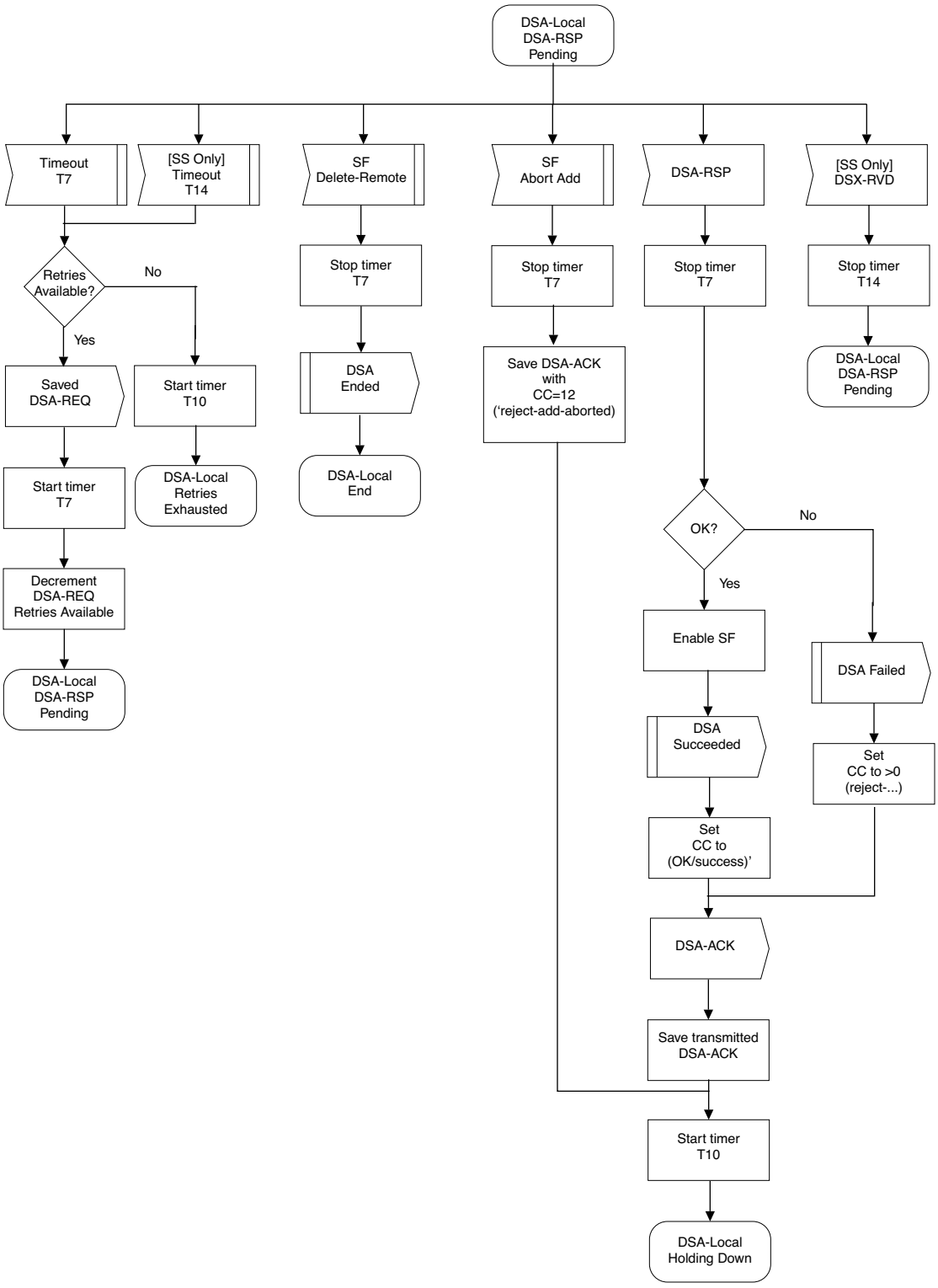


Figure 76—DSA—Locally initiated transaction DSA-RSP pending state flow diagram

In Figure 80, move arrows to remove mis-alignment.

6.2.13.8.4 Dynamic Service Change (DSC)

Change the eighth paragraph to read:

Any service flow can be deactivated with a DSA command by sending a DSC-REQ Message, referencing the Service Flow Identifier, and including a null ActiveQoSParamSet. However, if a Basic, Primary Management, or Secondary Management Connection of an SS is deactivated that SS is deregistered and shall re-register. Therefore, care should be taken before deactivating such service flows. If a service flow that was provisioned ~~during registration~~ is deactivated, the provisioning information for that service flow shall be maintained until the service flow is reactivated.

6.2.13.8.4.3 DSC state transition diagrams

Replace Figure 85 with a new Figure 85 as follows:

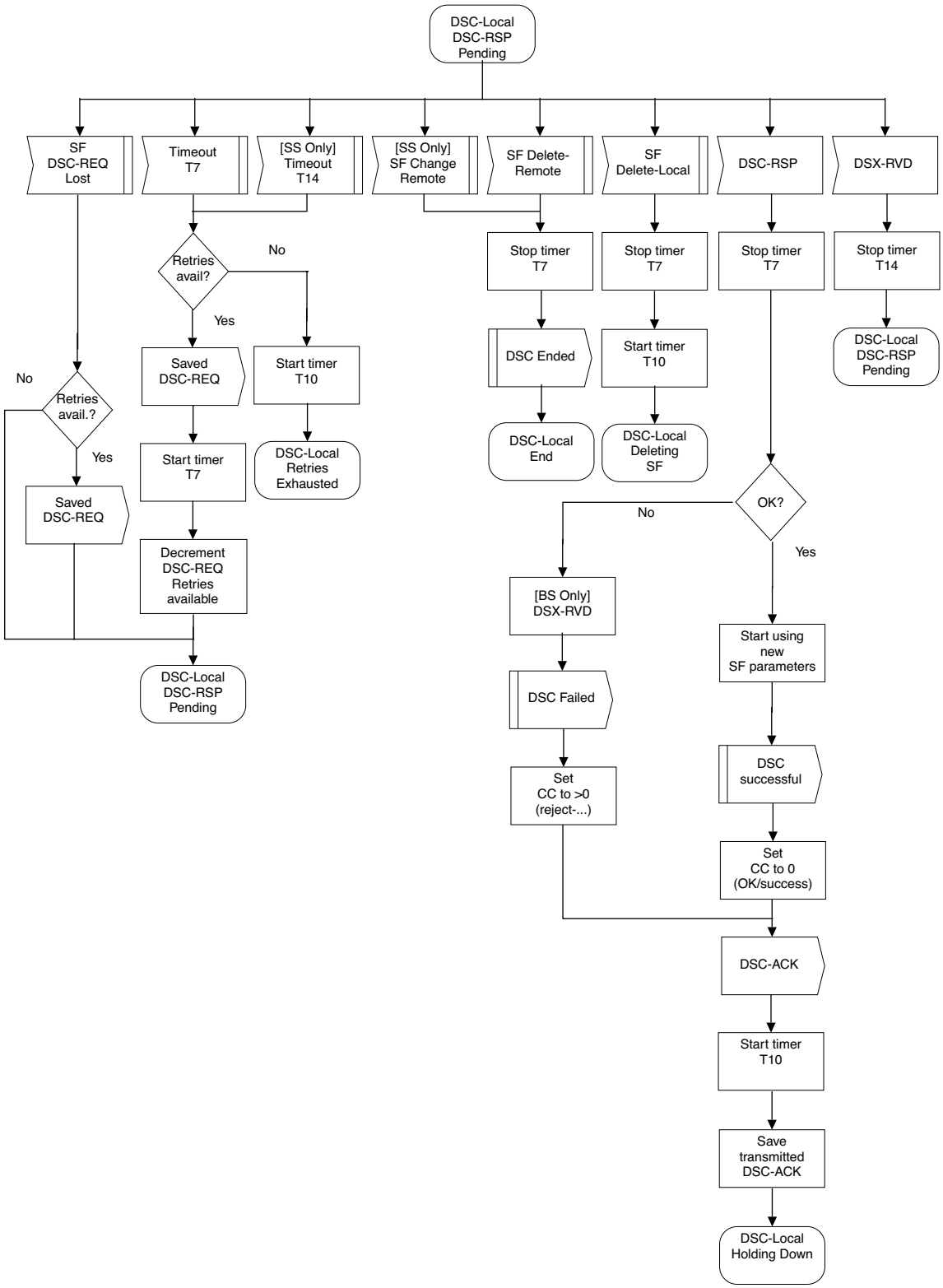


Figure 85—DSC—Locally initiated transaction DSC-RSP pending state flow diagram

6.2.13.8.5 Connection release

Change the first paragraph to read:

Any service flow can be deleted with the Dynamic Service Deletion (DSD) Messages. When a service flow is deleted, all resources associated with it are released. However, if a basic, primary management, or secondary management service flow of an SS is deleted, that SS is deregistered and shall ~~reregister. Also, if a service flow that was provisioned during registration is deleted, the provisioning information for that service flow is lost until the SS reregisters. However, the deletion of a provisioned service flow shall not cause an SS to re-register. Therefore, care should be taken before deleting such service flows.~~ re-initialize. Also, if a Service Flow for a provisioned service is deleted, the ability to re-establish the Service Flow for that service is network management dependent. Therefore, care should be taken before deleting such Service Flows. However, the deletion of a provisioned Service Flow shall not cause an SS to re-initialize.

6.2.13.8.5.3 DSD state transition diagrams

After Figure 96, insert Figure V as follows:

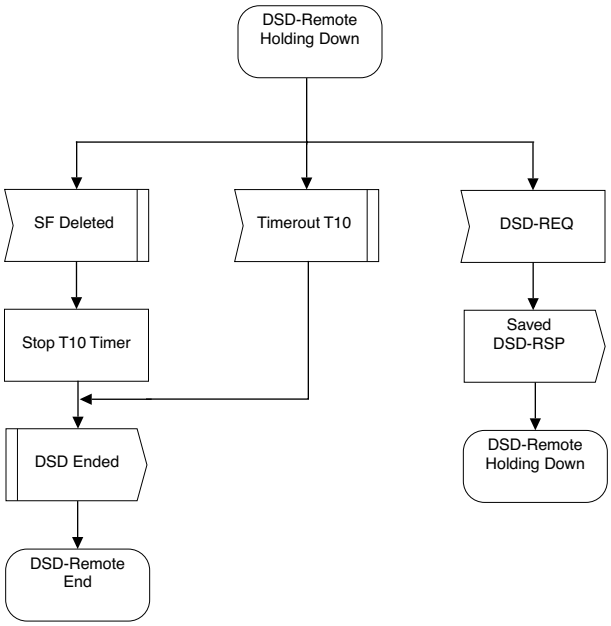


Figure V—DSD—Remotely Initiate Transaction Holding Down state flow diagram

7. Privacy Sublayer

7.1.3 Security Associations

Change the first paragraph to read:

A *Security Association* (SA) is the set of security information a BS and one or more of its client SSs share in order to support secure communications across the IEEE Std 802.16-2001 network. Three types of SAs are defined: *Primary, Static*, and *Dynamic*. Each SS establishes a Primary Security association during the SS initialization process. Static SAs are provisioned within the BS. Dynamic SAs are established and eliminated, on the fly, in response to the initiation and termination of specific service flows. Both Static and Dynamic SAs can by shared by multiple SSs.

7.2.1 SS authorization and AK exchange overview

Change the color of the reference in the second to last paragraph to black.

Change 7.2.4.3, as follows:

7.2.4.3 Events

Authorization Grace Timeout (Auth Grace Timeout): The Authorization Grace timer timed out. This timer fires a configurable amount of time (the Authorization Grace Time) before the current authorization is supposed to expire, signalling the SS to reauthorize before its authorization actually expires. The Authorization Grace Time ~~is~~ takes the default value from Table 119 or may be specified in a configuration setting within the Auth Reply message~~TFTP-downloaded SS Configuration File (9.2)~~.

Change the first paragraph of 7.2.4.4 to read:

7.2.4.4 Parameters

All configuration parameter values ~~are~~ take the default values from Table 119 or may be specified in the Auth Reply message ~~TFTP-downloaded SS Configuration File (see 9.2)~~.

Change the first paragraph of 7.2.5.4 to read:

7.2.5.1 States

Change the third paragraph to read:

Operational Reauthorize Wait (Op Reauth Wait): The wait state the TEK state machine is placed in if it does not have valid keying material while the Authorization state machine is in the middle of a reauthorization cycle.

7.2.5.4 Parameters

All configuration parameter values ~~are~~ take the default values from Table 119 or may be specified in the Auth Reply message ~~TFTP-downloaded SS Configuration File (see 9.2)~~.

Also change:

TEK Grace Time: Time interval, in seconds, before the estimated expiration of a TEK that the SS starts rekeying for a new TEK. TEK Grace Time ~~is~~ takes the default value from Table 119 or may be specified in a

configuration setting within the Auth Reply message~~TFTP-downloaded SS Configuration File (9.2)~~. and is the same across all SAIDs (see 11.2.19.6).

7.2.5.5 Actions

Change item a) of event "5-E" to read:

5-E Rekey Wait (*TEK Invalid*) → Op Wait

a) ~~clear Key Request retry timer~~ clear TEK refresh timer

8. Physical layer

8.1.1 Scope

Change the first paragraph to read:

This subclause contains a generic definition of the PHY service specification applicable to all PHY options, each of which may consist of two protocol sublayers as follows:

a) A ~~transmission CS~~ Transmission Convergence sublayer.

b) A Physical Medium Dependent (PMD) sublayer. Each PMD sublayer may require the definition of a unique ~~transmission CS~~ Transmission Convergence sublayer. If the PMD sublayer already provides the defined PHY services, the transmission convergence function might be null.

8.1.3.27.2 Semantics of the service primitive

Insert a new line between the opening and closing parenthesis with the content "RXSTATUS."

Change the heading of 8.2 as follows:

8.2 ~~PHY for 10–66 GHz~~ WirelessMAN–SC PHY Specification

8.2.1 Overview

Change the fourth paragraph to read:

The downlink PHY includes a ~~transmission CS~~ Transmission Convergence sublayer that inserts a pointer byte at the beginning of the payload to help the receiver identify the beginning of a MAC PDU. Data bits coming from the ~~transmission CS~~ Transmission Convergence sublayer are randomized, FEC encoded, and mapped to a QPSK, 16-QAM, or 64-QAM (optional) signal constellation.

8.2.5.1.1 Downlink burst preambles

Change the second paragraph to read:

Both preambles use QPSK modulation and are based upon +45 degrees rotated constant amplitude zero auto-correlation (CAZAC) sequences (Milewski [B15]). The amplitude of the preamble shall depend on the downlink power adjustment rule (8.2.5.4.7). In the case of the constant peak power scheme (power adjustment rule=0), the preamble shall be transmitted such that its constellation points coincide with the outermost constellation points of the ~~modulation scheme in use~~ modulation scheme(s) in the burst. In the case of the constant mean power scheme (power adjustment rule=1), it shall be transmitted with the mean power of the constellation points of the ~~modulation scheme in use~~ modulation scheme(s) in the burst.

8.2.5.1.2.3 UL-MAP allocation start time definition

Change the paragraph to read:

The allocation start time (Alloc Start Time) is the effective start time of the uplink allocation defined by the UL-MAP in units of ~~mini-slots~~ minislots.The start time is relative to the start of the frame in which the UL-MAP message is transmitted.

Change the subclause heading as follows:

8.2.5.3 Downlink ~~t~~Transmission ~~CS~~ Convergence sublayer

Replace Figure 113 with a new Figure 113 as follows:

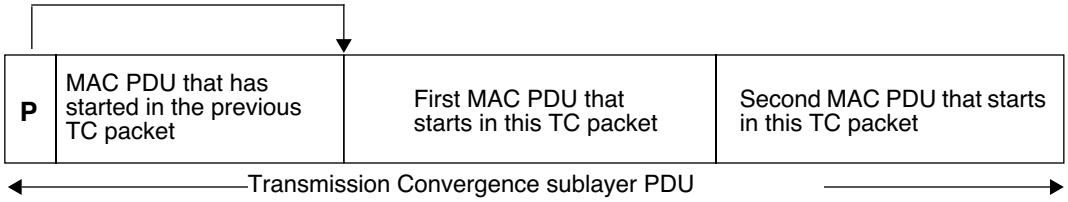


Figure 113—Format of the downlink transmission CS PDU

8.2.5.4.3 Randomization

Change the last paragraph to read:

At the beginning of each burst, the pseudorandom binary sequence register is cleared and the seed value of 100101010000000 is loaded. A burst corresponds to either a TDM burst beginning with the Frame Start Preamble or a TDMA burst beginning with a Downlink TDMA Burst Preamble (8.2.5.1.1). ~~The preambles are not randomized. The seed value shall be used to calculate the randomization bit, which is combined in an XOR with the first bit of data of each burst.~~ The seed value shall be used to calculate the randomization bits, which are combined in an XOR operation with the serialized bit stream of each burst. The randomizer sequence is applied only to information bits.

8.2.6.1.2 UL_MAP_Information_Element definition

Replace Table 107 with the following:

Table 107—UL_MAP_Information_Element

Syntax	Size	Notes
UL_MAP_Information_Element() {		
CID	16 bits	
UIUC	4 bits	
Offset	12 bits	offset, in units of minislots, of the preamble relative to the Allocation Start Time
}		

Change Table 108 to state:

Table 108—Uplink map IE

IE name	UIUC	Connection ID	Description
reserved	0	NA	Reserved for future use.
Request	1	any	Starting offset of request region.
Initial Maintenance	2	broadcast	Starting offset of maintenance region (used in Initial Ranging).
Station Maintenance	3	unicast	Starting offset of maintenance region (used in Periodic Ranging).
Data Grant Burst Type 1	4	unicast	Starting offset of Data Grant Burst Type 1 assignment.
Data Grant Burst Type 2	5	unicast	Starting offset of Data Grant Burst Type 2 assignment.
Data Grant Burst Type 3	6	unicast	Starting offset of Data Grant Burst Type 3 assignment.
Data Grant Burst Type 4	7	unicast	Starting offset of Data Grant Burst Type 4 assignment.
Data Grant Burst Type 5	8	unicast	Starting offset of Data Grant Burst Type 5 assignment.
Data Grant Burst Type 6	9	unicast	Starting offset of Data Grant Burst Type 6 assignment.
Null IE	10	zero	Ending offset of the previous grant. Indicates the first minislot after the end of the UL allocation. The burst profile is well known and shall not be included in the UCD message. Used to bound the length of the last actual interval allocation.
Empty	11	zero	Used to schedule gaps in transmission.
reserved	12-15	N/A	Reserved.

Change subclause heading as follows:

8.2.6.2 Uplink ~~transmission CS~~ Transmission Convergence sublayer

Change subclause heading as follows:

8.2.6.3 Uplink ~~PHY~~physical medium dependent (PMD) sublayer

8.2.6.3.4 Number of scheduled uplink bursts per frame

Replace content of the subclause with the following:

Only one scheduled burst (UIUC 4-9) per SS shall be included in the uplink map for any given frame.

9. Configuration file

9.2 SS Configuration File

Change 9.2.1 to read:

9.2.1 SS binary configuration file format

The SS-specific configuration data shall be contained in the SS Configuration File that is downloaded to the SS via TFTP. ~~This is a binary file in the same format defined for DHCP vendor extension data (IETF RFC 2132).~~ It shall consist of a number of configuration settings (1 per parameter) each ~~of the~~ in a TLV encoded form (see Clause 11). ~~shown in Table 109~~.

~~Table 109—Configuration setting format in SS binary configuration file~~

~~Type~~	~~Length~~	~~Value~~
~~1 byte~~	~~1 byte~~	~~1–254 bytes~~

~~Here~~

- ~~Type is a single-byte identifier which defines the parameter;~~
- ~~Length is a single byte containing the length of the value field in bytes (not including type and length fields);~~
- ~~Value is from 1 to 254 bytes containing the specific value for the parameter.~~

~~The configuration settings shall follow each other directly in the file, which is a stream of bytes (no record markers).~~

Configuration settings are divided into three types as follows:

- Standard configuration settings which shall be present
- Standard configuration settings which may be present
- Vendor-specific configuration settings

SSs shall be capable of processing all standard configuration settings. SSs shall ignore any configuration setting in the configuration file that it cannot interpret. To allow uniform management of SSs conformant to this specification, conformant SSs shall support a 8192-byte configuration file at a minimum.

Integrity of the configuration file information is provided by the SS MIC (message integrity check). The SS MIC is a digest which ensures that the data sent from the provisioning server were not modified en route. This is not an authenticated digest (it does not include any shared secret).

The SS MIC shall immediately be followed by the End of Data marker equal to 0xFF.

In case the file is a non-integer number of 32-bit words, the file shall be padded with zeros until next 32-bit boundary.

The file structure is shown in Figure 114:

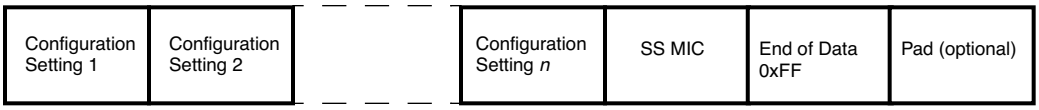


Figure 114—Configuration file structure

Change 9.2.2 to read:

9.2.2 Configuration file settings

The following configuration settings shall be included in the configuration file and shall be supported by all SSs:

a) SS MIC Configuration Setting

b) TFTP Server Timestamp

~~c) End Configuration Setting (end of data marker). End~~

The following configuration settings may be included in the configuration file and if present shall be supported by all SSs:

a) Software Upgrade Filename Configuration Setting (see 11.3.1)

~~b) SNMP Write Access Control (multiple) (see 11.3.4)~~

~~c) SNMP MIB Object (multiple) (see 11.3.5)~~

d) Software Server IP Address (see 11.3.2)

e) Pad Configuration Setting (as needed to hit 32-bit boundary in file) (see 11.3.2)

f) Vendor-Specific Configuration Settings

Replace 9.2.3 with the following:

9.2.3 Configuration file creation

The sequence of operations required to create the configuration file is as shown in Figure 131, Figure 132, and Figure 133.

a) Create the type/length/value (TLV) entries for all the parameters required by the SS.

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter *n*

Figure 131—Create TLV entries for parameters required by the SS

b) Calculate the SS MIC configuration setting as defined in 9.2.3.1 and add to the file following the last parameter using code and length values defined for this field.

type, length, value for parameter 1
type, length, value for parameter 2
type, length, value for parameter *n*
type, length, value for SS MIC

Figure 132—Add SS MIC

c) Add the end of data marker and pad with zeros to next 32 bit boundary if necessary.

type, length, value for parameter 1	
type, length, value for parameter 2	
type, length, value for parameter *n*	
type, length, value for SS MIC	
end of data marker	pad (optional)

Figure 133—Add end of data marker and pad

10. Parameters and constants

10.1 Global values

In Table 118, change the MAX MAP Pending row as follows:

BS	Max MAP Pending	The number of ~~mini-slots~~ mini-slots that a BS is allowed to map into the future			4096 mini-slot times beyond the Allocation Start Time

Insert the following rows into Table 118:

System	Name	Time reference	Minimum value	Default value	Maximum value
BS	T17	Time allowed for SS to complete SS Authorization and Key Exchange	5 min	5 min	
SS	T18	Wait for SBC-RSP timeout		50 ms	<< T9
SS	T19	Time DL-channel remains unusable			
SS	T20	Time the SS searched for preambles on a given channel	2 ms		
SS	T21	Time the SS searches for DL-MAP on a given channel			10 s

11. TLV encodings

Change the first paragraph to read:

The following type/length/value (TLV) encodings shall be used <u>for parameters</u> in both the configuration file (Clause 9) and MAC Management messages (6.2.2.3).

Delete the last paragraph of the subclause as follows:

~~The following configuration settings shall be supported by all BSs and SSs which are compliant with this specification. MAC management messages that do not contain all required encodings or contain encoding(s) with invalid length(s) shall be silently discarded.~~

11.1.4 RNG-RSP message encodings

Change Table 127 as follows:

Timing Adjust	1	4	Tx timing offset adjustment (signed 32-bit, units of 1/4 symbols) The time by which to offset frame transmission so that frames arrive at the expected minislot time at the BS. During periodic ranging, the range of the value of this parameter shall be limited to +/– 2 modulation symbols.

Change the title of the subclause to read:

11.1.5 MCA-REQ ~~and MCA-RSP~~ TLV encodings

Replace 11.3 and its subclauses with the following:

11.3 Configuration file encodings

These settings are found in only the configuration file. They shall not be forwarded to the BS in the Registration Request. Type fields and length fields are 1 byte in length.

11.3.1 Software upgrade filename

The filename of the software upgrade file for the SS. The filename is a fully qualified directory-path name which is in a format appropriate to the server. There is no requirement that the character string be null terminated; the length field always identifies the end of the string. The file is expected to reside on a TFTP server identified in a configuration setting option defined in 11.4.7.

Type	Length	Value
9	*n*	filename

11.3.2 Software upgrade TFTP server

This object is the IP address of the TFTP server on which the software upgrade file for the SS resides.

Type	Length	Value
21	4 or 16	IP Address

11.4 Common encodings

Insert Table A as follows:

Table A—Common Encodings

Type	Parameter
1	Secondary Management CID
5	SS Capabilities
6	Message Integrity Check
8	Vendor ID encoding
16	MAC version
19	TFTP Server Timestamp
20	TFTP Server Provisioned SS Address
24	Uplink SF Encodings
25	Downlink SF Encodings
27	HMAC Tuple
43	Vendor-Specific Information

Insert 11.4.0, as follows, under 11.4 before the subclause entitled "SS Capabilities encoding," and change the numbering of all subclauses in 11.4 to reflect this addition.

11.4.0 Secondary Management CID

This parameter contains the Secondary Management CID issued to an SS.

Type	Length	Value	Scope
1	2	Secondary Management CID	REG- RSP

11.4.1 SS Capabilities encoding

Insert Table B as follows:

Table B—SS Capability encodings

Type	Parameters
8	Uplink CID support
9	IP Version
12	Physical Parameters Supported
14	Multicast Polling Group Support
15	Bandwidth Allocation Support
16	PKM Flow Control
17	DSx Flow Control
18	MCA Flow Control
19	MAC CRC Support
20	Convergence Sublayer Support
21	Maximum Number of Classifiers
22	PHS Support

Change 11.4.1.9 to read:

11.4.1.9 Multicast polling group CID support

This field indicates the maximum number of simultaneous Multicast Polling Groups the SS is capable of belonging to.

Type	Length	Value	Scope
5.~~20~~14	1	0–255 default = 4	RNG-REQ RNG-RSP

11.4.3 Vendor ID encoding

Replace the content of this subclause with the following:

The value field contains the vendor identification specified by the 3-byte vendor-specific Organizationally Unique Identifier of the SS or BS MAC address.

When used as a subfield of the TLVs Vendor-specific information, Vendor-specific QoS parameters, Vendor-specific classifier parameters, or Vendor-specific PHS parameters, the Vendor ID encoding identifies the

Vendor ID of the SSs which are intended to use this information. A vendor ID used in a Registration Request shall be the Vendor ID of the SS sending the request. A vendor ID used in a Registration Response shall be the Vendor ID of the BS sending the response.

Type	Length	Value	Scope
8	3	v1, v2, v3	REG-REQ (see 6.2.2.3.7), DSx-REQ, DSx-RSP, DSx-ACK, and Configuration File

11.4.5.1 Convergence sublayer support

Replace the content of this subclause with the following:

This parameter indicates which service specific sublayers the SS supports.

Type	Length	Value	Scope
5.20	1	0: ATM 1: Packet, IPv4 2: Packet, IPv6 3: Packet, 802.3 4: Packet, 802.1Q VLAN 5: Packet, IPv4 over 802.3 6: Packet, IPv6 over 802.3 7: Packet, IPv4 over 802.1Q VLAN 8: Packet, IPv6 over 802.1Q VLAN 9-255 *reserved*, shall be set to zero	REG-REQ, REG-RSP

This TLV is repeated for each convergence sublayer supported by the SS.

11.4.8 Service flow encodings

Insert Table C as follows:

Table C—Service flow encodings

Type	Parameter
2	Service Flow Identifier
3	Connection Identifier
4	Service Class Name
5	Service Flow Error Parameter Set
6	QoS Parameter Set Type
7	Traffic Priority
8	Maximum Sustained Traffic Rate
9	Maximum Traffic Burst
10	Minimum Reserved Traffic Rate
14	Maximum Latency
15	Service Flow Scheduling Type
16	Request/Transmission Policy
18	Tolerated Jitter
24	Fixed-length versus Variable-length SDU Indicator
25	SDU Size
26	Target SAID
32	CS Specification
43	Vendor-Specific QoS Parameter
99–107	Convergence Sublayer Types

11.4.8.2 Connection identifier

Change the first paragraph as follows:

The value of this field specifies the CID assigned by the BS to a service flow with a non-null AdmittedQosParamSet or ActiveQosParamSet. ~~This is used in the bandwidth allocation map to assign uplink bandwidth.~~ The 16-bit value of this field is used in bandwidth requests and in MAC PDU headers. This field shall be present in BS-initiated DSA-REQ or DSC-REQ message related to establishing an admitted or active uplink service flow. This field shall also be present in DSA-RSP and DSC-RSP messages related to the successful establishment of an admitted or active uplink service flow.

11.4.8.11 Service flow scheduling type

Change the table as follows:

Type	Length	Value	Scope
[24/25].15	1	0: *reserved* 1: for Undefined (BS implementation-dependent[a]) 2: for Best Effort 3: for Non-Real-Time Polling Service 4: for Real-Time Polling Service 5: *reserved* 6: for Unsolicited Grant Service 7: through 255 are reserved for future use	DSx-REQ DSx-RSP DSx-ACK

[a]The specific implementation-dependent scheduling service type could be defined in a message of Type 24.43 (Vendor-specific QoS Parameters).

11.4.9.2 CS parameter encoding rules

Replace content of subclause with:

Each CS defines a set of parameters that are encoded within a subindex under the "cst" values listed below. In the cases of IP over IEEE 802.x, the relevant IP and IEEE 802.x parameters shall be included in the DSx-REQ message.

cst	Convergence sublayer
99	ATM
100	Packet, IPv4
101	Packet, IPv6
102	Packet, 802.3
103	Packet, 802.1Q VLAN
104	Packet IPV4 over 802.3
105	Packet IPV6 over 802.3
106	Packet IPV4 over 802.1Q VLAN
107	Packet IPV6 over 802.1Q VLAN

Replace 11.4.9.3 and all of its subclauses with the following:

11.4.9.3 Packet CS encodings for configuration and MAC-layer messaging

The following TLV encoded parameters shall be used in Dynamic Service Messages. The convergence sublayer specific type is denoted in the tables in the following sections by the variable "cst", which takes its value from the table in 11.4.9.2 (e.g., 100, 101, ...) depending upon the exact packet CS used for the service.

11.4.9.3.1 QoS-related encodings

The following TLV encodings shall be used in both the configuration file, registration messages, and Dynamic Service messages to encode parameters for packet classification and scheduling.

The following configuration settings shall be supported by all SSs that are compliant with this specification.

11.4.9.3.2 Classifier dynamic service change action

When received in a Dynamic Service Change (DSC) Request, this indicates the action to be taken with this classifier.

Type	Length	Value
[24/25].cst.6	1	0 — DSC Add Classifier 1 — DSC Replace Classifier 2 — DSC Delete Classifier

11.4.9.3.3 Classifier error parameter set

This field defines the parameters associated with Classifier Errors.

Type	Length	Value
[24/25].cst.8	*n*	Compound

A Classifier Error Parameter Set is defined by the following individual parameters: Packet Classifier Rule Index, Errored Parameter, Error Code, and Error Message.

The Classifier Error Parameter Set is returned in DSA-RSP and DSC-RSP messages to indicate the recipient's response to a Classifier establishment request in a DSA-REQ or DSC-REQ message.

On failure, the sender shall include one Classifier Error Parameter Set for each failed Classifier requested in the DSA-REQ or DSC-REQ message. Classifier Error Parameter Set for the failed Classifier shall include the Error Code and Errored Parameter and may include an Error Message. If some Classifier Sets are rejected but other Classifier Sets are accepted, then Classifier Error Parameter Sets shall be included for only the rejected Classifiers. On success of the entire transaction, the RSP or ACK message shall not include a Classifier Error Parameter Set.

Multiple Classifier Error Parameter Sets may appear in a DSA-RSP or DSC-RSP message, since multiple Classifier parameters may be in error. A message with even a single Classifier Error Parameter Set shall not contain any other protocol Classifier Encodings (e.g., IP, IEEE Std 802.1D™-1998, IEEE Std 802.1Q™-1998).

A Classifier Error Parameter Set shall not appear in any DSA-REQ or DSC-REQ messages.

11.4.9.3.3.1 Errored parameter

The value of this parameter identifies the subtype of a requested Classifier parameter in error in a rejected Classifier request. A Classifier Error Parameter Set shall have exactly one Errored Parameter TLV within a given Classifier Encoding.

Subtype	Length	Value
[24/25].cst.8.1	*n*	Classifier Encoding Subtype in Error

If the length is 1, then the value is the single-level subtype where the error was found; e.g., 7 indicates an invalid Change Action. If the length is 2, then the value is the multilevel subtype where the error was found; e.g., 9-2 indicates an invalid IP Protocol value.

11.4.9.3.3.2 Error code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in 11.4.12. A Classifier Error Parameter Set shall have exactly one Error Code within a given Classifier Encoding.

Subtype	Length	Value
[24/25].cst.8.2	1	Confirmation code except OK (0)

A value of OK(0) indicates that the Classifier request was successful. Since a Classifier Error Parameter Set applies only to errored parameters, this value shall not be used.

11.4.9.3.3.3 Error message

This subtype is optional in a Classifier Error Parameter Set. If present, it indicates a text string to be displayed on the SS console and/or log that further describes a rejected Classifier request. A Classifier Error Parameter Set may have zero or one Error Message subtypes within a given Classifier Encoding.

Subtype	Length	Value
[24/25].cst.8.3	*n*	Zero-terminated string of ASCII characters

NOTE—The length *n* includes the terminating zero.

11.4.9.3.4 Packet classification rule

This compound parameter contains the parameters of the classification rule. All parameters pertaining to a specific classification rule shall be included in the same Packet Classification Rule compound parameter.

Type	Length	Value
[24/25].cst.9	*n*	Compound

11.4.9.3.4.1 Classifier rule priority

The value of the field specifies the priority for the Classifier, which is used for determining the order of the Classifier. A higher value indicates higher priority.

Classifiers may have priorities in the range 0–255 with the default value being 0.

Type	Length	Value
[24/25].cst.9.1	1	0–255

11.4.9.3.4.2 IP Type of Service/DSCP range and mask

The values of the field specify the matching parameters for the IP ToS/DSCP [IETF RFC 2474] byte range and mask. An IP packet with IP ToS byte value “ip-tos” matches this parameter if tos-low <= (ip-tos AND tos-mask) <= tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.2	3	tos-low, tos-high, tos-mask

11.4.9.3.4.3 Protocol

The value of the field specifies a list of matching values for the IP Protocol field. For IPv6 (IETF RFC 2460), this refers to next header entry in the last header of the IP header chain. The encoding of the value field is that defined by the IANA document “Protocol Numbers.” If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.3	*n*	prot1, prot2,...prot *n*

11.4.9.3.4.4 IP masked source address

This parameter specifies a list of IP source addresses (designated "src_i") and their corresponding address masks (designated "$smask_i$"). An IP packet with IP source address "ip-src" matches this parameter if src_i = (ip-src AND $smask_i$) for any *i* from 1 to *n*. If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.4	*n**8 (IPv4) or *n**32 (IPv6)	src_1, $smask_1$,..., src_i, $smask_{i,}$..., src_n, $smask_n$

11.4.9.3.4.5 IP destination address

This parameter specifies a list of IP destination addresses (designated "dst_i") and their corresponding address masks (designated "$dmask_i$"). An IP packet with IP destination address "ip-dst" matches this parameter if dst_i = (ip-dst AND $dmask_i$) for any *i* from 1 to *n*. If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.5	*n**8 (IPv4) or *n**32 (IPv6	dst_1, $dmask_1$,..., dst_i, $dmask_{i,}$..., dst_n, $dmask_n$

11.4.9.3.4.6 Protocol source port range

The value of the field specifies a list of nonoverlapping ranges of protocol source port values. Classifier rules with port numbers are protocol specific; i.e., a rule on port numbers without a protocol specification shall not be defined. An IP packet with protocol port value "src-port" matches this parameter if sportlow <= src-port <= sporthigh. If this parameter is omitted, the protocol source port is irrelevant. This parameter is irrelevant for protocols without port numbers.

Type	Length	Value
[24/25].cst.9.6	*n**4	sportlow 1, sporthigh 2,...,sportlow *n*, sporthigh *n*

11.4.9.3.4.7 Protocol destination port range

The value of the field specifies a list of non-overlapping ranges of protocol destination port values. Classifier rules with port numbers are protocol specific; i.e., a rule on port numbers without a protocol specification shall not be defined. An IP packet with protocol port value "dst-port" matches this parameter if dportlow <= dst-port <=dporthigh. If this parameter is omitted, then the protocol destination port is irrelevant. This parameter is irrelevant for protocols without port numbers.

Type	Length	Value
[24/25].cst.9.7	*n**4	dportlow 1, dporthigh 2,...,dportlow *n*, dporthigh *n*

11.4.9.3.4.8 Ethernet destination MAC address

This parameter specifies a list of MAC destination addresses (designated "dst_i") and their corresponding address masks (designated "msk_i"). An Ethernet packet with MAC destination address "etherdst" corresponds to this parameter if dst_i = (etherdst AND msk_i) for any *i* from 1 to *n*. If this parameter is omitted, then comparison of the Ethernet destination MAC address for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.8	*n**12	dst_1, msk_1,..., dst_i, msk_i,..., dst_n, msk_n

11.4.9.3.4.9 Ethernet source MAC address

This parameter specifies a list of MAC source addresses (designated "src_i") and their corresponding address masks (designated "msk_i"). An Ethernet packet with MAC source address "ethersrc" corresponds to this parameter if src_i = (ethersrc AND msk_i) for any *i* from 1 to *n*. If this parameter is omitted, then comparison of the Ethernet source MAC address for this entry is irrelevant.

Type	Length	Value
[24/25].cst.9.9	*n**12	src_1, msk_1,..., src_i, msk_i,..., src_n, msk_n

11.4.9.3.4.10 Ethertype/IEEE Std 802.2-1998 SAP

The format of the Layer 3 protocol ID in the Ethernet packet is indicated by type, eprot1, and eprot2 as follows:

If type = 0, the rule does not use the Layer 3 protocol type as a matching criteria. If type = 0, eprot1, eprot2 are ignored when considering whether a packet matches the current rule.

If type = 1, the rule applies only to SDUs that contain an Ethertype value. Ethertype values are contained in packets using the DEC-Intel-Xerox (DIX) encapsulation or the Sub-Network Access Protocol (SNAP) encapsulation (IEEE Std 802.2™-1998, IETF RFC 1042) format. If type = 1, then eprot1, eprot2 gives the 16-bit value of the Ethertype that the packet shall match in order to match the rule.

If type = 2, the rule applies only to SDUs using the IEEE Std 802.2-1998 encapsulation format with a Destination Service (DSAP) other than 0xAA (which is reserved for SNAP). If type = 2, the lower 8 bits of the eprot1, eprot2 shall match the DSAP byte of the packet in order to match the rule.

If the Ethernet SDU contains an IEEE Std 802.1D-1998 and IEEE Std 802.1Q-1998 Tag header (i.e., Ethertype 0x8100), this object applies to the embedded Ethertype field within the IEEE Std 802.1D-1998 and IEEE Std 802.1Q-1998 header.

Other values of type are reserved. If this TLV is omitted, then comparison of either the Ethertype or IEEE Std 802.2-1998 DSAP for this rule is irrelevant.

Type	Length	Value
[24/25].cst.9.10	3	type, eprot1, eprot2

11.4.9.3.4.11 IEEE Std 802.1D-1998 User_Priority

The values of this field specify the matching parameters for the IEEE Std 802.1D-1998 user_priority bits. An Ethernet packet with IEEE Std 802.1D-1998 user_priority value “priority” matches these parameters if pri-low <= priority <= pri-high. If this field is omitted, then comparison of the IEEE Std 802.1D-1998 user_priority bits for this entry is irrelevant.

If this parameter is specified for an entry, then Ethernet packets without IEEE Std 802.1Q-1998 encapsulation shall not match this entry. If this parameter is specified for an entry on an SS that does not support forwarding of IEEE Std 802.1Q-1998 encapsulated traffic, then this entry shall not be used for any traffic.

Type	Length	Value
[24/25].cst.9.11	2	pri-low, pri-high Valid Range: 0–7 for pri-low and pri-high

11.4.9.3.4.12 IEEE Std 802.1Q-1998 VLAN_ID

The value of the field specifies the matching value for the IEEE Std 802.1Q-1998 vlan_id bits. Only the first (i.e., left-most) 12 bits of the specified vlan_id field are significant; the final four bits shall be ignored for comparison. If this field is omitted, then comparison of the IEEE Std 802.1Q-1998 vlan_id bits for this entry is irrelevant.

If this parameter is specified for an entry, then Ethernet packets without IEEE Std 802.1Q-1998 encapsulation shall not match this entry. If this parameter is specified for an entry on an SS that does not support forwarding of IEEE Std 802.1Q-1998 encapsulated traffic, then this entry shall not be used for any traffic.

Type	Length	Value
[24/25].cst.9.12	2	vlan_id1, vlan_id2

11.4.9.3.4.13 Associated Payload Header Suppression Index

The Associated Payload Header Suppression Index (PHSI) has a value between 1 and 255, which shall mirror the PHSI value of a payload header suppression rule. Packets matching the Packet Classification Rule containing the Associated PHSI parameter shall undergo PHS according to the corresponding PHS rule.

Type	Length	Value
[24/25].cst.9.13	1	index value

11.4.9.3.4.14 Packet Classifier Rule Index

The Packet Classifier Rule Index identifies a Packet Classifier Rule. The Packet Classifier Rule Index is unique per service flow.

Type	Length	Value
[24/25].cst.9.14	2	Packet Classifier Rule Index

11.4.9.3.4.15 Vendor-specific classifier parameters

This allows vendors to encode vendor-specific Classifier parameters. The Vendor ID shall be the first TLV embedded inside Vendor-Specific Classifier Parameters. If the first TLV inside Vendor-Specific Classifier Parameters is not a Vendor ID, then the TLV shall be discarded (see 11.4.11).

Type	Length	Value
[24/25].cst.9.255	*n*	

11.4.9.3.5 PHS dynamic service change action

When received in a DSC Request, this indicates the action that shall be taken with this PHS byte string.

Type	Length	Value
[24/25].cst.10	1	0 — Add PHS Rule 1 — Set PHS Rule 2 — Delete PHS Rule 3 — Delete all PHS Rules

The “Set PHS Rule” command is used to add the specific TLVs for an undefined payload header suppression rule. It shall not be used to modify existing TLVs.

When deleting all PHS Rules any corresponding PHSI shall be ignored.

An attempt to add a PHS Rule that already exists is an error condition.

11.4.9.3.6 PHS error parameter set

This field defines the parameters associated with PHS errors.

Type	Length	Value
[24/25].cst.11	*n*	compound field

A PHS Error Parameter Set is defined by the following individual parameters:

a) PHSI
b) Errored Parameter
c) Error Code
d) Error Message

The PHS Error Parameter Set is returned in DSA-RSP and DSC-RSP messages to indicate the recipient’s response to a PHS Rule establishment request in a DSA-REQ or DSC-REQ message.

On failure, the sender shall include one PHS Error Parameter Set for each failed PHS Rule requested in the DSA-REQ or DSC-REQ message. PHS Error Parameter Set for the failed PHS Rule shall include the Error Code and Errored Parameter and may include an Error Message. If some PHS Rule Sets are rejected but other PHS Rule Sets are accepted, then PHS Error Parameter Sets shall be included for only the rejected PHS Rules. On success of the entire transaction, the RSP or ACK message shall not include a PHS Error Parameter Set.

Multiple PHS Error Parameter Sets may appear in a DSA-RSP or DSC-RSP message, since multiple PHS parameters may be in error. A message with even a single PHS Error Parameter Set shall not contain any other protocol PHS Encodings (e.g., IP or IEEE Std 802.1D-1998/IEEE Std 802.1Q-1998).

A PHS Error Parameter Set shall not appear in any DSA-REQ or DSC-REQ messages.

11.4.9.3.6.1 Errored parameter

The value of this parameter identifies the subtype of a requested PHS Parameter in error in a rejected PHS request. A PHS Error Parameter Set shall have exactly one Errored Parameter TLV within a given PHS Encoding.

Type	Length	Value
[24/25].cst.11.1	1	Payload Header Suppression Encoding Subtype in Error

11.4.9.3.6.2 Error code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in 11.4.12. A PHS Error Parameter Set shall have exactly one Error Code within a given PHS Encoding.

Type	Length	Value
[24/25].cst.11.2	1	Confirmation code except OK(0)

A value of OK(0) indicates that the PHS request was successful. Since a PHS Error Parameter Set only applies to errored parameters, this value shall not be used.

11.4.9.3.6.3 Error message

This subtype is optional in a PHS Error Parameter Set. If present, it indicates a text string to be displayed on the SS console and/or log that further describes a rejected PHS request. A PHS Error Parameter Set may have zero or one Error Message subtypes within a given PHS Encoding.

Type	Length	Value
[24/25].cst.11.3	*n*	Zero-terminated string of ASCII characters

The length *n* includes the terminating zero.

11.4.9.3.7 PHS Rule

This field defines the parameters associated with a PHS Rule.

Type	Length	Value
[24/25].cst.12	*n*	

11.4.9.3.7.1 Payload Header Suppression Index (PHSI)

The PHSI has a value between 1 and 255, which uniquely references the suppressed byte string. The index is unique per service flow. The uplink and downlink PHSI values are independent of each other.

Type	Length	Value
[24/25].cst.12.1	1	index value

11.4.9.3.7.2 Payload Header Suppression Field (PHSF)

The PHSF is a string of bytes containing the header information to be suppressed by the sending CS and reconstructed by the receiving CS. The MSB of the string corresponds to first byte of the CS-SDU.

Type	Length	Value
[24/25].cst.12.2	*n*	string of bytes suppressed

The length *n* shall always be the same as the value for PHSS.

11.4.9.3.7.3 Payload Header Suppression Mask (PHSM)

The value of this field is used to interpret the values in the PHSF. It is used at both the sending and receiving entities on the link. The PHSM allows fields, such as sequence numbers or checksums (which vary in value), to be excluded from suppression with the constant bytes around them suppressed.

Type	Length	Value
[24/25].cst.12.3	*n*	bit 0: 0 = don't suppress first byte of the suppression field 1 = suppress first byte of the suppression field bit 1: 0 = don't suppress second byte of the suppression field 1 = suppress second byte of the suppression field bit *x*: 0 = don't suppress (*x*+1) byte of the suppression field 1 = suppress (*x*+1) byte of the suppression field

The length *n* is ceiling (PHSS/8). Bit 0 is the msb of the Value field. The value of each sequential bit in the PHSM is an attribute for the corresponding sequential byte in the PHSF.

If the bit value is a "1," the sending entity should suppress the byte, and the receiving entity should restore the byte from its cached PHSF. If the bit value is a "0," the sending entity should not suppress the byte, and the receiving entity should restore the byte by using the next byte in the packet.

If this TLV is not included, the default is to suppress all bytes.

11.4.9.3.7.4 Payload Header Suppression Size (PHSS)

The value of this field is the total number of bytes in the header to be suppressed and then restored in a service flow that uses PHS.

Type	Length	Value
[24/25].cst.12.4	1	number of bytes in the suppression string

This TLV is used when a service flow is being created. For all packets that get classified and assigned to a service flow with PHS enabled, suppression shall be performed over the specified number of bytes as indicated by the PHSS and according to the PHSM. If this TLV is not included in a service flow definition, or is included with a value of 0 bytes, then PHS is disabled. A non-zero value indicates PHS is enabled.

11.4.9.3.7.5 Payload Header Suppression Verification (PHSV)

The value of this field indicates to the sending entity whether or not the packet header contents are to be verified prior to performing suppression. If PHSV is enabled, the sender shall compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM.

Type	Length	Value
[24/25].cst.12.5	1	0 = verify 1 = don't verify

If this TLV is not included, the default is to verify. Only the sender shall verify suppressed bytes. If verification fails, the Payload Header shall not be suppressed.

11.4.9.3.7.6 Vendor-specific PHS Parameters

This allows vendors to encode vendor-specific PHS parameters. The Vendor ID shall be the first TLV embedded inside Vendor-specific PHS Parameters. If the first TLV inside Vendor-specific PHS Parameters is not a Vendor ID, then the TLV shall be discarded.

Type	Length	Value
[24/25].cst.12.255	*n*	—

11.4.9.4 ATM CS Encodings for Configuration and MAC-Layer Messaging

The TLV encodings listed in 11.4.9.4.1 through 11.4.9.4.3 shall be used in the configuration file, in SS registration requests (when applicable), and in Dynamic Service Messages (when applicable). All ATM specific TLVs are prefixed to begin with a Type value of [24/25]/99.

11.4.9.4.1 ATM switching encoding

This field defines the switching methodology for the service. If the field = 0, at least one VPI/VCI Classifier pair shall be defined for classifying the service. If the field = 1, exactly one VPI Classifier and zero or one VCI Classifier shall be specified for classifying the service. If the field = 2, exactly one VPI Classifier and one VCI Classifier shall be defined for classifying the service. If the field = 0, PHS is not allowed and the SDU size TLV shall equal 52. If the field = 1 and PHS is on for the service, the SDU size TLV shall equal 51; otherwise it shall be set equal to 52. If the field = 2 and PHS is on for the service, the SDU size TLV shall equal 49; otherwise it shall be set equal to 52.

Type	Length	Value
[24/25].99.0	1	0 = no switching methodology applied 1 = VP switching 2 = VC switching

11.4.9.4.2 ATM Classifier TLV

This field defines an ATM classifier. It is a compound TLV used to describe the VPI and associated VCIs for ATM classification.

Type	Length	Value
[24/25].99.1	Variable	Compound

It shall have the following form:

Field	Note
ATM Classifier ID	Always present
VPI Classifier	Always present except for DSC Change action deleting classifier
VCI Classification	0 or more instances (number apparent from ATM Classifier length field) if VPI Classifier is present

11.4.9.4.2.1 VPI classifier

This field defines the VPI on which to classify ATM cells for the service flow.

Type	Length	Value
[24/25].99.1.1	2	8 or 12-bit VPI field value

11.4.9.4.2.2 VCI classification

This field defines the VCI on which to classify ATM cells for the service flow.

This TLV shall immediately follow the VPI TLV with which it is associated.

Type	Length	Value
[24/25].99.1.2	2	16-bit VCI field value

11.4.9.4.2.3 ATM Classifier ID

This field is used to identify an ATM classifier.

Type	Length	Value
[24/25].99.1.3	16	16-bit classifier ID

11.4.9.4.3 ATM Classifier Dynamic Service Change Action

When received in a DSC-REQ message, this indicates the action to be taken on a classifier. If the action TLV is Add or Replace, the action is followed by a complete ATM Classifier compound TLV. If the action is delete, the action TLV is followed by the ATM Classifier compound TLV composed only of the ATM Classifier ID TLV.

Type	Length	Value
[24/25].99.2	1	0 – DSC Add Classifier 1 – DSC Replace Classifier 2 – DSC Delete Classifier

Replace Clause 12 with the following:

12. System profiles

This subclause defines system profiles that list sets of features to be used in typical implementation cases. Each profile is assigned an identifier for use in such documents as PICS proforma statements. Mandatory and conditionally mandatory features are listed for each profile. Any feature not mandatory or conditionally mandatory for a profile is optional for the profile except where otherwise forbidden by the standard. Optional features shall be implemented as specified in the standard.

12.1 WirelessMAN-SC (10–66 GHz) system profiles

This subclause defines system profiles for systems operating with the WirelessMAN-SC air interface.

Table 146—Profile definitions

Identifier	Description
profM1	Basic ATM MAC profile
profM2	Basic packet MAC profile
profP1	25 MHz channel PHY profile
profP1f	25 MHz channel PHY profile – FDD
profP1t	25 MHz channel PHY profile – TDD
profP2	28 MHz channel PHY profile
profP2f	28 MHz channel PHY profile – FDD
profP2t	28 MHz channel PHY profile – TDD

12.1.1 WirelessMAN-SC MAC system profiles

This subclause defines MAC profiles for systems operating with the WirelessMAN-SC air interface.

12.1.1.1 Basic ATM MAC system profile

Profile identifier: profM1.

Mandatory features:

— Support of PVCs.
— Support of VC-switched connections.
— Support of VP-switched connections.
— ATM payload header suppression is mandatory as a capability, but may be turned on or off on a per connection basis.
— IPv4 on the Secondary Management connection.
— Packing of multiple ATM cells into a single MAC PDU is mandatory as a capability, but may be turned on or off on a per connection basis.
— SDU fragmentation on the Primary Management and Secondary management connections.

Conditionally Mandatory features:

— If nrtPS or BE services are supported, then the SS responding to broadcast polling is mandatory.
— If multicast polling groups are supported, multicast polling must be supported.

12.1.1.2 Basic Packet MAC system profile

Profile identifier: profM2.

Mandatory features:

— Support of provisioned connections.
— IPv4 support on transport connection.
— Classification of packets in the SS based on the incoming physical port.
— Reception of multiple SDUs packed into a single MAC PDU is mandatory as a capability, but may be turned on or off on a per connection basis.
— Fragmentation of SDUs is mandatory as a capability, but may be turned on or off on a per connection basis.

Conditionally Mandatory features:

— If nrtPS or BE services are supported, then the SS responding to broadcast polling is mandatory.
— If multicast polling groups are supported, multicast polling must be supported.

12.1.1.3 Conventions for MAC Management Messages for profiles profM1 and profM2

The following rules shall be followed when reporting parameters in MAC Management messages:

— Service Class Names should not be used.
— No TLVs besides Error Encodings and HMAC Tuples shall be reported back in DSA-RSP and DSC-RSP messages.
— No TLVs besides HMAC Tuples shall be reported back in DSA-ACK messages.
— DSC-REQ messages shall not contain Request/Transmission Policy, Fixed vs. Variable Length SDU Indicator, SDU Size, ATM Switching, or Convergence Sublayer Specification TLVs.

12.1.1.4 MAC Management Message Parameter Transmission Order

The following subclauses define the order in which systems meeting profiles profM1 and profM2 shall transmit the TLV encoded parameters for mandatory features in the respective messages. Systems implementing either profile shall only include the parameters listed under the respective message in its transmission of said messages plus any parameters necessary for optional features. Parameters for optional features shall occur after those listed for support of mandatory features. Parameters with defined default values should be omitted if the desired value coincides with the default one. PHY specific messages are described in 12.1.2

12.1.1.4.1 DCD

The parameters of the DCD message are PHY profile specific.

12.1.1.4.2 DL-MAP

This message contains no TLV encoded information.

12.1.1.4.3 UCD

The parameters of the DCD message are PHY profile specific.

12.1.1.4.4 UL-MAP

This message contains no TLV encoded information.

12.1.1.4.5 RNG-REQ

— Requested DL Burst Profile
— SS MAC Address
— Ranging Anomalies

12.1.1.4.6 RNG-RSP

If ranging status equals “success” or “continue”:

— Ranging Status
— Timing Adjust (default to 0)
— Power Adjust (default to 0)
— DL operational Burst profile (only if changed)
— SS MAC Address (only on CID 0x0000)
— Basic CID (only on CID 0x0000)
— Primary Management CID (only on CID 0x0000)
— UL Channel Override (only if allowed by PHY profile)

If ranging status equals “abort”:

— Ranging Status
— SS MAC Address (only on CID 0x0000)
— DL frequency Override (if needed)

12.1.1.4.7 REG-REQ

— Vendor ID Encoding (optional)
— SS Capabilities Encoding (compound)
  — UL CID Support
  — PKM Flow Control (default = no limit)
  — DSx Flow Control (default = no limit)
  — MCA Flow Control (default = no limit)
  — IP version (default = IPv4)
  — MAC CRC support (default = support)
  — Multicast Polling Group CID support (default = 4)
  — Convergence sublayer support (1 instance for each CS supported)
  — Maximum number of classifiers (default = 0, no limit)
  — Payload header suppression support (default = 0, no PHS support)
— HMAC Tuple

12.1.1.4.8 REG-RSP

— MAC Version
— Secondary Management CID
— SS Capabilities Encoding (compound)
  — UL CID Support
  — Vendor ID Encoding (if present in REG-REQ)
  — PKM Flow Control (if present in REG-REQ or changed from default)
  — DSx Flow Control (if present in REG-REQ or changed from default)
  — MCA Flow Control (if present in REG-REQ or changed from default)
  — IP version (if present in REG-REQ or changed from default)
  — MAC CRC support (if present in REG-REQ or changed from default)
  — Multicast Polling Group CID support (if present in REG-REQ or changed from default)

— Vendor-specific information (Compound, only allowed if Vendor ID present in REG-REQ, and extensions provided)
  — Vendor ID
  — Vendor-Specific extensions
— HMAC Tuple

12.1.1.4.9 PKM-REQ: Authent Info

— CA-Certificate

12.1.1.4.10 PKM-REQ: Auth Request

— SS-Certificate
— Security Capabilities
— Version (default = 1)
— Cryptographic-Suite-List (default is that both no encryption and 56-bit DES are supported, no data authentication, and 3-DES EDE with 128-bit key)
— SAID

12.1.1.4.11 PKM-REQ: Key Request

— Key Sequence Number
— SAID
— HMAC Digest

12.1.1.4.12 PKM-RSP: SA Add

— Key-Sequence-Number
— SA Descriptor(s)
— SAID
— SA-Type
— Cryptographic Suite
— HMAC Digest

12.1.1.4.13 PKM-RSP: Auth Reply

— AUTH-Key
— Key-Lifetime
— Key-Sequence-Number
— SA-Descriptor(s)
— SAID
— SA-Type
— Cryptographic Suite

12.1.1.4.14 PKM-RSP: Auth Reject

— Error Code
— Display String (optional)

12.1.1.4.15 PKM-RSP: Key Reply

— Key Sequence Number
— SAID
— TEK-Parameters (Older)

  - — TEK
  - — Key Lifetime
  - — Key Sequence Number
  - — CBC-IV
- — TEK-Parameters (Newer)
- — TEK
  - — Key Lifetime
  - — Key Sequence Number
  - — CBC-IV
- — HMAC Digest

12.1.1.4.16 PKM-RSP: Key Reject

- — Key Sequence Number
- — SAID
- — Error Code
- — Display String (optional)
- — HMAC Digest

12.1.1.4.17 PKM-RSP: Auth Invalid

- — Error Code
- — Display String (optional)

12.1.1.4.18 PKM-RSP: TEK Invalid

- — Key Sequence Number
- — SAID
- — Error Code
- — Display String (optional)
- — HMAC Digest

12.1.1.4.19 DSA-REQ – BS Initiated Service Addition

- — Uplink Service Parameters
  - — Service Flow ID
  - — Transport CID
  - — Target SAID
  - — QoS Parameter Set Type
  - — Service Flow Scheduling Type
  - — Request/Grant Transmission Policy
  - — Convergence Sublayer Specification
  - — Fixed vs Variable Length SDU Indicator (default = variable)
  - — SDU Size (required if fixed, forbidden if variable SDU)
  - — Maximum Sustained Traffic Rate
  - — Minimum Reserved Traffic Rate (default = 0 for BE, Max Sust Rate for UGS, required for rtPS and nrtPS)
  - — Maximum Traffic Burst (required for rtPS and nrtPS, excluded otherwise)
  - — Traffic Priority (optional, BE only)
  - — Tolerated Jitter (optional)
  - — Maximum Latency (optional)
  - — Convergence Sublayer Specific Parameters (see 12.1.1.5 and 12.1.1.6)
  - — Vendor-Specific QoS Parameters
- — Downlink Service Parameters

  — Service Flow ID
  — Transport CID
  — Target SAID
  — QoS Parameter Set Type
  — Service Flow Scheduling Type
  — Request/Grant Transmission Policy
  — Convergence Sublayer Specification
  — Fixed vs. Variable Length SDU Indicator (default = variable)
  — SDU Size (required if fixed, forbidden if variable SDU)
  — Convergence Sublayer Specific Parameters (see 12.1.1.5 and 12.1.1.6)
  — Vendor-Specific QoS Parameters
— HMAC Tuple

12.1.1.4.20 DSA-RSP – BS Initiated Service Addition

— Uplink Service Parameters
  — Service Flow Error Parameter Set(s) (one per errored parameter)
      Errored Parameter
      Error Code
      Error Message (optional)
— Downlink Service Parameter(s)
  — Service Flow Error Parameter Set(s) (one per errored parameter)
      Errored Parameter
      Error Code
      Error Message (optional)
— HMAC Tuple

12.1.1.4.21 DSA-ACK

— HMAC Tuple

12.1.1.4.22 DSC-REQ – BS Initiated Service Change

— Uplink Service Parameters
  — Service Flow ID
  — Transport CID
  — QoS Parameter Set Type
  — Maximum Sustained Traffic Rate
  — Minimum Reserved Traffic Rate (default = 0 for BE, Max Sust Rate for UGS, required for rtPS and nrtPS)
  — Maximum Traffic Burst (required for rtPS and nrtPS, excluded otherwise)
  — Traffic Priority (optional, BE only)
  — Tolerated Jitter (optional)
  — Maximum Latency (optional)
  — Convergence Sublayer Specific Parameters (see 12.1.1.5 and 12.1.1.6)
  — Vendor-Specific QoS Parameters
— Downlink Service Parameters
  — Service Flow ID
  — Transport CID
  — QoS Parameter Set Type
  — Convergence Sublayer Specific Parameters (see 12.1.1.5 and 12.1.1.6)
  — Vendor-Specific QoS Parameters
— HMAC Tuple

12.1.1.4.23 DSC-RSP – BS Initiated Service Change

— Uplink Service Parameters
  — Service Flow Error Parameter Set(s) (one per errored parameter)
    Errored Parameter
    Error Code
    Error Message (optional)
— Downlink Service Parameter(s)
  — Service Flow Error Parameter Set(s) (one per errored parameter)
    Errored Parameter
    Error Code
    Error Message (optional)
— HMAC Tuple

12.1.1.4.24 DSC-ACK

— HMAC Tuple

12.1.1.4.25 DSD-REQ

— HMAC Tuple

12.1.1.4.26 DSD-RSP

— HMAC Tuple

12.1.1.4.27 MCA-REQ

— Multicast CID
— Assignment

12.1.1.4.28 MCA-RSP

Message contains no TLV encoded information

12.1.1.4.29 DBPC-REQ

Message contains no TLV encoded information

12.1.1.4.30 DBPC-RSP

Message contains no TLV encoded information

12.1.1.4.31 RES-CMD

— HMAC Tuple

12.1.1.4.32 SBC-REQ

— 10-66 GHz PHY SS Demod Support
— 10-66 GHz PHY SS Modulator Support
— 10-66 GHz PHY SS DL FEC Types
— 10-66 GHz PHY SS UL FEC Types
— BW Allocation Support

12.1.1.4.33 SBC-RSP

— 10-66 GHz PHY SS Demod Support
— 10-66 GHz PHY SS Modulator Support
— 10-66 GHz PHY SS DL FEC Types
— 10-66 GHz PHY SS UL FEC Types

12.1.1.4.34 CLK-CMP

The message contains no TLV encoded information.

12.1.1.4.35 DREG-CMD

— HMAC Tuple

12.1.1.4.36 DSX-RVD

The message contains no TLV encoded information.

12.1.1.4.37 TFTP-CPLT

— HMAC Tuple

12.1.1.4.38 TFTP-RSP

The message contains no TLV encoded information.

12.1.1.5 Message parameters specific to profM1

The following subclauses define the order in which systems meeting profile profM1 shall transmit the TLV encoded parameters specific to the ATM Convergence Sublayer. Parameters with defined default values should be omitted if the desired value coincides with the default one.

12.1.1.5.1 ATM CS Parameters for DSA-REQ – BS Initiated

— ATM Switching
— ATM Classifier Rule(s) (default = don't classify)
  — ATM Classifier ID
  — VPI Classifier
  — VCI Classifier(s) (must follow associated VPI, default = don't classify on VCI)

12.1.1.5.2 ATM CS Parameters for DSA-RSP – BS Initiated

— None

12.1.1.5.3 ATM CS Parameters for DSC-REQ – BS Initiated

— ATM Classifier Change Action
— ATM Classifier Rule(s) (default = don't classify)
  — ATM Classifier ID
  — VPI Classifier
  — VCI Classifier(s) (must follow associated VPI, default = don't classify on VCI)

12.1.1.5.4 ATM CS Parameters for DSC-RSP – BS Initiated

— None

12.1.1.6 Message parameters specific to profM2

12.1.1.6.1 Packet CS Parameters for DSA-REQ – BS Initiated

— Packet Classification Rule(s) (uplink service flows only, default is no classification)
  — Classifier Rule ID
  — Classifier Rule Priority (default to 0)
  — IP Type of Service/DSCP (only for IP CSs, default = don't classify on this)
  — Protocol (only for IP CSs, default = don't classify on this)
  — IP Masked Source Address (only for IP CSs, default = don't classify on this)
  — IP Destination Address (only for IP CSs, default = don't classify on this)
  — Protocol Source Port Range (only for IP CSs, default = don't classify on this)
  — Protocol Destination Port Range (only for IP CSs, default = don't classify on this)
  — Ethernet Destination MAC Address (only for Ethernet CSs, default = don't classify on this)
  — Ethernet Source MAC Address (only for Ethernet CSs, default = don't classify on this)
  — Ethertype/IEEE 802.2 SAP (only for Ethernet CSs, default = don't classify on this)
  — IEEE 802.1D User Priority (only for VLAN CSs, default = don't classify on this)
  — IEEE 802.1Q VLAN_ID (only for VLAN CSs, default = don't classify on this)
  — Associated Payload Header Suppression Index (default is no PHS for this classifier match)
  — Vendor-Specific Classifier Parameters
— Payload Header Suppression Rule(s)
  — Payload Header Suppression Index
  — Payload Header Suppression Size
  — Payload Header Suppression Field
  — Payload Header Suppression Mask (default is suppress all bytes of the suppression field)
  — Payload Header Suppression Verification (default is verify)
  — Vendor-Specific PHS Parameters

12.1.1.6.2 Packet CS Parameters for DSA-RSP – BS Initiated

— Packet Classification Rule(s) (uplink service flows only, default is no classification)
  — Classifier Error Parameter Set(s) (one per errored parameter)
    Classifier Rule ID
    Errored Parameter
    Error Code
    Error Message (optional)
— Payload Header Suppression Rule(s)
  — PHS Error Parameter Set(s) (one per errored parameter)
  — Payload Header Suppression Index
    Errored Parameter
    Error Code
    Error Message (optional)

12.1.1.6.3 Packet CS Parameters for DSC-REQ – BS Initiated

— Classifier Dynamic Service Change Action(s)
— Packet Classification Rule(s) (uplink service flows only, 1 per Action)
  — Classifier Rule ID
  — Classifier Rule Priority (default to 0)
  — IP Type of Service/DSCP (only for IP CSs, default = don't classify on this)

  — Protocol (only for IP CSs, default = don't classify on this)
  — IP Masked Source Address (only for IP CSs, default = don't classify on this)
  — IP Destination Address (only for IP CSs, default = don't classify on this)
  — Protocol Source Port Range (only for IP CSs, default = don't classify on this)
  — Protocol Destination Port Range (only for IP CSs, default = don't classify on this)
  — Ethernet Destination MAC Address (only for Ethernet CSs, default = don't classify on this)
  — Ethernet Source MAC Address (only for Ethernet CSs, default = don't classify on this)
  — Ethertype/IEEE 802.2 SAP (only for Ethernet CSs, default = don't classify on this)
  — IEEE 802.1D User Priority (only for VLAN CSs, default = don't classify on this)
  — IEEE 802.1Q VLAN_ID (only for VLAN CSs, default = don't classify on this)
  — Associated Payload Header Suppression Index (default is no PHS for this classifier match)
  — Vendor-Specific Classifier Parameters
— PHS Dynamic Service Change Action
— Payload Header Suppression Rule(s) (1 per Action)
  — Payload Header Suppression Index
  — Payload Header Suppression Size
  — Payload Header Suppression Field
  — Payload Header Suppression Mask (default is suppress all bytes of the suppression field)
  — Payload Header Suppression Verification (default is verify)
  — Vendor-Specific PHS Parameters

12.1.1.6.4 Packet CS Parameters for DSC-RSP – BS Initiated

— Uplink Service Parameters
  — Service Flow Error Parameter Set(s) (one per errored parameter)
      Errored Parameter
      Error Code
      Error Message (optional)
— Downlink Service Parameter(s)
  — Service Flow Error Parameter Set(s) (one per errored parameter)
      Errored Parameter
      Error Code
      Error Message (optional)

12.1.2 WirelessMAN-SC Physical Layer Profiles

This subclause defines PHY profiles for systems operating with the WirelessMAN-SC PHY.

12.1.2.1 WirelessMAN-SC 25 MHz Channel PHY Profile

Profile identifier: profP1.

Mandatory features:

— Frame Duration of 1 ms
— QPSK and QAM-16 in the DL
— QPSK in the UL
— Roll-off Factor = 0.25
— RS outer codes with $t \in \{0, 4, 8, 10, 12\}$.
— Fixed and shortened last code word operation.
— RS block lengths of 6–255.
— 20 Mbaud symbol rate
— 5000 PS per frame

SSs implementing profP1 shall meet the minimum SS performance requirements listed in Table 147:

Table 147—SS Minimum Performance requirements for profP1

Capability	Minimum Performance
Tx Dynamic range	>= 40 dB
Rx Dynamic Range	>= 40 dB for QPSK
Tx RMS Power Level at Maximum Power Level Setting for QPSK	>= 15 dBm
Tx Power Level minimum adjustment step	0.5 dB
Tx Power level adjustment step accuracy 0.5dB <= Step size < 2dB	monotonic
Tx Power level adjustment step accuracy 2dB <= Step size < 5dB	+/– 2 dB
Tx Power level adjustment step accuracy Step size >= 5 dB	+/– 3 dB
Peak-to-peak symbol jitter, referenced to the previous symbol zero crossing of the transmitted waveform, as percentage of the nominal symbol duration when measured over a 2 second period	2%
Tx burst timing step size	+/– 0.25 of a symbol
Tx burst timing step accuracy	+/– 0.125 of a symbol
Spectral mask (OOB)	Local regulation
Ramp up/ramp down time	<= 24 symbols
Output noise power spectral density when Tx is not transmitting	<= –80 dBm/MHz
Modulation accuracy when measured with an ideal receiver without an equalizer for QPSK	12%
Modulation accuracy when measured with an ideal receiver without an equalizer for 16-QAM	6%
Modulation accuracy when measured with an ideal receiver with an equalizer for QPSK	10%
Modulation accuracy when measured with an ideal receiver with an equalizer for 16-QAM	3%
Modulation accuracy when measured with an ideal receiver with an equalizer for 64-QAM	1.5%
BER performance threshold for QPSK, BER=10^{-3}	–94 + 10log(25) dBm
BER performance threshold for 16-QAM, BER=10^{-3}	–87 + 10log(25) dBm

Table 147—SS Minimum Performance requirements for profP1 *(continued)*

Capability	Minimum Performance
BER performance threshold for 64-QAM, BER=10^{-3}	–79 + 10log(25) dBm
BER performance threshold for QPSK, BER=10^{-6}	–90 + 10log(25) dBm
BER performance threshold for 16-QAM, BER=10^{-6}	–83 + 10log(25) dBm
BER performance threshold for 64-QAM, BER=10^{-6}	–74 + 10log(25) dBm
Transition time from Tx to Rx and from Rx to Tx	TDD: 2 us H-FDD: 20 us FDD: n/a
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–9 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–2 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	+5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–1 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	+6 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	+13 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–34 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–27 dB

Table 147—SS Minimum Performance requirements for profP1 *(continued)*

Capability	Minimum Performance
2^{nd} adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	–20 dB
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–30 dB
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	–22 dB
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	–16 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–30 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	–23 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	–16 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–26 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	–20 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	–12 dB
Tx Power Level absolute accuracy	+/– 6 dB

BSs implementing profP1 shall meet the minimum transmitter performance requirements listed in Table 148. The receiver shall meet the minimum performance requirements in Table 149.

Table 148—BS Tx minimum performance requirements for profP1

Capability	Minimum Performance
Peak-to-peak symbol jitter, referenced to the previous symbol zero crossing of the transmitted waveform, as percentage of the nominal symbol duration when measured over a 2 second period	2%
Tx RF frequency	10-66 GHz
Tx RF frequency accuracy	+/– 10 ppm
Spectral mask (OOB)	local regulation
Spurious	local regulation
Ramp up/ramp down time	<= 24 symbols
Modulation accuracy when measured with an ideal receiver without an equalizer for QPSK	12%
Modulation accuracy when measured with an ideal receiver without an equalizer for 16-QAM	6%
Modulation accuracy when measured with an ideal receiver with an equalizer for QPSK	10%
Modulation accuracy when measured with an ideal receiver with an equalizer for 16-QAM	3%
Modulation accuracy when measured with an ideal receiver with an equalizer for 64-QAM	1.5%

Table 149—BS Rx minimum performance for profP1

Capability	Minimum performance
Dynamic Range	27 dB for QPSK
BER performance threshold for QPSK, BER=10^{-3}	–94 + 10log(25) dBm
BER performance threshold for 16-QAM, BER=10^{-3}	–87 + 10log(25) dBm
BER performance threshold for 64-QAM, BER=10^{-3}	–79 + 10log(25) dBm
BER performance threshold for QPSK, BER=10^{-6}	–90 + 10log(25) dBm
BER performance threshold for 16-QAM, BER=10^{-6}	–83 + 10log(25) dBm
BER performance threshold for 64-QAM, BER=10^{-6}	–74 + 10log(25) dBm
1^{st} adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–9 dB
1^{st} adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–2 dB
1^{st} adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	+5 dB

Table 149—BS Rx minimum performance for profP1 ***(continued)***

Capability	Minimum performance
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–1 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	+6 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	+13 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–34 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–27 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	–20 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–30 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	–22 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	–16 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–30 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	–23 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	–16 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–26 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	–20 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	–12 dB

12.1.2.1.1 FDD Specific WirelessMAN-SC 25 MHz Channel PHY Profile Features

Profile identifier: profP1f.

Mandatory features:

— FDD operation
— BS must respect half-duplex nature of half-duplex SSs

12.1.2.1.2 TDD Specific WirelessMAN-SC 25 MHz Channel PHY Profile Features

Profile identifier: profP1t.

Mandatory features:

— TDD operation

12.1.2.2 WirelessMAN-SC 28 MHz Channel PHY Profile

Profile identifier: profP2.

Mandatory features:

— Frame Duration of 1 ms
— QPSK and QAM-16 in the DL
— QPSK in the UL
— Roll-off Factor = 0.25
— RS outer codes with $t \in \{0, 4, 8, 10, 12\}$.
— Fixed and shortened last code word operation
— RS block lengths of 6–255
— 22.4 Mbaud symbol rate
— 5600 PS per frame

SSs implementing profP2 shall meet the minimum SS performance requirements as listed in Table 150.

Table 150—SS Minimum performance for profP2

Capability	Minimum Performance
Tx Dynamic range	>= 40 dB
Rx Dynamic Range	>= 40 dB for QPSK
Tx RMS Power Level at Maximum Power Level Setting for QPSK	>= 15 dBm
Tx Power Level minimum adjustment step	0.5 dB
Tx Power level adjustment step accuracy Step size [0.5, 2) dB	monotonic
Tx Power level adjustment step accuracy Step size [2, 5) dB	+/– 2 dB
Tx Power level adjustment step accuracy Step size >= 5 dB	+/– 3 dB
Peak-to-peak symbol jitter, referenced to the previous symbol zero crossing of the transmitted waveform, as percentage of the nominal symbol duration when measured over a 2 second period	2%
Tx burst timing step size	+/– 0.25 of a symbol
Tx burst timing step accuracy	+/– 0.125 of a symbol
Spectral mask (OOB)	Local regulation
Ramp up/ramp down time	<= 24 symbols
Output noise power spectral density when Tx is not transmitting	<= –80 dBm/MHz
Modulation accuracy when measured with an ideal receiver without an equalizer for QPSK	12%
Modulation accuracy when measured with an ideal receiver without an equalizer for 16-QAM	6%
Modulation accuracy when measured with an ideal receiver with an equalizer for QPSK	10%
Modulation accuracy when measured with an ideal receiver with an equalizer for 16-QAM	3%
Modulation accuracy when measured with an ideal receiver with an equalizer for 64-QAM	1.5%
BER performance threshold for QPSK, BER=10^{-3}	–94 + 10log(28) dBm
BER performance threshold for 16-QAM, BER=10^{-3}	–87 + 10log(28) dBm
BER performance threshold for 64-QAM, BER=10^{-3}	–79 + 10log(28) dBm
BER performance threshold for QPSK, BER=10^{-6}	–90 + 10log(28) dBm
BER performance threshold for 16-QAM, BER=10^{-6}	–83 + 10log(28) dBm

Table 150—SS Minimum performance for profP2 *(continued)*

Capability	Minimum Performance
BER performance threshold for 64-QAM, BER=10^{-6}	–74 + 10log(28) dBm
Transition time from Tx to Rx and from Rx to Tx	TDD: 2 us H-FDD: 20 us FDD: n/a
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–9 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–2 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	+5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–1 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	+6 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	+13 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–34 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–27 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	–20 dB

Table 150—SS Minimum performance for profP2 *(continued)*

Capability	Minimum Performance
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–30 dB
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	–22 dB
2^{nd} adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	–16 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–30 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	–23 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	–16 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–26 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	–20 dB
2^{nd} adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	–12 dB
Tx Power Level absolute accuracy	+/– 6 dB

BSs implementing profP2 shall meet the minimum transmitter performance requirements listed in Table 151. The receiver shall meet the minimum performance requirements in Table 152.

Table 151—BS Tx minimum performance for profP2

Capability	Minimum Performance
Peak-to-peak symbol jitter, referenced to the previous symbol zero crossing of the transmitted waveform, as percentage of the nominal symbol duration when measured over a 2 second period	2%
Tx RF frequency	10–66 GHz
Tx RF frequency accuracy	+/– 10 ppm
Spectral mask (OOB)	local regulation
Spurious	local regulation
Ramp up/ramp down time	<= 24 symbols
Modulation accuracy when measured with an ideal receiver without an equalizer for QPSK	12%
Modulation accuracy when measured with an ideal receiver without an equalizer for 16-QAM	6%
Modulation accuracy when measured with an ideal receiver with an equalizer for QPSK	10%
Modulation accuracy when measured with an ideal receiver with an equalizer for 16-QAM	3%
Modulation accuracy when measured with an ideal receiver with an equalizer for 64-QAM	1.5%

Table 152—BS Rx minimum performance for profP2

Capability	Minimum Performance
Dynamic Range	27 dB for QPSK
BER performance threshold for QPSK, BER=10^{-3}	–94 + 10log(28) dBm
BER performance threshold for 16-QAM, BER=10^{-3}	–87 + 10log(28) dBm
BER performance threshold for 64-QAM, BER=10^{-3}	–79 + 10log(28) dBm
BER performance threshold for QPSK, BER=10^{-6}	–90 + 10log(28) dBm
BER performance threshold for 16-QAM, BER=10^{-6}	–83 + 10log(28) dBm
BER performance threshold for 64-QAM, BER=10^{-6}	–74 + 10log(28) dBm
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–9 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–2 dB
1st adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	+5 dB

Table 152—BS Rx minimum performance for profP2 *(continued)*

Capability	Minimum Performance
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–5 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	+2 dB
1st adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	+9 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–1 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	+6 dB
1st adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	+13 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for QPSK	–34 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 16-QAM	–27 dB
2nd adjacent channel interference at BER=10^{-3} for 3 dB degradation C/I for 64-QAM	–20 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for QPSK	–30 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 16-QAM	–22 dB
2nd adjacent channel interference at BER=10^{-3} for 1 dB degradation C/I for 64-QAM	–16 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for QPSK	–30 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 16-QAM	–23 dB
2nd adjacent channel interference at BER=10^{-6} for 3 dB degradation C/I for 64-QAM	–16 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for QPSK	–26 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 16-QAM	–20 dB
2nd adjacent channel interference at BER=10^{-6} for 1 dB degradation C/I for 64-QAM	–12 dB

12.1.2.2.1 FDD Specific WirelessMAN-SC 28 MHz Channel PHY Profile Features

Profile identifier: profP2f.

Mandatory features:

— FDD operation
— BS must respect half-duplex nature of half-duplex SSs

12.1.2.2.2 TDD Specific WirelessMAN-SC 28 MHz Channel PHY Profile Features

Profile identifier: profP2t.

Mandatory features:

— TDD operation

12.1.2.3 Conventions for MAC Management Messages for profiles profP1 and profP2

The following rules shall be followed when reporting parameters in MAC Management messages for systems operating PHY profiles profP1 or profP2:

— Symbol Rate, Frequency, and Roll-off Factor shall not be reported in UCD messages.
— BCC Code Type shall not be reported in UCD messages.
— Frame Duration shall not be reported in DCD messages.
— BCC Code Type shall not be reported in DCD messages.
— UL Channel Override shall not be reported in RNG-RSP messages.

12.1.2.4 UCD and DCD parameter transmission order for profP1 and profP2

The following subclauses define the order in which systems meeting profiles profP1 and profP2 shall transmit the TLV encoded parameters in the respective messages. Systems implementing either profile shall only include the parameters listed under the respective message in its transmission of said messages. Parameters with defined default values should be omitted if the desired value coincides with the default one.

12.1.2.4.1 DCD

— BS Transmit Power
— PHY Type
— Power Adj Rule
— Downlink Burst Profile(s)
— Modulation Type
— FEC Code Type (default to RS only if omitted)
— RS Information Bytes
— RS parity bytes
— Last Codeword Length (default to shortened if omitted)
— Exit Threshold
— Entry Threshold
— Preamble Present (default to ‘not present’ if omitted)

12.1.2.4.2 UCD:

— SS Transition Gap (default to 24 symbols if omitted)
— Power Adjustment Rule
— Contention-based Reservation Timeout
— Uplink Burst Profile(s)
  — Modulation Type
  — Preamble Length
  — FEC Code Type (default to RS only)
  — RS Information Bytes
  — RS Parity Bytes
  — Scrambler Seed
  — Last Codeword Length (default to shortened)

12.1.2.5 Initial Maintenance IE usage for profP1 and profP2

BSs implementing profP1 or profP2 shall include exactly one Initial Maintenance IE in the UL-MAP for each intended opportunity for an SS to perform Initial Ranging.