Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Editorial instructions pertaining to comments submitted in P802.16c/D3 ballot**	
Date Submitted	**2002-09-11**	
Source(s)	Carl Eklund Nokia P.O. Box 407 FIN-00045 Nokia Group	Voice: +358718036566 Fax: +358718036851 mailto:carl.eklund@nokia.com
Re:	P802.16c/D3 Sponsor Ballot	
Abstract	This document contains the suggested editorial instuctions.	
Purpose	Comment resolution	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.	

Comment I

Change section 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 which 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 11). ~~shown in Table 1~~.

Table 1~~—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 1:

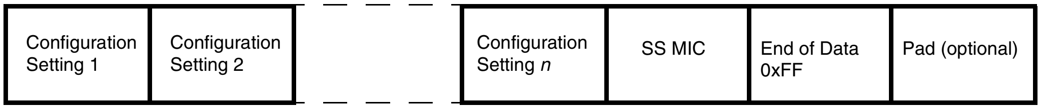


Figure 1—Configuration file structure

Delete section 11.3.1 and 11.3.2

Comment II

Change section 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 11.3.3)

~~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 11.3.6)

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

f) Vendor-Specific Configuration Settings

Delete sections 11.3.4 and 11.3.5

Comment III

Replace section 9.2.3 with:

9.2.3 Configuration file creation

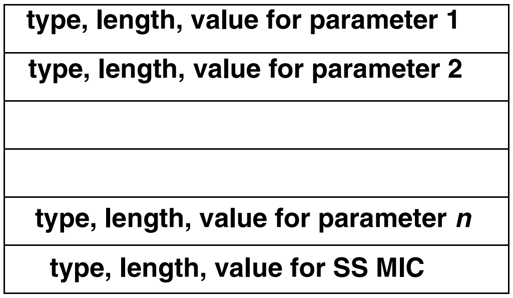
The sequence of operations required to create the configuration file is as shown in Figure 131, Figure 132, and Figure 133.

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

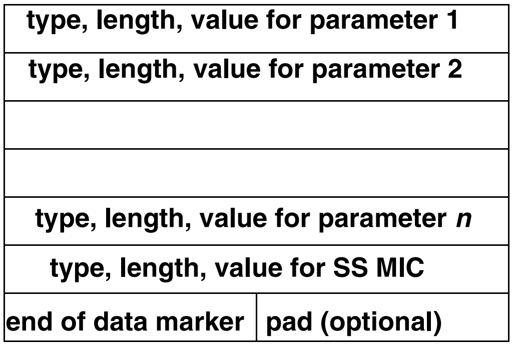
type, length, value for parameter 2

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

Comment IV

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 the SS is authorized to access.

The Auth Reply may also contain PKM configuration settings overriding 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.

In 7.2.4.3 change:

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)~~.

In 7.2.4.4 change the first paragraph to:

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)~~.

In 7.2.5.4 change the first paragraph to:

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).

Comment V

6.2.2.3 MAC Management Messages

Change 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 parmeters or contain errenously encoded parameters shall be silently discarded

11. TLV encodings

Change first paragraph of section to read:

The following type/length/value (TLV) encoding~~s~~ shall be used for parameters in both the configuration file (Clause 9) and MAC Management messages (6.2.2.3).

Delete last paragraph of section:

~~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.~~

Comment VI

Change first sentence of 11.4.9.3 to:

11.4.9.3 Packet CS encodings for configuration and MAC-layer messaging

The following TLV encoded~~ings~~ parameteres shall be used~~ in both the configuration file, in SS registration requests and~~ in Dynamic Service Messages

Comment VII

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.

Comment VIII

12.1.2.5.1 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

12.1.2.5.2 REG-RSP

- MAC Version
- Secondary Management CID
- SS Capabilities Encoding (compound)
  - UL CID Support
  - Vendor ID Encoding (if present in REG-REQ or changed from default)
  - 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

Comment IX

Change section 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

Comment X

Change last paragraph of 6.2.2.3.8 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)

Comment XI

Replace figures 50a and 50b with figures below

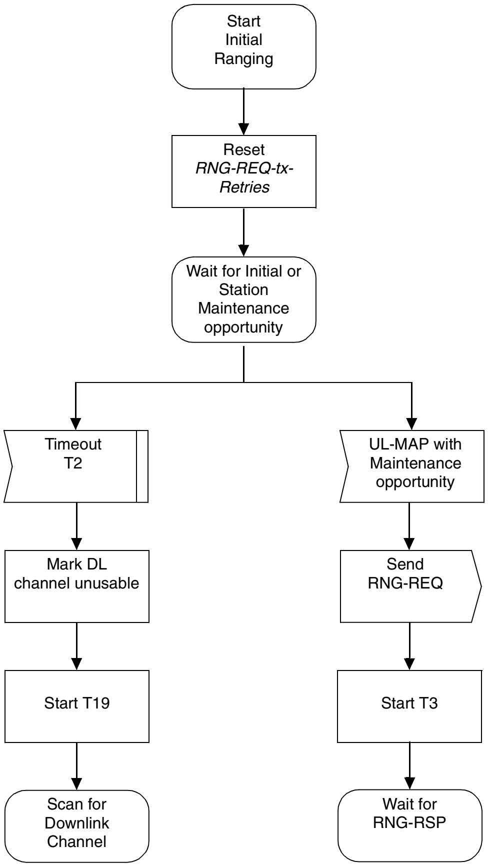
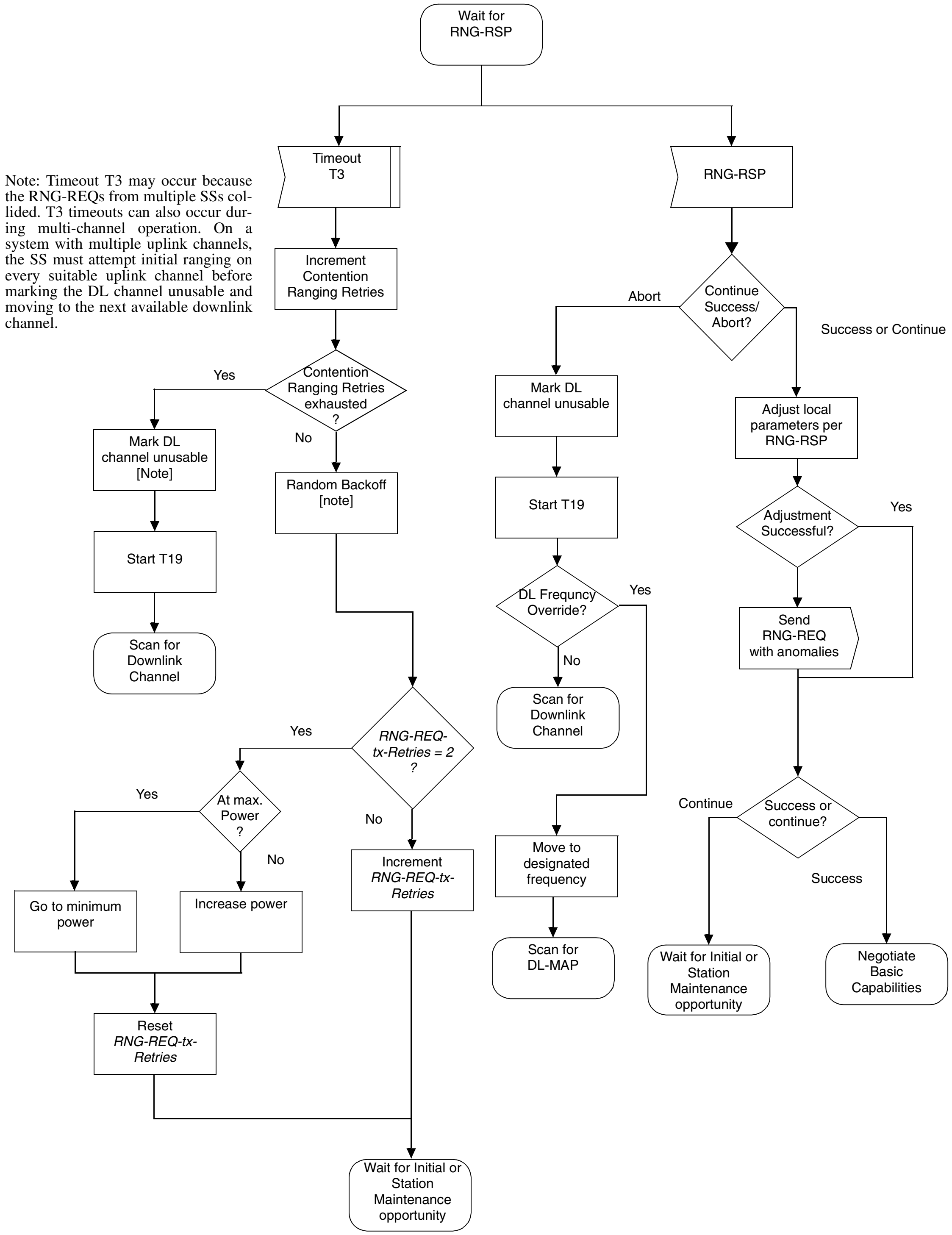


Figure 50a—Initial Ranging – SS (part 1)


Wait for RNG-RSP
Timeout T3
RNG-RSP
Increment Contention Ranging Retries
Continue Success/ Abort?
Abort
Success or Continue
Contention Ranging Retries exhausted ?
Yes
No
Mark DL channel unusable [Note]
Random Backoff [note]
Start T19
Scan for Downlink Channel
Mark DL channel unusable
Start T19
DL Frequncy Override?
Yes
No
Scan for Downlink Channel
Move to designated frequency
Scan for DL-MAP
Adjust local parameters per RNG-RSP
Adjustment Successful?
Yes
Send RNG-REQ with anomalies
Success or continue?
Continue
Success
Wait for Initial or Station Maintenance opportunity
Negotiate Basic Capabilities
RNG-REQ-tx-Retries = 2 ?
Yes
No
At max. Power ?
Yes
No
Go to minimum power
Increase power
Increment RNG-REQ-tx-Retries
Reset RNG-REQ-tx-Retries
Wait for Initial or Station Maintenance opportunity

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)

Change paragraph 6 of 6.2.9.5 to read:

~~The SS shall first send the RNG-REQ at minimum power level, and if it is not successful, the SS shall resend it at the next Initial Maintenance transmission opportunity at one step higher power level until successful.~~ The SS shall send the first send the RNG-REQ at minimum power level. If the SS has not received a RNG-RSP after two retries at the same power level the SS shall increase its transmission power and try again.

Comment XII

Replace figure 46 with the figure below.

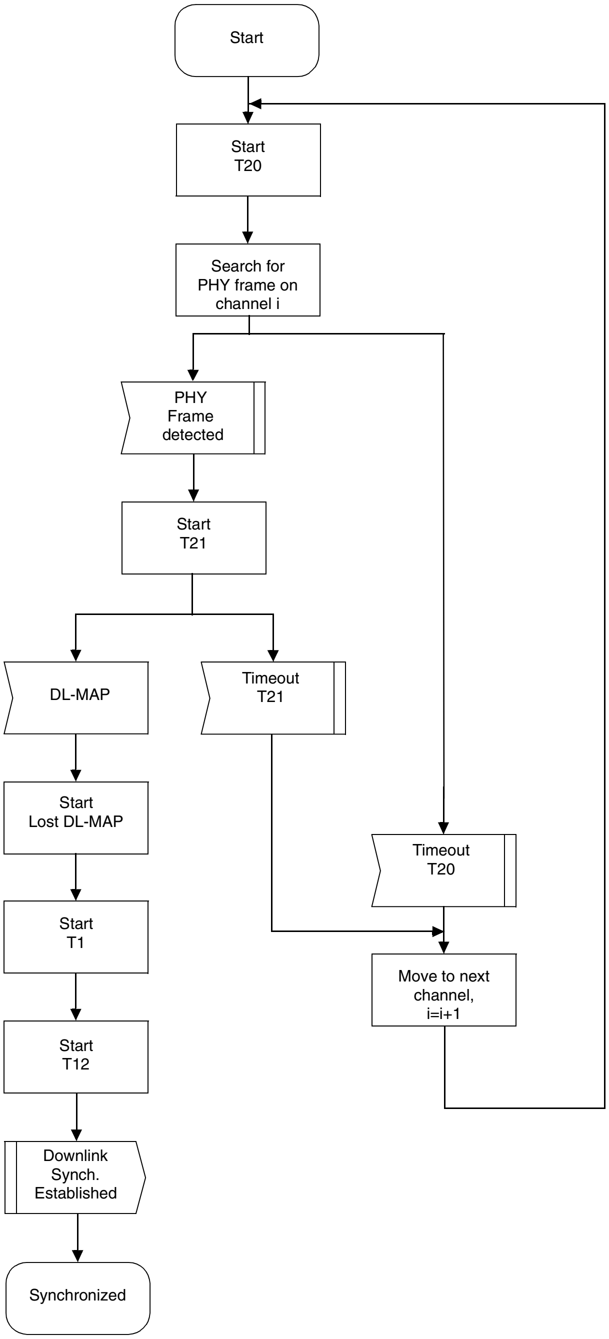


Figure 46—Obtaining downlink synchronization