Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Management Issues**
Date Submitted	**2001-01-15**
Source(s)	Ken Stanwood, Stanley Wang, Robert Johnson Ensemble Communications 9890 Towne Centre Drive San Diego, CA 92121 Voice: (858) 404-6559 Fax: (858) 458-1401 mailto:ken@ensemblecom.com mailto:stanley@ensemblecom.com mailto:robert@ensemblecom.com
Re:	IEEE 802.16.1-01/02: Call for Comments on IEEE 802.16.1D1-2000
Abstract	This document addresses comments that were deferred to group in session 10 and not resolved before the release of the current draft of the air interface spec.
Purpose	This document is the supporting text for separately submitted comments to address issues that were deferred to the MAC management task group at session 10.
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 text 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Management Issues

Ken Stanwood, Dr. Stanley Wang, Robert Johnson
Ensemble Communications

This document suggests resolution of some of the MAC management issues that were deferred to the group at session 10.

1. Basic Capability Negotiation

Explanation

Currently the SS physical layer capabilities are reported to the BS in the REG-REQ message. This message, unfortunately, is preceded by the establishment of IP connectivity, establishment of time of day, and the transfer via TFTP of the configuration file. This is shown in Figure 58 on page 108 of the air interface specification. Unfortunately, until the REG-REQ message the BS is not aware of the SSs capabilities at the physical layer. This effectively requires that the BS communicate with the SS using the control channel FEC. This is a very inefficient use of bandwidth.

Additionally, the BS does not know whether the SS is GPC or GPT. Since some of the interaction to this point should happen on the SSs basic connection and some should happen on its secondary management connection, this unduly complicates the initialization process.

An SS Basic Capabilities Request (SBC-REQ) and Response (SBC-RSP) should be added in the initialization sequence between ranging and the establishment of IP connectivity. The SBC-REQ should be from the SS to the BS and should contain the following TLVs that are currently in the REG-REQ messages. The SBC-RSP would return those that the SS is allowed to use as is currently being done by the REG-RSP message. Only those relevant to the particular PHY or SS should be included.

- 5.12.1 Physical Layer Type (it is actually recommended that this TLV be eliminated since it serves no purpose)
- 5.12.2 10-66 GHz PHY SS Demodulator Types
- 5.12.3 10-66 GHz PHY SS Modulator Types
- 5.12.4 10-66 GHz PHY Mode A SS Downstream FEC Types
- 5.12.5 10-66 GHz PHY Mode B SS Downstream FEC Types
- 5.12.6 10-66 GHz PHY SS Upstream FEC Types
- 5.14 Duplexing Support (it is actually recommended that this TLV be eliminated since it serves no purpose)
- 5.15 Bandwidth Allocation Support

These TLVs would then be removed from the REG-REQ and REG-RSP messages.

Specific Changes to Air Interface Specification

The following specific changes should be made to the air interface specification:

1. On page 43, line 25, add two rows to Table 2 for the following 2 new MAC management messages:

26	SBC-REQ	SS Basic Capability Request
27	SBC-RSP	SS Basic Capability Response

2. On page 43, line 26 change the reserved message types to 28-255.

3. On page 59, line 21 add the following parenthetical remark at the end of the line:

"(excluding Physical Parameters Supported and Bandwidth Allocation Support)"

4. On page 88, line 23 add the following sections:

6.2.1.2.x SBC-REQ Message
The SS Basic Capability Request shall be transmitted by the SS during initialization. An SS shall generate SBC-REQ messages in the form shown in Figure x.

<<Insert figure here identical to Figure 22 on page 58 for REG-REQ except message type field = 26.>>

An SS shall generate SS Basic Capability Requests including the following parameter:

Basic CID (in the MAC Header)
The CID in the MAC Header is the Basic CID for this SS, as assigned in the RNG-RSP message.

All other parameters are coded as TLV tuples.

Basic Capability Requests contain those SS Capabilities Encodings that are necessary for effective communication with the SS during the remainder of the initialization protocols. The following parameters are included in the Basic Capabilities Request:

Physical Parameters Supported (see 11.4.5.3)
Bandwidth Allocation Support (see 11.4.5.4.1)

6.2.1.2.x SBC-RSP Message
The SS Basic Capability Response shall be transmitted by the BS in response to a received SBC-REQ.

To provide flexibility, the message parameters following the Response field shall be encoded in a TLV format.

<<Insert figure here identical to Figure 23 on page 60 for REG-RSP except message type field = 27.>>

A BS shall generate SS Basic Capability Responses in the form shown in Figure x, including both of the following parameters:

CID (in the MAC Header)
CID from corresponding SBC-REQ to which this response refers (this acts as a transaction identifier)

Response
A one-byte quantity with one of the following values:
0 = Okay

The following parameters shall be included in the registration response if found in the SS Basic Capability Request:

SS Capabilities (see 11.4.5)
The BS response to the subset of SS capabilities present in the SBC-REQ message. The BS responds to the SS capabilities to indicate whether they may be used. If the BS does not recognize an SS capability, it must return this as "off" in the SBC-RSP.

Only capabilities set to "on" in the SBC-REQ may be set "on" in the REG-RSP as this is the handshake indicating that they have been successfully negotiated.

5. On page 107, line 49 insert the following line between items c and d, renumbering the rest of the list:

d) Negotiate basic capabilities

6. On page 108, line 29 add the negotiation of basic capabilities to Figure 58 between Ranging and Establishment of IP connectivity.

7. On page 117, line 1 add the following section before the current section 6.2.3.8 (renumbering the following sections):

6.2.3.8 Negotiate Basic Capabilities
Immediately after completion of ranging, the SS informs the BS of its basic capabilities by transmitting an SBC-REQ message with its capabilities set to "on". The BS responds with an SBC-RSP message with the intersection of the SS's and the BS's capabilities set to "on".

8. On page 313, line 28 through page 316, line 15 change the scope of the TLVs to be SBC-REQ and SBC-RSP.

2. Basic and Secondary Management Connection Usage

Explanation

1. The current air interface specification does not clarify what information is sent on basic connections and what information is sent on secondary management connections. The purpose of the secondary management connection is to allow management information that may be comprised of large, delay insensitive data to be reliably transmitted without blocking or impacting the QoS of real-time management and high QoS user data connections. To this end, the 802.16 specific MAC management messages defined in Table 2 on page 42 of the air interface specification should be transmitted only on basic connections (including the initial ranging and broadcast connections). Management that uses previously defined standards such as DHCP, TFTP, SNMP, and IP should be transmitted on the secondary management connection. The secondary management connection should use the Ethernet convergence sublayer.

2. There are actions that are performed on the basic connections that can have multiple instances outstanding simultaneously. It would be useful to have flow control to allow the BS or the SSs to limit the number of simultaneously outstanding instances in which they are involved. Those management message types that fall into this category are:

- PKM
- DSx
- MCA

Each of these message types should be added to the SS capability negotiation that is performed via the REG-REQ and REG-RSP messages.

3. The basic connections actually have two different classes of messages from a QoS point of view. There are short messages that require quick response such as an unsolicited RNG-RSP. There are larger messages that are not quite as real-time in nature. These larger, less delay sensitive messages should not block or delay either the more real-time MAC management messages or USG traffic. But they should not be lumped in with the IP type traffic of the secondary management connection either. Which messages fall in which class is shown in the following table:

Message	Message Class
UCD	Short, real-time
DCD	Short, real-time
DL-MAP	Short, real-time
UL-MAP	Short, real-time
RNG-REQ	Short, real-time

Message	Message Class
RNG-RSP	Short, real-time
REG-REQ	Longer, more delay tolerant
REG-RSP	Longer, more delay tolerant
REG-ACK	Longer, more delay tolerant
PKM-REQ	Longer, more delay tolerant
PKM-RSP	Longer, more delay tolerant
DSA-REQ	Longer, more delay tolerant
DSA-RSP	Longer, more delay tolerant
DSA-ACK	Longer, more delay tolerant
DSC-REQ	Longer, more delay tolerant
DSC-RSP	Longer, more delay tolerant
DSC-ACK	Longer, more delay tolerant
DSD-REQ	Longer, more delay tolerant
DSD-RSP	Longer, more delay tolerant
DCC-REQ	Longer, more delay tolerant
DCC-RSP	Longer, more delay tolerant
MCA-REQ	Short, real-time
MCA-RSP	Short, real-time
DBTC-REQ	Short, real-time
DBTC-RSP (not in document, but should be)	Short, real-time
ARQ-ACK	Short, real-time
SBC-REQ	Short, real-time
SBC-RSP	Short, real-time

The short, real-time messages should never be fragmented. The longer, more delay tolerant messages should be allowed to be fragmented, but with slightly different rules than those used on a data or secondary management connection. The reason for fragmenting these is simple. A 500+ byte PKM message should not delay the transmission of USG data, for instance. The fragmentation rules need to be slightly different, however, to address the fact that there really are 2 different QoS of information on the basic connections.

For user data and secondary management connections, there is only one SDU in a state of fragmentation at a time. A new SDU may not be transmitted until the previous one is fully transmitted. If the receiving side receives a FIRST fragment or an UNFRAGMENTED SDU before receiving the END fragment of a fragmented SDU, the assumption is that the END fragment was lost and the fragmented SDU is discarded.

For basic connections, there would also be only one MAC management message in a state of fragmentation at a time. But, one of the short real-time MAC management messages may be sent UNFRAGMENTED in the middle of the fragmented message, as if they were actually on different connections – one with fragmentation allowed, and one with fragmentation disabled. This works because the two classes of MAC management messages are for completely separate protocols. So, within a protocol exchange, all messages are delivered in order.

Specific Changes to Air Interface Specification

1. Insert a new section on page 35, line 59 by moving the text from page 286, line 51 through page 287, line 24:

6.2.1 Connections

Modify this moved text:
Page 286, line 60 change “registration” to “initial access”.
Page 286, line 61 change “registration” to “initial access”.
Page 286, line 62 add the following at the end of the paragraph: “The secondary management connection uses the Ethernet Convergence Sublayer.”

2. On page 90, line 10 add the following section:

6.2.1.4.2 Fragmentation on Basic Connections

Fragmentation is allowed on basic connections, but only certain MAC Control messages are allowed to be fragmented. The MAC control messages that may be fragmented are shown in Table x. All other MAC Control messages shall not be fragmented. From a fragmentation point of view, fragmentable MAC Control messages and unfragmentable MAC Control messages shall be treated as if they are on separate connections. An unfragmentable MAC Control message may be transmitted between the fragments of a fragmentable MAC Control message.

Table x: MAC Control Messages Allowed to be Fragmented

REG-REQ
REG-RSP
REG-ACK
PKM-REQ
PKM-RSP
DSA-REQ
DSA-RSP
DSA-ACK
DSC-REQ
DSC-RSP
DSC-ACK
DSD-REQ
DSD-RSP
DCC-REQ
DCC-RSP

4. On page 117, line 8 add: "Establishment of IP connectivity shall be performed on the SS's secondary management connection."

5. On page 117, line 47 add "Establishment of time of day shall be performed on the SS's secondary management connection.

6. On page 118, line 8 after "TFTP" add "on the SS's secondary management channel".

7. On page 316, line 16 add the following sections:

11.4.5.6 PKM Flow Control
This field specifies the maximum number of concurrent PKM transactions that may be outstanding.

Type	Length	Value	Scope
5.16	1	0 indicates no limit 1-255 indicate maximum concurrent transactions default = 0	REG-REQ REG-RSP

11.4.5.7 DSx Flow Control
This field specifies the maximum number of concurrent DSx transactions that may be outstanding.

Type	Length	Value	Scope
5.17	1	0 indicates no limit 1-255 indicate maximum concurrent transactions default = 0	REG-REQ REG-RSP

11.4.5.8 MCA Flow Control

This field specifies the maximum number of concurrent MCA transactions that may be outstanding.

Type	Length	Value	Scope
5.18	1	0 indicates no limit 1-255 indicate maximum concurrent transactions default = 0	REG-REQ REG-RSP

3. Connection Provisioning

Explanation

There are 3 scenarios where connections are established.

Provisioned connections at SS initialization
Dynamic connections
Provisioned connections added to an SS at some point after initialization

The last two scenarios require the use of the DSA-REQ/RSP/ACK protocol to set up connections in response to network management, signaling, or some other external stimulus.

The first scenario is currently specified to work in the following manner:

- The SS TFTPs a configuration file containing the parameters for its currently provisioned service flows.
- The SS sends the service flow information to the BS in the REG-REQ message.
- The BS responds with connection IDs in the REG-RSP message.

Not only is the use of the REG-REQ/RSP in this scenario inconsistent with the presence of the DSA protocol, there are issues regarding the timing of the setup and use of the connections. Figure 58 on page 108 shows that authentication and key exchange happen after registration. But the current protocol allows SSs to setup and start using connections before they are fully authenticated. To avoid this race condition and to eliminate redundant methods for achieving the same goal, the following sequence of events should be used to set up the connections for the service flows that are listed in the SS's configuration file.

- The SS TFTPs a configuration file containing the parameters for its currently provisioned service flows.
- The SS registers, but does not provide service flow parameters in the REG-REQ
- The SS is authenticated
- The SS uses a series of DSA-REQ/RSP protocols to set up the connections for the service flows that were in the configuration file.

Specific Changes to Air Interface Specification

1. On page 58, delete line 64.

2. On page 59, delete line 1.

3. On page 59, line 27 add:
   - Uplink Service Flow Configuration Settings
   - Downlink Service Flow Configuration Settings

4. On page 60, delete lines 41-43.

5. On page 60 delete line 49 through page 61, line 13.

6. On page 62 delete lines 10-26.

7. On page 108, line 38 add a step to Figure 58 called “Establish provisioned connections” between privacy and operational.

8. On page 118, line 26 delete the phrase “provisioned set of service flows and any other”.

9. On page 120, line 16, remove the phrase “Setup Service Flows &” from the rightmost box.

10. On page 120, line 51 delete step d).

11. On page 120, line 60 delete the phrase “If the Registration Request contains Service Flow encodings,”

12. On page 121, line 29-37 delete the 2 decision diamonds and their associated “No” actions.

13. On page 121, line 45-46 delete the “Create Requested Services” box.

14. On page 122, line 16-17 delete the “Destroy Services” box.

15. On page 122, line 33 add the section:

6.2.3.9.3 Service Flow Setup
After privacy is initialized, or after registration if privacy is disabled, the SS shall send DSA-REQ messages to the BS for to set up connections for the service flows listed in the configuration file. The BS shall respond with the DSA-RSP message.

16. On page 130, line 62 delete “Registration Response,”

17. On page 131, line 14 delete “REG-RSP”

18. On page 131, line 25 delete “REG-REQ”

19. On page 133, line 42 change “a Registration Request” to “multiple DSA-REQ messages”.

20. On page 133, line 43 change “Registration Response” to “DSA-RSP” and change “Registration Acknowledge” to “DSA-ACK”.

21. On page 134, line 1, replace the figure with a flowchart that better describes sending multiple DSA messages after registration.

22. On page 134, delete line 57 through page 135, line 59.