Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Clarification of optional features**
Date Submitted	**2004-03-11**
Source(s)	Vladimir Yanover Alvarion Ltd. 21 A Habarzel St. Ramat - Hahayal Tel - Aviv 69710 P.O. Box 13139, Tel-Aviv 61131, Israel Voice: +972-36457834 Fax: +972-36456222 mailto:vladimir.yanover@alvarion.com
Re:	The document was contributed within the process of 802.16REVd Sponsor Ballot comments
Abstract	The document is intended to clarify status of several capabilities of 802.16 compliant devices to help development of PICS document
Purpose	The document must be considered during 802.16REVd comments resolution procedure
Notice	
Release	
Patent Policy and Procedures	

Clarification of optional features

Vladimir Yanover (Alvarion Ltd.)

1. Goal

Certain functionalities are not explicitly defined in 802.16REVd as mandatory or optional. Some of them are negotiable between BS and SS, at the step of capability exchange or connection setup. It makes many of them actually optional for implementation. Seems reasonable to add explicit clarifications where relevant.

2. Specific Items

2.1. Fragmentation, Packing, Piggybacked Requests

2.1.1. Background

Consider packing at DL connection, set up by the request of BS. There is no way for SS to see whether fragmentation or packing will be applied at the connection. In some cases, TLV type = [145/146].12 may be used to indicate that packing will NOT be applied (see 11.13.14). But in absence of such (negative) indication, it is at the discretion of BS whether packing will be applied for each single SDU.

Fragmentation and piggybacked bandwidth requests functions are in the same position.

It seems messy to decide that SS with non-implemented packing function should reject any DSA-REQ with TLV [145/146].12 not preventing packing at the connection. Therefore, we have to add more clarifications:

- Specify explicitly whether implementation of fragmentation, packing is mandatory or optional
- Provide a mechanism to learn packing capabilities of another side

It is suggested to make implementation of fragmentation **mandatory,** as it is very important from the point of view of system performance. Implementation of packing (both fixed and variable size SDUs) and Piggybacking bandwidth requests is suggested to define as **optional**.

2.1.2. Specific Changes

[Change in 6.4.3.3]

6.4.3.3 Fragmentation

Fragmentation is the process by which a MAC SDU is divided into one or more MAC PDUs. This process is undertaken to allow efficient use of available bandwidth relative to the QoS requirements of a connection's service flow. Implementation of reassembly function is mandatory.

[Change in 6.4.3.4]

6.4.3.4 Packing

If packing is turned on for a connection, the MAC may pack multiple MAC SDUs into a single MAC PDU. Implementation of packing/unpacking capability is optional. Packing makes use of the connection attribute indicating whether the connection carries fixed-length or variable-length packets. The transmitting side has full discretion whether or not to pack a group of MAC SDUs in a single MAC PDU.

[Change in 6.4.6.1]

Requests refer to the mechanism that SSs use to indicate to the BS that they need uplink bandwidth allocation. A Request may come as a stand-alone bandwidth request header or it may come as a PiggyBack Request (see 6.4.2.2.2). Implementation of Piggyback Request function is optional.

[Change in 6.4.2.2.2]

6.4.2.2.2 Grant Management subheader

The Grant Management subheader is two bytes in length and is used by the SS to convey bandwidth management needs to the BS. This subheader is encoded differently based upon the type of uplink scheduling service for the connection (as given by the CID). The use of this subheader is defined in 6.4.6. The Grant Management subheader is shown in Table 9. Its fields are defined in Table 10. Implementation of Grant Management subheader at both BS and SS is optional.

[Add before 11.8.2 a new section]

11.8.2. Capabilities for Construction and Transmission of MAC PDUs

Type	Length	Value	Scope
4	1	Bit #0 - ability to unpack MAC PDUs that contain multiple packed SDUs (or fragments) Bit #1 - ability to receive requests piggybacked with data All other bit positions are reserved	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)

All other bit positions are reserved.

2.2. Capability of Payload Header Suppression

2.2.1. Background

Note the following from the Table 327 (Optional feature requirements profM3_PMP):

Optional Feature	Required?	Conditions/Notes
Payload header suppression	No	

Assignment of PHS to the connection might be rejected by DSA-RSP with non-zero CC (Confirmation Code). So capability associated with this feature is de-facto optional

2.2.2. Specific Changes

[Change in 802.16-REVd/D3]

5.2.4 PHS

In PHS, a repetitive portion of the payload headers of the higher layer is suppressed in the MAC SDU by the sending entity and restored by the receiving entity. Implementation of of PHS capability is optional. On the uplink, the sending entity is the SS and the receiving entity is the BS.

11.13.22.3.6.2 Error code

This parameter indicates the status of the request. A nonzero value corresponds to the CC as described in 11.13.1. A PHS Error Parameter Set shall have exactly one Error Code within a given PHS Encoding.

Type	Length	Value
[145/146]. cst.5.2	1	CC except OK(0) as specified in Table 309

3. Encryption Capabilities

3.1. Background

At the level of the standard, capabilities associated with Privacy sublayer (X.509 digital certificates and the RSA public key encryption algorithm for AK etc.) is defined as optional. To signal that, a new capability bit is introduced (the whole solution is copied from 802.16e document). Nevertheless, at the level of ProfM3_PMP profile, options specified in Table 327 stay “required”.

3.2. Specific Changes

[Add in Section 7, page 255, line 15]

If during capabilities negotiation, SS specifies that it does not support 802.16 Privacy method, step of authorization and key exchange shall be skipped. BS, if provisioned so, shall consider the SS authenticated; otherwise SS shall not be serviced. Neither key exchange nor data encryption performed.

[Add a new section 11.7.6.7 Authorization Policy Support]

This TLV indicates authorization policy that both SS and BS need to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.” If this TLV is omitted, then both SS and BS shall use the IEEE 802.16 Privacy method, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy.

Type	Length	Value	Scope
5.25	1	Bit# 0: IEEE 802.16 privacy supported Bits #1-7: Reserved	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)