IEEE P802.11

Wireless Access Method and Physical Layer Specification

Exclusion of Unencrypted MSDUs

Michael Fischer
Digital Ocean, Inc.
4242–3 Medical Drive
San Antonio, TX 78229
Telephone: +1–210–614–4096
Facsimile: +1–210–614–8192
email: mfischer@CHILD.com

Summary

This submission contains modifications to the contents of 5.3 to add the ability to instruct a station to discard any received data type MSDUs received without WEP encryption. See document 95-187 for discussion of the reasons for this recommendation. Voters favoring this proposal can cite this document as the source of replacement text for their D2.0 letter ballot comments.

NOTE TO EDITORS: These text changes should be applied AFTER the editorial corrections to sections 5.2 and 5.3 contained in document 95–212 (which were adopted at the July, 1995 meeting but not fully applied to the D2.0 text).

Changes to Section 5.3.2

The default value for all WEP keys shall be Null. This indicates an invalid WEP key. An attempt to use WEP with a Null key shall result in an error condition.

To support shared key configurations, the MIB contains a variable called “Default_WEP_Key”. The default value for this variable is Null. If not null, this variable contains the deafault key to be used with WEP.

An additional variable called “WEP_Default” is a boolean. If set True then on transmit, Data frames shall be encypted using Default_WEP_Key and on receive they shall be decrypted using Default_WEP_Key. The MIB shall not allow WEP_DEfault to be set to TRUE if Dfault_WEP_Key is Null. The default value of WEP_Default is False.

An additional variable called “aExclude_Unencrypted” is a boolean. If set True then MSDUs of any Data subtype received by the station with the WEP bit equal to zero in the frame control field shall be discarded, and the only Data subtype MSDUs that shall be forwarded to LLC and/or DSS are those which have successfully been decrypted by WEP.

802.11 does not require that the same WEP key be used for all stations. The MIB supprts the ability to have a separate WEP key for each station which which a Station directly communicates. This is supported by a MIB variable which is a two dimensional array called “WEP_Key_Mapping”. The array is indexed by MAC address and contains two fields for each entry: “WEP_ON” and the corresponding WEP_Key. The MIB shall not allow WEP_ON to be set to TRUE if the corresponding WEP_key entry is Null. The default value for all WEP_ON fields is False. This variable is always indexed by either RA to TA addresses (since WEP is applied only to the wireless link).

The values in this array variable take precedence over the WEP_Default and Default_WEP_Key variables.

The minimal length of WEP_Key_Mapping shall be 10. This value represents a minimum capability that may be assumed for any station which implements the WEP option.

The maximum length of WEP_Key_Mapping shall be implmementation dependant and the actual length of the array can be inquired from the read only MIB variable "WEP_Key_Mapping_Length".

The interactions between these variables is described below:

```
    Transmit case:
        if WEP_Key_Mapping(RA, WEP_On) = Ture then use WEP_KEY_Mapping(RA, WEP_Key) for
            encryption,
        if WEP_Default = Ture then Use WEP_Default for encryption,
        otherwise do no encypt the frame.

    Receive case:
        if WEP_Key_Mapping(TA, WEP_On) = Ture then use WEP_KEY_Mapping(TA, WEP_Key) for
            decryption,
        if WEP_Default = Ture then Use WEP_Default for decryption,
        otherwise do no attempt to decypt the frame.
```

MIB Definition to add to appropriate subsection of Section 8.4

aExclude_Unencrypted

```
Exclude_Unencrypted ATTRIBUTE
WITH APPROPRIATE SYNTAX
    boolean;
BEHAVIOUR DEFINED AS
    "This attribute is true when the station discards received MSDUs which have the WEP frame control bit equal to
    zero, rather than forwarding these MSDUs to LLC and/or DSS.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(10036) SMT(1) attribute(7) exclude_unencrypted(#) };
```