

## 1. P802.1AB Outstanding Comments

### **Comment 1 Les Bell**

COMMENT TYPE: TR

CLAUSE: 12

PAGE: 63

LINE: 31 << Editor's note - should be line 13) >>

COMMENT START:

The default value for this object should be expressed as a list of the enumerated values that are to be set. See RFC 2578, section 7.9.

COMMENT END:

SUGGESTED CHANGES START:

Replace "DEFVAL { "0xF0" } with

"DEFVAL { { portDesc, sysName, sysDesc, sysCap } }".

SUGGESTED CHANGES END:

### **Disposition of Comment 1**

Accept

### **Comment 2 Les Bell**

COMMENT TYPE: ER

CLAUSE: C.1.1

PAGE: 91

LINE: 16

COMMENT START:

This paragraph is commentary intended as guidance to MIB authors for what to include in the MIB security section.

COMMENT END:	1
SUGGESTED CHANGES START:	2
Delete this paragraph.	3
	4
	5
SUGGESTED CHANGES END:	6
	7
	8
<b>Disposition of Comment 2</b>	9
	10
See resolution to next comment	11
	12
	13
<b>Comment 3      Les Bell</b>	14
	15
	16
COMMENT TYPE: ER	17
CLAUSE: C.1.1	18
PAGE: 91	19
LINE: 24	20
COMMENT START:	21
	22
This paragraph is commentary intended as guidance to MIB authors for what to include in the MIB security section.	23
	24
	25
	26
	27
COMMENT END:	28
SUGGESTED CHANGES START:	29
Replace this line with a list of all sensitive MIB objects, stating why they are sensitive	30
	31
	32
SUGGESTED CHANGES END:	33
	34
<b>Disposition of Comment 3</b>	35
	36
Accept:	37
	38
Delete annex C	39
Number the MIB definition in clause 12 as 12.1.	40
	41
Add new subclause	42
	43
	44
12.2 Security Considerations (For LLDP base MIB module)	45
	46

1 There are a number of management objects defined in this MIB module  
2 with a MAX-ACCESS clause of read-write. Such objects may be  
3 considered sensitive or vulnerable in some network environments. The  
4 support for SET operations in a non-secure environment without proper  
5 protection can have a negative effect on network operations.  
6

7 Setting the following objects to incorrect values can result in an  
8 excessive number of LLDP packets being sent by the LLDP agent:  
9

10 lldpMessageTxInterval  
11 lldpTxDelay  
12

13 Setting the object, lldpMessageTxHoldMultiplier, to incorrect values  
14 can cause the LLDP agent to transmit LLDPDUs with too-high TTL values,  
15 which affect the expiration time of objects associated with the given  
16 LLDP agent in lldpRemTable.  
17

18 Setting the following objects to incorrect values can result in  
19 improper operation of LLDP:  
20

21 lldpPortConfigAdminStatus  
22 lldpPortConfigTLVsTxEnable  
23 lldpManAddrPortsTxEnable  
24

25 All readable objects in this MIB module (i.e., objects with a  
26 MAX-ACCESS other than not-accessible) may be considered sensitive or  
27 vulnerable in some network environments. This concern applies both  
28 to objects that describe the configuration of the local host, as  
29 well as for objects that describe information from the remote hosts,  
30 acquired via LLDP and displayed by the objects in this MIB module. It  
31 is thus important to control even GET and/or NOTIFY access to these  
32 objects and possibly to even encrypt the values of these objects when  
33 sending them over the network via SNMP.  
34

35 It is thus important to control even GET and/or NOTIFY access to  
36 these objects and possibly to even encrypt their values when sending  
37 them over the network via SNMP.  
38

39 SNMP versions prior to SNMPv3 did not include adequate security.  
40 Even if the network itself is secure (for example by using IPsec),  
41 even then, there is no control as to who on the secure network is  
42 allowed to access and GET/SET (read/change/create/delete) the objects  
43 in this MIB module.  
44

45 It is RECOMMENDED that implementers consider the security features as  
46 provided by the SNMPv3 framework (see RFC3410, section 8),

including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

**Comment 4 Les Bell**

COMMENT TYPE: ER

CLAUSE: C.1.2

PAGE: 91

LINE: 26 - 43

COMMENT START:

This section is commentary intended as guidance to MIB authors for what to include in the MIB security section for MIBs with no objects that may be SET by the user.

COMMENT END:

SUGGESTED CHANGES START:

Delete this section.

SUGGESTED CHANGES END:

**Disposition of Comment 4**

Accept - See proposed resolution in previous comment

**Comment 5 Les Bell**

COMMENT TYPE: ER

CLAUSE: G.6.5

PAGE: 91

LINE: 104 -117

COMMENT START:

1 There should be a Security Considerations section for this MIB, similar to Annex  
2 C.

3  
4  
5 COMMENT END:

6 SUGGESTED CHANGES START:

7 Either:

- 8 (1) Add a Security sub-clause for Annex G; or  
9 (2) Include the relevant MIB objects from this MIB in Annex C.

10 This also applies to the MIB in Annex H.

11  
12  
13 SUGGESTED CHANGES END:

### 14 ***Disposition of Comment 5***

15  
16  
17  
18 Accept - This is similar to comments 32, 33, and 34.

19  
20 Add new subclause:

#### 21 **G.6.6 Security Considerations (For LLDP 802.1 extension MIB module)**

22  
23  
24 There are a number of management objects defined in this MIB module  
25 with a MAX-ACCESS clause of read-write. Such objects may be  
26 considered sensitive or vulnerable in some network environments. The  
27 support for SET operations in a non-secure environment without proper  
28 protection can have a negative effect on network operations.

29  
30 Setting the following objects to incorrect values can result in  
31 improper operation of LLDP:

32  
33 `lldpXdot1ConfigPortVlanTxEnable`  
34 `lldpXdot1VlanNamePortsTxEnable`  
35 `lldpXdot1ProtoVlanPortsTxEnable`  
36 `lldpXdot1ProtoPortsTxEnable`

37  
38 All readable objects in this MIB module (i.e., objects with a  
39 MAX-ACCESS other than not-accessible) may be considered sensitive or  
40 vulnerable in some network environments. This concern applies both  
41 to objects that describe the configuration of the local host, as  
42 well as for objects that describe information from the remote hosts,  
43 acquired via LLDP and displayed by the objects in this MIB module. It  
44 is thus important to control even GET and/or NOTIFY access to these  
45 objects and possibly to even encrypt the values of these objects when  
46 sending them over the network via SNMP.

It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt their values when sending them over the network via SNMP.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see RFC3410, section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

Also add a new subclause

**H.5.6 Security Considerations (For LLDP 802.3 extension MIB module)**

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations.

Setting the object, lldpXdot3PortConfigTLVsTxEnable, to incorrect values can result in improper operation of LLDP:

All readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. This concern applies both to objects that describe the configuration of the local host, as well as for objects that describe information from the remote hosts, acquired via LLDP and displayed by the objects in this MIB module. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46

1 It is thus important to control even GET and/or NOTIFY access to  
2 these objects and possibly to even encrypt their values when sending  
3 them over the network via SNMP.  
4

5 SNMP versions prior to SNMPv3 did not include adequate security.  
6 Even if the network itself is secure (for example by using IPSec),  
7 even then, there is no control as to who on the secure network is  
8 allowed to access and GET/SET (read/change/create/delete) the objects  
9 in this MIB module.  
10

11 It is RECOMMENDED that implementers consider the security features as  
12 provided by the SNMPv3 framework (see RFC3410, section 8),  
13 including full support for the SNMPv3 cryptographic mechanisms (for  
14 authentication and privacy).  
15

16 Further, deployment of SNMP versions prior to SNMPv3 is NOT  
17 RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to  
18 enable cryptographic security. It is then a customer/operator  
19 responsibility to ensure that the SNMP entity giving access to an  
20 instance of this MIB module is properly configured to give access to  
21 the objects only to those principals (users) that have legitimate  
22 rights to indeed GET or SET (change/create/delete) them.  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46