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:
SUGGESTED CHANGES START:

Delete this paragraph.

SUGGESTED CHANGES END:

Disposition of Comment 2

See resolution to next comment

Comment 3 Les Bell

COMMENT TYPE: ER

CLAUSE: C.1.1

PAGE: 91

LINE: 24
COMMENT START:

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

COMMENT END:
SUGGESTED CHANGES START:

Replace this line with a list of all sensitive MIB objects, stating why they are sensitive

SUGGESTED CHANGES END:

Disposition of Comment 3

Accept:

Delete annex C
Number the MIB definition in clause 12 as 12.1.

Add new subclause

12.2 Security Considerations (For LLDP base 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 following objects to incorrect values can result in an excessive number of LLDP packets being sent by the LLDP agent:

lldpMessageTxInterval
lldpTxDelay

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

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

lldpPortConfigAdminStatus
lldpPortConfigTLVsTxEnable
lldpManAddrPortsTxEnable

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.

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.

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:

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

COMMENT END:

SUGGESTED CHANGES START:

Either:
(1) Add a Security sub-clause for Annex G; or
(2) Include the relevant MIB objects from this MIB in Annex C.
This also applies to the MIB in Annex H.

SUGGESTED CHANGES END:

Disposition of Comment 5

Accept - This is similar to comments 32, 33, and 34.

Add new subclause:

G.6.6 Security Considerations (For LLDP 802.1 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 following objects to incorrect values can result in improper operation of LLDP:

lldpXdot1ConfigPortVlanTxEnable
lldpXdot1VlanNamePortsTxEnable
lldpXdot1ProtoVlanPortsTxEnable
lldpXdot1ProtoPortsTxEnable

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.

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.

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.