Port based Network Access Control

Draft Summary of changes to 802.1D-1998

Mick Seaman

This is an incomplete first cut at the changes to 802.1D-1998 that would be required for a supplement on "Port based Network Access Control". This is based on discussion with Tony Jeffree.

Text in angle brackets <thus> is intended to be replaced by actual wording. The current contents of the brackets is likely to be very rough and ready.

Clause 1. Overview

Add an item[1]:

e) <supporting validation of access to the network>

Clause 1.2 Scope

Item f) ought to be removed as an item of maintenance, indeed Scope ought to be reviewed and brought up to date by going through the rest of the clauses.

Add an item:

x) <support of authentication and authorization protocols that require enforcement of network access, or something like that>

Clause 2. References

Add EAP and Radius references.

As a maintenance item there ought to be a reference to the IEEE website as a rather quicker way of finding out about standards than writing to or calling the IEEE. Ask Kristen's replacement about supporting material.

Clause 3. Definitions

No changes.

Clause 4. Abbreviations

Add EAP, EAPOL (?), EAPOE, EAPOTR.

Clause 5. Conformance

<The Port based Network Access Control capability is optional>

Clause 6. Support of the MAC Service

Clause 6.1 Support of the MAC Service

Add <only support the MAC Service for authenticated and authorized devices, this helps availability, but note exchanges taking place to gain access also use the MAC service>

Clause 6.3.1 Service availability

<denial of service (to unauthorized stations) necessary, deliberate denial of service is already an idea in this section, extend it>

Clause 6.3.2 Frame Loss

<needs item b) 5) to cover deliberate discard from unauthorized port>

Clause 6.4 Internal Sublayer Service provided within the MAC Bridge

<Needs the idea of a physical MAC being there or not : up/down, enabled/disabled, operational/not operational, as part of the service. This is also a requirement for the "rapid reconfiguration" work, and should be worked as part of that effort.>

Clause 6.5 Support of the Internal Sublayer Service by specific MAC procedures

<Add the mapping of up/down (see 6.4) to the individual MACs of interest, i.e. at least 802.3 and 802.5>

Clause 7.1.1 Relay

In the list of functions that "support the relaying of frames and maintain the Quality of Service" there ought to be an item already between c) and d) to discard for loop suppression purposes. Add an item for discard for access control of

[1] Assumes that we have already inserted item d) for Rapid Reconfiguration.

non-authorized ports, and add two similar items on the outgoing side, probably between h) and i).

Clause 7.1.2 Filtering and relaying information

Add an item to allow discard from non-authorized ports. Probably fits best just after topology maintenance.

Clause 7.2.4 Higher Layer Entities

Add a description of the BAE[2], the "Bridge Access Entity".

Clause 7.3 Model of Operation

Add a figure (7-8) to illustrate the operation of the BAE. This should look very similar to Figure 7-7 (for GARP) except that arrows go to Port State, rather than the other way around. A short descriptive paragraph is required. Perhaps the figure needs to be asymmetric to show the use of a higher layer protocol stack on at least one side, on perhaps stacks on both sides.

Note that a separate item of maintenance is required to modify all these figures by substituting "MAC Client" for "LLC" and then to explain that the "MAC Client" is the logical union of the LCC and Ethertype demultiplexing capabilities. Needs reconciling with 802.3 in detail and probably some text in clauses 6.5.

Clause 7.4 Port State, Active Ports and the Active Topology

Basically the Port State is:

Enabled iff BPE Enable &&
BAE Enable &&
Mgt Enable

or to put it another way, the Port State is Disabled if has been Disabled by the BPE (Bridge Protocol Entity) to prevent loops, by the BAE (Bridge Access Entity) to prevent unauthorized access, or by other management choice.

This means that data frames will not be relayed. Of course Authentication and Authorization information is forwarded, with an appropriate change of wrapper/transport encoding by the BAE. Fortunately it is already said (repeatedly throughout the document) that the BPE does not send and receive frames on Disabled ports, so an unauthorized port neither transmits BPDUs nor does it do anything (except discard) received BPDUs.

Modify the first paragraph of this clause appropriately. This has the effect of excluding unauthorized ports from the *Active Topology*.

After the fourth paragraph add a new paragraph explaining the use/effect on the Port State information of the BAE.

Clause 7.7 The Forwarding Process

Expand the first paragraph to include the access control functionality[3].

Clause 7.12.3 Bridge protocol entities and GARP protocol entities

Change the heading of this clause to "Bridge Protocol, Bridge Access, and GARP Entities.

Describe the transmission and reception requirements for Bridge Access Entities including their use of higher layer protocol stacks and eventual transmission and reception via DL_request and DL_indication primitives. Add all the required addressing and identification information, including references as necessary to higher layer documentation.

Add an Ethertype assignment (if required) for EAP over Ethernet in a new Table, as already done for the LLC assignment. Add an LLC SNAP assignment for EAPOTR (if required).

Clause 7.12.7 Points of attachment and connectivity for Higher Layer Entities

Need small update to 1st para, 1st sentence of 7.12.7.

Careful clarification required here. Some higher layer entities may take notice of the Enabled/Disabled port operational status, but not of Port States as defined by the Spanning Tree. This is not a technical change as Spanning Tree itself already does this – BPDUs are transmitted out of Listening, Learning, and Forwarding ports (when they are Designated), and received on Listening, Learning, Forwarding and Blocked ports, but never transmitted or received on Disabled ports.

The MAC address used by EAPOE should be put in the Filtering Database if you are running a BAE.

BAE (as currently proposed) has one attachment per port and then an IP attachment. Modify 7.12.7 second paragraph which claims that "Higher Layer Entities fall into two distinct categories ..".

Define and discuss IP points of attachment. Note that these need a port that has already been authenticated if the bridge is not to cut itself off.

[2] A more accurate name and better acronym than BSE, for "Bridge Security Entity".

[3] I have another note that says "leave it alone" because access control is just a topology restriction so we don't need to change it. Have to assess what it looks like when other changes are in.

Clause 8.4.5 Disabled

Perhaps a change here to specify what is meant by “operation of management” to include a port not being authorized.

Clause 12. Generic Attribute Registration Protocol (GARP)

It is unclear what GARP does on Disabled ports at present, and even unclear if we care, since registrations will not propagate until authentication has occurred. Need a firm decision and a decision where to record this in clause 12.

Clause 14. Bridge Management

Access to bridge management is not denied through Disable ports, even if the port is Disabled because it is not authorized, unless access to management requires relaying a frame. It is up to an implementation to decide where bridge management is connected.

Clause 14.1.4 Security management

Add in this clause.

Clause 14.2 Managed Objects

Add an item g).

Clause 14.10 Bridge Access Entity

Add a new clause, with this number and title, containing whatever objects are necessary.

Clause 15. Management Protocol

In Figure 15-1 hang the BAE off the port object as per GARP.

Clause X. Bridge Access Control

A new clause explaining the relaying function of the BAE, starting at the high level requirements and protocol exchange scenarios, what has to be mapped across, success/failure codes, initiating the dialog etc. etc.

Clause Y. EAP over LANs

Encoding over raw Ethernet (if required). Probably best to start on this, if the IETF will take it up promptly that is O.K. but we should not plan not to have this until that actually happens.

Annex X. Port based Network Access Control

A new Annex explaining design rationale and illustrating use of port based access control.

If material on service location is purely advisory it should go here rather than in the main body of the standard.

Other

Need an SNMP MIB for this.