IEEE 802.1 Interim meeting
Ottawa, Canada
5/23/00 - 5/25/00
Minutes Taken by Andrew Smith

Attendees:

Alan Chambers
Andrew Smith
Anil Rijsinghani
Hesham ElBakoury
Joe Lawrence
Leroy Nash
Les Bell
Luc Pariseau
Mick Seaman
Neil Jarvis
Norman W. Finn
Paul Congdon
Sharam Hakimi
Tony Jeffree

802.1X Port-based Network Access Control

Full WG ballot has only 10 responses of yes/no, the rest are abstains.
Should we consider this a valid ballot? We decide to proceed with comment resolution and issue a recirculation ballot.

Incorporation of material for RADIUS backends from

draft-congdon-radius-8021x-00.txt: Also, discussion of Glen Zorn's comments on this draft. We want to add this material as an informational annex to 802.1X, maybe need some editorial license in pasting this into 802.1X e.g. to handle non-802.11 cases.
Error numbers: not clear which is the normative definition of the codes: we do not really want to invent any new ones here (Glen Zorn suggests a new "re-authentication error" code) - we would like to re-use the RADIUS error codes so we should/can not own them or define new ones.
NAS-IP-Address - need some guidance as to which IP to choose NAS-Port - what does this include for 802.11? It needs to represent the 802.11 association. Also, some issues for 802.3ad link aggregation. These are probably "interface numbers" of some sort.
Need another term for "bridge or Access Point"
NAS-Port-Type needs to be defined by reference to the appropriate place in RADIUS specs.

Conformance issues:
General issue of statistics collection: we have 31 per-port counters right now. General feeling that this is too many. Include the new counters proposed by Bernard Aboba for Authenticator and backend state machines as optional - general feeling that these are too heavy to implement. Re-authentication should be mandatory.

Relationship of 802.1X to 802.11 and 802.3ad: discussion of what we mean by the term "port". Probably need some discussion of how we map onto each technology. Also need some related cleanup of our scope statement (8.2) - out of scope is a scenario with multiple Supplicants talking to a single Authenticator.

In particular there is the issue of whether to allow a "in-only" link to join an 802.3ad aggregate - requirement is that all links be in a "like" mode. Such ports signal "oper up" when running 802.3ad. Seem to need a note to indicate that you might need kludges similar to the bridge-detect machine if you have higher-layer protocols that get broken by a unidirectional link.

It appears that you cannot simultaneously run EAPOL at both physport and aggregate levels (addressing issues in the protocol): need to pick one. Should the standard pick for us? Yes: in the presence of 802.3ad, you must run 802.1X on physical ports only. Port numbering in the presence of 802.3ad: not now an issue - just use physport as the identifier.

Control/status of ports: some discussion of what admin controls are needed and how these reflect back as operational states. There are several valid formulations of this. We agree that:
We need to report back more detailed status anyway: e.g. output of bridge-detect, output of state machine.
We should have separate controls for "control mode" {force-authorized, auto, force-non-authorized} and "controlled direction control" {both, in-only}.
We should have separate status reporting for "control status" {authorized, not-authorized} and "controlled direction status" {both, in-only}.
Note that this allows for a "forced, out-only" mode (some discussion of whether this is useful or harmful).

Need more expansion from Tim Moore of the 802.11 material on Key Descriptor formats (7.6).

Who "owns" EAP Identifier values? intermediate system must not break end-to-end EAP. But the initial EAP request/id is generated by the intermediate system so we need some rules.

Proposal to add a transition for Supplicant from HELD to ACQUIRED if it receives a Request from the Authenticator: this seems to be a good optimisation, rather than waiting for the heldWhile timer to expire before being allowed to respond. Possible denial-of-service but we ought to trust the Authenticator here. Add it.

802.1w Rapid Reconfiguration

Mick Seaman - Recasting of state machines to make them more intelligible:

high-level blocks for protocol migration, retransmit timers, port role selection, port state transitions (allows for time delay between protocol actions and hardware responding to them), topology computation and port information maintenance. Low-level detail of each block - many states that are really just procedure-calls but they are broken out for clarity.

There is also an alternate formulation for this whole set of machines which reflects more of the rationale for the protocol design but seems further from the obvious implementation. We think the former is the best one to include in the specification.

Reordering - paper presented by Tony Jeffree. His conclusion was that there were no serious issues with the additional misorderings that could be introduced by RSTP operation. Assertion is that NETBEUI/SNA, LAT and LLC2 are still significant and would be affected materially. It is possible that these can all be handled by appropriate VLAN configuration, making sure that all such protocols go over a Spanning-Tree that is using the old protocol - this needs further investigation.

802.1t Maintenance of 802.1D

Resolution of ballot comments. Specific issues:
Dropping of GDMO: there appears to be no significant demand from customers for this (maybe CORBA?).
Figures 7-15 and 7-16 are broken: need to fix the modeling of where some applications sit e.g. GARP.
Should we try another "recommended renumbering" scheme for STP Port Cost - we would recommend how to renumber your old bridges when you add new ones with high-speed links. RSTP would have to include different "add up cost" algorithms. Still needs more discussion but for now we adopt Norm's proposed "plan A" but multiplied by 2 i.e.:

10T	2
1T	20
100G	200

10G 2000
1G 20000
100M 200000
10M 2000000
etc.

Need some initial state values for GARP (Applicant/Registrar should be VO/MT).

Bridge detect: is optional. But claiming support for 802.1w and 802.1X will make it mandatory.

Should we add a new "testing" state to the MAC Enabled parameter? This would match MIB-2 and all newer interface MIBs:

```
ifAdminStatus OBJECT-TYPE
   SYNTAX  INTEGER {
              up(1),       -- ready to pass packets
              down(2),
              testing(3)   -- in some test mode
           }
   MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
           "The desired state of the interface.  The testing(3) state
           indicates that no operational packets can be passed.  When a
           managed system initializes, all interfaces start with
           ifAdminStatus in the down(2) state.  As a result of either
           explicit management action or per configuration information
           retained by the managed system, ifAdminStatus is then
           changed to either the up(1) or testing(3) states (or remains
           in the down(2) state)."
```

It is not clear however what "some test mode" means: decide to leave this alone as a binary enabled/disabled switch.

802.1u Maintenance of 802.1Q

Resolved all pending comments - nothing major.
We need to have one new object added to the RFC2674 Bridge MIB - people will discuss this issue with IETF Bridge MIB WG, no action required for 802.1.

802.1s Multiple Spanning-Trees

A new draft will be written up that uses the new STP formulations from 802.1w. Norm Finn will join Alan Chambers as co-Editor for the project.
Plan to ballot this ASAP, before July plenary.