# IEEE 802.1 Minutes, January 2008

## Opening Meeting, Monday AM, January, 28 2008

Administrative and Agenda – Tony Jeffree

IEEE Patent Policy – Tony Jeffree

The call for patents was made and no one spoke up

The required five slides where shown and the patent policy was reviewed

Future interim meetings – Tony Jeffree

May 2008: Israel, week of 12th, letter of invitation and security form will be provided to ease exit screening

Sept 2008: ChengDu, China, week of 15th, joint with 802.3, see Linda Dunbar if you need an invitation letter to get business visa

Jan 2009: ideas/offers solicited

Resilient Rings idea discussion - John Lemon, Norm Finn

Forwarding process presentation - Norm Finn

Identifying issues with queuing in the current 802.1 model

Issues with 802.1Q revision – Glenn Parsons

TG agendas – Tony Jeffree

IW: comment resolutions (ah, ap, aj, ak, ab, ay) first, then new work at end if time.

Security: af and ar

AVB: review of assumptions, AS draft review, timestamp passing interface between 802.3 and 802.11y and 802.1AS, Qat draft review, Qav comment resolution, joint meeting with 802.11, develop PAR for profile network

DCB: Qau, Qaz transmission selection, work on proposed priority flow control PAR

## Monday PM, January, 28 2008

In the afternoon each of the task groups met separately

Security Task Group

Review of draft 1.8 – Mick Seaman

Hot topic is network advertisement

Review of what changes from the previous draft

Discussion at last plenary on group addresses and scope

- Motion was probably wrong need to correct
- 1.8 now is consistent with .1ab

MKA with regard to different crypto algorithms

- Algorithm agility parameter now in the draft

- Don’t need to change spec if a new algorithm comes along
- Clause 11
  - New sub-clause for PAE transmit and receive
  - How to manage virtual ports and where to the management objects live
- Clause 12
  - Now basically a reference diagram and pointers to the rest of the document
- Network advertisement
  - Simplification of Joe’s proposal and we need review and sorting through
- Management Stuff
  - Clause 11.9 provides pointers to the rest of the text
  - Figure 11.3 Page 104
    - Herald – entity to handle advertising within the domain of 802.1af
    - Discussion of the relationship of virtual ports to physical ports and the requirements and needed information to managed
  - MIB discussion, where are we and what are the next steps Clause 13
    - What to do with the MIB
      - Keep old MIB and leave it EAP related
      - Create new MIB that handles PAE stuff
    - Or
      - Map the old MIB to the new MIB and leave for historical reason so folks can follow the trail to the new MIB
      - Of course, new folks will need to implement two MIBs
      - Because there is not an EAP MIB we will probably need to keep the current MIB to provide some required and helpful information
      - Probably want pre-configured virtual ports
- Discussion about Advertisement and its requirements

## <u>Tuesday AM, January, 29 2008</u>

<u>Internetworking Task Group</u>

- <u>Call for patents and review of the patent policy – Steve Haddock</u>
- <u>Ballot Comment Resolution of 802.1ak Corrigendum – Tony Jeffree</u>
  - Discussion about should or should not the version number in the protocol be changed
    - Since the protocol is broken and no one has implemented the protocol it is not an issue to leave the protocol version as is
    - The consensus is the version number should stay at zero
      - There can be no working implementations deployed so this is not an issue
  - EndMark optimization
    - It is too late to make this change
- <u>Ballot Comment Resolution of 802.1AB-Rev – Tony Jeffree</u>
  - Discussion of Mick’s ballot comment concerning a model of an entity to represent an 802.1AB in such a way that use, management, and control can be described in the document
    - Mick’s proposal will be a basis for the next draft and then folks can sort through the issues with words in the draft
  - 802.3 has asked a couple of questions that we need to deal with

802.3at DTE Power Enhancements is looking to use 802.1AB

If 802.3 adds a subtype can it be referenced in 802.1AB?

Discussion

The issue is logistics

802.3 needs/wants to understand where and how this needs to done

We can reserve a subtype and create a pointer to the 802.3 document

We could remove the 802.3 annex and simply give it to 802.3

Is there issues with the 802.3 MIB?

802.3 has not started the process to move the MIB from IETF to 802.3 so it would be hard to get this into the MIB right now

Tony will send a note back to 802.3 that reflect the discussion and consensus

Running LLDP on both the controlled and uncontrolled port

Discussion

Need to support both the controlled and uncontrolled port. Need to appear as different port numbers (ifindexes) but we should add a common port ID – see AF as to how this should be done

Ballot Comment Resolution of 802.1AJ – Tony Jeffree

## Tuesday PM, January, 29 2008

Security Task Group

P802.1AR Draft Review – Max Pritikin

Section 6.3.2.1 review

Discussion about whether we need to add may support SHA-1 or to require SHA-256. SHA-1 is needed to support existing and deployed equipment

After more discussion drop reference to SHA-1 and change to the following to allow

Change DER encoding reference to blob and the signing operation is as currently indicated

Section 6.3.2.5 Key Delete

Should the IDevID keypair be deleted?

What is the definition of deleted?

There will be two operations for key deletion operations to prevent unintentional deletion of the IDevID

Section 6.3.2.6 Generation of request for DevID credential (CSR)

Should this require SHA-256

Yes, require SHA-256 and optional SHA-1

## Wednesday AM, January, 30 2008

Security Task Group

P802.1AF Draft review – Mick Seaman

- It is suggested that advertisement can be put in EAPOL Start to avoid the find out by timeout that service is not available
- Always send an EAPOL start so that the state machines are synced
- Now a discussion about how to encode the start such that version 1 – no advertisement and a new version that supports advertisement can work within the same network
- Suggested that there should be a request for advertisement to avoid advertisement floods
    - Discussion
        - There are several issues that we need to sort through
        - A single request bit
- There should only be one herald for each physical port to send advertisements
- EAPOL Logoff
    - Only allow multicast to help damp down DOS issues
    - If logoff is a packet that terminates the secured session then it is dangerous
    - We need to understand where we are today in the other dot technologies so we can handle logoff is a acceptable and logical manner
    - Discussion about how to drop a secured connection
        - Stop sending MKA stuff
    - Discussion about the relationship between EAPOL Logoff and account stop
        - How to terminate and propagate session termination to upper levels
    - What is implied by EAPOL Logoff in .11
        - Does not flush anything
        - Encrypted in .11 so it cannot be forged
- Discussion about things that should be in which MIB
    - Session Octets and their relationship to Interface MIB
    - Should be in PAE MIB
    - Virtual Port – there are virtual ports that will be semi-permanent so they need a way to maintain information
- Network access and fallback scenarios
    - What is an advertisement PDU?
        - Front same as LLDP – Chasis id and port id
        - We need to be careful so we don’t trip over LLDP
        - Don’t reinvent an LLDP
        - This is herald id – way to think about this
    - Review of Table 9-8
        - Remove bit 4 and advertise in NID
        - Need some guidelines to explain the security issues of various uses and failure scenarios

## Wednesday PM, January, 30 2008

Security Task Group

- P802.1AF draft review – Mick Seaman
    - Along with NID when the EAPOL starts should some of the other options that could be selected by shown?
        - Something the supplicant is going to say to the authenticator

- Say 802.1x with WebAuth as a fall back because don't have 802.1x simply go to WebAuth
- Optimization and it helps to sync
  - Allows both sides to know quicker what is going on
- There should be a new frame type to EAPOL start to not automatically kick off EAP

P802.1AR –

- Critical and non-critical extensions
  - WiMax wants critical extensions
  - We need to make a modification to allow AR to be in alignment with WiMax
  - Allow key usage to be marked critical and specify that it is the only critical extension
- ECC text
  - Review of API to make sure it can handle both ECC and RSA
- Management Issue
  - Showing of public key in DevIDIDDevIDEntry

Tomorrow agenda

- More P802.1AF
  - We can troll through the doc to see what folks need to sort out
  - Review Bernard's slides and see if everything was covered

## Thursday AM, January, 31 2008

Security Task Group

P802.1AF Draft Review – Mick Seaman

- Multiple Authenticator discussion
  - This is an attempt to provide redundancy
  - This is not an issue we need to worry about it
- Key Cache
  - Talk about but not provide management?
    - Operations
      - Enumerate
      - Relationship with NID
      - Need MIB that controls what goes in the advertisement

```
SYSTEM (Potential Advertisement)               NETWORK
|--NID                                         KMD
|  |                                           |
|  |---- KMD list                              |----CKN
|  |                                                |
|  |---- MacSec Cipher list                         |---life, time, who
|  |
|  |-----AuthReqmts
|
|---Port
     |
     |-----NIDEnable
```

Clause 5 Conformance

- Should be organized in such a way that someone can claim conformance to 802.1X-2004
- Authenticator and supplicant will get their own sub clause
- Control direction approach has been replace

Attendees of January Interim

| **NAME** | **SURNAME** | **Affiliation** |
|---|---|---|
| Bernard | Aboba | NOT CONFIRMED |
| Osama | Aboul-Magd | Nortel Networks |
| Zehavit | Alon | Nokia Siemens Networks |
| Alex | Ashley | NOT CONFIRMED |
| Dave | Bagby | NOT CONFIRMED |
| Florin | Balus | Alcatel-Lucent |
| Hugh | Barrass | Cisco |
| Caitlin | Bestler | Neterion |
| Jan | Bialkowski | Infinera, Inc |
| Rob | Boatright | Harman Pro |
| Jean-Michel | Bonnamy | France-Telecom |
| Paul | Bottorff | Nortel Inc |
| Rudolf | Brandner | Nokia Siemens Networks |
| Alex | Busch | BMW group |
| Craig W. | Carlson | Qlogic |
| Frank | Chao | Cisco Systems, Inc |
| Edgar | Chung | NOT CONFIRMED |
| Paul | Congdon | Hewlett Packard |
| Todor | Cooklev | NOT CONFIRMED |
| Diego | Crupnicoff | Mellanox |
| Claudio | Desanti | Cisco |
| Thomas | Dineen | Self |
| Linda | Dunbar | Futurewei Technologies |
| Hesham | Elbakoury | Nortel |
| David | Elie-Dit-Cosaque | Alcatel-Lucent |
| Yacine | Elkolli | Canon |
| Darwin | Engwer | NOT CONFIRMED |
| Don | Fedyk | Nortel |
| Felix Feifei | Feng | Samsung |
| Norm | Finn | Cisco Systems |
| Bob | Frazier | Ericsson |
| John | Fuller | Gibson Guitar |
| Geoffrey | Garner | Samsung |
| Eric | Geisler | NOT CONFIRMED |
| Anoop | Ghanwani | Brocade |
| Franz | Goetz | Siemens |
| Mark | Gravel | Pro Curve Networking by HP |
| Eric | Gray | Ericsson |
| Ken | Grewal | Intel |
| Craig | Gunther | Harman Pro |
| Mitch | Gusat | IBM Research |
| Steve | Haddock | Self |
| Brian | Hart | NOT CONFIRMED |

| | | |
|---|---|---|
| Asif | Hazarika | Fujitsu |
| Ian | Hood | Cisco Systems |
| Romain | Insler | France Telecom |
| Tony | Jeffree | Self, Cisco, Broadcom, Hewlett Packard, Adva |
| Joy | Jiang | NOT CONFIRMED |
| Michael | Johas Teener | Broadcom |
| Prakash | Kashyap | Extreme Networks |
| Stuart | Kerry | NOT CONFIRMED |
| Keti | Kilcrease | Cisco Systems |
| Yongbum | Kim | Broadcom |
| Philippe | Klein | Broadcom |
| Raghu | Kondapalli | Marvell |
| Bruce | Kwan | Broadcom Corp |
| Ashvin | Lakshmikantha | BRCM |
| Yannick | Le Goff | France Telecom |
| Marcus | Leech | Nortel |
| Zhi-Hern | Loh | Fulcrum Microsystems |
| Gael | Mace | Thomson |
| David | Martin | Nortel Networks |
| Riccardo | Martinotti | Ericsson |
| Brad | Matthews | BRCM |
| Alan | McGuire | British Telecommunications PLC |
| David | Melman | Marvell |
| Menucher | Menuchery | Marvell Semiconductors |
| John | Messenger | Adva Optical Networking Ltd |
| Dinesh | Mohan | Nortel |
| Matthew Xavier | Mora | Apple Inc |
| Kevin | Nolish | Ericsson |
| Don | O'Connor | Fujitsu Network Communications |
| Stephen | Oliva | Sprint |
| David | Olsen | Harman Pro |
| Stephen | Palm | NOT CONFIRMED |
| Rong | Pan | Cisco Systems |
| Don | Pannell | Marvell |
| Glenn | Parsons | Nortel Networks |
| Alex | Pavlovsky | Finisar Corp |
| Mark | Pearson | Hewlett-Packard |
| Joe | Pelissier | Cisco |
| Max | Pritikin | Cisco |
| Rekha | Ramachandran | Cisco Systems |
| Pasula | Reddy | Fujitsu |
| Dwayne | Reeves | Fujitsu Network Communications |
| Edward | Reuss | NOT CONFIRMED |
| Robert | Roden | Lightstorm Networks |
| Derek | Rohde | Qlogic |
| Moran | Roth | Corrigent Systems |
| Jessy V | Rouyer | Alcatel-Lucent |
| Dick | Roy | Connexis |
| Ali | Sajassi | Cisco |
| Joseph | Salowey | Cisco |
| Panagiotis | Saltsidis | Ericsson |
| Satish | Sathe | Brocade |
| Mick | Seaman | Mick Seaman |
| Koichiro | Seto | Hitachi Cable |
| Suman | Sharma | NOT CONFIRMED |

| | | |
|---|---|---|
| Ravi | Shenoy | Emulex |
| Meera | Siva | Extreme Networks |
| Graham | Smith | NOT CONFIRMED |
| Nurit | Sprecher | Nokia Siemens Networks |
| Dorothy | Stanley | NOT CONFIRMED |
| Kevin B | Stanton | Intel |
| Bob | Sultan | Huawei Technologies |
| Richard | Sun | Dallas Semiconductor |
| Muneyoshi | Suzuki | NTT |
| George | Swallow | Cisco Syatems |
| Attila | Takacs | Ericsson |
| Francois | Tallet | Cisco |
| Bert | Tanaka | Woven Systems |
| John | Terry | Brocade Communications |
| Pat | Thaler | Broadcom |
| Geoff | Thompson | Nortel/GCSI |
| Oliver | Thorp | Fujitsu |
| Dimitry | Vaysburg | AMCC |
| Maarten | Vissers | Alcatel-Lucent |
| Manoj | Wadekar | Intel |
| Niel D | Warren | Apple Inc |
| Brian | Weis | Cisco |
| Ludwig | Winkel | Siemens AG |
| Michael D. | Wright | Panoptic Security |
| Chien-Hsien | Wu | Broadcom |
| Ken | Young | Gridpoint Systems |