IEEE 802.1 Minutes, July 2004

Meeting attendees

Osama Aboul-Magid  Bill Lane
Brandon Barry  Tom Mathey
Les Bell  Bill McIntosh
M Borza  Dinesh Mohan
Paul Bottorff  Ken Mooney
Rudolf Brandner  Bob Moskowitz
Jim Burns  Ravi Nalamati
Dirceu Cavendish  Satoshi Obara
Vincent Chanal  Don O'Connor
Rongfeng Chang  Karen O'Donoghue
Paul Congdon  Hiroshi Ohta
Sharam Davari  Glenn Parsons
Arjan de Heer  Ken Patton
Craig Easley  Harry Peng
Anush Elangovan  Rick W. Pimpinella
Hesham Elbakoury  John Roese
David Elie-Dit-Cosaque  Josef Roese
Norm Finn  Allyn Romanow
Bersani Florent  Dan Romascanu
David Frattura  Jessy V Rouyer
Gerard Goubert  Ali Sajassi
Ken Grewal  Dolores Sala
Steve Haddock  Sam Sambasivan
Onn Haran  John Sauer
Takashi Hasegawa  Mick Seaman
Ran Ish-Shalom  Kapil Sood
Vipin Jain  Matt Squire
Neil Jarvis  Muneyoshi Suzuki
Tony Jeffree  Yoshihiro Suzuki
Peter Jones  Geoff Thompson
Ulf Jonsson  John Viega
Mohan Kalkunte  Preeti Vinayakray-Jani
Tetsuya Kawakami  John Vollbrecht
Do-Yeon Kim  Dennis Volpano
Kwangio Kim  Karl Weber
Yongbum Kim  Ludwig Winkel
Sreenivas Kottapalli  Robert Wu
Glen Kramer
**Pre-Meeting Monday, July 12, 2004**

Two simultaneous meetings - AB and AD. AB doing disposition of comments.

**802.1AD- Mick Seaman**
- Need a new approach.
- Several people not happy with scaling of provider bridges
- Break this out into a new PAR

**Backbone Provider Bridging Networks - Paul Bottorff,**
- PAR - Backbone Provider Bridge PAR
- backbone is separate from the provider bridge
- Comment - this is MAC in MAC, with different terminology
- This is Paul's understanding of where the MAC and MAC technology is
- Mick- thinks if split things are split apart this way, it's more useful

**Opening Plenary Monday, July 12, 2004**

**Agenda - Tony Jeffree**

**Administrative Stuff**

**Website** http://www.ieee802.org/1/

**Voting Membership** - Review of voting rules – need to attend 5 sessions, if attend 2 such meetings, can gain voting rules at the next Plenary meeting.
- Credits valid within the span of 4 plenary meetings
- To maintain, must attend two meetings, one of which is plenary, within a 4-plenary time period.
- Voting is obligation to participate

**Review of 802.1 WG and Task Group operation**

**Review of different types of ballots**

**Review of IEEE patent policy**
- Slides #1 and #2 where shown to the committee and the policy was reviewed.
- It is up to the patent owner to assert their patent is used in a standard

**Scheduling interim**
- Will be Oct. 4 in Ottawa– It was very difficult to schedule, because of too many conflicts in September.

**Review of inappropriate topics of conversation for IEEE WG Meetings**

**Liaison reports**
- Craig Easley- liaison to 802.3
- 802.3ah EFM was ratified
- Backplane, 10G-BT, technical presentation
- Joint plenary tues am to discuss frame format extensions,
- New CFI from Nortel and others, including Gibson Guitar, on Residential Ethernet for Audio Visual over Ethernet
- SG on Congestion management
- Ongoing maintenance activities

**Bob Moskowitz- 802.11**
11.s has approved PAR, mesh networks
11.p vehicular system requirements

IETF – Paul Congdon
- Processes to share info between IEEE and IETF
- Questions on proper review of work
- EAP methods run over IEEE
- SNMP mibs
- RADIUS attributes- new WG RADIUS extensions WG, including specific to IEEE networks

TIA – need a liaison

Tony circulated proposed PARs for new work. We have a chance to comment, but must be by end of day Tuesday. Tony felt not much we cared about, but could be wrong. Check and see.

What’s been happening in the EXEC? Met Monday morning- Tony Jeffree reported
- Approvals – 802.3ah, 802.11i, and 802.17
- IEEE continues to expand attendance – 1400 this week
- Task Force between 802 and IEEE Standards Association (SA)
- Indemnification – looks like everyone will be covered
- Downloads- they need more money for them
- Tutorials- Norm Finn, Connectivity Fault Management 6:30-8 Monday
- Policies & Procedures – rules for 802 going through revision
- New P&P so that SA can review them better
- Online training materials for would-be 802 officers
  - There has been a face to face effort, now going to make permanent web based resources available.
  - Tues 8-9:30 on use of Frame Maker. Jennifer Longman running it
- This week 802.3 is raising PAR for extending of frame size
- IETF asked for access to IEEE working drafts.
- Formation of new 802 Architecture Group- Paul Nikolich asked this be done.
  - Tony is heading it up. Will be a standing committee of the SEC, appointed representatives from each working group, two representatives from each.
  - People with broad understanding as well as in depth on the particular WG.
  - Will be Sunday afternoons at plenary meetings. Known problems of how architecture of different MAC groups fits in.
  - 802.11 has now formed its own internal architecture group.

Agenda Setting- Mick
- AE – make sure to have internetworking people there- important to consider security for internetworking

Monday
9.00-10.30 Interworking : P802.1ad Provider Bridges [Queen Marie - ES]
  Backbone/Core scaling proposal (Bottorff et al)
9.00-10.30 Interworking : P802.1AB LLDP [Roy Yates - ES]
  Sponsor Ballot resolution (Paul Congdon)
1.00- 3.00 802.1 WG : Opening Plenary [Queen Marie - ES]
  Chair's opening remarks.
  Agenda setting and confirmation for week.
Tuesday morning, July 13, 2004
802.1AE First Disposition of Comments on Draft 2.0 – Allyn Romanow

Review of all comments except those that seemed to be editorial only in nature.
See disposition of comments.
Tuesday afternoon, July 13, 2004

802.1af Overview of KSP- Mick Seaman- slides
Not a spec yet.

Kwangjo Kim- Key Management for Link Level Security - slides
Review of .11i, followed by a new proposal.
Comments on the presentation- the assumptions here don’t match our problem.
This isn’t the operational environment we’re working in, this is point to point only. We don’t have this luxury.
 Assumes global unique MAC address. This is not a realistic assumption. Too weak to hang security on. MAC address is an “accidental” property of the system.
In the L2 world, the MAC address is really a hint to the infrastructure, not really permanent. Need a different type of credential in the system presented.
The presentation has a number of interesting points.
What other standard groups might be interested? .11? They have different constraints than we do.

John Viega- Initial Keying for KEYsec
http://www.ieee802.org/1/files/public/docs2004/AFJul04Viega_KeySec_Initial_Keying.ppt
Initial Key installation. Want a simple, out of the box way to install keys
New device- needs to be set up with pair wise keys. Purchase new device, want to have it talk to other device or devices. Want it to be plug and play
Want way to identify and validate own devices. Assign devices unique 128-bit IDs, loaded with MAC address by the manufacturer
32 bit vendor ID, 96 bits vendor dependent, unique, random number is fine
Use RSA to validate device owns ID and exchange pair wise keys
Use mini-PKI. Vendor installs private key and certificate with public key
Certificate signed by vendor’s signing credentials.
Its credentials signed by a root certification authority, IETF has offered to do it, An EAP method could leverage this.
Binds an ID to a device. Don’t use MAC address
Auxiliary benefits-
Solves L2 part of ARP problem, would provide signed ARP to IETF to solve problem
Prevents counterfeiting hardware- device that’s a clone, stolen, would be able to tell
Provides a basis for establishing trust in firmware
Assuming TPM chip? Or flash? Any write–once memory
Drawbacks
Need to integrate into manufacturing process
Requires hash function for signing, probably SHA1
DOCSIS does same thing
Don’t have to do it every time, this is initial key installation
Use this, or other things, to construct a group key, which can be used many times
Mick’s KSP is distribution and derivation, where everyone already shares a single key. Assumes provisioning of group key.
Requires another protocol for getting group key from pair wise master keys.
Bob Moscowitz comment – a lot of track record for this type of approach
Privacy concerns- do you trust the vendor?
Requires access to support resources- backend resources - Somebody needs to create the ACL-
Backend necessary for authorization not for authentication
CA meaning certificate authority, always spell out, so as to not confuse with Connection Association
Big discussion ensued about registration authorities in this context
In conclusion, this work may be better done elsewhere

Wednesday AM, July 14, 2004
Mick Seaman - .802.1AD Interworking
Went over mapping priorities cl 6.7
Joint meeting with 802.3
802.1 update
Kevin Daines – update on Frame Expansion, 802.3 Frame Expansion Ad-hoc
http://www.ieee802.org/3/frame_study
Also got requests from MPLS
Ad hoc met yesterday, 30 people
Frame formats, draft PAR
Concerns raised - Is this really necessary? Are there any alternatives? All the alternate suggestions were patently unacceptable.
Is this a guise to standardize 9k jumbo frames?
Certainly not 802.1’s intent. 802.1 has asked to increase *header* size. It’s a different question whether to increase data size
Backward compatibility
What happens to overall efficiency? QoS? Increased jitter?
Questions for 802.1
Discovery mechanism, or magically work? How did you think this would work?
Do other groups also need additional fields, e.g., 802.17?
UNH has offered to do some testing, experimentation
Ad hoc meeting to request a SG, Vote had 18 participate, 12 separate orgs.
Want to submit a PAR after September, 50 day deadline for December Sec meeting. When and where meet in Sept.? Co-locate with 802.1? or prior week near PA. More people wanted to go to Ottawa.
Interim plans
Vote on who would attend the frame expansion SG at different proposed dates
9/27 – 20 people
10/4 – 36 people
A decision will be made.

Draft liaison response to ITU-T Q9, Q12/SG 15 from IEEE 802.1 and 802.3
Review of the status of the SG.

Wednesday PM, July 14, 2004

Weds afternoon LinkSec and Interworking WGs meet separately
Linksec

John Vollbrecht – 802.1af Discussion
http://www.ieee802.org/1/files/public/docs2004/AFjul04Vollbrecht802_1_a e-af.ppt
Clarification of KSP
  Discovery –
  Beacon every ½ second, to prove liveness, announcing itself
  Review of KaY functions
  Review of EAP and RADIUS issues with respect to KaY functions
  Not clear that using EAP and RADIUS is doable, if doable, it would take a lot of work
  Other option- distribute a weak CAK, the coffee shop model
  Vollbrecht – worries that everyone knows same key, vulnerable
  Protected the network from me, but not protected me from other members of CAK. Discussion of this.
Weak key proposal
  Get weak key, join a provisional CA –
  When get credentials, then get onto the real CA
  Prevents against the most brain dead attacks
Deployment tool
  Not a strong form of security, there to provide services to pull down credentials
Wants to not use RADIUS/EAP
Comments
  Coffee house model
  Model is point to point – makes the big difference
  If shared media- need a muxing method. In worst case, use address

Thursday AM, July 15, 2004
Paul Congdon – Sponsor Ballot comment resolution for 802.1AB
802.1AB Sponsor Ballot comment resolution for comments greater than 72 was covered from 9:00 to 10:30. All AB/D10 Sponsor Ballot comments have been processed at this point and a confirmation ballot will be planned
prior to the next interim meeting.

Allyn Romanow – Task Group Ballot comment resolution 802.1AE
Continuation from Tuesday.

Muneyoshi Suzuki- Per-priority Flow Control
Per-priority Flow Control.pdf

Closing Plenary Thursday PM, July 15, 2004 Closing Plenary,
Agenda – Tony Jeffree
Administrative Stuff – Tony Jeffree
  Officers
  Voting Membership
  Voting Members
  Current Voters
  802.1 WG and TG operation
TG, WG, and Sponsor Ballots
  Presentation to Tony of Certificate of Appreciation dated March 1990 – Mick
Seaman
Patent Policy
  The required two slides were presented and the committee was made
  aware of the IEEE patent policy

Inappropriate Topics for WG meetings

Future meetings
  Ottawa 4-7 Oct
  Jan – Sacramento? –tentatively week of the 10th preferred, 24th second
  choice?
  May – Barcelona? – tentatively second week?
  Sept 2005– not the 8th or the 20th?

Liaison reports
  802.3 Don Pannell
    Kevin Daines writing PAR for extending frame size
    Residential CFI got a lot of support
    When will we meet jointly? 802.3 meeting one week earlier in
    Ottawa. Bob Grow is considering splitting .3 so that CMSG and
    Framesize might meet the same week we do
  802.11 Bob Moskowitz
    Mesh workgroup .11s – security and routing ad hoc design teams,
    Bob M. is moderating the security ad hoc design team. Get in
    touch with him if you are interested. Want to have requirements by
    next plenary, and to have criteria done by November meeting.
    Sunday there was a meeting to define .11 architecture
  802.20 doing security. A few people from 802.1 went. They are doing
  requirements
  802.16 will be getting in touch, see what convergence is possible.
Sanity check on our work Review current PARs and PAR end dates – Tony Jeffree
802.1Q-REV: Must drive this forward ASAP. End date is Dec ’05. Mostly Tony and Mick will work on it and do a Task Group Ballot. Want draft by end of November.

802.1X-REV: Nearly done – should be a done deal by November.

802.1AB: Nearly done – should be a done deal by November.

802.1AC (MAC Service): Initial draft – are we able to make progress on this yet? End date is Dec ’05. – nothing contingent on it. 3 pieces of text. The original MAC Service definition. An ISO standard. ISS definition and EISS definition taken from .1D and .1Q. Stuff to be done to it, consequent on .1AD. Needs updating in light of some current work, security in particular.

802.1ad (Provider Bridges): TG ballot. End date is Dec ’05

802.1AE (MAC security): TG ballot. Finishing depends on .1af. End date is May ’06

802.1af (Key agreement): Editor’s draft. End date is Dec ’06

802.1ag (CFM): Editor’s draft. End date is July ‘07

Web page needs to be updated – John Messenger

Motions

802.1 approves the March ‘2004 and May ‘2004 meeting minutes.

802.1 Proposed: Romanow
Second: Congdon
   – For: 24 Against: 0 Abstain: 2
   Allyn will remove website username and password from March notes

802.1 appoints David Frattura as liaison to TIA TR41.4
802.1 Proposed: Congdon Second: Seaman
   – For: 23 Against: 0 Abstain: 2

802.1 resolves to hold an interim session in Ottawa, Mon 4th October 9:00 AM through Thurs 7th October 5:00 PM, hosted by Nortel
Proposed: Parsons
Second: Congdon
   – For: 25
   – Against: 0
   – Abstain: 1

802.1 resolves to hold a pre-meeting on the Monday morning of the November 2004 plenary session.
802.1 Proposed: seaman
Second: Finn For: 24 Against: 0 Abstain: 0

802.1 requests conditional approval from the SEC , as per current P&P, to forward P802.1X-REV to RevCom following completion of further recirculation ballot(s).
802.1 Proposed: Bell Second: Sala
   For: 25 Against: 0 Abstain: 0
SEC Proposed: Jeffree, Second:
For: Against: Abstain:

802.1 requests conditional approval from the SEC, as per current P&P, to forward the P802.1AB draft to RevCom following completion of the upcoming recirculation ballot(s).

SEC Proposed: Jeffree, Second:
– For: Against: Abstain:

802.1 resolves to assign the following group MAC address: 01-80-C2-00-00-0E, taken from Table 7-10 of 802.1D, as the “all stations this LAN” MAC address, and the OID arc value “2” for use in P802.1AB.

SEC Proposed: Jeffree, Second:
– For: Against: Abstain:

802.1 instructs the Second editor of P802.1ad to prepare a further draft taking into account the discussions during the July 2004 meeting, and issue the draft for a further Task Group ballot.

SEC Proposed: Jeffree, Second:
– For: Against: Abstain:

802.1 authorizes its October interim meeting to further develop the “Media Converter” PAR, and to instruct the Chair to forward the PAR to the SEC per the 30-day rule, should the proposal be considered by that meeting to be ready to go forward.

SEC Proposed: Jeffree, Second:
– For: Against: Abstain:

802.1 approves the attached liaison statement to ITU-T SG13 regarding LLDP.
Proposed: Congdon Second: Finn
For: 19 Against: 0 Abstain: 0
Text of statement from 802.1 to ITU-TSG13 regarding LLDP:

To ITU-T Q.16/13
Ref: COM13-LS05-E
From: IEEE 802.1

IEEE 802.1 appreciates the need of the edge router to discover the topology of an attached bridged network. Some explanation of the purpose of IEEE P802.1AB Link Layer Discovery Protocol is in order:

1. The function of LLDP is to collect the data from which the topology of the network may be deduced. The transmission of the collected data to a central location is a separate problem, one with well-known existing solutions (e.g. SNMP), and is therefore out of the scope of LLDP.
2. All information passed by LLDP must fit into a single data frame.
3. LLDP cannot pass through a bridge, so is restricted to a single LAN.
4. LLDP is prohibited from relaying information from one port to another port on one device, and therefore prohibited from relaying information through a bridged network.
5. LLDP is not a stimulus-response protocol, but an advertisement-discovery protocol. LLDP typically runs on a 30-second transmit timer. Therefore, it may not meet your expectations for timely and reliable collection of topology information.

These restrictions on LLDP are purposely severe. The amount of information that one device might want to know about its neighbor is very large. Therefore, the purpose of LLDP is to provide the minimum amount of information required to make it likely that a system administrator with access to one device can acquire enough information about a neighboring device to enable the administrator to access that neighbor device with further queries. By minimizing the complexity of LLDP, the probability that implementers will include LLDP in their products is maximized. The collection function described in TD 24 Rev. 1 (WP 2/13), Annex A, point (2), lies out of the scope of P802.1AB.

We would point out that, if a Layer 2 solution for the collection function is required, there exists an Ethertype for carrying SNMP queries and responses at Layer 2. Also, at Layer 3, SNMP can be transmitted over TCP, rather than UDP, in order to simplify the reliable collection of data.

As to the three specific data items you mention for inclusion in LLDP:
1. The spanning tree state of a device is available in that device's Bridge MIB.
2. The link speed is available in the Interfaces MIB, as well as the 802.3 Auto-negotiation TLV.
3. The full/half duplex state of a port is transmitted through LLDP, in the 802.3 Auto-negotiation TLV, described in Annex G of P802.1AB Draft 10.