IEEE 802.1 Minutes, March 2004

Pre-Meeting Monday, March 10, 2003

LLDP – meeting concurrently for ballot review
MACSEC
Review of IEEE P802.1AE D1-2 Frame Format – Mick Seaman

- Look at proposed header/frame format of the MACSEC
- Do some background on how we got here so folks understand what is going on
- Review of section 7
  - What are we trying to code in the frame
  - Section 6 is what does MACSEC means to us
  - Only saying the folks plugged in are allowed
  - Not saying anything else – nothing about MAC addresses
  - Number of security relationships
  - Review of Figure 7-3
    - Why two one-way secure channel instead of one two-way secure channels
      - Keys are only one way and this with will scale to point to multipoint
  - Figure 7-6
    - Discussion – this can be done with one key (John V)
    - But if the key changes for one then must change for all (Mick)
  - Figure 7-7
    - How Secure Channel Identifier (SCI) is formed from what pieces

Frame Format Slide presentation – Mick Seaman

- SecTAG – some header information followed by secure data and an ICV trailer
- With GCM no change to the size of the data
- Other algorithms will increase up to a block size
- How many bits for ICV?
  - Not clear if 64 bits or 128 bits
- SecTAG identifies the secure channel and replay protection
- Back to Length of ICV
  - This is a discussion item. Probably need 128 bit
- Replay attacks have time sensitive so this will affect the size of the ICV
- Since some 802 media have high rates the ability to replay is inversely proportional to the size of the ICV
- Now the discussion is should the size be 12 or 16
  - Get the extra bits now – 16 bits
  - If 12 or 16 is there a compatibility issue with algorithms that use 8
    - If 8 pad the extra bits
  - SECTag format
  - SCI optional – if multipoint or for debugging (who is putting this stuff on my network?)
  - Replay number
  - SL – short length

- TCI – tag control information
- AN – association number
- SAI – composed AN + SCI
    - EPON only needs AN case
    - 32 bits for PN gives 10 minutes protection for 10 gig Ethernet
- Short Length issue
- Ethernet requires 64 bits but no length. Can't in general tell from the MAC
- Must know the frame length to get the ICV location
- TCI & AN
    - TCI is 6 bits
    - AN is two bits
    - TCI bits
    - Version number bit
    - ES – end station bit can get the SA from source MAC address
        - SC – secure channel is present in the tag
        - SCB – single copy broadcast – for EPON support
            - Why does MACSEC needs this information
                - Good mapping to EPON
        - Caveat – given that the foundation is shared key SCB channel does not assure you that frame was transmitted by the OLT. There is a way to break in to the SCB channel. SCB is has weakness in a provider network. If using SCB don't use it for control traffic of the network infrastructure because of this weakness. This is providing communication security not authentication of the transmitter
- SecTAG issues
    - Review of the current view of SecTAG issue

<u>Review of 802.1af Functional Architecture – Jim Burns</u>

- Functional overview of what will be in af and how they will work with ae
- Discovery component
- Authentication component
- Authorization phase
- Enable session phase – key exchange to get transient keys
- Discovery discussion
    - Topics that are being discussed
    - Job to find potential connections
    - Want to avoid DOS attacks
    - Should discovery be secured
        - Discovery has not been authentication
    - Discovery is viewed as hints
        - What cipher suites sender can accomplish
    - Discovery has to be ongoing
    - Discovery must be fast

It appears that the discovery is building a protocol. May not be needed the discovery can use things going on around it to figure out what is going on in the network.
More to discovery than simply defining a protocol that everyone obeys.
There are cases where you discover that you can not start the security stuff because not all nodes on the network have been updated to run the secure stuff.
Need to keep discovery and security apart – Mick

Key caches need to be clarified

Authorization
In some cases authorization is same as authentication
There are preconditions that must be defined and understood
Need to have a clear indication of failure of authorization and authentication. This makes it administration easier

What is discovery?
What is going in and out of the discovery component?
Three main users - network, which creates a list of ports in the making.
Higher layer, which controls which "ports in the making" gets turned into ports.
Other .1af processes need access to discovery to control when discovery starts really searching for others.

What information is passed back and forth?
SecY to KaY
List of cipher suites
Connection types – point to point or point to multipoint
Impending exhaustion of keying material
Operstatus – link down
Indication that one SAI in an overlapped pair of SAI has been retired – a change of key has occurred
Indication exhaustion of PN
Is this really needed since key exhaustion covers this case
Need to be more specific on what impending exhaustion means
Need a cipher suite independent state machine
KaY to SecY

Opening Plenary, Monday, March 15, 2004

Agenda – Tony Jeffree

Administrative stuff – Tony Jeffree
Officers
Chair and Vice-Chair reaffirmation/election
Happens every 2 years
Cannot be re-elected more than 4 times
Both Tony and Paul are planning on standing for re-election
Will vote Thursday
Voting membership
How to achieve and maintain voting membership
Rules are still broken – 75% of meetings per session

- 3 qualifying sessions (2 must be plenaries)
- Voting rights are properly regarded as an obligation, not a privilege
- Task Group ballots will now be included in order to maintain voting membership. There has not been enough response to previous task group.
- You can submit a "lack of expertise" to maintain voting rights. Lack of time vote will not maintain voting rights.

802.1 WG and TG operation
- Consensus process
- No RR
- Offline discussions are essential
- TG ballots for most of the time. WG only when nearly done

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

May Interim – Barcelona, 17-20 May
- Will need a headcount

September Interim – need to start thinking about

Liaison reports
- 802.3 Don Pannell presentation on website
- 802.11 Bob Moskowitz
  - Mesh networking – 802.1x will have issues
- IETF – Paul Congdon
  - Discussions about how to share information between IETF and IEEE
  - A formal process is being put in place
  - MIB work – the MIB work should be done in IEEE, which is how things are working but what about the old stuff. The bridge MIB is outdated and needs some update
  - Will need a coordinator in 802.1
  - How to manage MIBs
  - Do we need a PAR to do the bridge MIB?
    - Yes, but need folks to do the work.

<u>Executive Committee Report – Tony Jeffree</u>

802.21 Handoff – approved PAR

Last 2 meetings surplus – may adjust registration fees downward

802.1B, 802.1E, and 802.10 withdrawn
- 802.10 is looking to disband

802.1D-2004 approved

802 Task Force – meets Tuesday 2-3

New liaison person from IEEE to 802 Amy Icowitz

Indemnification update

Get IEEE 802
- 1.4M downloads, YTD 86K downloads, Financials on target

Corporate Advisory Group
- Issue with how projects have corporate sponsorship

- Is it a valid for CAG to sponsor a project that was denied by an existing working group?
- SA voting rules
  - Votes via email require majority of the voting membership for approval
    - Abstains will count with no votes
    - We will have some bits of changes to make sure we follow the letter of the new rules
  - Could be a problem for ballots if we run the 50% return rule
- Financial workshop
  - Is there a way for IEEE 802 to support interim meetings?
  - Each working group would work with Face to Face directly
- Re-elections
  - Geoff Thompson standing down as vice chair
  - Bill Quackenbush continuing as Treasurer but not for full 2 years
- 802 reorganization
  - Keep it together or split into wired/wireless tracks
  - Meeting Tuesday 9-11

Agenda for rest of the week – Mick and Dolors

- Monday
  - 9.00 – 10.30 LLDP
  - 9.00 – 10.30 MACSec
  - 1.00 – 3.00 Opening Plenary
  - 3.30 – 5.00 Frame Size Requirements
- Tuesday
  - 9.00 – 10.30 .1ad provider bridging ballot resolution
  - 11.00 – 12.00 .1ad drop precedence breakout
  - 11.00 – 12.00 LinkSec
  - 1.30 – 3.00 .1ad Drop precedence
  - 3.30 – 5.00 .1ad Provider Bridges
- Wednesday
  - 9.00 – 10.00 .1ag Connectivity Fault Management PAR
    - Other WG and ITU input consideration
  - 10.30 – 12.00 Joint meeting with 802.3
  - 1.30 – 3.00 .1ad breakout 2
  - 1.30 – 3.00 LinkSec .1af Architecture/General Structure
  - 3.30 – 5.00 LinkSec .1ae MACSec – progress towards next ballot
- Thursday
  - 9.00 – 10.30 .1ad Provider Bridges – D2 ballot resolution/wrap up
    - .1ag presentation
  - 11.00 – 12.00 .1af KeySec
  - 2.00 – 3.30 Real Time Ethernet Presentation
  - 3.30 – 5.00 Closing Plenary

<u>Major Objectives for the week – Mick Seaman</u>

- .1ab – conclude WG confirmation ballot, request approval for Sponsor ballot, run another WG confirmation ballot

.1ac – MAC service definition – no work at this meeting. Work on .1ae has helped this effort along, plan par time extension
.1ad – Provider Bridges – progress key topics from task group ballot
Disposition of comments
Dropped precedence
SVID size
.1ag – Connectivity Fault Management – Progress PAR
Security Objectives
.1af KeySec agreement on top level architecture and formulate requirements
.1ae MACSec Document in editing/D1.2, TG ballot before next meeting
Editor collecting guidance for next ballot

Frame Size Requirements – Tony Jeffree

Run through of what we will be talking to 802.3 Wednesday
Frame size and related issues relative to 802.1ad, 802.1ae, and 802.1ab issues
Issues related to 802.1ad and 802.1AE that affect 802.3
Issues with 802.1ad
Issues with 802.1ae – inclusion of security header, minimum frame size, relative placement of Link Aggregation and MACSec
Minimum frame size problem
No explicit length in Ethernet frames
Relative Placement of Link Aggregation and MACSec
MACSec may well need to operate below Link Aggregation
Link Aggregation has to see unencrypted data
Why MACSec should remain MAC independent?
Issues related to 802.1AB
EtherTypes is not define anywhere in 802
802.3 needs to define and explain what it is - the 802.1 standards then point to the correct reference

Tuesday AM, March 16, 2004

802.1ab d8 – Ballot Review – Paul Congdon

The official ballot disposition is at http://www.ieee802.org/1/files/private/ab-drafts/d8/IEEE%20P802.1AB-D8%20proposed%20comment%20resolution.pdf

802.1ad Disposition of comments – Mick Seaman

The official ballot disposition is at http://www.ieee802.org/1/files/private/ad-drafts/d2/802-1ad-D2-pdis.pdf

SVID size issues – some are saying it needs increasing and some say it is fine were it is. A simple vote will not solve this problem; the committee must come to a consensus. 802.1 will avoid the path of creating an option that would allow both sides but create interoperable problems in the field. What are the architectural issues? This is the way to make progress finding a solution to the SVID size problem.

Disposition of Comments

Number of comments with regards to terminology and definitions
Discussion of MEF service model and how provider bridges map to this service model
Where is the boundary between the service provider and the customer's equipment?

The provider bridge model is a response to allow customer's bridge network to work.
If this does not work with MEF then the MEF service model will not work with bridges.
The issue is where you map the MEF UNI or the ambiguity of where the UNI maps to the provider bridge model.
The MEF service model can be extended – the problem is terminology

Edge ports

Mick has made minor changes in this area. Provider port, provider edge ports, and customer's port makes it easier to write the document. If anyone has concerns or thoughts let Mick know

Acceptable frame types

Comment 21 – Admit Only un-tagged frames make it optional for customer bridges and optional or required for Provider Bridges
This is a small but useful changes and Mick believes it should be accepted. Folks should think about this and be sure it is okay.

SVID Size

Number of comments in a couple of groups

Global VID space versus uniqueness in a individual Provider Bridge network

This can be extended without interoperable problems

There is a difference running a network that renumbers at each link versus a network that renumbers at the edge
No one disagrees that for public service 4096 VIDs is sufficient. How do we extend?
Need to share a lot more information about how we anticipate using this many VIDs.
If one implements 802.1s bridges in a naïve manner then yep 4096 is the limit. If you think about it you can make large bridges by making certain observations about 802.1s
To make the world interoperable then you will have a version of IP – the best world is bridges at the edge and IP in the middle. Hard to make interoperable with a large VID size
Have to consider the types of technologies and provisioning of services. Plug and play will not be as big of an issue in provider networks.
One thing to look at is what traffic a bridge sees and what ports are seen by the bridge.

<u>Discussion about model and scope of the standard</u>
There is a bridge and a wire – what we do not want to do is believe that all services must be preformed at the bridge level.
Circuit technology has always been add a port
Discussion about how to map bridges to existing core network protocols or how to map bridges/customer networks to provider service instances
Provider Network providers want to see how to map bridges to their problems – this is a problem for vendors not for the standard. If provider says this how I want my network to work folks are going to have to understand how provider bridges fit into all of the protocols. There is limit to what we can standardize – the standard can not define the world. We need to limit the scope to get a basic standard and if folks want more then raise a PAR and do the work
When talking about increasing SVID size it is to allow protection switching.
The question is within the scope of provider bridges can we increase the SVID size? Is this a desirable goal of this group?

If increasing SVID size then can not provide more services – will need some connection oriented services
Every port on bridge has a 4K vector (2bits per VLAN) 24 bit size requires 16 million vectors. It is a problem to change 4K vectors – 16 million would be a bit of work. Every provider wants a count of packets per port. Increasing the size has ramifications beyond simple the size of the SVID. Everyone agrees that the 4096 is a limit but disagrees about how to fix. This process tedious – remember the .1Q issues – after we got through it things worked!
.1ad is to a standard with some interoperability quickly – in another effort we can work on SVID size.
There are many economic ramifications to increasing the SVID size.
Different angles – scalability – if the SVID size is larger then what are the costs? Need to look at. There needs to be a conversation about how to push bridge configuration protocols.
At 11am the committee divided into two sections – dropped precedence and .1af

802.11i, a Retrospective – Bernard Aboba

http://www.ieee802.org/1/pages/linksec/meetings/Mar04.html
Hints to .1af based on 11i experience
Rfc3748 – EAP threat model, generic set of threats for EAP methods
DOS vulnerability is a problem
- Leveraged attack – one message causes a lot of pain
- Un-leveraged attack – many messages are necessary

We should have a colored diagram that shows relationships
Performance – what is the backward compatibility?
- .1af needs to think about whether we are designing for Greenfield or need to be backward compatible. If so, need a transition path

TKIP – what can be done on any chip set? Now TKIP is being rejected because it does not handle DOS attacks.

Another more conventional proposal, slower than TKIP, was rejected and TKIP was chosen. It had worse integrity check properties. It was a bad choice.
- Now, proprietary alternatives are being employed.
- The criteria for acceptance should have been integrity checking strength.

Hardware always improves overtime, this has implications for design
Discovery wasn't secured – a big mistake
11i doesn't secure management or control. They will have to go back and fix it.
What is meant by protection? Integrity? Needs to be thought through carefully

EAP methods
- .11i does not have one mandatory EAP method to implement. Because of where they were in the standards process, they felt they could not choose one to be mandatory. But this had a lot of implications.
- Need an authentication server.
- They are doing requirements for EAP method only now

Explosion of EAP methods, then drafted the requirements, methods had to be revised. Now on the third generation of EAP methods.
Interoperability problems
If a method is insecure, it is worse than WEP
It is most important to define a mandatory EAP method
See requirements draft-walker-ieee802-req-00.txt
What EAP methods should we consider? Follow the draft walker and get the IETF to help, he suggests

11i authenticated key mgmt

4 way handshake
Eventual synchronization between parties
Group key only goes one way, only AP can multicast, but when went to peer to peer they had a problem
Communication originated by authenticator, but supplicant had to go first
Actually a 6-way exchange, a lot of redundancy, two protocols doing the same thing.
Took too long.
Roaming application complained
Keys need to be deleted as well as installed

We should draw simple box diagrams so everyone understands
General discussion that .1af would like to do something correct and useful, even if it takes longer.

Mick - wants to separate out discovery from the rest of the security functionality, and have no dependence.
We will be able to have outside review of the document before standardization
802.1 policy is that the doc can be released to anyone who wants to review it.
.1af can not be seen as a replacement for .11i
Need a narrow scope so we can figure out what we are doing

Tuesday PM, March 16, 2004

IEEE 802.1af Goals and Requirements – Jim Burns

http://www.ieee802.org/1/pages/linksec/meetings/Mar04.html

usage cases (NAS – Network Access Server)

NAS to NAS
End Station (ES) to NAS

3 categories –

provider enterprise
provider bridge
remote access – access device has access point, NAP, with a number of SPs behind it

.1af goals – provide and manage a cryptographic key framework to provide keys to SecY
Typical phases – diagram following Bernard's slides, all running at the same time
Discovery continued

Suggestion to use the word "announce" instead of "discovery", discovery is too loaded a term

Multicast announcement from access device
What capabilities the access device can provide
Tends to be a long process if not designed correctly – this would impact roaming negatively
Come on to the network, need to find out what's available.
Station sends a multicast announce request to find what capabilities are available
Response is unicast to the station
Why do unicast rather than multicast? Someone else could hear the multicast. Unicast protects against certain kinds of attacks.
What is .1af discovery all about? It enables other layers to feed information between devices.
Similar to how .1X leverages higher level for authentication
Provides a limited way for higher layers to pass information

Differences in the Bridge to Bridge case, than the host to Bridge case
Bring link up for a period of time in the absence of a back end server. Two bridges talking – they have a shared secret already set up – a PMK - Pairwise Master Key.

The process of authentication means to create a key from nothing, as distinct from key management, where the key already exists, and you refresh, etc.

TSK, Transient Session Key is done by the key management function.
There are two ways you could think of getting the TSK from the PMK. In one case, someone distributes the TSKs. But a second way is better – each member calculates the TSKs for themselves, derived from the PMK that they share.
Implicitly derived. In this case, the members have to agree which sequential derivative TSK they want to use. You can use the secrecy from the existing TSK, to set up the next one.
Send an AN, the stations derive the TSK for themselves.
This part must be in .1AE– the state machine for installing the TSK.
Have to make sure maintain up state as switch TSKs.

Announcement Phases
A special phase – announce, authenticate, authorize, do key management
Announcement goes out to all ports
Original physical port transmits and receives
Create virtual port from the pool of potential ports, (PITM)
Pool of ports on ES consists of one port
Pool of ports on access device, can be 50 ports
Announcement process runs continuously and collects PITMs
Information is passed back and forth during the announcement stage, and when done, have a list of PITMs
Second phase is port selection, which is done at a higher level than the KaY.
Notifies SecY, .1AE, which allocates the port
Need to describe how to do allocation, what if not enough ports are left?

What do you do when the port is dead?
Rule- never use your last port, on the network side

Goals of announcement- provide sufficient information for .1af to decide on another .1af entity to which to connect. Provide no more information than that.
The end result is a port on which the remaining .1af processes shall operate

Requirements:

-Do at maximum rate of announcement that does not constitute a DoS attack. Limit DoS impact. Use the maximum possible rate that leaves rest of processes runnable. Can expand if no other work is to be done. But can't take all resources and starve other processes.

-Assume announcement unprotected, but don't preclude use of separate protection for Discovery

There is not protection prior to authentication – but there could be. There could be network access device authentication. How discovery is protected is not in the scope of .1af.

Not mutually authenticated – the connection between ES and access has no mitm attack – but nothing else can be said.

In general, in the bridge to bridge case, what kind of security screen is provided is contextually dependent.

NAS can have a credential. But don't require a credential to run .1af

If discovery is protected, it would protect against some of the DOS attacks that we are not dealing with. For example, can buy a network access card in a coffee shop.

Trust is between NAS and ES, or NAS and NAS

-EPON control frames may need to be protected.

This needs to be carefully looked at on a case by case basis. Consideration of protection in EPON against DoS attacks should be taken on the side, not part of the standard, but perhaps an annex.

It is possible can't secure EPON control in some cases without some re-design. Needs to be examined carefully.

We make no claim about security prior to discovery, or prior to authentication

At what point in the dialogue can start protecting?

WRT EPON, for example, the KaY can deliver key material (PMK) below to the MAC (not as part of the AE standard). Then if EPON wants to protect control frames, say, after the network is up, they can bind the same crypto to our framework. Can use the same crypto framework developed by .1AE.

Plugins to the standard. We want to "hold close" some of the technology and not vary it, but we can have plugins to use the system.

More announcements requirements

-Announce capabilities

-Announce distinguished names

For each NAP, announce distinguished names for SPs

-Fast delivery of announcements when asked

Network solicitation is a better term

TLV's What do we mean by distinguished names?

Could have a normative annex with TLVs
Could not allow vendor specific extensions
All ports, port
Creation of a port ISS MILSAP
Minimal process – limit DoS impact

Announcement information
What are the supported authentication methods
What are the supported cipher suites
Optional – announcement key, outside the scope of.1af- securing prior to discovery
Send a key ID
Protect this information, put in TLV a signed hash and key ID for integrity protection.
An index into a local key store
Is the authentication method an EAP method, or .1af frames, or https, or what?

Authentication Goals
Enable identity verification via higher layer, don't do it ourselves

We are trying to secure communication on the LAN. Result of authentication is the PMK

Mick- if we use an EAP method, we will want to incorporate it in our standard.
Does not want to specify an interface to a higher layer that we are hostage to – doesn't want it in another standard, wants it defined in .1af
Want to control one method.
Entity that runs the EAP is in the KaY, means we will understand the addressing requirements. Must tie to port, the .1AE data structures are in the port.
Is this a 3 party or 4 party model? A crucial distinction
Central management component, network access device, end station– 3 entities

Mick – argues authentication and authorization are intertwined
Where there are chains of SPs, what's .1af's role?
May assume a particular business model

Wednesday AM, March 17, 2004

Connectivity Fault Management
Will give a tutorial in the July meeting

Liaison report for Ethernet OAM – Hiroshi Ohta
Presentation is at http://www.ieee802.org/1/files/public/docs2004/Mar04-liaison-ITU-T-SG13-Q3.pdf
http://www.ieee802.org/1/files/public/docs2004/3-033.pdf current draft Ethernet OAM
Consider a joint interim in September

Ethernet OAM – Dinesh Mohan

Presentation is at http://www.ieee802.org/1/files/public/docs2004/ieee8021-Eth-oam-v0.ppt

Metro Ethernet Forum OAM – Matt Squire

Presentation is at http://www.ieee802.org/1/files/public/docs2004/MEF-IEEE-2004-03-121.ppt

Joint meeting with 802.3 – Tony Jeffree

Presentation is at http://www.ieee802.org/1/files/public/docs2004/Joint%20802-1%20802-3%20tech%20plenary.pdf

Request sent to 802.3 is http://www.ieee802.org/1/files/public/docs2004/8021%20Frame%20Size%20Revision%20Request%20to%208023.pdf

Four Issues

- Frame size
- Position of Link Aggregation
- Minimum frame size
- TLV used by 802.3 in 802.1ab
- Presentation is at http://www.ieee802.org
- Frame size expansion
  - Looking at increase 24 octets point to point and 32 on multipoint for MACSec
  - Provider Bridge TAG will require 4 octets
  - 32 Customer security tag
  - 32 Provider security tag
  - 4 Provider TAG
  - Caveats
    - Federal cipher suite requirements
    - Request for provider tag size and duplicate FCS have not yet been resolved
  - Wider frame size problem
    - Other technologies will ship bigger frames
    - Any oversize frames will be limited to IP
  - Discussion of the problem
    - Customers do not like 1500 byte limit, chip vendors need an absolute size – every one supports that number end of problem
    - Disagree in degree – disagree that “genie is out of the bottle” with regard to 802.3 control of frame size.
- Link Aggregation and MACSec
  - Link Aggregation requires unencrypted frames therefore MACSec must be below Link Aggregation
  - Discussion
    - Can setup statically so don’t need MACSec below Link Aggregation
    - Should have all the protocols work together
- Minimum Frame Problem

No frame length when EtherTypes/Length field is used as EtherTypes

802.1AB Issues

802.3 related TLVs

This is looking at values in the MIB that should not change but the MIB will always be changing

EtherType

EtherType has not been defined – needs to be defined 802.1 believe it should be defined in 802.3

Back to Frame Size Problem

How to proceed?

Needs to be a project

Need someone in 802.3 to handle the project

There is some work to figure out how to word smith

May not be useful to include frame format

Do not want to give the world a way to increase payload

It would not be a problem if this did not complete until March 2005

Thursday AM, March 18, 2004

Agenda for the day

.1ad – d2 ballot resolution

.1ag presentation – already happened no more time needed

.1af no more time needed

Real Time Ethernet – do it earlier

11 am for the plenary

Real Time Ethernet – Ludwig & Karl

Industrial automation application

Presentation is at http://www.ieee802.org/1/files/public/docs2004/IEEE802.1_RTE_Classes20040114_e3.ppt

Discussion

What to do now?

802.1 could create an addendum to support IEEE 1588 and redo the priority scheduling scheme so vendors could add this.

This is a distinct market

Folks are going to check with hardware designers to see how much trouble

We can see the scope of the work for this project

We would need some outside source to analyze the failure modes of the system – because of the environment we need to do good due diligence to make sure things fail safely

Before we take this on need to make sure these folks are available and willing to do the work

Closing Plenary, Thursday, March 18, 2004

Agenda – Tony Jeffree

Officers – Tony Jeffree

Voting Membership – Tony Jeffree

Voting Members – Tony Jeffree
Administrative Stuff – Tony Jeffree
Chair and Vice-Chair reaffirmation – Tony Jeffree
Are there any other candidates for Chair?
None
Are there any other candidates for Vice-Chair?
None
Presentation to Tony of Certificate of Appreciation dated March 1990 – Mick Seaman
Patent Policy – Tony Jeffree
The required two slides were presented and the committee was made aware of the IEEE patent policy
May Interim – Barcelona May 17-20
Thanks to Dolors and Norm
Headcount of those who will probably attend 35
Liaison reports
802.3 Don Pannell
Back plane study group
The current PAR does not have congestion management
There will be a motion to create a study group to study congestion management
Majority of the focus has been electrical – they want to get that part going forward
Don is drafting a proposal for frame size to go to 802.3
EtherType issue – already in the queue for 802.3
802.11 Bob Moskowitz
802.11s (mesh networking) PAR will probably be approved
Discussion about will the standard be stand alone or addendum
Standard will use infrastructure and not ad-hoc
Security can not be met by .11i they will need to use .1af
Discussions and issues about hopping
They will need some support for 802.1 to make sure the internetworking will not be broken
IETF – Paul Congdon
EAP updates is now RFC 3748

Motions

802.1 requests that the SEC affirm the appointment of the following Officers of 802.1:

- Chair: Tony Jeffree
- Vice-Chair: Paul Congdon

Proposed: Lane
Second: Romascanu

- For: 32
- Against: 0
- Abstain: 0

802.1 resolves to hold an interim session in Barcelona, Mon 9:00 AM through Thurs 5:00 PM of the week of 17th May 2004 (17th through 20th May), hosted by Dolors/Norm
Proposed: Wright
Second: Finn
- For: 31
- Against: 0
- Abstain: 0

802.1 approves the November '2003 and January '2004 meeting minutes.
Proposed: Wright
Second: Lane
- For: 29
- Against: 0
- Abstain: 1

802.1 resolves to hold a pre-meeting on the Monday morning of the July 2004 plenary session.
Proposed: Wright
Second: Lane
- For: 29
- Against: 0
- Abstain: 2

802.1 requests conditional approval from the SEC to forward P802.1X-REV to RevCom following completion of the Sponsor ballot that is currently in progress and any recirculation ballot(s) that may be necessary.
Proposed: Wright
Second: Burns
- For: 28
- Against: 0
- Abstain: 0

802.1 requests conditional approval from the SEC to forward the P802.1AB draft for Sponsor Ballot following completion of the upcoming recirculation ballot
Proposed: Lane
Second: Wright
- For: 28
- Against: 0
- Abstain: 1

802.1 instructs the Editor for P802.1ab, Bill Lane, to issue the next draft for Working Group recirculation ballot by April 15th, 2004
Proposed: Lane
Second: Wright
- For: 30

- Against: 0
- Abstain: 0

802.1 requests permission from the SEC to forward the P802.1ag "Connectivity Fault Management" PAR to NesCom
Proposed: Wright
Second: Finn
- For: 31
- Against: 0
- Abstain: 0

802.1 instructs the Editor for P802.1ae, Allyn Romanow, to revise the document taking account of the discussion during this meeting and to issue the revised draft for Task Group ballot by 1st May 2004.
Proposed: Romanow
Second: Wright
- For: 26
- Against: 0
- Abstain: 2

802.1 appoints Craig Easley as a second liaison to 802.3.
Proposed: Pannell
Second: Lane
- For: 28
- Against: 0
- Abstain: 1

802.1 approves the attached liaison statement to NIST regarding GCM.
Proposed: Seaman
Second: Wright
- For: 25
- Against: 0
- Abstain: 6

802.1 requests approval from the SEC to send the attached liaison statement to NIST regarding GCM
Proposed: Seaman
Second: Wright
- For: 22
- Against: 0
- Abstain: 4

802.1 approves the following liaison statement to ITU-T SG13 Q3:
802.1 values the ongoing collaboration with SG13 Q3, and thanks SG13 Q3 Rapporteur, Hiroshi Ohta, for attending our March Plenary meeting and presenting your liaison contribution.

We have generated a Project Authorization Request to initiate work on Connectivity Fault Management; we will keep SG13 Q3 informed of our progress with this project, and will value input from you as the project develops.
Given that both SG13 Q3 and 802.1 are considering holding an interim meeting in the September timeframe, 802.1 would welcome the possibility of co-locating those meetings in order to provide further opportunity for collaboration between the two groups.
Proposed: Wright
Second: Lane

- For: 25
- Against: 0
- Abstain: 3

802.1 requests the SEC to approve the following liaison statement to ITU-T SG13 Q3:
802.1 values the ongoing collaboration with SG13 Q3, and thanks SG13 Q3 Rapporteur, Hiroshi Ohta, for attending our March Plenary meeting and presenting your liaison contribution.
We have generated a Project Authorization Request to initiate work on Connectivity Fault Management; we will keep SG13 Q3 informed of our progress with this project, and will value input from you as the project develops.
Given that both SG13 Q3 and 802.1 are considering holding an interim meeting in the September timeframe, 802.1 would welcome the possibility of co-locating those meetings in order to provide further opportunity for collaboration between the two groups.
Proposed: Lane
Second: Wright

- For: 27
- Against: 0
- Abstain: 2

802.1 Dropped Precedence

The presentation is at 802-1ad-DropPrecedenceArchitecture-Haddock-v3.ppt
Discussion about how to map drop precedence to traffic classes
Switch from the detail to have a sane method of proceeding

802.1 instructs the editor of P802.1ad to prepare a further draft taking into account the discussions on Drop Precedence at the March 2004 meeting, specifically including

- optional support for drop precedence within the existing priority bits

- optional support for drop precedence encoding in the 'CFI' bit

- rules to ensure no frame misordering within a priority

- extension of the EISS interface parameters to include drop precedence

Proposed: Seaman
Second: Haddock
- For: 21
- Against: 0
- Abstain: 2

802.1 requests Don Pannell to submit the 802.3 revision request, as presented, and with changes to be made as discussed, to 802.3 for their consideration.
Proposed: Pannell
Second: Finn
- For: 21
- Against: 0
- Abstain:3

Motion to adjourn
Proposed: Wright
Second: Messenger
Unanimous

The following attended one or more meetings during the March session:

Glenn Algie
Paul Amsden
Paul Amsden
Siamack Ayandeh
Florent Bensami
Rudolf Brandner
Jim Burns
Nancy Cam-Winget
Dirceu Cavendish
Charles Chen
Girish Chiruvolu
Su-il Choi
Jacob Christensen
Paul Congdon
Sharam Davari
Craig Easley
Anush Elangovan
Hesham Elbakoury
David Elie-Dit-Cosaque
Lars Ellegard
Norm Finn
David Frattura
Steve Haddock
Fred Haisch

March 2004 Orlando, FL

Onn Haran
David Harrington
Ran Ish-Shalom
Tony Jeffree
Ulf Jonsson
Mohan Kalkunte
Samian Kaur
Tetsuya Kawakami
Yongbum Kim
Shobhan Lakkapragada
Bill Lane
Loren Larsen
Yannick Le Goff
Marcus Leech
Seyoun Lim
Fabio Maino
Bob Mandeville
Bill McIntosh
John Messenger
Katsuya Minami
David Minodier
Dinesh Mohan
Bob Moskowitz
Dave Nelson
Don O'Connor
Karen O'Donoghue
Hiroshi Ohta
Don Pannell
Glenn Parsons
Ken Patton
Antti Pietilainen
Karen Randall
Anil Rijsinghani
Allyn Romanow
Dan Romascanu
Jessy V Rouyer
Ali Sajassi
Dolors Sala
Sam Sambasivan
John Sauer
Mick Seaman
Yetik Serbest
Koichiro Seto
Matt Squire
Yoshihiro Suzuki
Michel Thorsen

March 2004 Orlando, FL

Sandra Turner
John Viega
Preeti Vinayakray-Jani
John Vollbrecht
Dennis Volpano
Jesse Walker
Karl Weber
Michael Williams
Ludwig Winkel
Michael D. Wright
Robert Wu
Ilan Yerushalmi