IEEE 802.1 Minutes, November 2003,

Pre-Meeting Monday, November 10, 2003
<u>Agenda – Mick Seaman</u>
<u>L2 Packet Marking for Drop Precedence – Steve Haddock</u>
      Presentation is on the website
      RFC 2597 – Dual rate service
      All packets IP
      Provider bridges have to have knowledge of IP
      Drop service is not priority that is the marking is temporal
      Drop precedence must maintain
      Use the CFI bit
            Look at the consequences of using CFI
            Some bridges do higher Level parsing is disabled if the CFI bit is not set
      Backwards Compatibility Comparison
            Single rate service
      Summary
            Use the CFI bit in Provider Tags to indicate drop precedence
      Relationship to MPLS
            If use CFI there will be a mapping from Ethernet Traffic Class/Drop
            Precedence (TC/DP) to MPLS TC/DP
      Discussion
            The world is IP – make IP fast and don't worry about the rest
            But don't want to tell customer that they have to use IP and if Providers
            are doing Layer 2 provider network don't want to go into the packet to
            layer 3, too much over head.
<u>Bit of where we are and what this discussion is about – Mick Seaman</u>
      Drop Precedent has changed context.
      Right now not talking about redoing the existing Q tag
      May have to redo the provider Tag
      Can not be consistent across a network
      Provider network are not structured networks
      Consistency does not mean the whole network does not handle packets the same
      across the whole of the network
      Do the provider network and see how the drop precedent fits do the enterprise
      "classic" network support for drop precedent needs to be handled as a separate
      problem
<u>Discussion – Ali Sajassi</u>
      Thought process analysis
      This is to see if everybody agrees on things
      Everybody understands the need for drop precedent
      Question is whether the drop precedent is explicit or implicit
      Pros and Cons of explicit or implicit
            Lest disruption to bridges and backward compatibilities
            Optimize for IP

            MPLS already has deployed this kind of functionality

            IP no explicit dropped precedent IP does have DiffServ

            Within a class can not have mis-ordering

            Deployment scenario – MPLS and Frame Relay

            Don't see any advantage to explicit

            Implicit is backwards compatible

        Discussion

            Need a formal presentation

            Encoding section of .1ad needs to be fixed

            Mick would like to close on a draft of the encoding by the end of the week

            Steve and Ali need to create a matrix to see where the problems will occur

            Need to get closer on the things we can agree on

            Probably will have both and will build both

            Discussion about what is the benefit of taking this back into the enterprise

            Ali will go over this with Steve and get a more detailed discussion going so the difference can be understood

            Goal is to get a consensus

             What type of classes and what type of SLAs will be supported

            Mick – goal is give some benefit and do not harm

            Paul Batorf– There are differences between enterprise and provider, so is the drop precedent a benefit to provider and do no harm to the enterprise

            Paul B– we must find a solution for L2 drop precedent may not need to worry about the enterprise

            Paul Congdon – many enterprise folks would like to have some of this functionality

            Paul B – How come enterprise can not simply by provider equipment

            Paul Congdon – that would require a re-architect of the enterprise network

            Need some offline discussions to clear up confusion in the encoding section

Matrix of the implicit and explicit - Steve Haddock

        Discussion about the interface between 802.1Q and provider networks

        Consequence of packets with drop marking arriving at 802.1Q bridges

            If explicit packets either dropped or treated the same as green

                No risk of miss ordering

            If implicit drop precedence not supported Yellow packets either treated the same as green or, if inconsistent configuration, yellow and green may be miss ordered

Opening Plenary, Monday, November 10, 2003

Agenda – Tony Jeffree

Administrative stuff – Tony Jeffree

        Officers

            Neil Jarvis will step down as vice chair at this meeting. Thursday a new vice chair will be elected

        Website

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

            Username: p8021 Password: go_wildcats

Voting membership

> Review of the rules about how to gain an maintain voting membership
> There is a problem in the 802 rules and policy and procedures about voting membership. The 802 exec is working to fix this problem
> 802.1 rules will continue to be consistent with the intent of the 802 rules
> The 75% rule will be five meetings for this plenary

Vice Chair

> Neil has indicated his wish to stand down as Vice Chair of 802.1
> We will have an election Thursday

Need to appoint liaisons from 802.1 to 802.3

> Is anyone interested?
> 802.3 folks have asked who we are going to appoint
> Not for sure someone is needed.

802.1 WG and TG operation – Tony Jeffree

Some comments about how 802.1 works. 802.1 is geared toward building consensus by discussion rather than voting
We do not take votes in working group meetings
Use the document ballot procedures to establish consensus
Hence a formal WG ballot is a test of consensus, which we believe we have
Anyone can comment on a document, working groups are required by IEEE to consider all comments and give those comments a fair hearing
Focus on technical progress rather than some formal process

Patent Policy – Tony Jeffree

Tony showed the two slides required by IEEE office to inform the committee of the IEEE patent policy
The policy is described in Clause 6 of the IEEE SA Standards Board Bylaws.
The policy includes both granted and patents that have been applied for
Tony asked if anyone knew of any patents that were relevant to 802.1

Report on Exec Committee - Tony Jeffree

July – 1370 attendees record attendance
PARS from 802.3, Handoff SG, and 802.1 will be on the Friday SEC agenda

> Is there any discussion – need to be completed by Tuesday 5 pm

802.1 B and E will be officially withdrawn in December
GET 802

> Appears to meet its budget
> Currently it is pilot program the GET 802 folks are going to recommend that GET 802 become a regular program

Need "volunteer" to attend WG/TAG financial workshop, Loren volunteered
There will be a tutorial for editors this evening
Operating rule changes

> Precedent rules and financial operations changes are pretty much done
> Will go out for a vote in a couple of months

802 news bulletin

> Launched March 2001
> Give outside world a better view of what we are doing
> If anyone wants to do this Tony would appreciate it

Hand off
 Media Independent Handover
  The scope and purpose are too much
  Establish as a new working group
 802 reorganization
 Large group and hard to track and control
 Howard Frazier will chair an "ad-hoc" Tuesday 10-12 AM
 Need 802.1 presences at this meeting
 Network service contract update
 Have a contract for continuing network services at the meeting
 Affirmation of 802.20, Wireless access for vehicles, chair and vice chair issue
 Because of IEEE ruling on SEC indemnification (there is not any) several
 members of the SEC departed the room
 The ballot was carried out as secret ballot
 The original officers were allowed to become officers of 802.20
 This is not a good precedent
 The IEEE office is being asked to look at the indemnification issue

Future meetings - Tony Jeffree
 Interim meeting, most of 802, in Vancouver week of the 12, January
 March 2004 venue will be Walt Disney World Hilton, Orlando, week of 14,
 March
 Need to think about in May

Awards – Tony Jeffree
 802a, Playpen Ethertypes, for Mick and Tony

Task Group stuff – Mick Seaman
 Agenda – Mick
  Monday 9 – 10:30 Provider Bridging – drop precedence encoding
  discussion
  Monday 1 – 3 802.1 WG opening Plenary
  Monday 3.30 – 4.00 Interworking (P802.1ad Provider Bridging –
  objectives for the week
  Monday 4.00 – 5.00 Interworking: Provider Bridging – Loop Detection
  (Muneyoshi)
  Tuesday 9.00 – 10.30 Interworking: PB direction to editor for preparation
  of next TG ballot
  Tuesday 11.00 – 12.30 Connectivity Fault Management PAR – discussion
  Tuesday 2.00 – 4.30 LinkSec 802.1x Rev Recirculation ballot comments
  Tuesday 4.30 – 5.00 Interworking (Liaison, NWI/FYI)
  Wednesday 9.00 – 9.30 LinkSec (Response to input from other groups on
  Authenticated Key Agreement PAR)
  Wednesday 9.30 11.30 MACsec Draft
  Wednesday 11.30 – 12.30CWC John Viega
  Wednesday 2.00 – 5.30 Authentication for PONS
  Thursday 9.00 – 12.30 Interworking – P802.1ab LLDP ballot resolution
  Thursday 2.00 – 3.30 LinkSec Security for GRID computing
  Thursday 3.30 – 5.00 802.1 WG closing Plenary

Agenda – Dolores

Provider Bridging – Meeting Objectives – Mick Seaman

Facilitate preparation of P802.1ad for Task Group Ballot

Requires direction on

Current TAG format consistency

Terminology and combination of items: Provider Bridge, Provider Edge
Bridge

Loops Detection OAM for PB – Muneyoshi Suzuki

Presentation is on the website

Problem Statement

Loops fatal in Bridge network

Users can cause loops in PB, whether the providers take precaution

Customer side must not have back door connection else the PB network can be
looped

Discussion

Providers should be able to have a loop detection mechanism

Review of the decomposition of the VLAN problem statements

Can a provider think of these as a single case?

Is the purpose to be a tool for the service provider or for the customer?

The customer would like to know if they are putting too much traffic onto
the provider network

Need to make sure we keep the problem bounded

Loops by customer into the provider network is not as big issue because
customers can generate the same amount of traffic without loops but a
loop in the provider network is really bad

Customers would like to know about this (your phone has been off hook
for five hours)

This is a good proposal that allows providers to add value to their
networks

Don't add loop breaking – this should be loop detection only

One immediate action – need further discussion about how to fit this into
the .1ad architecture

Does this help in any other environment?

Tuesday AM, November 11, 2003

Handoff PAR – David Johnston

Explanation of the Handoff PAR

Media independent handoff

802.1ad Discussion – Mick Seaman

What changes should be made before sending out for TG ballot

Since there is not a consensus on the CFI bit usage Mick will attempt to put both
mechanism in the draft so folks can start commenting and a consensus can be
developed

Paul B had a couple of slides that shows Provider Bridge and MEF network
relations

Paul B. emailed this to the reflector this morning

It will be posted on the web

Two different worlds – Paul is attempting to show how the MEF defines the UNI

Discussion about UNI interface and Provider Bridge

Some issues with terminology - PE Bridge PB Bridge are terms that mean equipment to some folks, Paul proposed P Bridge to be an architecture term not an equipment term

MEF Layer Reference Model – Slide

VB Relay is The Service Aware Component – Slide

Calling the VB a Customer Bridge (CPE) is confusing

The VB could be called a Provider Service Bridge

The term PE should not be used for the VB since the VB is a functional element not a physical device. The VB is the UNI-N component of the provider PE device

Norm had a question about current draft – did not see anything in the draft about a new BPDU address. It is there but obscure – Mick will make it clearer.

P802.1ag - Connectivity Fault Management PAR - Mick Seaman
- Dinesh - Need to address coordination between ITU and IEEE
- Mick - Division of labor: IEEE concentrates 'how to implement the tools' and ITU concentrates on the requirements for the tools.
- Mick - Liasons: Can try to put it in the 5 criteria but probably not in the Scope.
- Richard - liason from .3 to .1 - What about 802.2 tools?
- Mick - We will take into account the failures of 802.2 for broad market appeal.
- Richard - what about tools in EFM being developed in .3?
- Mick - Concentrating on hopping through bridges, not going down into the lower level media type tools.
- Norm - Xid and Test (layer 2 ping, but can be sent to broadcast address) should be discussed in PAR to quell concerns of readers who remember 802.2.

Ethernet OAM study in ITU-T Question 3. ITU-T SG13, Q.3/13 - Hiroshi Ohta
- Norm - Support - we need expertise found in all groups
- Dinesh - Support - specific example for tracert why we need all groups expertise.
- Mick - Wants to put info in the 5 criteria of .1ag about the ITU document Y.17 ethreq to make the liason more concrete.

Tuesday PM, November 11, 2003
Ballot Comment Disposition IEEE 802.1X – Tony Jeffree

The complete disposition of comments is maintained in the disposition of comments document maintained by the editor; the document can be found on the website

Below are notes of comments that had some level of discussion in the meeting

May have to go forward with some negative comments

Discussion of Bernard's comment 17

Tony will distribute RLS version of the text

Need to look at this one off line to understand its ramifications

Comment 22

Jim Burns pointed out that accepting this comments requires .1x to analyze EAP
packets. The EAP layer should handle the EAP packets and the lower layers
should not filter

Comment 30

Mick raised the issue that things don't seem to be terminating

It is time to have some code running these state machines so we understand what
is going

The analysis complexity is going up and we do not understand what is going on in
the EAP state machines

The comment was rejected to avoid having .1x have to knowledge of the EAP
state machine

Wednesday AM, November 12, 2003

Review of the Key Agreement P802.1af PAR – Dolores

Discussion of what is unchangeable in .1x and what can change in .1x

Purpose

EAPOL may change

Controlled and Uncontrolled port concept will not change

Broad market potential

No discussion

Compatibility

Distinct Id

Technical Feasibility

This should be approved by the EXEC Friday

Review of MACSec draft – Allyn Romanow

The idea is to get input on the draft so that we can ask the editor to create a draft
that can go to TG ballot

Need input on the ideas not necessarily on the text

Cls 3, 6, 8, 9, and z

Mick will do 8 and 9

Allyn will do the other sections

What is left out of the definitions?

Review of the current definitions

Discussion about the use of message authentication versus message
integrity

Connection versus Connectionless – Mick gave a network definition, Bob
Moskwitz would like to have this definition. The definition for connectionless is
in an IP world the sending packet 1, 2, 3, 4, 5 and the receiver receiving 1,3,4,5 IP
is fine. But upper layers may have a problem. Discussion of what does it mean
packet/frame independence

High-speed Encryption and Authentication – John Viega

This presentation is on the website

Looking at message integrity

Assume key exchange has happened securely

Want to provide message integrity in a high assurance level

Message integrity the recipient can detect whether the message is in its intended form, or whether there has been tampering
In reality, absolute assurance is not practical
Integrity is more often important than secrecy
A non-option
- Encryption with redundancy
- Depends on the redundancy function
- Usually don't work
- Attacks against many proposed schemes

Composition Approaches
- Combine encryption and integrity schemes
- Select a suitable encryption mode and MIC
- Example SSL/TLS
- How to combine
  - Should be easy but not
- Three paradigms

Generic Composition: Cipher modes
- Review of various algorithms to see there parallelizable and pre-calculation ability

Nonces
- Data that is unique per message
- Repeats must occur with very low probability
- Common contents
  - Message counter, session id, info uniquely id client/sender
- Random value

Authenticated Encryption Schemes
More Authenticated Encryption Schemes
Feature Comparison

Discussion about patent issues – Tony Jeffree
The criteria that an algorithm should not be used because a patent exist in not correct. If an organization gives a letter of assurance then the standard should be able to use that algorithm.

Clause 8 of the MACSec draft – Mick Seaman
- Principles of MAC Security Entity operation
- Overview of what is in the clause and its current state and what is needed to go forwarded
- Need to understand the relationship of this to Key Agreement work
- MACSec
- 8.1.1 Secure Transmission
  - Mick believes there is an issue in clause 8 with the definition of SAID?
    - Current definition is "What key is in use?"
  - Mick has left the door open for group associations if it is needed in the future so existing system will not have to change their behavior
    - SOA – Secure Origin Authenticity
    - Need feedback on SOA
      - Discussion

In the point to point case it seems it is not needed
In multipoint case may not be needed because SOA
could be source MAC address but would need a bit
that says the SOA is the MAC address
What is here is here to force discussion and get
folks to sort out what is needed where and when

Fig 8-1 Architecture and Operations
Trying to put the cipher suite in context
Do you want any choice of cipher suite? Is there more than one cipher
suite?
Do need to account for the NULL cipher suite to handle the
unsecured network hence at least two cipher suites are required
One of the goals is to build a bridge where the data is unencrypted
but the BPDU are encrypted – Norm
This will require some .1D and possible .1X work
Observation the controlled port with a NULL cipher suite is
different that the uncontrolled port. This needs some
thinking to get this sorted out

8.1.3 Secure Reception
What is the relationship of the crypto/integrity and what is in the security
header?
May have TAG fields that are not fully defined by the security
requirements
Currently, the format of the header is orthogonal to the cipher suite
Need to make sure we do not wreck connectivity because the security has
forced a certain frame format that breaks interoperability
Another way is if a fixed format of frame then no interoperability problem
if each cipher suite has a frame format then can break interoperability
Hence, if point to point everything is okay but if another switch is
dropped into this network the new switch can break things or it can
not communicate with the existing network

Back to Fig 8-1 Architecture and Operations
Terminology issue – verification parameter set
Reason why this has to be mention document must say change
keys without disruption of the network
Must have the notion current set and the future key set
Discussion about how this figure fits with EPON
Multicast would imply a NULL cipher suite - Mick
Norm – need a note in the text to point this out
Mick – layer two is not a copy of layer three
If you have different cipher suite can you seamless change between
them? Nope port will go down but change parameters of existing
cipher suite should not be disruptive
Observation - Management should be here rather than moved off some where else

Wednesday PM, November 12, 2003

Key Agreement Protocol for EPON - SuGil Choi

 Introduction
   Each ONU can listen to all downstream traffic
   Goal of protocol mutual authentication between OLT and each ONU
 Requirements
   Key freshness
   Forward Secrecy and Backward Secrecy
   Message Protection
   System Requirements
     Must operate on the link layer
   Communication Efficiency
   Fast Reconnects
 Key types
   Master key
     Used for long time
   Primary key
   Secondary key
 Protocol to get primary and secondary key
   Secondary key derived from primary key
   Primary key derived from secondary
 How key protocol works (math notations here)
 Key Update Process
 Protocol Analysis
 Conclusions
   Symmetric key cryptosystem
   Key agreement protocol between OLT and specified ONU
   Group key agreement protocol is open problem
 Discussion
   Need to have the requirements of various topologies so that key agreement
   protocol can be judged against such requirements
   Observation - This protocol has the property that it assumes frames can be
   injected and observed by any station
   What are the steps to identify what architecture and protocols that we can
   borrow?
     Bob M - Can put media in groups such as point to point or shared
     Present to other groups these findings to see how the general
     solution maps to different media
     Mick – all of the media must be looked as shared and intercept-
     able
       Requirements comes from the context that folks use stuff
       for example 802.1x and it relationship to EAP and Radius
       Look at what context we have to put key agreement
   The idea there is layer 2 and layer 2 must remain within layer 2 is not
   correct. There are ideas or concepts from other layers that are acceptable
   to LinkSec

Dolores asked for everyone to help put together the ideas or identify person that can do such a thing

LAN Edge Radius Attributes – Paul Congdon

Considering extension to the Radius specifications
Adding attributes to radius for configuring switches
RFC 3580

Discussion of KEYsec

- What key agreement mechanisms can we use?
  Bob M.- see what different media need - find a mechanism that can be generally used.
- Mick- from a security viewpoint all the media need to be considered shared media, i.e., vulnerable
  Requirements come from context in which things are used, we need to look at the different deployment contexts.
  assumptions on the media - just open, shared media
- PKI - requires upper layers for CRL
  disagreement about the importance of this for us
- Difference between using public key technology and being embedded in full PKI architecture. they are different. can use public key tech., eg SSH, light weight public key
- Customers of Linksec - service providers and IT departments
  want presentations on how they do authentication for next meeting in January
- protocols we own, protocols above that we don't control that we need to be controlled e.g., ARP spoofing. fill in gap between where we end and IPsec begins

Largest IEEE 802.1b network – John Martell

Jonn.martell@ubc.ca
1300 APs 5000 users
Radius server is most critical part
Accounting goes into SQL databases
Would like login id map into a specific VLAN
This guy is looking at a need for "AP management"
http://Ettercap.sourceforge.net – great tool to do ARP spoofing
How to steal MAC addresses on switched networks
EAP is the problem – not deployable
How to distribute the keys
How to put in the correct VLAN
Campus wide VLAN

Clause 9 Mick

Thursday AM, November 13, 2003

P802.1ab LLDP ballot comment review – Bill Lane

162 comments

The complete disposition of comments is maintained in the disposition of comments document maintained by the editor; the document can be found on the website

Below are notes of comments that had some level of discussion in the meeting

Will not review comments that are accepted

Norms comments about validation of TLVs in clause 7 will be removed from 7 and moved to clause 9

Comment 16 – MIBs and SNMP

> Stating MIBs does not imply an implementation require of SNMP. MIB are a way to organize the data no transmission mechanism is implied

Comment 41 – max length of data

> No arbitrary restrictions on length allow data to be 2**9 since that is what the length field allows

Comment 140

> It was noted this suggestion is of the type "This is one of the thousands of extensions to this protocol."
>
> The value of this is problem diagnosis. One bridge is running 802.1s and a neighbor bridge is running some other protocol. This will allow for the detection of incompatible protocol configurations
>
> There was much discussion about what this should really be
>
> It is not possible to enumerate all of the control protocols and states with a TLV both because of number and proprietary control protocols
>
> Mick has a suggestion about a possible new idea
>
>> One way to describe the protocol is I am using a control protocol that is using the following Ethertype
>>
>> The receiver of this can determine if it is receiving that Ethertype and if not then you can know an problem exist
>
> Consensus check
>
>> Port state is not a good idea but advertising supported protocols is a good idea. Will go back to the commenter with this to insure it is acceptable to them

Comment 143

> Discussion – we do not want to get into creating a number space.
>
> Discussion about mapping enterprise MIB to the known LLDP extensions

Next step

> Is it ready for working group ballot?
>
> Discussion
>
>> Should the PICS be added?
>>
>>> Mick – In general PICS should be added earlier
>>>
>>> How much pain will the editor go through if there are major changes?
>>>
>>> It does not appear there will be major changes here
>>>
>>> It should be here so there is time to make sure the mandatory and optional stuff is correctly tagged

Discussion Bernard Aboba Comment 15 802.1aa – Tony

> Bob has produced a rejection text for the comment

Text on screen
Discussion of the rejection text
> No signal that mutual authentication was achieved only that some authentication
> There is some signaling between EAP and 802.1x that is not yet defined
> 802.1x level can not know if mutual authentication achieved
> Mutual authentication implies on side has a local database for authentication and does not require the network, which is behind the other side's network
> Success can be defined by authentication or by a management action
> Fig 6-6
> Add a Note to the effect that one of the consequences of the bi-direction auth situation is that it may be necessary for both parties to force their supplicant state to Authorized in order to ensure that both can have access to the authentication server.
> Decided that the note raises more questions that it answers delete the note
> Much more discussion
> A new proposal is relate to the old version that supplicant state can be controlled by management to keep port open
> After much discussion it was decided that the solution is
> If port has both authenticator and supplicant exist then the authenticator controls the port
> Further variable for the supplicant that determines if the supplicant state should be consider

Thursday PM, November 13, 2003

MACsec Draft- Questions and Issues: Allyn Romanow

6.2 Preservation of the MAC service
- Is the service list complete?
  There are some things missing – Mick
  MAC operational, status, features included, and point to point connectivity
- Want the service to work the way it use to
  What are the words to say this?

Section 9.2 and figure 9-1 SecY Architecture and Operation
- What goes in the packet?
  Ethertype/SOA/SAID/Packet Number/User Data/ICV
  Ethertype, SOA, and SAID make up SecTAG

Discussion about what is input to the nonce
- Allyn thought the four fields Ethertype, SOA, SAID, and packet number
- Discussion about including Ethertype
  Since the Ethertype is fixed it is not necessary to include the Ethertype
- John V will take a look at the bits that are going into the nonce and make sure it is correct

- The data that uniquely identify the sender and receiver should be included in the nonce

Discussion about the strength of the ICV

- All of these fields will be included in the ICV

Frame expansion

- What is happening with 802.3 and frame expansion?
  Nothing can not go to 802.3 until we have our frame format ready, and it should be by next   meeting – Tony

6.3.6 Frame Lifetime

- What is the policy when there is a frame to transmit and there is no SA?
  Drop it
  Should the frame be buffered and then sent? – No, just dropped
- Discussion about the startup issues with how to create the SA
- This is a hard problem and currently there is not a general solution
  Informal answer within the bridge is drop it
  Formal within the architecture "what frame?"

6.2.7 MAC Service is transitive with respect to connectivity

- This section needs to be filled out more
  Allyn requests help getting this section- wants more examples
  What other protocols? GARP or IGMP has the property of observing traffic and concluding you have connectivity when in fact you do not because you have not yet established an SA
  Observation - Any registration protocol will have this problem

Discussion whether it is necessary to have SA in both directions - yes
Overlapping SAs in order to deliver continuous service
        Have two SAs so that the next SA can be used to maintain connectivity
Replay protection - Probably get for free

Discussion Frame format – Mick

        DA
        SA
        Ethertype
        2 Bytes (for word alignment)
        SOA optional
        Packet Number

- The SAID is within the two Bytes and the SOA is separate
- If shared connection, then the SOA disambiguates the SAID
- Within the two bytes, possible, MSB is zero on transmit and checked on receive, if not zero discard.   This will solve the version problem
  In a new version this bit would be 1 hence a different version
- Bit 1 set means SOA is present, and Bit 2 set is SOA is SA
- This leaves thirteen bits
- You could make an argument that you only need one bit for SAID - old key, new key

What are the arguments for making it bigger than one bit?
If 8 bits is not enough, then use the SOA field
To start, use 8 bits and argue for less or more
Then the SOA contains the SAID if the SA is not the SAID[?]
- This is a starting point to begin the discussion
- Note that this format is not ready for folks to start putting in ASICs

China different security system – Dolores
- China has their own cipher suites
- What should we consider?
- We should stay out of this, not get involved in international issues
- What about different cipher suites?
  We already isolate the cipher suite so different ones can be plugged in

Closing Plenary, Thursday PM, November 13, 2003
Agenda – Tony Jeffree
   Officers
Vice Chair
   Need a new person
   Nominations
      Marcus Leech
      Paul Congdon
   No other nominations
   Review of duties
      Only requirement is vice chair can stand in for the chair
      Optional work responding to email from exec, submitting docs
      And other random stuff to make the committee work
   Resume of Marcus and Paul given by each person
Discussion
   How long is this for?
      Term of office will be until end of the March meeting
Only voting members
Voting member list was displayed and read to the committee
Vote
   Paul Congdon 17
   Marcus Leech 6
   SEC must approve
   Many thanks to Neil
   Many thanks to Marcus for standing
Need to appoint liaisons from 802.1 to 802.3 – Tony Jeffree
   Don Pannell has volunteered
   The job involves understanding what is going on in .3 and how it affects us
   Will have a motion a bit later for Don
Need to merge LinkSec exploder & website into the 802.1 exploder & website

Issues

Some permission issues that have were resolved this week

Merge the two lists and have one exploder

Leave pointer on the old LinkSec web site area to the 802.1 LinkSec areas

Patent Policy – Tony Jeffree

Review of the IEEE patent policy

Clause 6 in IEEE SA Standards Board Bylaws

The policy was reviewed by the Chair to insure everyone in the room understands the policy

The two slides were shown to the committee

Future meetings – Tony Jeffree

Jan 12, 2004 Vancouver (Monday through Thursday)

Mar 14, 2004 Walt Disney World Hilton Orlando

Liaison letter response ITU-T Q12/15 – Paul Bottorff

Discussion of the letter

Mick would like the addition of text that requests the inclusion of the ISS

"The link you provide as a whole should provide the ISS"

Word Smithing to get the above statement in the letter

Mick's picture will be added to the letter

Motion

Motion: Forward the above liaison from IEEE 802.1 to the ITU-T Q12/15
Move Bottorff
Second Wright
For 17 Against 0 Abstain 1

802.1 requests that the SEC confirm the appointment of Paul Congdon as vice Chair of 802.1
Proposed: Wright
Second: Seaman
For: 17 Against: 0   Abstain: 0

802.1 resolves to hold an interim session in Vancouver, Mon 9:00 through Fri Noon of the week of 12th Jan 2004 (12th through 15th Jan), hosted by 802
Proposed: Seaman
Second: Wright
For: 18 Against:0 Abstain: 0

802.1 approves the July '2003 and Sept '2003 meeting minutes.
Proposed: Wright
Second: Romanow
For: 17   Against: 0   Abstain: 2

802.1 resolves to hold a pre-meeting on the Monday morning of the March 2004 plenary session.
Proposed: Romanow

Second: Wright
For: 16   Against: 0   Abstain: 0

802.1 requests conditional approval from the SEC to forward P802.1D-REV to RevCom
following completion of the Sponsor recirculation ballot that is currently in progress.
Proposed: Seaman   Second: Wright
802.1 For: 19 Against: 0   Abstain: 0

802.1 requests approval from the SEC to forward the 802.1F Reaffirmation to RevCom.
Proposed: Lane Second: Wright
For: 21 Against: 0 Abstain: 0

802.1 instructs the Editor for P802b to revise the document in accordance with the agreed
disposition of ballot comments and to forward the revised draft for Sponsor recirculation
ballot.
Proposed: Wright Second: Bell
For: 21 Against: 0   Abstain: 0

802.1 requests conditional approval from the SEC to forward P802b to RevCom
following completion of its upcoming Sponsor recirculation ballot.
Proposed: Wright Second: Bell
For: 20 Against: 0   Abstain:0

802.1 instructs the Editor for P802.1ab, Bill Lane, to issue the next draft for Working
Group ballot by December 8th 2003
Proposed: Lane
Second: Wright
For: 20 Against: 0 Abstain: 0

802.1 instructs the Editor for P802.1X-REV, Tony Jeffree, to revise the document in line
with the comment dispositions agreed during this meeting and issue the next draft for a
WG confirmation ballot.
Proposed: Jarvis Second: Wright
For: 21 Against: 0   Abstain: 0

802.1 requests conditional approval from the SEC to forward P802.1X-REV to Sponsor
Ballot following completion of its WG recirculation ballot.
Proposed: Wright Second: Bell
For: 20 Against: 0   Abstain: 0

802.1 instructs the Editor for P802.1ad, Mick Seaman, to revise the document taking
account of the discussion during this meeting and issue the next draft for a second Task
Group ballot
Proposed: Seaman Second: Wright
For: 21 Against: 0 Abstain: 0

802.1 requests permission from the SEC to forward the P802.1af "Key Agreement" PAR to NesCom.
Proposed: Leech Second: Sala
For: 20 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 8th December 2003.
Proposed: Romanow Second: Larsen
For: 20 Against: 0   Abstain: 0

802.1 appoints Don Pannell as liaison to 802.3.
Proposed: Romanow Second: Lane
For:20   Against: 0   Abstain: 0

802.1 authorizes its January interim meeting to revise the P802.1AG draft PAR and, if approved by the interim, circulate it to the SEC under the 30-day rule.
Proposed: Wright   Second: Larsen
For: 21 Against: 0   Abstain: 0

Any other business – Tony Jeffree
None

Motion to Adjourn
Proposed: Wright
Second: Lane
Unanimous

Attendees:
Brian Arnold
Andrew Baek
Chuck Bailey
Brandon Barry
Alexei Beliaev
Les Bell
Paul Bottorff
Richard Brand
Jim Burns
Marco Carugi
Dirceu Cavendish
Su-il Choi
Paul Congdon
Sharam Davari
Anush Elangovan
Hesham Elbakoury
David Elie-Dit-Cosaque

Norm Finn
Helena Flygare
David Frattura
Vivek Gupta
Steve Haddock
Cheng Hong
Ran Ish-Shalom
Atsushi Iwata
Neil Jarvis
Tony Jeffree
Yongbum Kim
Scott Kortla
Hiroaki Kurihara
Shobhan Lakkapragada
Bill Lane
Loren Larsen
Yannick Le Goff
Marcus Leech
Wei Liy Lim
Tom Mathey
David Melman
John Messenger
Hidekazu Miyoshi
Dinesh Mohan
Bob Moskowitz
Dave Nelson
Hiroshi Ohta
Don Pannell
Chan Young Park
Glenn Parsons
Antti Pietilainen
Ivan Reede
John Roese
Allyn Romanow
Jessy V Rouyer
Ali Sajassi
Dolors Sala
Mick Seaman
Koichiro Seto
Muneyoshi Suzuki
John Viega
Karl Weber
Ludwig Winkel
Michael D. Wright
Robert Wu

Shawn Yang
Ilan Yerashami