IEEE802 Link Security Executive Committee Study Group
January 2003 Interim Meeting,
Jan 9-10, 2003, Vancouver, BC, Canada

Meeting Minutes
recorded by Allyn Romanow (allyn@cisco.com)

Meeting Summary

The two-days meeting covered the presentations including discussion on requirements, architecture model, and PAR and 5 criteria, and lengthy discussion on scenarios, placement of the project and the need of traffic analysis. The group also discussed the location and dates of the next interim meeting.

Major decisions made

1. The SG will recommend to the executive committee in the next IEEE802 plenary meeting to place the project in 802.1
2. The next interim meeting in May will not be co-located with EFM in Korea, but will be in Ottawa hosted by Nortel late May early June and co-located with P802.3 10GBASE-CX4, P802.3 10GBASE-T SG, and P802.1.
3. Developed an initial set of scenarios. See http://www.ieee802.org/linksec/meetings/MeetingsMaterial/Jan03/LinkSecUsageCases_0103.pdf
4. A work plan for development of project PAR(s) was identified. See http://www.ieee802.org/linksec/meetings/MeetingsMaterial/Jan03/ LinkSecWorkPlan_0103.pdf.
5. Three technical tutorials will be prepared for next plenary meeting to introduce SG participants to the three major areas involved in this project. The areas are Bridging, EPON and Security. The volunteers to organize or prepare the tutorials were: Norm Finn (nfinn@cisco.com) to prepare the Bridging tutorial, Jonathan Thatcher (Jonathan.Thatcher@worldwidepackets.com) to organize the EPON tutorial, and Bill McIntosh (bmcintosh@fortresstech.com) to prepare the Security tutorial.

Summary of Straw Polls

1. Where should the next LinkSec Interim meeting be held? Specifically, are you will to go if:
    a. Co-lo with .3 in Seoul - 14
    b. Co-lo with .11 in Singapore - 10
    c. Meet with late may June in Ottawa – 30

2. Who thinks the approach outlined by Mick for development of the PAR(s) (see Jan03/LinkSecWorkPlan_1_0103.pdf) is a good one?
    Yes – 36
    No – 0

3. Are you in favor of moving this SG group to 802.1?
    Yes - 26

Negative - 0
Abstain – 12

Thursday January 9th 2003

Dolors opens the meeting and presents agenda_01_0103.pdf. Rules governing the SG operations and patent policy are shown. Allyn Romanow is assigned recording secretary for the meeting. Overview of the group activities is summarized giving home page and reflector information, and informing of the weekly calls.

All thursday and Friday morning were common sessions with 802.1. Friday morning session was also attended by EPON track members of EFM.

Presentations of the material submitted for the meeting posted at:
http://www.ieee802.org/linksec/meetings/MeetingsMaterial/Jan03

Presentation: EPON Subscriber Access Security Requirements – Antti Pietilainen

Background -EFM, point to multipoint
Provider operates optical network same way as did copper, regulated
OLT in a locked position, cables owned by operator. Cable ownership changes to house owner when goes inside.
In Europe ONU will be inside house
Cables not accessible except by operator
Threat scenarios - Case a)
Easy, especially with Ethernet with its promiscuous mode, can be downloaded from internet, no expertise required to eavesdrop Unlike APON where security risks are much lower in cases b) and c)
Culprit puts in wires, a felony, Antti wants to leave this out, because it's difficult to deal with
Also, provider not considered responsible for b and c

To conform to legal requirements, minimum requirement is encryption
Authentication not strictly speaking required to be lawful
Authentication required to ensure customer gets contracted level of service, to make sure the right customer is getting the service

Suitable features- privacy - can't see to whom packets are going
Control packets in EPON should be encrypted
Difficult to do testing- want to be able to turn off encryption temporarily
Should be possible to recognize DOS attacks thru anomalous behavior

Conclusion - subscriber access is a good market
Security is needed desperately
What’s the chance of EPON being successful? Some experienced people think there's no chance for EPON, but Antti thinks good chance, one interface for many customers.
Risk we won't succeed, so Antti hopes requirements will be taken seriously so EPON can succeed

Question- what's the difference between authentication and message authentication?
Answer - message authentication is a protocol that allows verification that each message comes from the purported sender.
Includes MAC Message Authentication Code in an extension header of packet, can prove the source it came from.
There exists a secret that is unique between us, e.g. keys for an algorithm that generates MAC, a large integer in the header. Use an algorithm to verify the message came uniquely from you.

Question- encryption required in one direction from OLT to ONU and not in reverse direction?
Answer- meant especially in downstream direction, but in certain situations upstream traffic can also be listened to, therefore upstream also required to be encrypted.
Marcus - hard to understand how asymmetric will be useful, costs the Same to do it symmetrically.
Antti concurs.

Mani- dynamic allocation of LLIDS can be performed.

Tom- ONU might be a privately owned card that's turned on and off
Another issue - this group needs to have objectives
For a security project to have objectives need a threat analysis
What level of security do you want to support?
Scenario a) is clear; b) and c) require a lot more resources. Reasonable for group to decide not to take this on.

Dolors- more discussion if b and c should be considered
Norm- scenarios that have been described are accurate for residential access, but there are needs beyond residential access, and man-in-middle attack is important and needs to be defended against.

Marcus- even if b and c attacks aren't likely, protecting against them, from the cryptographic point of view, is only marginally more effort.
Assume someone will do b and c attacks, even if not likely right now. Defending against them is so cheap, might as well protect against them anyway.

Antti - thinks they are much more difficult, makes packets more lengthy

Bob M - getting back to goals, this is a good presentation for EPON,
but this SG is supposed to consider a wider domain
b and c are common configurations and attacks easy to perform.
In terms of frame lengths, some protocols have done fine tuning to save bits on wire.
They are media specific.
If we are doing a general solution those are things to avoid

Marcus - once you've swallowed key management, then from implementation point of view, not much effort to protect in both directions. The work is up front.

Richard - can't discount b and c categorically, therefore we should provide for it.

APON allows options b and c.
As a network provider can use topologies b and c

Dolors- it helps to make clear what's easy and what's difficult in security.
We need contributions beyond what we have.

Note: Main point of discussion- should we do b and c?

Presentation: Link Security Architecture- Mick Seaman

Wants to talk about architecture
Find architecture with broadest appeal for least cost
Security in terms of snooping the link may not be the problem we want to solve

Assumed problem-
Take 802.1x architecture as a starting point
The problem is interconnecting networks; end station is a special case
L2 connected networks
A lot of focus on theft of service and due care

Originally, he had the feeling that L2 security was hokey, but learned from corporate security departments that this is not the case.
E.g., they feared an attacker willing to rent an office for a year proximate to their bldg. to steal secrets.
Solution must be non-disruptive - customer doesn't want to be inconvenienced for security
Have to work with currently existing networks
Network mgmt wants holes in security all over
Solution has to be deployable, craft compatible

Nature of solution
Not end to end- subsets of L2 connections
Prevent access - perimeter, firewall
Multi-layer- authentication by many methods
Encryption at lowest possible layer
Leverage existing components

802.1x a good starting point
History - started out to solve problem of conference rooms - open outlets, want to Protect corporation, restrict usage
Solution is 3 party relationship - authenticator, supplicant - laptop or person on it, authentication server. Few threats, simple.
We should leverage existing authentication servers, make solution as undisruptive and as cheap as possible
Encrypt on access line

Model for solution - make sure network correctly connected to next switch
When get active signal can make sure it's correct
Authenticator talks in both directions
Continuous checks that no one has sneaked into network

May or may not have encryption
A variant - net to net attachment. How do nets agree to join and expose resources?
Knock hole in firewall to connect these two nets?
Traffic segregation - let people in, but not access to the whole of the net.
Because a firewall solution can segregate traffic as it comes in, restrict access
to certain planes, separate VLANs.
Not strong security

Extend the solution

Nature of assumed problem
Could find solution for 802.3 EPON that looks at threats and comes up with
something like .11 WEP, without holes.
In some cases, knowing the device is attached to right place is sufficient for
Security.

Absolutely necessary that we have a completely specified solution
Advisory solutions have not had a high success rate in 802

Traffic analysis attacks - take attitude catch as catch can
Not fool ourselves about level of protection we can get on shared media
But there is a core that has appeal across wide range
Most of solution must be built already, better yet, someone's pushing it as an agenda
.1x wouldn't have taken off without a large company pushing it as part of
their corporate agenda

Dennis- firewall model, firewall in each ONU?
No, OLT implements firewall on/off, ONU does firewall on/off function
Consider 802.1 provider bridges
Boundary between MAC specific and what MAC gets from the general effort

Jonathan - what's the degree of protection, data and/or control? Both?
Resolved at .1 layer, carried as encrypted? Lower layers?

Mick - primarily data frame mechanism. May be possible to protect some
control frames, not sure know why want to protect control frames in most cases.
To what degree control frame attacks are detectable?
Theft of service attack, want to know where coming from.
Exactly what is being protected?
What gets out of ONU into rest of net?
If customer traffic can't be snooped or something injected into it,
that's sufficient protection
We need an analysis of control frame attacks, how likely they are, can they be done
for an extended time?
How worried are providers?

Jonathan - encrypt MAC addresses.
Mick - it's important that MAC addresses are protected, but to defeat traffic analysis,
he suspects unlikely it's a good strategy to succeed.
Marcus- only useful at an aggregation point
Even if MAC addresses are encrypted, can still do analysis

Mick – he was thinking of reading the address on the wire
Marcus- there's a difference between encrypting and protecting MAC address
Mick – MAC address should be protected, but not hidden

Antti- We've had a big discussion about encrypting MAC addresses already
In EPON every ONU can listen to traffic as an aggregation point,
listen to other ONUS.
If Ethernet MAC addresses not encrypted, eavesdropper can do traffic analysis
Concerned because doesn't require any expertise, programs for snooping can be downloaded from the internet

Dolors- multi-layer- what layers?
Mick- encryption should be at the lowest possible layer, below MAC service, above all frames, not on all bytes. Need some control in clear
Bridging layer is for connection between nets -see VLANs
Enforcement and authentication functions are way up in layers
Not controversial

Presentation: Scope and Purpose – Dennis Volpano

Background – He thought we wouldn't converge quickly because usage scenarios are missing.
Dave Nelson on teleconf proposed some usage models
Dennis put together a PAR based on Dave's suggestions
Is this really a link security effort? Or is this an effort to provide security for bridging?

Scope
Provider bridging is the relevant framework
Left open whether control packets are protected
802.1ad is where worry about treating frames from a customer bridge
We are doing security for this domain

Purpose
Secure bridged or virtual bridged LANs to number of users

He views this as a secure bridging effort
Open issues
Two trusted bridges separated by one that is not trusted
Mick – there are islands of trust

802.10 if need to change topology have to discover endpoints,
Russ agreed this is where the bulk of the work lies
Mick thinks its not a big issue
This group needs to decide scope

Norm - Mick's and Antti's presentations are good- they suggest different sets of constraints on our output.
He disagrees that PAR should say to design secure bridged LANs, or to secure provider nets.
The scope should be more circumscribed. For example, could say the purpose is to produce better encapsulation for 802.10 and enable us to use .1x

for key exchange.
Norm thinks the truth is in between these two extreme definitions of the goal.

Paul - wants narrower focus that is more broadly applicable.

Mick – Dennis' presentation helps with partitioning the problem
Be careful on how we borrow from existing technology
If you have a MAC that does encryption on data frames, what are the remaining threats on control frames?
Large commonality between MACs on authentication, authorization side.
Doesn't know how much commonality there is concerning MAC encryption.
Work towards multiple parts of the solution and narrowly focus the solution toward some of the parts

Jonathan - which MACs in 802 need to be included?
Out of hibernation, for example token ring?
Mick - how approach which MACS we should consider?
For example, .11 people aren't here

Dennis -802.1(?) clause 3 needs to be revised

Dolors - several MACs, a common spec and a MAC specific spec.
We don't need to do all the MACs.
Do we need to consider what all the MACs might require?
It impacts the general approach.
So identifying which MACs we are including is important.
Norm - practically speaking, he is more in favor of a MAC that is easy than one that is difficult.
Dolors - so how should we carry this out? Look at all of the MACs?

We should base it on effort - who shows up to support a MAC. We'll look at and see how difficult it is. We are driven by market demand.

Bill McIntosh - shouldn't our solution work with all MACs?

Mick – has concerns
Bob M- control frames - get touchy

Mick - put .1x as a general framework,
not saying it should be adopted wholesale, uncritically.
Some aspects seem to work well, others more obscure
Look really carefully at .10 and make sure it's not doing more than we want
It was oriented end to end. More complex than what we need.
Russ on the mailing list said this would then be a lot easier.

Dennis - key management is the hard part
Why did .10 fail?
Maybe answer is timing
Depends who you talk to
Focus was e2e L2 in which no one is interested. Link to link was an add-on.
Now a lot of things have changed.

At that time, people weren't generally interested in security,
Felt they had a guard on the door, in the enterprise
Now we're going into provider space.
Also, back then, general knowledge of key exchange mechanisms was more problematic, less well-known.
Minorly, they used LLC in which no one is interested

Presentation: Straw man PAR and 5 Criteria – Glen Zorn, with Dave Halasz

802.10 authentication options limited and not sufficiently flexible
Recommend the work goes back into 802.10
Specify a new SDE
Specify using 802.1x for authentication

Scope-
New SDE format and provide .1x for authentication
Purpose -
Use .10
Tony - Surely not. Purpose relates to why we're doing this, not which technology we want to leverage.
General agreement.
Change scope to - Provide link level security for generic 802 protocols

Broad market potential-
Enhance functionality and capability of all 802 LAN technologies and devices.

Should add something about security.

Compatibility- Will conform to former 802.10 as much as possible.
Jonathan - mean backward compatibility? Even with systems that don't do this security?
What if connected to entity that doesn't support security?
Interoperates but without security?
Tony - if security on my device, then I don't want it to interoperate with a non-secure device.
Right - so need to specify
Glen – compatibility means we're not developing IPSec
Norm - purpose of compatibility is so that a minimum of changes is necessary
Distinct identity- not re-invent wheels, because it's an amendment to .10
Tony – we need to express this more fully.

Technical feasibility- .1x solutions exist today.
802.11i redefines 802.1x key management
Are you suggesting this group augment .1x for key management?
That's Dave Halasz's idea.
Glen - thinks .10 should be changed to supply key management technology.
He doesn't like TGI, so he does not want to continue it here.
Big issue

Economic feasibility

Claim it doesn't much impact economic factors, existing LAN MAN solutions
Norm – No, there is a change because difference in gate count of port
ASIC with and without encryption is very different.
The cost is commensurate with the benefits that can be realized.
Costs more money but get a positive value.

Mick - we're going down a tunnel
Fix up .10, he doesn't disagree
We should be partitioning functionality for deployability
Doesn't want to have to buy the whole thing. Wants authorization without authentication, etc., without encryption etc.
Wants to make sure can apply pieces as needed.
NEED this for critical mass, for mass adoption, important.
Wants system level partitioning, before submitting the PAR
Next step then apply to PAR
Important. Action element to partition functionality, then revise PAR accordingly

Tony- extending .10 standards may not require invoking the .10 as a WG.
E. g. 8021d has sections contributed by other WGs.

Norm- on the PAR. They had a good discussion in 802.1 about .1x.
Whether it's suitable for this and other functions. 802.1x not adequate for all purposes we want.
So we will have work items for 802.1 to update .1x.
Can't replace .10 key exchange with .1x key exchange. 802.10 is end to end.
802.1x can't go thru a bridge.
Mick - partitioning, which pieces of STDs we should remove and throw away
Make .1x smaller.
If remove e2e from .10 that may be good

Dolors - how do you describe what problem you're trying to solve?

Glen- .10 authentication is not sufficiently flexible

Norm - Dennis' statement of purpose was valuable
Useful for PAR to capture that security features will be useful for public nets

E2e means can go thru a bridge? Yes

When designing a net, want to manage and administrate it the same way as today.
In a few years 802.11i will be widely deployed,
we'd like to be able to administrate similarly to 802.11i.
Glen - Radius, higher level stuff will be similar.

Presentation: Scope, Develop a Framework – Mani Mahalingam

Norm – PAR is not an authorization to go do work.
It is an authorization to write a STD.
Component for .3ah, 802.1x, .10

At least 2, maybe 3 or 4 PARs will come out of this, not just one PAR

General Discussion – Dolors Sala

Operating rules
Consensus on action items
Scope, objectives, how to proceed today and tomorrow
Should we break into subgroups?

Discussion topics
What are our top priorities?

Dennis -subgroup address difference between enterprise and provider.
Agree on differences so they can be looked at
Mani volunteered for enterprise model

Norm – we need a catalogue of configurations that we want to support,
don't want to support,
how much they cost, what's above and below threshold of cost.
Will help us understand and reach consensus on the requirements.
Need to all understand and share what we want to do.

Dolors - what work will help us identify architecture?

Mick - basic usage scenarios,
1. What is connected to what?
End station, customer net, fragment of customer net, provider, part of provider
2. With what? Point to point? Shared, wires?
3. Who is being protected? Provider being protected against threat?
4. From what being protected? Identity protection? Interference with the service? Replay? Masquerade?
5. What’s the scope of the protection? A link?
Set of enterprise connections over provider with multipoint capability, and point to point
6. For how long? Is this device moving about? Who does what to whom for how long?

If they don't fit on a page, you’re not doing it at the right level of analysis

Antti - at the higher layer, through a bridged network applies to all the MACs, when go from a wireless LAN into bridged network, MAC specific
Migrating from wireless, don't like that they change their security architecture.
Could divide work in terms of higher layer, above MAC and what needs to be done in the MAC. Division between different tasks that the group might take.
Security in a bridged network is different than the security required in an EPON.

Mick- functional split, what gets done where? Split between authentication, key mgmt, policing, segregation, and encryption.
Want to catalogue so that we can understand and prioritize

Glen - working from usage scenario is good way to develop products, relatively short term.
Not good for developing architectures, which evolve over time.

Norm - yep, but we got to start someplace. Can thrash in idea space forever.
Mick's idea- what exactly are you trying to do? Get each other's views on what we are trying to do - we can converge and then generate architecture. We need to start from both ends, from top down and bottom up.

Mick – a useful process he follows for designing architecture is to think about what he wants to cover, write it down, requirements, syntactic processing, changes yes to no, vice versa, then tests again whether he still believes the statements, then can go top down.
Right now it's important that everyone uses the thinking tools they are happy with, because there is no right way to approach a new topic.

Dolors - how to split up the work items

Bob- the process is - scenarios - architectural components – work items,
will need multiple PARs
Overlapping work groups
Everyone has own view of it
Cannot be pressure to finish up soon
First step, work as a team at this point
At the moment we are all working on the same thing

Where should we have interim meeting in May?
Nortel offers to host joint meeting in Ottawa
We could have it in June in Ottawa, and then .11 people could come
If we don't go to Asia, how will Asian's feel?

Poll
Co-lo with .3 in Seoul - 14
Co-lo with .11 in Singapore - 10
Meet with late may June in Ottawa - 30

=====================================

Brainstorming

Whiteboard

Scenarios
What is connected to what?
How is it connected?
Who is being protected?
From what?
Scope of the protection
How long to protect?

Mick
Develop chart of Use cases –see Meetings/Jan03/LinkSecUsageCases_0103.doc/.pdf
Laid out questions as column heads
Quick notation

ES end system
EN enterprise net
PN provider net
Which cases are we actually worried about?
.3pt-pt, .3ah EPON, .11, RPR

Simultaneous .11, .15
Look alike from our perspective
Shared media

Assumptions about communication server?

Mesh wireless networks
.15 different assumptions than .11
3 way authentication

Which MACs should we include?
.16 has copied everything from DOCSIS
In scope, shared media multi-access
Unless you understand a lot about how a bridged infrastructure works, It's hard to talk about how to secure it
Similarly .15, and for all the MACs
If we are to do useful work for different media, requires active participation from someone in the media to liaise between LinkSec and the MAC group.

Bob- are we looking at how the medias might be used in a network?
.16 a trunk circuit between bridges, because shared, greater risk than fiber between trunks, easier to sniff, launch man-in-middle attack, but serves same role
Then we go to .16 people, ask how it differs from a piece of fiber
Two layers of activity here
.16 and .3 as bridged trunk, aren't they the same??

.16 - Shared media, pt to multi-point,
Mick - this group can't do anything in a MAC layer without active participation

Aren't there certain things that are common to all protocols?
Message integrity, Authentication, key management
What are the MAC layer packets that need to be protected?
That's an add-on
Then at bottom, do you scramble MAC addresses?

Solve world hunger. Look at every 802 dot group and address their security needs.
We are discussing what the extent of world hunger is.
The rule should be show up or you're left out.

Another point of view is that you need to see the commonalities

Dolors- what are people interested in? then do straw polls.
Norm - it's not time yet to say no to anything

Suppose just protect data, not control, doesn't that work for all the MACs?
May solve 95% of possible attacks.
Doesn’t help if 5% is downloaded from the internet.
Need to protect against the cheap ones to make any effort worthwhile
Norm – state goal for the group as – It should be impossible to not touch a wire and screw things up, .e.g. from downloading. Can’t download something from the internet and defeat security. A good first step.

.11 AP and stations, looks like a hub

.3ah should differentiate between pt to pt and pt to multipoint, important?
Similarly for .3ah Cu pt to pt
Different cable types may be relevant for threat models

Mike Wright - .11 from client to access point. Okay for some situations, but sometimes want to go from point to another point.
Manage hundreds of access points
Hot spots

Leaving open to router or bridge. .1x works for both

Broadcast key
Do we need to distribute a key on a broadcast media?
.11 at airport
There will be at least one laptop talking, so when can you distribute a new key, would have a new key and an old key at the same time
Secure multicast

Do I need an array of multicast keys at the link layer? Do I need a broadcast key?
.ah needs to think about
Do you need a group key, a broadcast key?
Mike - in .11 it was said, e2e responsibility of application provider and user
Link to link protection is the responsibility of the provider

Worried about theft of bandwidth?

Mani - a case for protecting multicast at the link layer?
Norm - doesn't know an app that needs a key for each multicast stream
At L2 can't distinguish L2 multicast streams. Can differentiate at L3, not at L2

Any need for SA that passes through a bridge. Has implications for bridge makers.
Will impact MTU or make packet bigger. Can deal with if it's terminated and repackaged, but not if it passes thru the bridge.
Build bridges with 1536 Byte buffer.
An SA that requires large size won't work.
.1x doesn't do this.
Strategic solutions. Put in IPSec tunnel, do today
Or use .10 multi-hop thing

We get to pick.
This is line 6 in the table
This with the AppleTalk example...

Next step, after this table
Categorize threats
Some threats listed in Mick's doc
What do we need to know about the threats?
How threat model impacts
Dennis--reliability, ability to control
Mick's - there are threats he'd love to get rid of, because they're really impossible to deal with.
Like the traffic analysis threat.
Someone- but should put it in table, then reduce table later
Description of the service trying to offer
Elaborate. Want completeness, then hone to something reasonable

Norm- provide a standard that's interoperable
And doesn't specify value add
Mick - got to work such that plain vanilla is usable, without value-adds.

Think list of threats, threats to include and exclude
Use Mick's table to choose the scenarios that are of interest
Should have a description of each row in the table, in terms of the service it provides (?)

Friday January 10th 2003

Summary of previous day was given for new attendees who attended EFM the day before.
Mick went over table; the table of configurations is a starting point for serious thought

Dennis Volpano - Scope slide, from presentation
To develop bridge, (.1D) protocols, compatible with a Provider Bridged
Local Area Network (.1ad) to provide separate and reliable instances
of the MAC service to multiple independent users of a Bridged Local Area Network
(.1D, .1Q) in a manner that allows the Provider to control the MAC service on shared
and non-shared-media LAN segments (.3ah, .11, .16, .17)

Norm - provider bridges are one important use of link security.
This scope is interesting but it doesn’t cover the entire scope of the group.
We can work with it, as long as we recognize it’s only a piece of the puzzle.
Geoff Thompson - don't want to build a model that is only bridge centric
Rather, we should look at something which is a shim we can put in any situation.

Dan - bridging security is a sub aspect of the scope of the group
Should be part of the .1ad charter, but not the scope of this group

We are trying to develop the scope of the group

Jonathan- remove .3ah from the scope statement

Dennis -securing link is not the hard part
Doesn’t like 802.10c, doesn't think it scales up for bridges.
Says Russ confirmed on the teleconf, he knows it's the area that needs work.
If we address this part of the STD then SDE will work for bridges.

Mick- has been emphasizing bridge but also applicable to end station or router.
Bridge is particular interesting because it continues a L2 connection, but other devices on L2 are also interesting.

Norm -first sentence for scope- to develop protocols, compatible with bridged LANs (.1D, .1Q) and provider bridges (1ad) to provide separate and reliable security associations among 802 MAC ports.

Is it bridges or is LAN links secure on one side and not on the other?
Geoff - emphasis on bridges over done. Links between bridges, router, etc.
But when there are breeches of security, they will be done by grabbing the link, putting a general device on it that will spoof. Wants to say what goes into a link is secure, rather than something that is on a bridge is secure.

Norm - 802.10. Security Associations (SAs) between 2 MAC address, LSAP points.
Not interested in SA to MAC address, *. Since we are at layer 2, we can't make SAs to TCP ports. What’s the addressing point?

Geoff- MAC address is one element of the security point.
Jonathan- interprets norm's sentence as an assoc between any two MAC ports regardless of what lies between them, link, bridge or entire network. Is that your intent?

Norm - yes, could be. Doesn’t want to rule out in our scope at this early stage.
Hope we rule out as we progress, but not take it out of scope now.

Mick- we're discussing use cases without a list of use cases.
We're constructing words acceptable to everyone. For what purpose?
Do we need to define scope in order to talk?
Mick friendly amendment-
The Task in Front of Us (not the scope)

- identify use cases (network configs)
- classify (& reduce threats) into business case relevance
- agree (use case x threat)
-importance/relevance difficulty
-remove threats covered by other mechanisms
- devise a top level architecture partitioning for a system solution into
-mechanisms providing: Mac level 'protection'
 -port level enforcement
 -bridge level traffic segregation
 -higher level key distribution
  higher level authenticity
-outline PARs for above to provide functions to defined interfaces

This is what we should be doing right now
Agreement

What’s it mean to have multiple PARs? - doesn't require multiple WGs.
Work can be organized within one WG, subgroups or whatever.
Converges to a set of PARs. How quickly?
It might take longer than someone would like, but it's required to get a useful ouput
EPON waiting

VOTE Who thinks this is a good approach to take? 36
Not a good approach? -0

Discussion on the placement of the project

Concern if we aren't part of .1 there could be a scheduling conflict
And we have so much participation from .1 participants, could be problematic
If we want the attention of .1, being part of it is a good way to get its time
If we want to just the work done, and have no other agendas, being part of another group, is an expedient tactic

To extent anyone has heard of .l0, it's as a failed VLAN protocol

Glen Zorn – We need to be co-located with EFM since EPON offers the immediate application for this effort. It seems more appropriate to be an independent group to be able to decide the meetings co-locations.

Tony Jeffree – 802.1 has been co-locating with EFM for quite a while. The co-location decisions can be equally decided regardless if the group belongs to 802.1 or is an independent group.

Dolors - Are there any technical constraints attached to putting the group in .1?

Tony Jeffree- No effect, even if .10 modification is required, whatever is needed can be done from within .1. Some pieces of work may be parceled out to other groups to .1 or .3, etc.

Marcus- Reviving work in .10 may bring more security people out than by tucking into 802.1. In IETF, this happens. Security people more likely to get involved if the work is done in Security area.

But in IEEE .10 is in hibernation, whereas going into a WG that has a good track record is another story. Also, 4 officers of .10 haven't been able to come to any of the LinkSec.

Because of the protocol support needed, it would be good to be in .1 Policy, negotiating, generating and managing protocols and keys

Paul – Being part of 802.1 means that the link sec members need to review and vote on all documents produced by 802.1, and hence may require to build this expertise to keep WG membership.

Tony Jeffrey – As long as members of WG vote, they keep membership. Linksec members can be aside of other related 802.1 activities by just voting “abstain for lack of technical expertise”.

Might mean 802.1 needs to meet an extra day.
May need more structure and a schedule we know in advance.
Yes would be a necessary consequence.
Structurally form a second task group to cover this activity, where appropriate, task group sessions meet in parallel
More sensitive time planning, work thru to Friday morning

It would be good t have tutorial for people who aren't familiar with bridging
And tutorials on EPON and on security. All would be useful, welcome

Norm will do bridging tutorial
Jonathan- will find volunteers -.3ah tutorial including EPON
Bill McIntosh –security tutuorial
We’ll get a tutorial slot- Monday or Tuesday evening

Straw poll -
Move this group to 802.1?
Yes - 26
Negative - 0
Abstain – 12

Plan to meet Monday morning early at the Plenary

Dolors – wants to take straw polls on things from yesterday
Not work on .16 and .15
-define a common security umbrella for 802.3, RPR, 802.11 networks
-define security mechanism for all.3 links (p2p, EPON, copper, fiber, shared)
-define security mechanism for RPR
-define security mechanism for .l1 links
-define security mechanism for .15 links
-define security mechanism for .16 links

Need to take out any reference to .11

What is right way to take an invitation to the other groups?
Tony takes care of it
Action item Tony solicits input from other groups

What participation do we have now?
Who is qualified for which MACs?
Too late, people left already

Mick - group be very sensitive that .10 is very valuable and value added by participation of .10 people.

Homework - read and understand 802.10. Foundation of our work
Can we get a tutorial?

Bill will do 802.10 tutorial

10b not on website will be put there

Meeting breaks for lunch

Friday Afternoon

Presentation on preventing malicious traffic analysis in EPON - Antti

Marcus - How much bandwidth will you turn over for preventing traffic analysis?
Classic method is padding, with substantial steps
Need to give up a fair amount of bandwidth in order to flatten patterns in the traffic

Discussion of what the problem is

Antti – proposes the solution of encrypting MAC address
Marcus- Actually this is identity protection-
When have encrypted MAC address can't map to LLID
This is identity protection for users NOT traffic analysis
Antti wants to protect individual privacy
Worried about someone finding things out by analyzing packet flow

Marcus - traffic analysis is way ambitious, we shouldn't deal with it at this early stage,
If ever.
Identity protection is doable

Geoff - EPON was the prime motivator.
Shouldn't take security beyond the point you get with pt to pt wired network.

Big discussion about physical security on the ONU

The meeting was adjourned at around 3:30pm.