Summary Report of Joint 802.1/802.3 Meeting

March 18, 2004

Orlando, Fla.

Richard Brand, rbrand@nortelnetworks.com

4 Main Topics:

- Maximum Frame size issues relative to 802.1ad, 802.1AE (MAC Security);
- Relative placement of Link Agg and MACSec;
- Minimum frame size issues relative to 802.1AE;
- 802.1AB issues (Station and Media Access Control Connectivity Discovery) "Ethertype" Standardization

TOPIC 1: Frame Size Expansion Requirements (as currently known)

- MACSec Secure Frame Format – 24 octets (point to point), 32 octets (shared medium)
- Provider Bridge TAG – 4 octets
- Total possible for mandatory secure cipher suite:
  32 (Customer security) plus
  32 (Provider security) plus
  4 (Provider TAG)

Caveats:

• Possible use of cipher suites to meet Federal
requirements – 64 octets
• Larger cipher blocks for greater security –
160 octets
• Requests for larger Provider TAG and
duplicate FCS (yet to be resolved)

802.3 Response

Will take a new 802.3 PAR

TOPIC 2: Relative Placement of Link Agg & MACSec

- 802.3 didn't want an embedded (within MAC) solution to MACSec
  – Looks like this was the right decision
  – However, some problematic architectural issues: MACSec may well need to operate below LinkAgg

Why below Link Agg?

- Goal of MACSec to confine/localize DoS attacks
- Having Link Agg under MACSec would allow additional attacks (spoofing aggregation membership, for example) as LACP would be in clear
- -> MACSec must be placed below LinkAgg to remove these DoS pportunities

What 802.1 should do in MacSec with 802.3's explicit knowledge

• Document the placement of MACSec as being below LinkAgg in the Bridge Port's "MAC Stack"

The longer term plan

• Continue to work with 802.3 to converge the 802.1 ISS, the 802.3 MAC service, and the P802.1AC MAC Service definition
– 802.3 service used to lack the SA; this has now been fixed
– ISS currently has user priority and access priority – largely a hangover from 802.4 and 802.5 MACs – can and should be reduced to a single parameter
– *Local "return codes"* seem to have disappeared from 802.3 some while ago *(Non Issue)*
– Once we have service convergence, ensure the management view fits together properly
• This may take some time; in the meantime it is clear what the protocols need to do.

TOPIC 3: Minimum frame size problem - 1

• **No explicit length in Ethernet (Type interpretation) frames:**

– For large frames, length is recovered from physical frame length

– For small (minimum frame length) frames, determination of the actual number of user data frames is possible only by the recipient protocol entity

• **MACSec protected frames carry an ICV trailer (after the user data):**

– With current MACSec proposal, minimum sized secured frames can contain 0-28 octets of PAD

– Padding likely to be (but not necessarily) applied after MACSec

– For some combination of minimum frame length and ICV length, the ICV position may therefore be indeterminate

– Therefore, need a user data length indication (more strictly, an ICV position indication)

Minimum frame size problem – 2

• Remedy: Indicate the position of the ICV in short frames (less than 63 octets)
– 6 bits available for this (see frame format earlier)
– 1 bit to indicate "Get length from physical frame size"
– 5 bits to indicate explicit length/ICV position

"EtherType"

- One of the ballot comments on P802.1AB pointed out that this term (which is already in common usage), or an agreed variant of it,needs to be standardized
- We believe the right place to do this is in the 802.3 standard
- It would then be appropriate for 802, 802.1AB, …etc. to reference that definition
- The IEEE Registration Authority web pages also use the term; they should make use of whatever term is agreed for insertion into 802.3

802.3 Response

Submit an 802.3 Maintenance
Request – *Already in Process*