Security Is A Requirement

A Short Summary

Brian Ford	BellSouth
Kent McCammon	SBC
Sam Sambasivan	SBC
Yannick Le Goff	France Telecom
Charles Cook	Qwest
David Thorne	British Telecom

- Many Public Network Providers want Interoperable Layer 2 security prior to deployment of EPON.
- End Users want it. (Customers of Public Net Providers)
  - Business Users prefer a layered approach to security that includes encryption at Layer 2.
  - Residential Users do not want their data sent in the clear (much like difference between analog and digital cellular phone calls).
- Competing Technologies Include Layer 2 Encryption:
  - DOCSIS
  - ITU-T / FSAN
  - Need similar/superior capabilities and features to be competitive.

Security Objectives for Ethernet Passive Optical Networks (EPON)

Charles Cook-Qwest
Brian Ford-Bellsouth
Onn Haran-Passave Networks
Yannick Legoff-France Telecom
Mani Mahalingam-Avaya
Kent Mccammon-SBC
Richard Michalowski-Sprint
Antti Pietilainen-Nokia
Yukihiro Fujimoto-NTT
Dan Romascanu-Avaya
Dolors Sala-Broadcom
Sam Sambasivan-SBC TRI

- A list of security objectives for EPON (P2MP) are provided for discussion during the Security Meeting at the 802.3ah October Interim meeting in New Orleans
- The objectives are driven by the proposed application of EPON to public networks

Security Objectives for Ethernet Passive Optical Networks (EPON)

- IEEE should start a work item to develop a security specification specific to EPON for use in public access networks.
- EPON downstream encryption of payload is a requirement for use in public networks.
- MAC address encryption should be a study item.
- EPON upstream payload security may be required.
- Downstream and upstream ONT authentication is desired.
- A threat model specific for Ethernet PON should be developed with interested stakeholders such as service providers, vendors, users etc. in the appropriate group within IEEE 802.
- The strength of encryption should meet or exceed the level provided in other point to multi-point public access networks such as wireless networks, cable networks, etc.
- Residences and businesses should be able to use the same security model and coexist on the same PON.
- The protocol accommodation for security and the specific encryption algorithms should be separated to enable the specification to incorporate stronger encryption solutions in the future with none or minimal protocol changes.
- IEEE 802 should consider a separate yet complementary study effort to the EPON work items with the objective of developing common security mechanism across multiple IEEE 802 Groups. For example, using a security solution common to 802.11, 802.16, 802.17, and 802.3ah.