Link Security for IEEE 802 Networks

Call For Interest

Presented by

Dolors Sala

IEEE 802 Plenary Meeting

Kauai, Nov 12, 2002

Contributors and Supporters

Charles Cook, Qwest
Frank Effenberger, Quantum Bridge
Norm Finn, Cisco
Brian Ford, BellSouth
Yukihiro Fujimoto, NTT
Bob Gaglianello, Lucent
David Halasz, Cisco
Onn Haran, Passave
Masoud Khansari, Centillium
Jin Kim, Samsung
Yannick Le Goff, France Telecom
Kent G. Mccammon, SBC
Mahalingam Mani, Avaya
Richard Michalowski, Sprint
Gerry Pesavento, Teknovus
Antti Pietilainen, Nokia
Allyn Romanow, Cisco
Dan Romascanu, Avaya
Dolors Sala, Broadcom
Sam Sambasivan, SBC
Bruce Tolley, Cisco

The Need for Link Security

- **The immediate need is link security for EPON**
- **Link security is becoming a need for some IEEE802 wireline networks as these technologies are extended to operate in new applications**
  - 802.3 extends to LAN/MAN/WAN in enterprise and subscriber access networks
  - 802.17 is a metro service provider operated network
  - On the other hand, 802.5, 802.6 networks have not evolved to any of these scenarios to require security functionality
- **Future 802 MACs (wireless or wireline) will need to be designed having link security considerations in mind**
- **Therefore, there is the need for a set of global guidelines and/or specifications that guarantees commonalities and avoids duplication in designing the above**

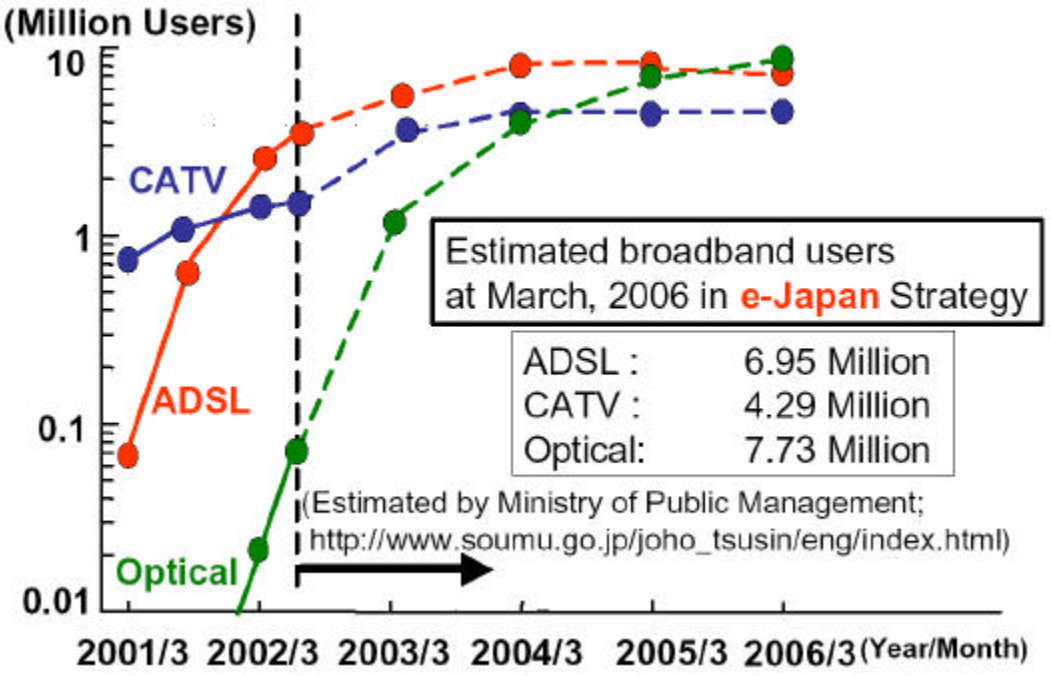
Why L2 Security

- **There are many protocols that are not securable via Layer 3: NetBEUI, Spanning Tree, Link Aggregation, GxRP, DHCP, ARP, IPX, …**
- **The organization legally or practically responsible for the solution may not have Layer 3 access to the endpoints**
- **An L2 secure link is “lighter”, i.e. involves fewer protocol elements than an L3 secure link**
- **Security provides value-add for Layer 2 carriers**

Multi-Layer Security

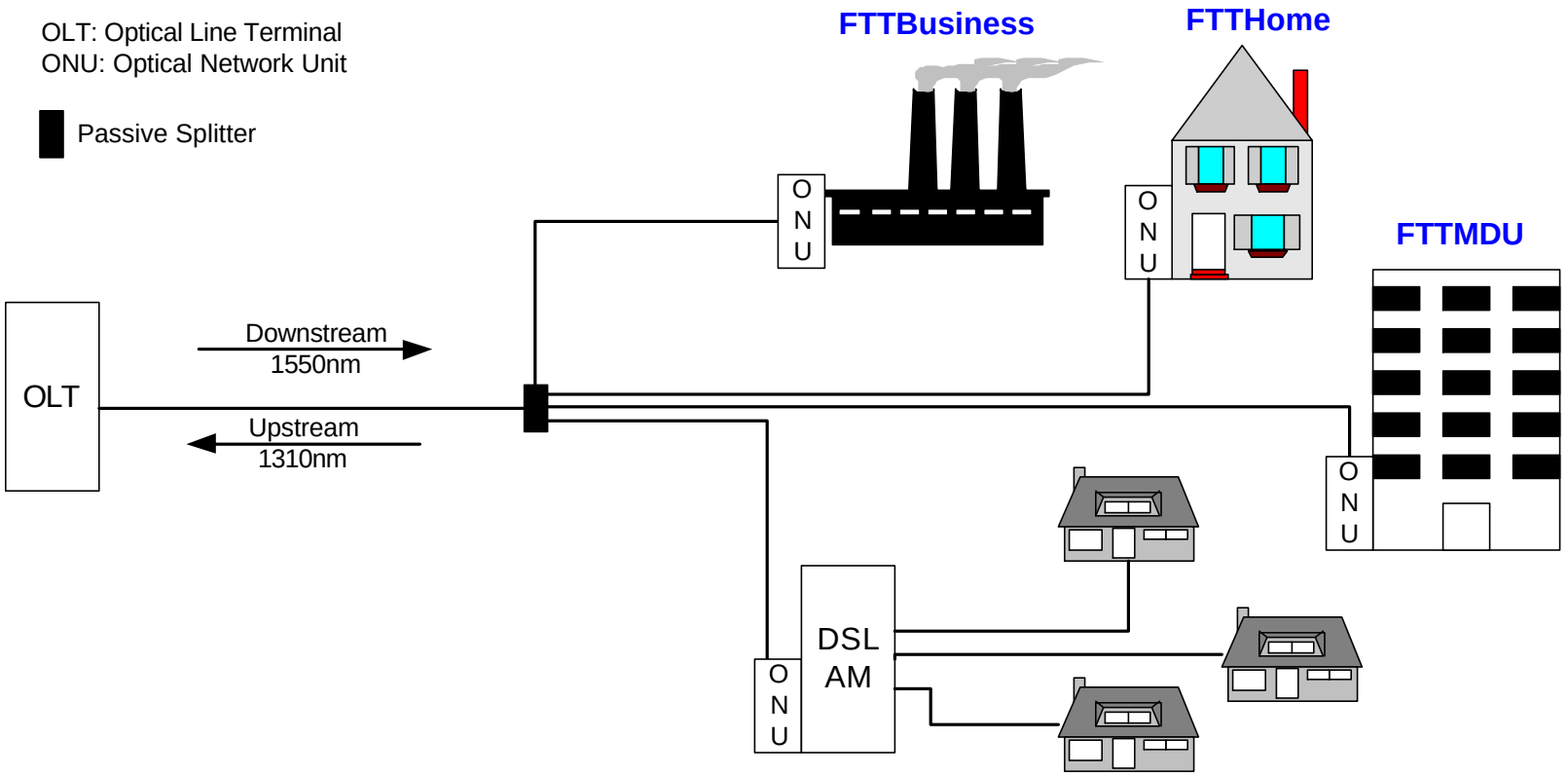
- **Why, today, do I run HTTPS over VPN/IPSEC over secure DOCSIS?**
- **HTTPS protects my credit card number across the big-I Internet.**
- **VPN/IPSEC connects my PC to a point behind my company firewall**
- **DOCSIS prevents my neighbors from stealing my cable bandwidth**
- **Three different scopes of responsibility, three different sets of requirements: a triply-encrypted packet**

Why Now: Japanese Broadband Access



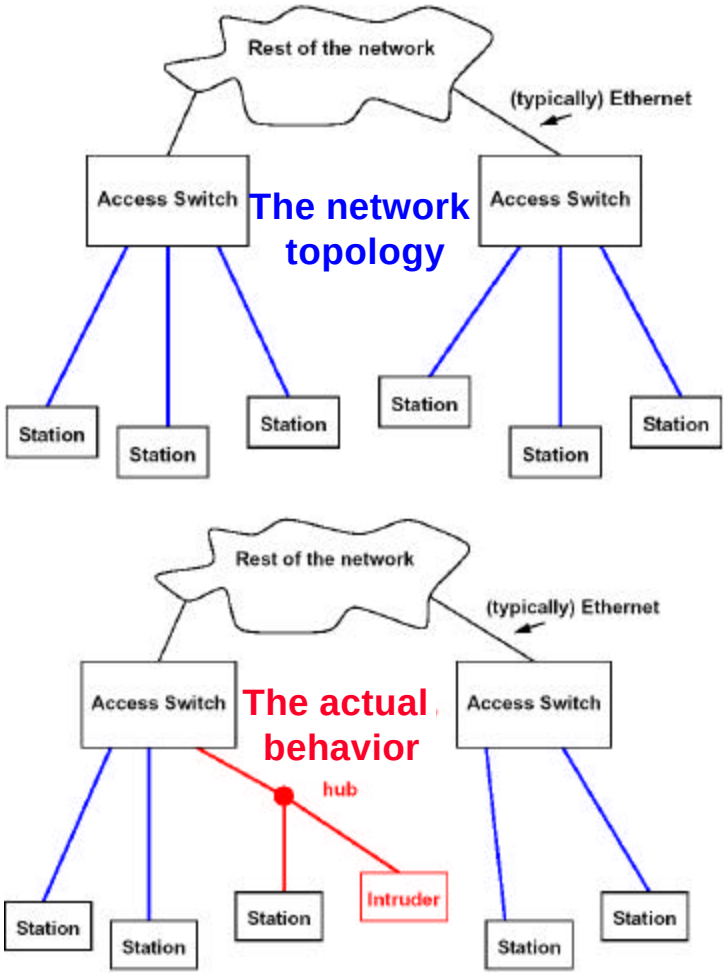
More than 4 million FTTH in three years, 100K PON by the end of the year
A significant portion of the optical is PON (needed for mass deployment and to reduce monthly fee)
The Asia/Japanese market is ready
Ethernet PONs needs link security for deployment now!

Passive Optical Networks (PONs)



- Shared upstream & broadcast downstream
- Observers sitting at home or office receive the data of their neighbors (i.e. eaves-dropping)

Threat Scenario Applicable to All IEEE 802 Networks



- **Any device in the network can**
  - Masquerade as another
  - Spoof information
- **Establishing security associations (SAs) in the link can detect and prevent such behavior**
- **The SA can be established**
  - Point-to-point: Between two authorized users
  - Multicast: Between a group of authorized users
- **Secure multicast needs special attention**
  - Key management is more demanding
  - Layer 3 may be more appropriate for P2P scenarios
  - But shared networks should be able to take advantage of broadcast nature of the media

Link Security in IEEE 802

- **802.10 defined a general link security framework in anticipation of the future IEEE 802 security needs**
  - Resides at the LLC layer (can protect payload but not MAC fields and MAC control and management messages)
  - Highly configurable protocol
    - It cannot be applied until a configuration document is defined
    - Each MAC application can define its MAC specific functionality overwriting the general specification
    - Specifies a fragmentation mechanism to handle the increase of frame size due to security fields
      - Specific MAC applications can define their own mechanism if fragmentation is not desired
  - It had the right general view however it suffers from too much generality
  - It is not currently used

Link Security in IEEE 802

- **The first use of link security in IEEE 802 was in wireless networks**
  - The shared media combined with the easy access to the (air) media has created the first need of link security to protect the bandwidth and information transmitted
- **Each MAC has designed its own mechanism as needed (independent of the 802.10 framework)**
- **802.1x has already emerged as a common framework for authentication**
- **These experiences offer**
  - Expertise on how to solve the link security problem for specific MACs
  - Experience to identify the common functionality independent of MAC details

A Broader Approach

Study the possibility to define a link security mechanism that can be applied to as many MACs as needed, allowing MAC dependent specification where required

Objectives of the Proposed SG

- **The objective is to define a link security mechanism that is applicable to as many IEEE 802 applications as possible, and flexible to allow for MAC differentiation when needed, to incorporate new security needs as they become important for new MACs or networking applications, and to evolve according to new technology advances**

- **The recommendation is to form an Sponsored Executive Committee Study Group (SEC SG) to evaluate the design tradeoffs and recommend the best approach to take towards the specification of the next IEEE 802 link security mechanism. The SG should take a global view and consider the future security needs of IEEE 802 networks, but give priority in the work schedule to the immediate needs of EPON**

SG Tasks

- **Specific tasks of the SG group will be:**
  - Threat analysis
  - Evaluate main security design criteria in order to recommend
    - A set of functionality that can be the basis for a common framework applicable to all existing and future IEEE MACs
    - Whether there is the need of MAC specific functionality
    - Whether the framework should be defined with a set of guidelines as design criteria or a set of specifications defining the actual link security mechanism
    - The placement of this work in the 802 organization and/or layer model
  - Write a PAR and 5 criteria for the specification of a link security mechanism applicable to at least EPON networks and based on the above recommended work plan

Threat Analysis

- **The threat analysis is the characterization of the security vulnerabilities of the network**
- **The counter measures are the mechanisms used to protect the vulnerabilities**
- **The importance of each threat and the potential counter measures to apply may depend on the application**
  - Example: absolute MAC addresses are a vulnerability source for denial of service attack, traffic analysis…
    - The number of MAC addresses in a 802.11 network is assumed to be equal to the number of hand set devices. Therefore, 802.11 can afford to use temporary MAC addresses as counter measure of this threat.
    - On the other hand, EPON is just another segment in a 802.3 network. In this case, the use of temporary MAC addresses is less viable

The Level of Protection

- **There is no such thing as perfect protection. Any system can be cracked with enough time and resources**
- **The level of protection applied is rather subjective based on the network threats, the cost of the security mechanism, and the ability of the expected attackers in this scenario**
- **The security analysis is the process of identifying how much protection should be applied in the system to consider the network secure enough to operate for the target applications and/or scenarios**

Layer Model

- **The layer model depends on the counter measures applied**
- **Should a single layer model be defined? Or can it be implied by the set of counter measures if a combination of them can be applied?**
- **Some considerations on the layer model:**
  - Should MAC control and management frames be protected?
  - Is it important to forward frames across bridges without the need of decrypting and encrypting again?
  - Is traffic analysis important?
  - Should MAC fields be assigned double functionality and reused to avoid security fields?

MAC Independence

- **A MAC independent specification can be achieved if the security mechanism is applied either above or below the MAC as long as the two are maintained independent**
  - Above the MAC may allow easier bridging
  - Below the MAC it protects all frames and fields
- **The level of dependence and independence between the two needs to be evaluated. This includes factors such as:**
  - Power
  - Complexity
  - Risk level of the Threat
  - Cost
  - MAC protocol design

Common Framework

- **Can the common framework be defined as a set of specification rules which selects the specific counter measure to use for every threat? Or should a set of guidelines be defined instead?**
- **Is it worth defining a link dependent security specification to account for the MAC/media differentiation?**
  - Are MAC/media constraints important enough to consider differentiation?
    - Ex: should the same encryption mechanism (i.e. DES/AES) be applied at Kbps than Gbps?
  - Is it worth to take advantage of MAC specific functionality to assist link security mechanism?
    - Ex: Use the EPON global clock to avoid transmitting the IV
- **Can the additional functionality be added to the corresponding MACs and hence avoid most of the link dependent specification?**

Benefits

- **A common link security for IEEE 802 offers an initial solution for all MACs that need one**
- **The wireless MACs with existing link security (802.11, 802.15, 802.16) mechanisms can continue to use their own**
  - We will use their experience and expertise
- **A common framework flexible to allow differentiation and to evolve as needed can offer the right balance for a long lasting link security mechanism for IEEE 802 networks**
- **A common approach for link security also offers a single approach of the IEEE 802 security scope and the division of this functionality with higher layers**

Summary

- IEEE 802 Wireless networks have shown the need of link security
- While defining the link security solution for Ethernet P2MP networks, we would like to take maximum advantage of all existing work by borrowing all common functionality in a common framework that can be applied to all IEEE 802 networks
- An executive study group should be formed to evaluate the viability of this general solution and to recommend a work plan and write a PAR and 5 criteria to execute the plan
- In this presentation, some of the aspects to be evaluated have been described, more may arise. Additional material on this work can be found in http://www.ieee802.org/3/efm/public/sep02/sec/