Comparative Analysis of Link Security Mechanisms

Mani Mahalingam, Avaya

Dolors Sala, Broadcom

Antti Pietilainen, Nokia

Link Security

- **Imposing end-to-end security to accommodate a shared link in the path is not an option**
  - What protocol should be used? IPsec? IEEE 802.10?
  - How can we mandate the use of security to all end equipment in the world?

- **Link security has been added to all subscriber access technologies with shared topologies:**
  - 802.11i
  - 802.15
  - 802.16/DOCSIS (BPI+)
  - FSAN G983.1 (ITU-T Q.2 SG15)

- **Is there a middle ground?**

IEEE 802.11 Security

- **802.11 most widely deployed Wireless LAN standard**
- **Most common topology: Hub–Spoke (AP-station) model**
  - Hubs (AP) may connect to wired network (infrastructure) (BSS)
  - Broadcast medium that any outsider WLAN station/AP can listen on & transmit to.
- **AdHoc networks (peer-peer) of stations allowed (IBSS)**
- **Current WEP security flawed, new draft standard in the works, 802.11i – a.k.a RSN (Robust Security Network)**
  - RSN is a common framework that addresses the AdHoc and Infrastructure modes.

802.11 Threats

- **Spoofing**
  - An AP or station identity may be impersonated.
- **Tampering**
  - Message transmissions can be modified and retransmitted undetectably
- **Repudiation**
  - Sender / receiver may not be accountable for an exchange of information.
- **Information Disclosure**
  - Lack of confidentiality, identity protection.
- **Denial of Service**
  - An unauthenticated outsider station can disrupt legitimate communication, e.g., by sending disassociates (to clients/AP).

802.11i RSN Security Services

- **Upper Level Source Authentication (above)**
  - 802.1X (EAPOL)
    - Star/hub-spoke: for station (client) -AP (in a BSS)
    - Peer-peer: station-station (in ad-hoc mode)
    - May use multiple authentication methods. Typically
      - Typically TLS (two-way): EAP-TLS
      - EAP-TTLS, EAP-PEAP
        - One-way TLS authentication with supplementary client auth.
- **Data confidentiality, Privacy**
  - Encryption performed at the MPDU level
- **Message Integrity**
  - Also performed at the MPDU level
- **Replay Detection**
  - Uses sequence counters with protected datagrams
- **DoS Protection**

RSN Security Model

- **IEEE 802.1X used for upper layer authentication**
  - Also used for key management: temporal key distribution.
- **Three privacy protocols supported :**
  - TKIP (legacy equipment), WRAP and CCMP protocols: CCMP is of interest here.
  - All above use 802.1X for authentication and key distribution.
- **<802.1X, CCMP> extended to IBSS (adhoc network) security.**
- **Confidentiality, integrity of data protected, marginal protection for DoS,**
  - Unicast & Multicast security.
- **Control, management messages not protected.**

Key Management (1)

- **Pairwise set of keys for unicast traffic**
  - A set of five keys per client-AP pair: two EAPOL Keys; and three transient keys
  - Transient keys exchanged in a four-way handshake of EAPOL key messages.

- **Group keyset for multicast traffic**
  - Three keys per BSS.
  - Conveyed to client in a two-way handshake.

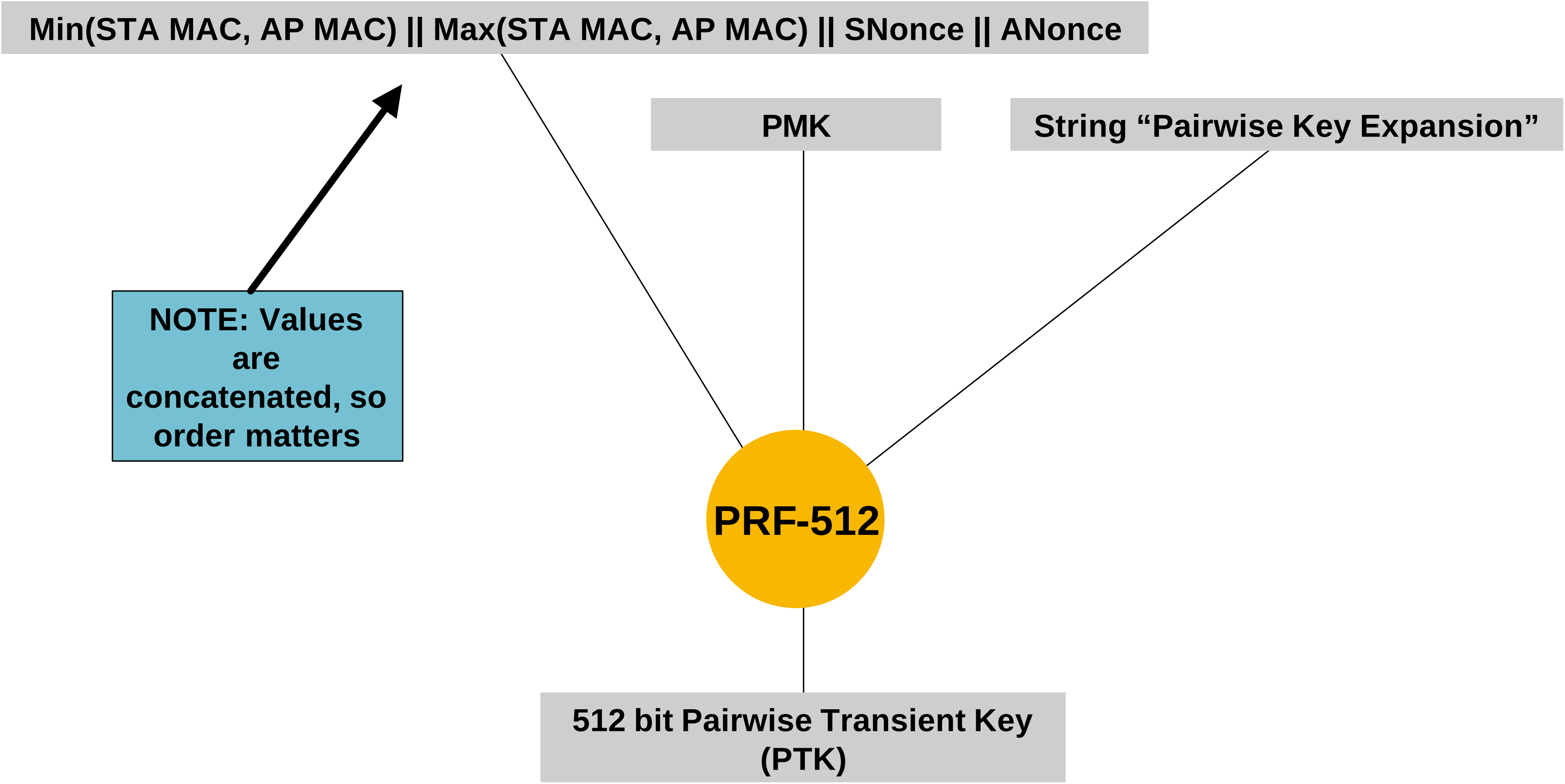
- **Client traffic blocked until the above two exchanges are complete.**

Key Management (2)

- **Pairwise Keys: Unicast data**
  - Master Key (PMK): generated out of 802.1X auth. Exchange
  - Five keys are derived with master key (PMK)
  - Transient Keys (PTK pairwise transient keys)
    - A TEK: encryption
    - 2 MIC's (TMK): for message integrity (upstream, downstream)
    - EAPOL-KEK (encryption), EAPOL-KMK (message integrity)

- **Group Keys**
  - Used for multicast, broadcast
  - The keys are shared common across the BSS by the AP.
  - Group Master Key (generated by AP)
  - Group Transient Key (GTK): derived from GMK
    - Derive three keys: 2 MIC keys (GTMK) and one (GTEK)
  - In very marginal TSN's the GTK is used for encryption
    - Boils down to old WEP-level security vulnerability.

The Pairwise Key Hierarchy



Min(STA MAC, AP MAC) || Max(STA MAC, AP MAC) || SNonce || ANonce

PMK

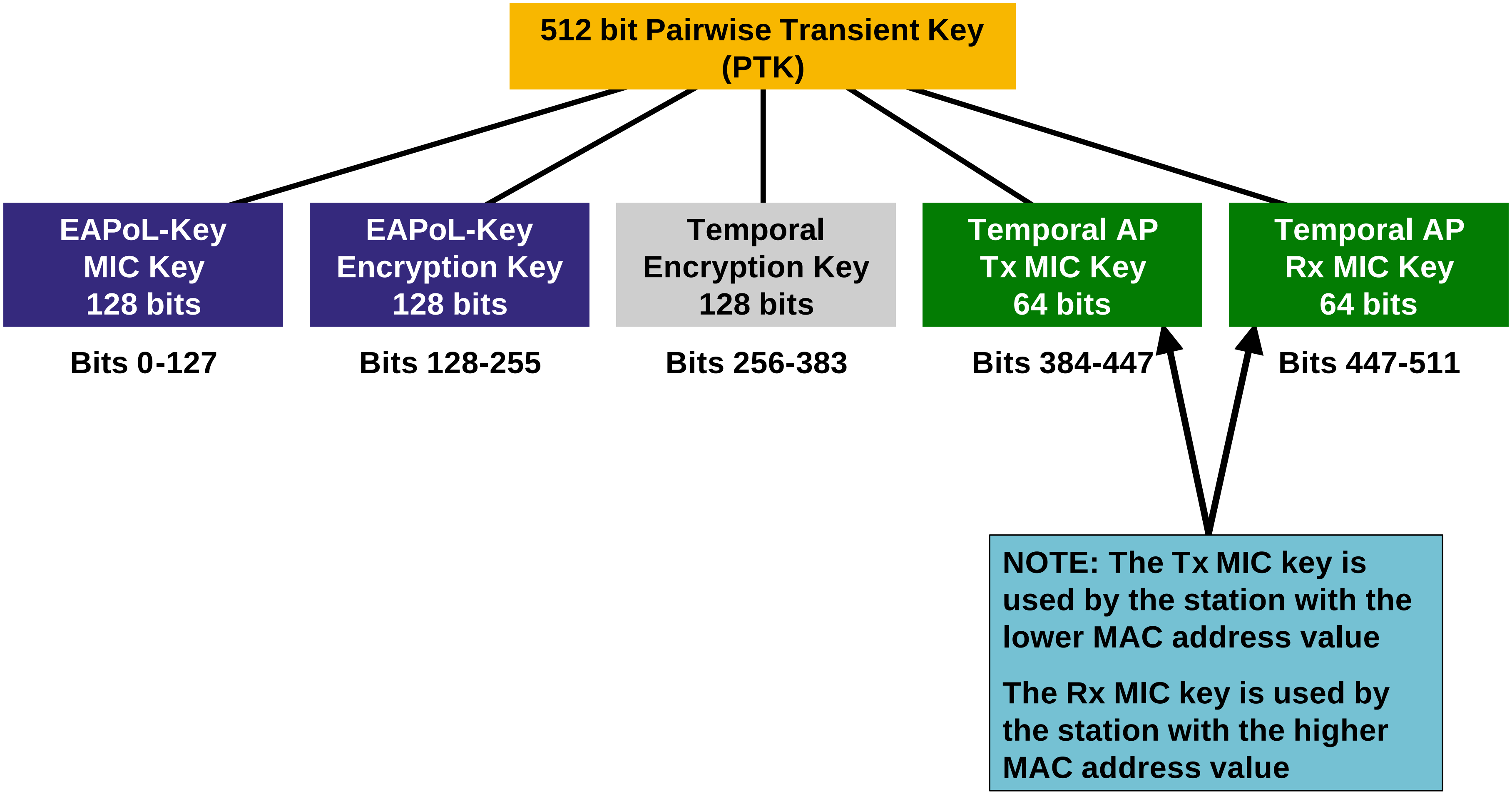
String “Pairwise Key Expansion”

NOTE: Values are concatenated, so order matters

PRF-512

512 bit Pairwise Transient Key (PTK)

The Pairwise Key Hierarchy



512 bit Pairwise Transient Key (PTK)

EAPoL-Key MIC Key 128 bits

Bits 0-127

EAPoL-Key Encryption Key 128 bits

Bits 128-255

Temporal Encryption Key 128 bits

Bits 256-383

Temporal AP Tx MIC Key 64 bits

Bits 384-447

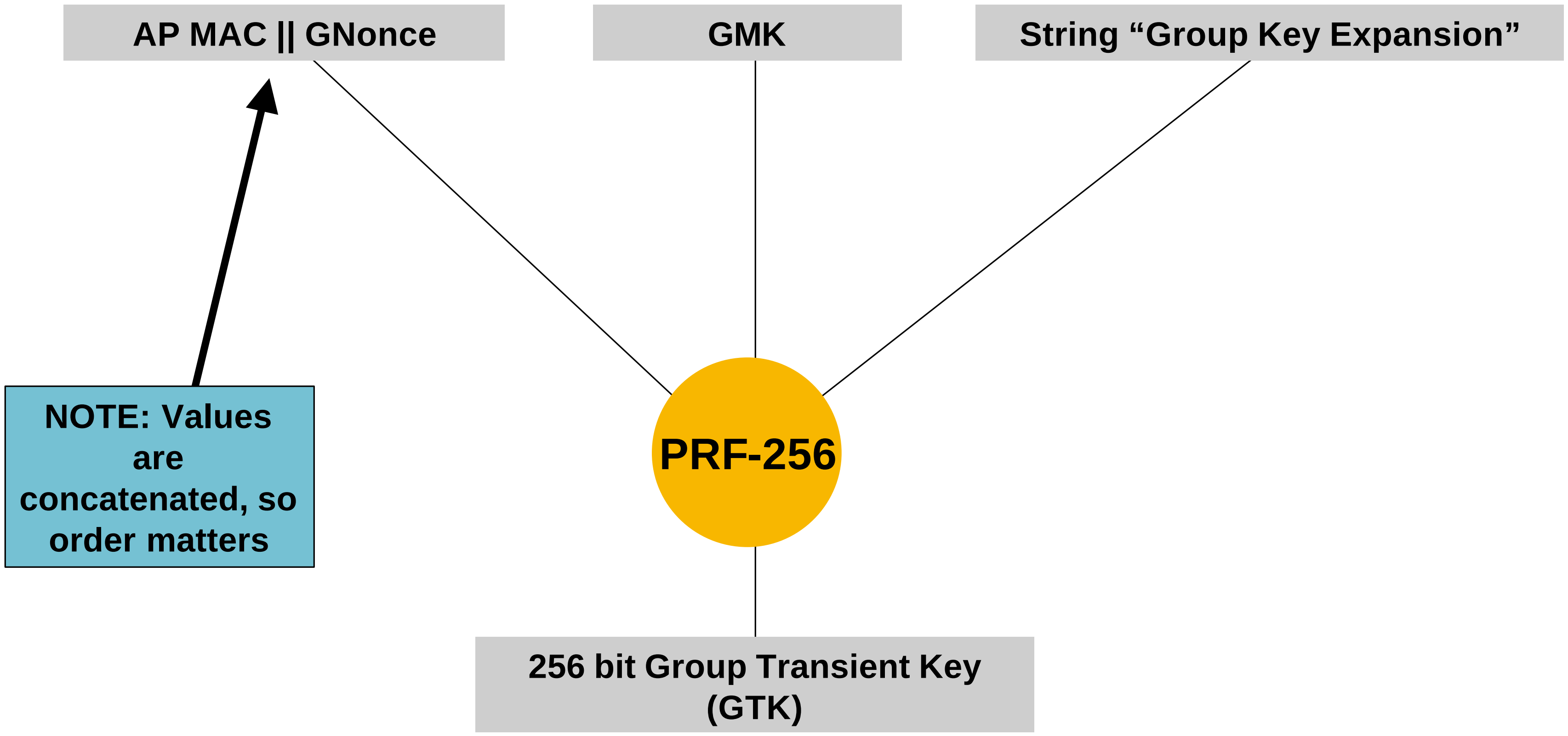
Temporal AP Rx MIC Key 64 bits

Bits 447-511

NOTE: The Tx MIC key is used by the station with the lower MAC address value

The Rx MIC key is used by the station with the higher MAC address value

The Group Key Hierarchy



AP MAC || GNonce

GMK

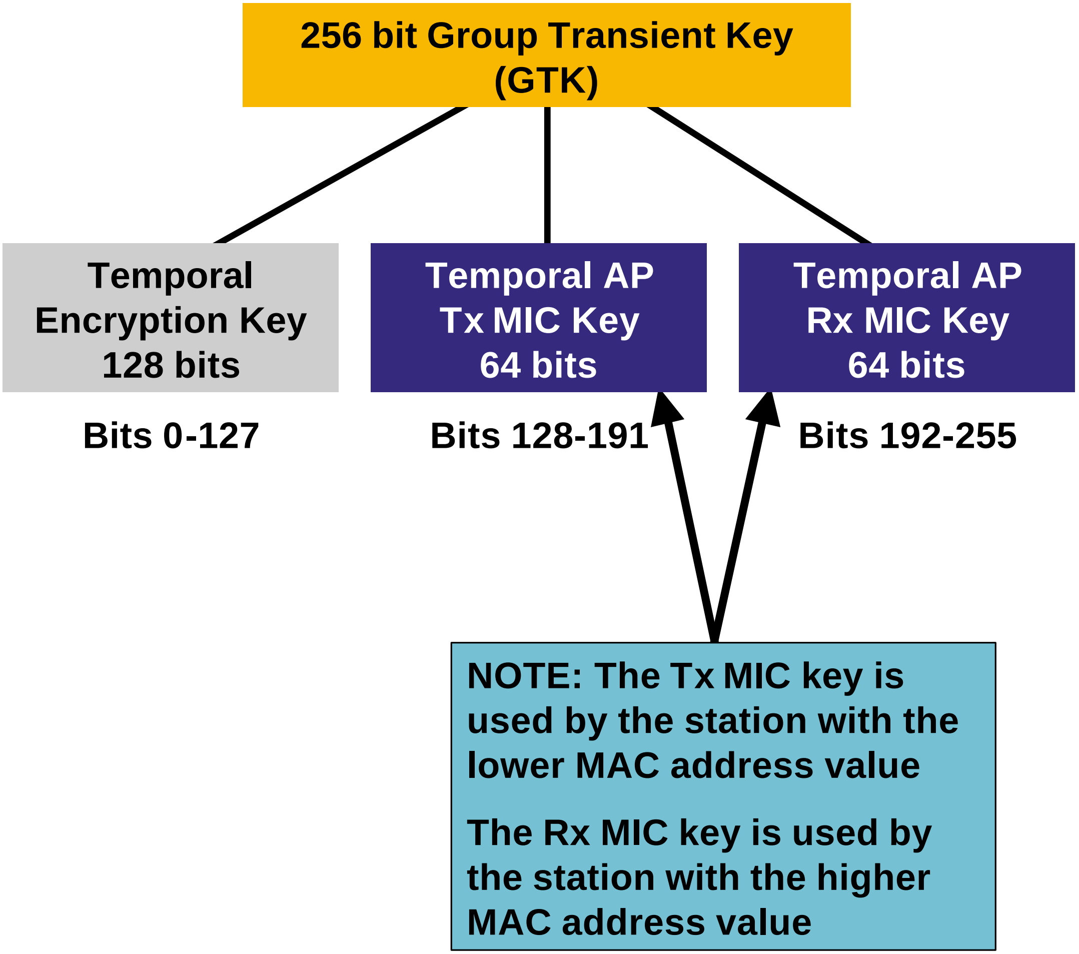
String “Group Key Expansion”

NOTE: Values are concatenated, so order matters

PRF-256

256 bit Group Transient Key (GTK)

The Group Key Hierarchy



256 bit Group Transient Key (GTK)

Temporal Encryption Key 128 bits

Bits 0-127

Temporal AP Tx MIC Key 64 bits

Bits 128-191

Temporal AP Rx MIC Key 64 bits

Bits 192-255

NOTE: The Tx MIC key is used by the station with the lower MAC address value

The Rx MIC key is used by the station with the higher MAC address value

Security for 802.11 IBSS

- **Each station now treated as a <AP, station, AS> to rest of members**
  - A model very identical to ESS is applied each way.
- **Pairwise Keys: Same approach as for ESS but with subtle difference as below:**
  - Each pair of stations perform key exchange separately in each direction (since each acts as supplicant in turn)
  - Therefore two sets of pairwise keys are produced
  - Unicast messages are encrypted with key from the Authenticator with the lower MAC address
- **Group Keys**
  - Each STA uses its own group key for its multicast transmissions – this is same concept as in ESS AP case.
  - Consider STAx. All other STAs that want to communicate with STAx must first exchange keys. STAx sends its multicasts using its own group key. All valid STAs can understand if they know STAx's group key.
  - This is true for every STA – it has own group key and shares it only with those STAs that exchange pairwise key.
  - Method for creating and sending group key is the same as for ESS case (AP to STA)

IEEE 802.15 WPAN

- **AdHoc networking: open comm. medium**
  - devices may or may not have ever met before
  - Piconet is a basic unit: star-network topology
- **No connection to external networks assumed**
  - the normal case for WPAN
- **Assumed that devices external to the network can both listen on and transmit data**
  - Upstream & downstream
- **Piconet controller (PNC) is the security coordinator – normally the master of the Piconet**

802.15 Threat Model

- **Threats in 802.15 very similar to those of 802.11**
  - Hub-like wireless medium where
    - a device in range can listen in on communication between two parties
      - device can pose a man-in-the-middle threat
      - Can fake a PNC or a device.

- **Non-goals (threats to protect from)**
  - Denial of service
  - Individual source authentication on group messages
  - Traffic analysis

Threat Assumptions

- **Computational capabilities**: It is assumed that the attacker has state of the art technologies to perform rapid computations.
- **Listening capabilities**: It is assumed that the attacker is within listening range of the DEVs in the piconet and understands the communication mechanism.
- **Broadcast capabilities**: It is assumed that the attacker has sophisticated broadcasting equipment that is able to synchronize with the piconet and transmit data for the DEVs in the piconet at the appropriate time.
- **Security setup**: The security setup for the DEVs occurs either before entry into the piconet or after the piconet has been established.No assumptions are made about the presence of attackers during security setup.

802.15.3 Security Services

- **Trust establishment**
- **Authentication of devices**
  - TLS-like public key mutual authentication between PNC and device; or peer-peer between devices
- **Key management**
  - Using public keys or digital certificates during auth.
  - Authent. is basis for establishing comm. keys for encryption and integrity (below).
- **Freshness detection (against replay)**
  - Liveness of transmissions using counters
- **Message Integrity Protection**
  - Both data payloads and commands
- **Confidentiality, Privacy Protection as well on data payloads**

802.15 Security: MAC formats

Beacon Frame Format: Integrity-protected by MIC

Beacon header	Current SSID	Time token	Message Integrity Code(MIC)

Command Frame Protection Format

Cmd. header	**Current SSID**	**Time token**	**counter**	**IV**	**Encrypted payload (cmd)**	**Message Integrity Code(MIC)**

Data Frame Protection Format

Data Header	**Current SSID**	**Time Token**	**IV**	**Payload (encrypted data)**	**Message Integrity Code (MIC)**

IEEE 802.16 - WMAN (DOCSIS)

- Baseline Privacy Plus (BPI+) Interface Specification
  - Finished on March 2002 based on BPI (started 1998)
  - BPI+ adds CM authentication to BPI, SAIDs and improves encryption
- BPI+ employs X.509 version 3 digital certificates for authenticating key exchanges between the CM and CMTS
  - Key exchange messages are encrypted with 3DES with double key and message authentication adding a 20 bytes digest (RFC 2104)
- BPI+ establishes Security Associations (SAs) to encrypt traffic upstream and downstream
  - User data is encrypted with DES using a 64 bits key
- The DOCSIS system supports the remote downloading of code to its network cable modems. There are multiple levels of protection.
  - The manufacturer of the CM code always applies a digital signature to the code file
  - In addition, an MSO may later apply their code signature
  - The CM must verify both signatures with a certificate chain that extends up to the DOCSIS root before accepting a code file.

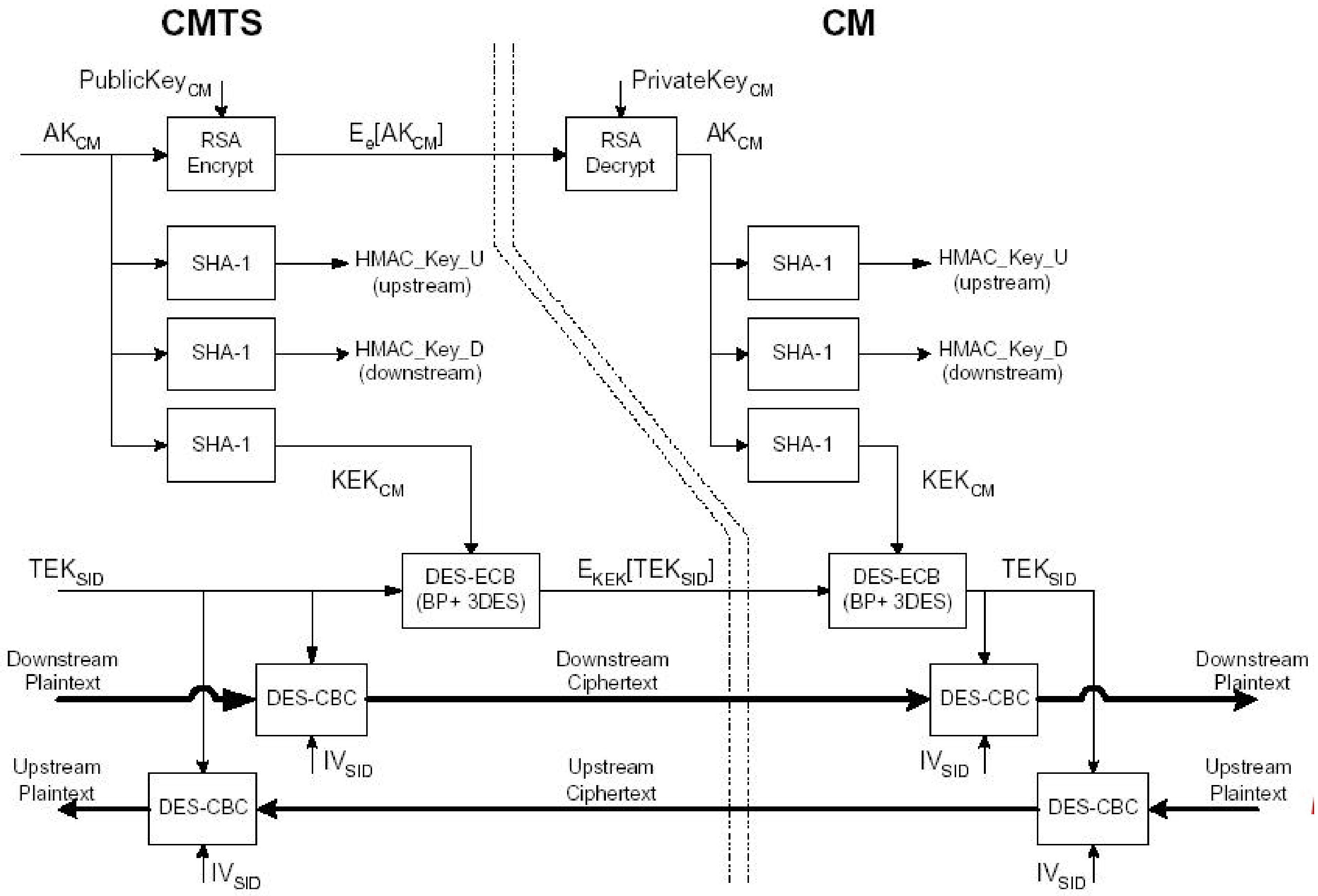
BPI+ Keys Hierarchy (1)

- RSA Public/Private Key:
  - Unique to each CM, they provide a secure way to communicate with an individual CM.
  - They are used to encrypt the Authorization Key for delivery to a specific CM.
  - A CM will keep the same RSA key pair over its entire operational lifetime.
- Authorization Key (AUTH_KEY):
  - Unique to each CM, the AUTH_KEY is sent by the CMTS to the CM once the CM has been approved for Baseline Privacy authorization.
  - The AUTH_KEY has a limited lifetime and must be periodically renewed

BPI+ Keys Hierarchy (2)

- Traffic Encryption Key (TEK): (64 bits, DES)
  - Each TEK is associated with a specific security association.
  - The cable modem must be capable of maintaining two active sets of TEK information.
  - Each TEK has a limited lifetime and must be periodically renewed.
- Key Encrypting Key (KEK): (128 bits, 3DES double 64 bit keys)
  - Derived from a CM’s AUTH_KEY
  - The KEK is used to encrypt TEKs for delivery to a CM.
- Message Authentication Keys: (RSA SHA-1)
  - Derived from a CM’s AUTH_KEY
  - Used to key the HMAC-SHA algorithm to calculate a message digest for downstream and upstream Key Request/Response messages.
  - A separate key for upstream and downstream HMAC-digest calculations

BPI+ Key Handling



Baseline Privacy Authorization

- The CM sends an authorization request to the CMTS that includes the CM’s
  - Unique MAC address, RSA Public Key, and one or more assigned unicast SIDs (first assigned during initialization).
- The CMTS will verify the CM’s service authorization.
- If the CM is approved for authorization, the CMTS will send an authorization reply including a list of assigned unicast and multicast SIDs, and an encrypted authorization key (AUTH_KEY) unique to the cable modem.
- The AUTH_KEY is RSA encrypted with the CM’s public key.
- Once the cable modem has been authorized, the CM shall initiate a TEK (Traffic Encryption Key) State Machine for each SID

Baseline Privacy Authorization

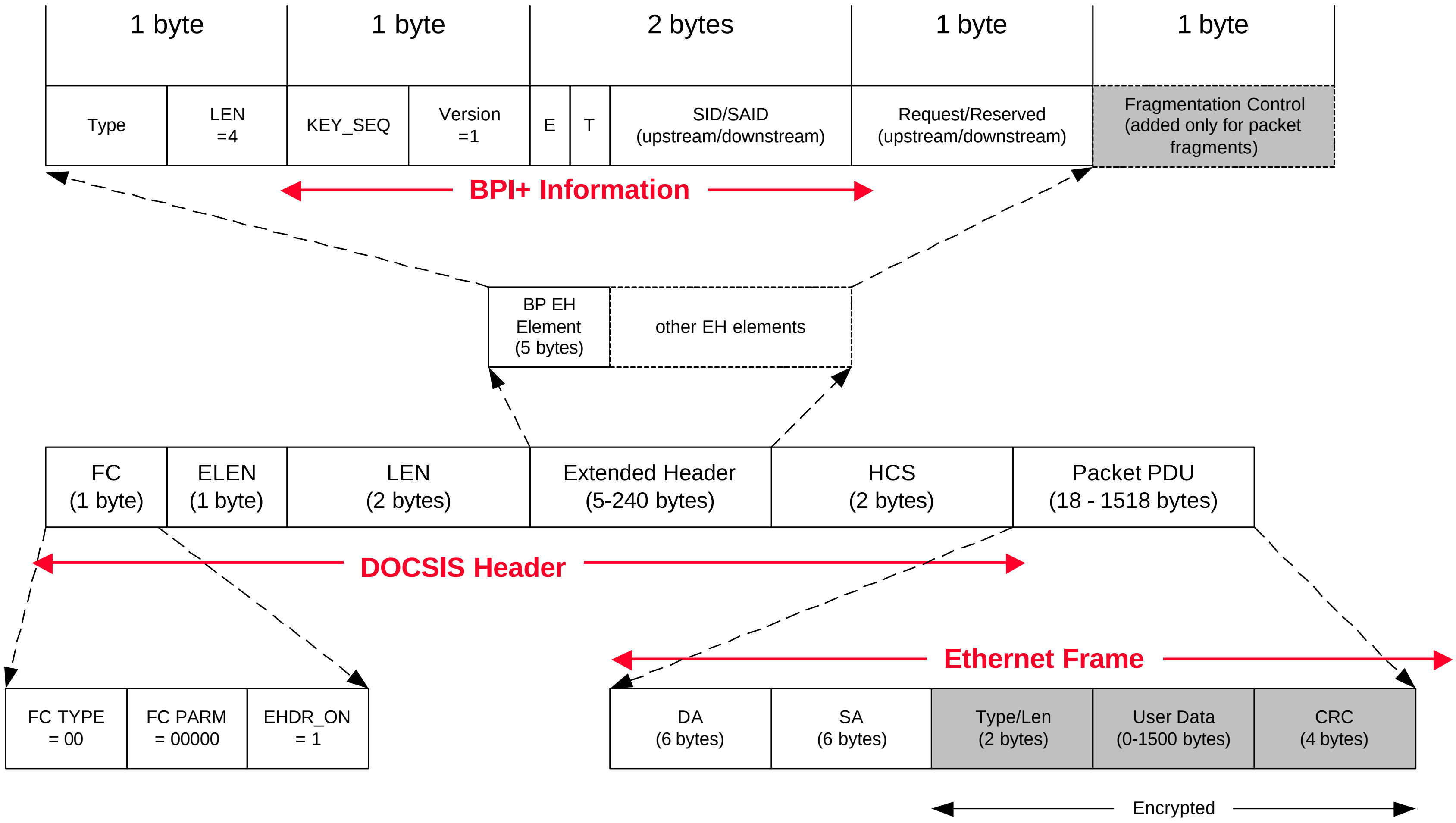
- The CM can now request and obtain traffic keys from the CMTS.
  - Traffic Keys are used to encrypt packet data traffic between the CM and CMTS.
  - To obtain TEKs, the CM will send a key request, requesting a TEK for each SID.
  - Key requests are authenticated using a Baseline Privacy HMAC digest.

- In response to key requests from an authorized cable modem, the CMTS will
  - Send key reply messages to the cable modem that contain an encrypted TEK, initialization vector (IV), key sequence number, and key lifetime (in seconds).
  - The key reply message is authenticated using the HMAC digest and an HMAC key derived from the CM’s authorization key.

BPI+ Security Associations (SA)

- Security Associations (SAs)
  - Identified with a 14-bit Security Association ID (SAID)
  - There is a primary SAID established at registration time
  - Additional SAIDs can be established
- All traffic upstream is encrypted using Primary SAID.
  - The value used for the primary SAID is identical to the CM's primary SID (service ID)
- On the downstream additional SAIDs are used for multicast traffic
  - IGMP management mechanisms in the CM triggers BPI+ Map Request messages that query the CMTS for the mapping of an IP multicast group address to an SA.

DOCSIS BPI+ Extended Header



1 byte		1 byte		2 bytes			1 byte	1 byte
Type	LEN =4	KEY_SEQ	Version =1	E	T	SID/SAID (upstream/downstream)	Request/Reserved (upstream/downstream)	Fragmentation Control (added only for packet fragments)

BPI+ Information

BP EH Element (5 bytes)	other EH elements

FC (1 byte)	ELEN (1 byte)	LEN (2 bytes)	Extended Header (5-240 bytes)	HCS (2 bytes)	Packet PDU (18 - 1518 bytes)

DOCSIS Header

FC TYPE = 00	FC PARM = 00000	EHDR_ON = 1

Ethernet Frame

DA (6 bytes)	SA (6 bytes)	Type/Len (2 bytes)	User Data (0-1500 bytes)	CRC (4 bytes)

Encrypted

FSAN G983.1- A/BPON

- **FSAN provides low level of protection for data confidentiality based on a data scrambling mechanism (Churning)**
  - It uses a 24-bit encryption key. Key update rate is at least 1 update per second per ONU.
- **Assumes a “secure” upstream channel, and hence all confidential information is generated by ONU and only transmitted in upstream**
  - ONU generates the keys and sends them to OLT
  - It prevents masquerade by ONU sending identification password to OLT on the upstream
- **Churning is used on P2P data connections on the downstream**
  - Churning is enabled or disabled per VP at its set up
- **The use of higher layer security is recommended if churning is not enough to meet the security requirements of a particular service**
- **FSAN is in the process of upgrading the definition**

G983.1- Key Change

- **G983.1 does not incurs any upstream overhead per cell transmission**
  - Key change indication is done with management messages

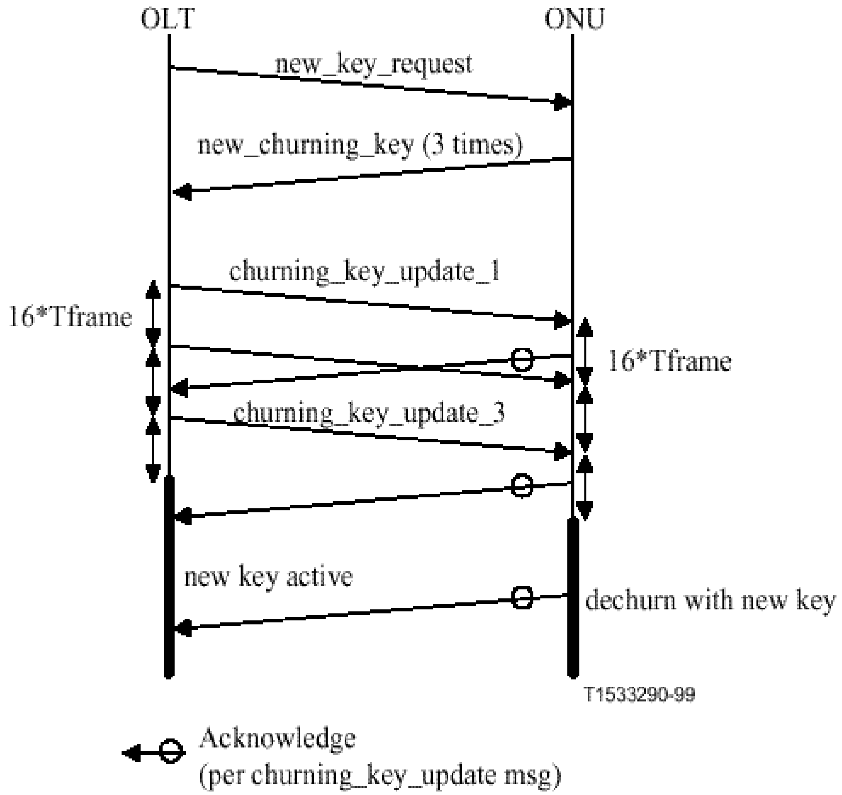


Figure 17/G.983.1 – Churning message flow

IEEE 802.10 Framework

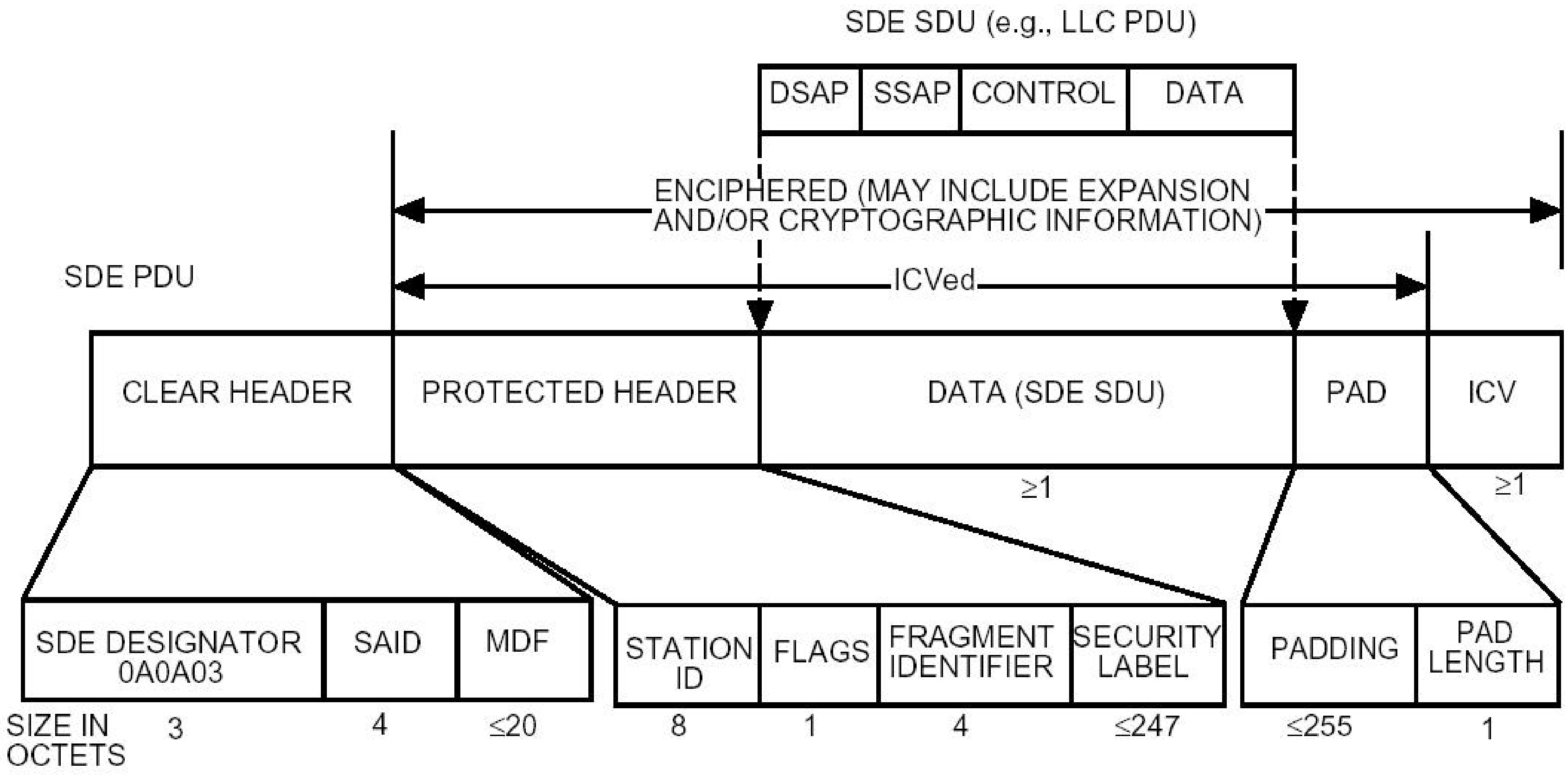


Figure 2-3—Structure of the SDE PDU

Comparison of Threats

	802.11	802.15	802.16/ DOCSIS	802.10	FSAN
Confidentiality	ö	ö	Up/Down	ö	Downstrm
Authentication	ö	ö	CM (Up)	ö	ONU (Up)
Msg Authentication	ö	ö	ö	ö	´
Data Integrity	ö	ö	ö	ö	´
Access Control	ö	ö	ö	ö	´
Privacy	ö	´	ö	ö	ö
Non repudiation of delivery	´	´	´	ö	´
Denial of Service	ö	ö	´	´	´

Comparison of Mechanisms

	802.11	802.15	802.16	802.10	FSAN
Encryption	AES-CCM	AES-CCM	DES 64bits 3DES;2xKey		Churning; 24 bit key
Authentication	802.1X	E22:TLS-like	CM (Up)		ONU (Up)
Msg Authentication	AES-CCM	AES-CCM	HMAC-SHA-1 FCS		´
Data Integrity	ö	ö	ö		´
Digital Signature	X.509, PSK	X.509, PSK	X.509		´
Replay Detection	ö	ö	´	ö	?
Protected Fields	SA,DA, data payload	payload of data, mgmt	Payload + FCS	Frame payload	Only cell payload
Layer	Below MAC	Below MAC	Below MAC	MAC client	MAC Client
Per frame OH	18-20		3 bytes		0 bytes
Secure Multicast	ö	ö	ö		´

TBS: to be specified

Conclusions

- **Link Security is needed for any shared subscriber access technology**
  - Mechanism is combined with access protocol
- **Ethernet must define its own security mechanism to operate in point-to-multipoint subscriber access networks**
- **It can leverage expertise and experience from all of these systems**

References

- **BPI+ : http://www.cablemodem.com/downloads/specs/SP-BPI+-I09-020830.pdf**
- **FSAN: ITU-T G.983.1 Broadband optical access systems based on Passive optical networks (PON)**
- **IEEE submissions: 11-02-551r1, 11-02-499ar1, 802.11i-D2.3**
- **IEEE 802.15.3**
  - Draft standard
  - http://www.securemulticast.org/GSEC/gsec3_ietf53_Singer.pdf