NEA Working Group
IETF virtual interim meeting
Jan 28, 2010

nea[-request@ietf.org

http://tools.ietf.org/wg/nea

Co-chairs: Steve Hanna shanna@juniper.net
Susan Thomson sethomso@cisco.com

Agenda Review

0800 Administrivia
- Jabber & Minute scribes
- Agenda bashing

0805 WG Status, Meeting Goal and Consensus Check Process

0810 Review PT submissions: TLS
- http://www.ietf.org/id/draft-sangster-nea-pt-tls-00.txt

0830 Review PT submissions: EAP
- http://www.ietf.org/internet-drafts/draft-hanna-nea-pt-eap-00.txt
- http://www.ietf.org/id/draft-cam-winget-eap-nea-tlv-00.txt
- http://www.ietf.org/id/draft-cam-winget-eap-tlv-00.txt

0930 Plan for developing WG I-Ds

0950 Next Steps

1000 Adjourn

WG Status

- In RFC Editor Queue
  - PA-TNC -06 I-D (Oct 2009)
  - PB-TNC -06 I-D (Oct 2009)

- Individual PT proposals submitted (Jan 4)

Meeting Goal

- Review individual PT proposals
- Propose path forward re developing WG drafts

Consensus Check Questions

- Do you support work on TLS-based PT?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

- Do you support adoption of PT-TLS as a -00 WG draft?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

Consensus Check Questions

- Do you support work on EAP-based PT?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

- What should we adopt as EAP-based PT?
  - EAP-TNC
  - NEA TLV
  - Other

PT-TLS Evaluation

What is PT-TLS?

- L3 PT Proposal Coming from TCG
  - Identical to TNC protocol IF-T Binding to TLS
- NEA Exchange Over TLS
  - Carried As Application Data
  - No Change to TLS
- Meets All Applicable PT Requirements

Why L3 PT?

- PT-5 says PT SHOULD be able to run over TCP or UDP
- Motivating Use Cases on Next Slide

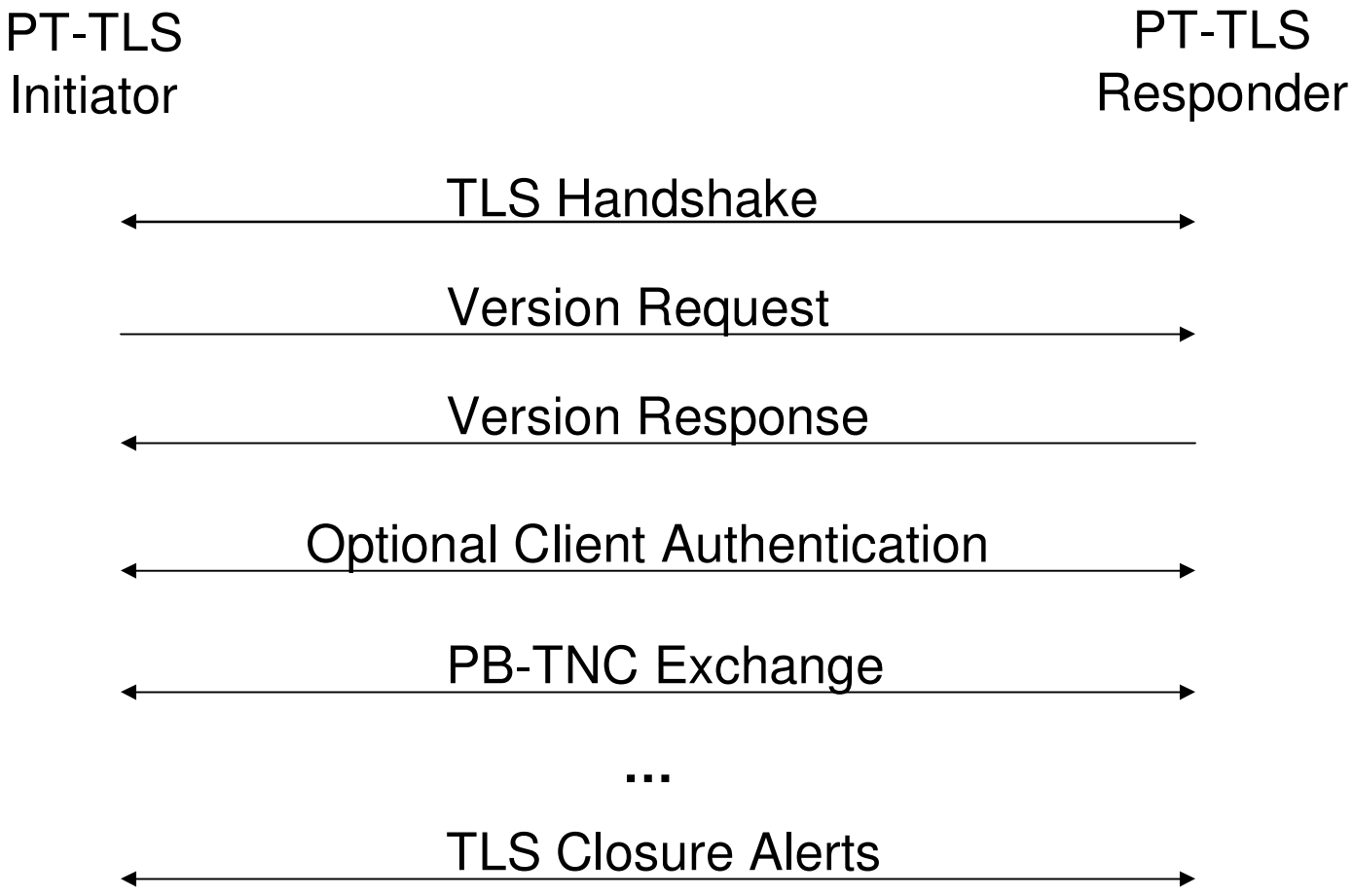
Use Cases for PT-TLS

- NEA Assessment on Non-802.1X Network
  - Legacy Network
  - Remote Access
- Large Amount of Data in NEA Assessment
  - For example, Installed Packages
  - Unsuitable for EAP Transport
- Posture Re-assessment or Monitoring After 802.1X Assessment
- Application Server Needs to Perform NEA Assessment

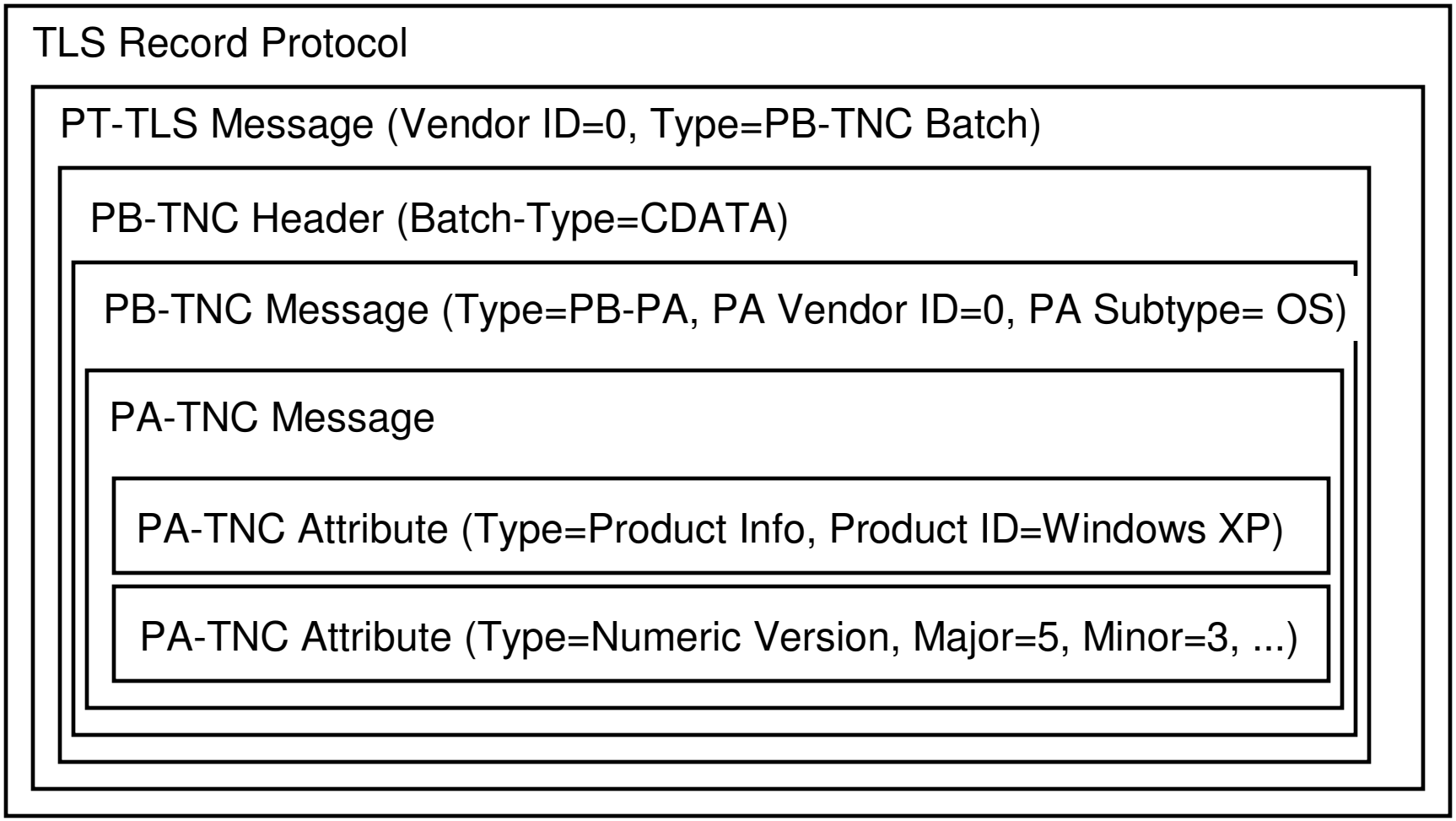
Three Phases of PT-TLS

1. TLS Handshake
   - Unmodified
2. Pre-Negotiation
   - Version Negotiation
   - Optional Client Authentication
3. Data Transport
   - NEA Assessments

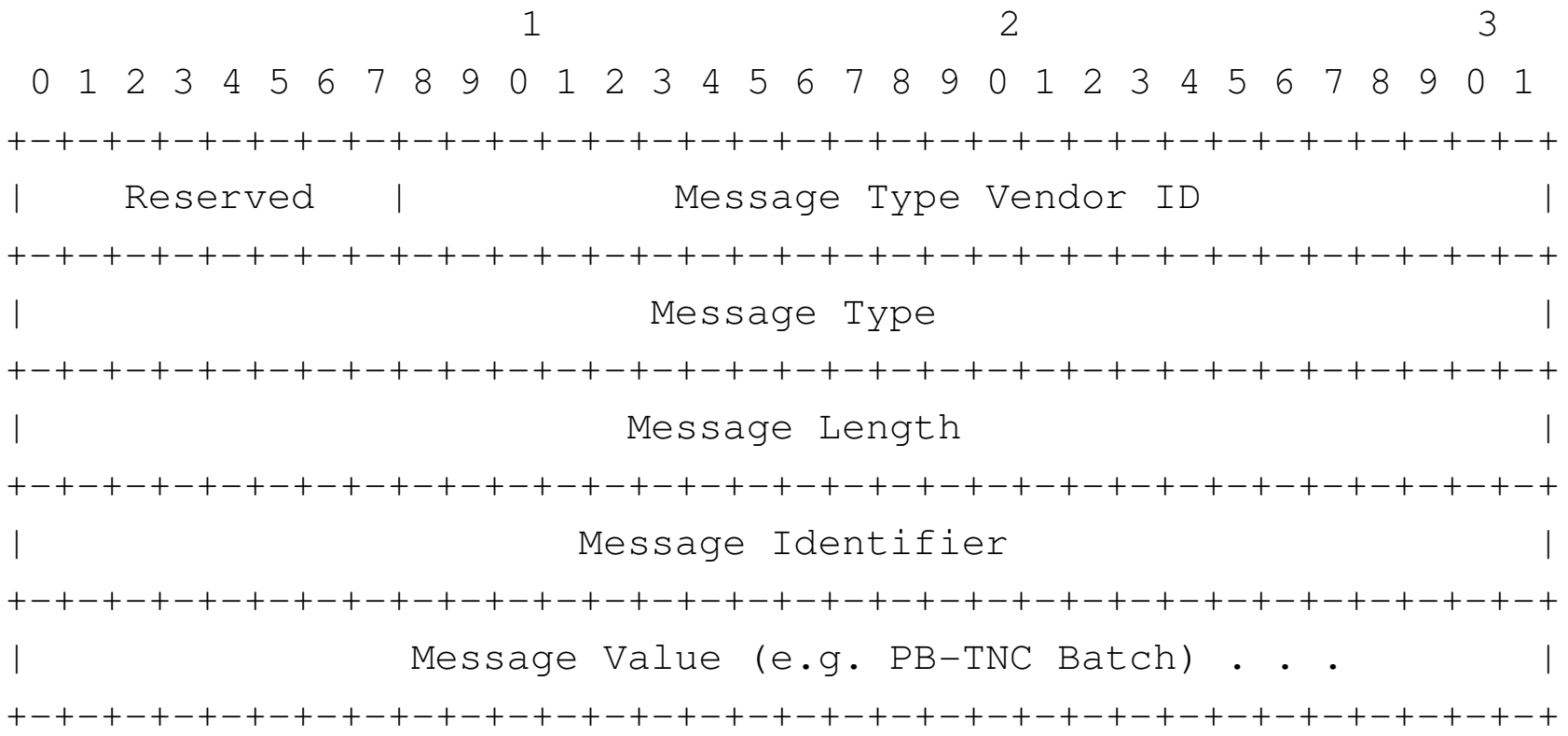
PT-TLS Sequence Diagram



PT-TLS Message Encapsulation



PT-TLS Message Format



Implementations of PT-TLS

- Fairly new spec
  - Announced May 2009
- Several implementations rumored but none publicly announced

Evaluation Against Requirements

C-1 MUST support multiple round trips in a single assessment

YES

C-2 SHOULD let NEA Client or NEA Server initiate assessment or reassessment

YES

C-3 MUST protect against active and passive attacks by intermediaries and endpoints including replay prevention

YES

Evaluation Against Requirements

C-4 PA and PB MUST be able to run over any PT

N/A

C-5 Selection process MUST prefer the reuse of existing open standards

YES

C-6 MUST be highly scalable; MUST support many Posture Collectors, NEA Clients, NEA Servers, and Posture Validators

YES

Evaluation Against Requirements

C-7 MUST efficiently transport many attribute messages — YES

C-8 MUST operate efficiently over low-speed links — YES

C-9 MUST support adapting user-visible strings to user's language preferences — YES

Evaluation Against Requirements

C-10 MUST support UTF-8 string encoding

YES

C-11 MUST expose PT limitations to NEA Client and NEA Server

YES

PT-1 MUST NOT interpret contents of PB messages

YES

Evaluation Against Requirements

PT-2 MUST support mutual authentication, integrity, confidentiality, and replay protection of PB messages

YES

PT-3 MUST provide reliable delivery

YES

PT-4 SHOULD be able to run over 802.1X and IKEv2

NO

Use case for PT-EAP

Evaluation Against Requirements

PT-5 SHOULD be able to run over TCP or UDP

YES

PT-6 MUST be connection oriented

YES

PT-7 MUST be able to carry binary data

YES

Evaluation Against Requirements

PT-8 MUST provide flow control and congestion control

YES

PT-9 MUST describe capabilities and limitations

YES

Pros of PT-TLS

- Layered on established secure protocol (TLS)
  - No changes to TLS, only application data over it
- Compatible with TCG's IF-T/TLS
  - Same IPR grant as PA-TNC and PB-TNC
- Full Duplex
- High Bandwidth
- Congestion Controlled
- Reliable
- Easy to Implement using any TLS library
- Works over any IP network
- Extensible

Cons of PT-TLS

- Client Authentication (Optional)
  - Need to add broader set of existing authentication schemes (e.g. EAP)
  - However, extensible so possible without base protocol changes
- Not Independent of Application Protocol
  - Not a part of TLS handshake, so not independent from application protocol
  - However, enables easier implementation and adoption and wasn't a requirement

Questions?

PT-EAP Evaluation

What is PT-EAP?

- L2 PT Proposal Coming from TCG
  - Identical to TNC protocol EAP-TNC (aka IF-T Protocol Bindings for Tunneled EAP Methods)
- NEA Exchange Over EAP Tunnel Methods
  - Supports PEAP, EAP-TTLS, and EAP-FAST
  - No Change to the EAP Tunnel Methods
- Meets All PT Requirements

Why L2 PT?

- PT-4 says PT SHOULD be able to run over 802.1X or IKEv2
- Motivating Use Cases on Next Slide

Use Cases for PT-EAP

- NEA Assessment on 802.1X Network
  - Consider posture in network access decision
  - Isolate vulnerable endpoints during remediation
  - Block or quarantine infected endpoints
- NEA Assessment during IKEv2 Handshake
  - Assess posture before granting network access
  - Isolate vulnerable endpoints during remediation
  - Block or quarantine infected endpoints

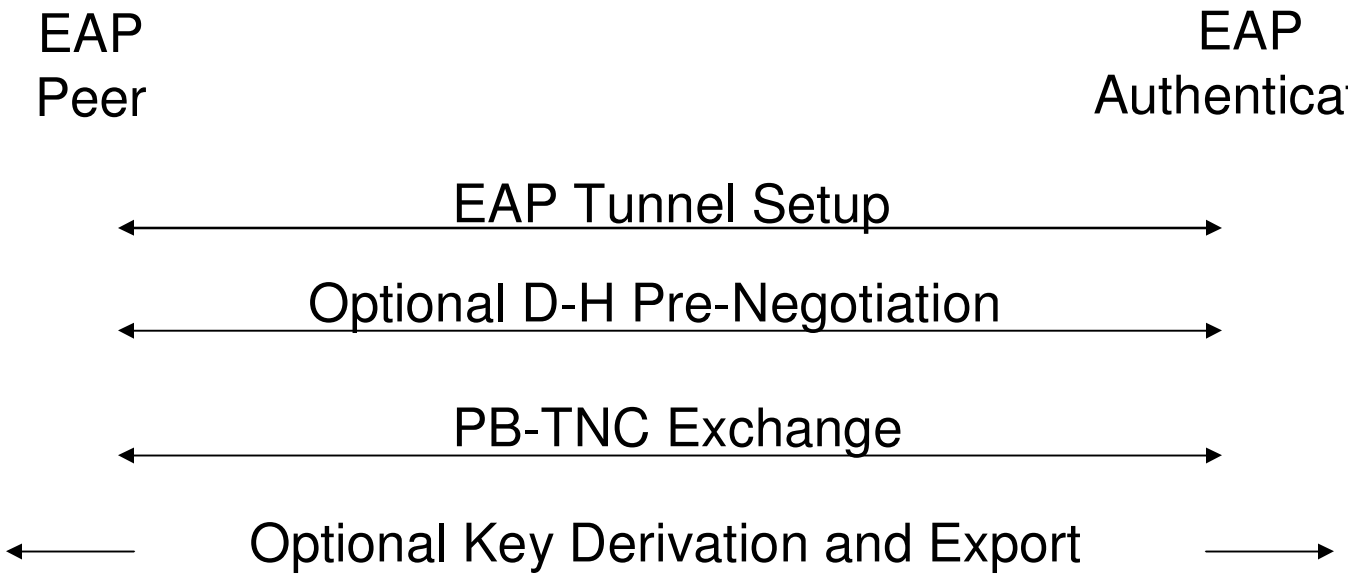
PT-EAP Operation

- Runs as an inner EAP method
  - Can be chained with other EAP methods for user or endpoint authentication
  - Supports key derivation, allowing inner method to be cryptographically tied to tunnel
  - Supports fragmentation and reassembly, when needed
- Due to EAP limitations…
  - Only one packet in flight (half duplex)
  - Large data transfer not recommended

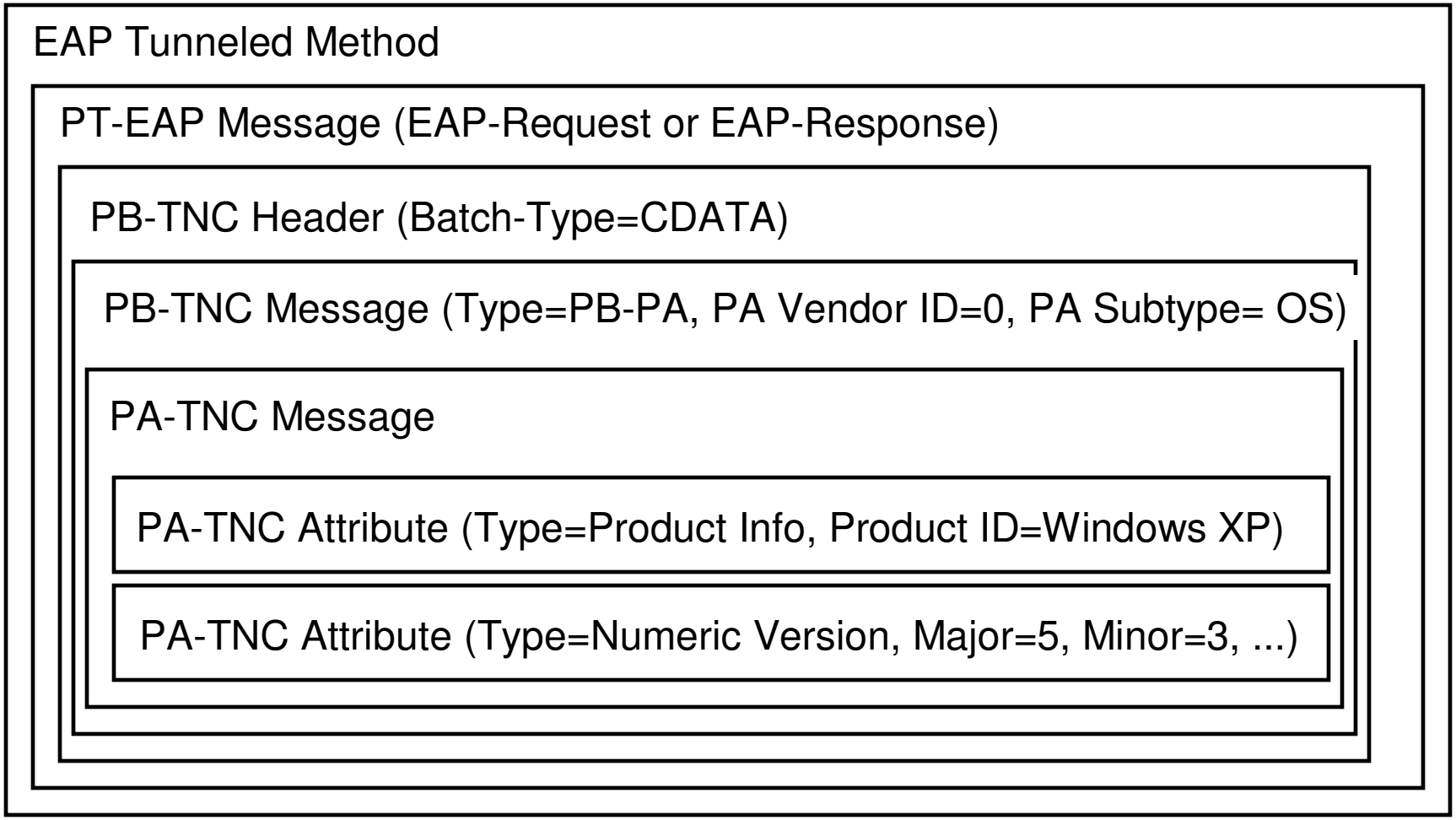
Three Phases of PT-EAP

1. Optional Diffie-Hellman Pre-Negotiation
   - Establishes initial key
2. PB-TNC Exchange
   - NEA Assessments
   - Hashed into eventual key
3. Optional Key Derivation and Export

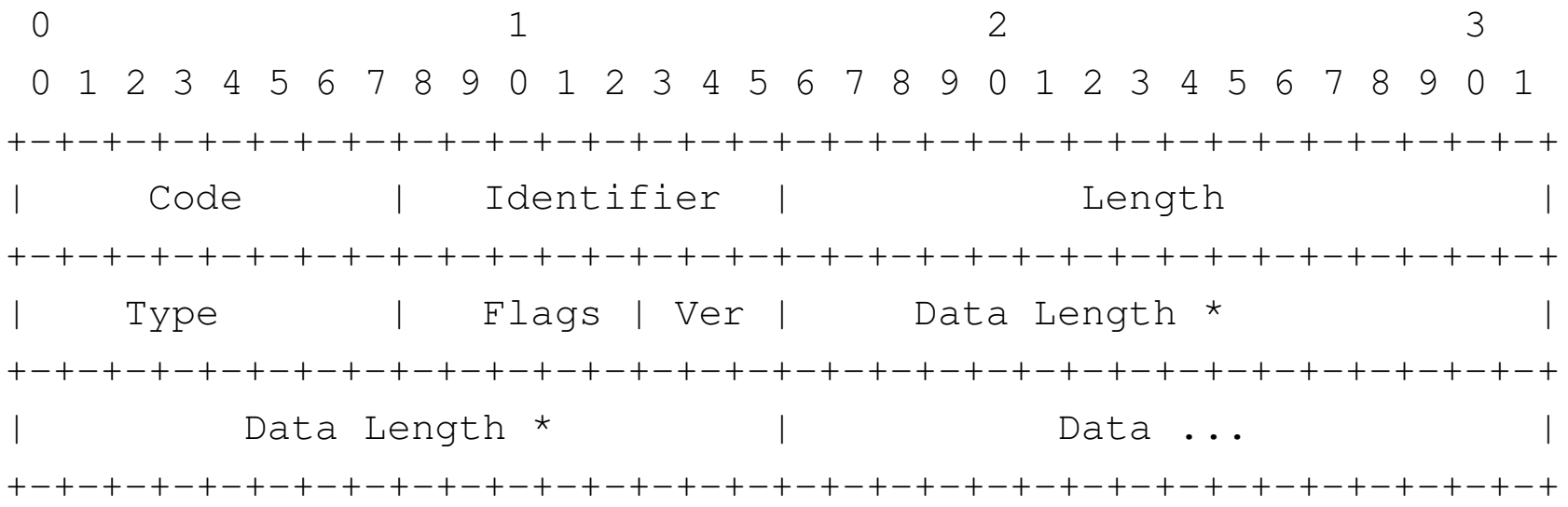
PT-EAP Sequence Diagram



PT-EAP Message Encapsulation



PT-EAP Message Format



* Only when using fragmentation

Implementations of PT-EAP

- Several open source implementations
  - TNC@FHH
  - OpenSEA
  - wpa_supplicant
  - FreeRADIUS
  - libtnc
- Commercial implementations also

Evaluation Against Requirements

C-1 MUST support multiple round trips in a single assessment

YES

C-2 SHOULD let NEA Client or NEA Server initiate assessment or reassessment

NO

Except with Disconnect-Request, EAPOL-Logoff, etc.

C-3 MUST protect against active and passive attacks by intermediaries and endpoints including replay prevention

YES

Evaluation Against Requirements

C-4 PA and PB MUST be able to run over any PT

N/A

C-5 Selection process MUST prefer the reuse of existing open standards

YES

C-6 MUST be highly scalable; MUST support many Posture Collectors, NEA Clients, NEA Servers, and Posture Validators

YES

Evaluation Against Requirements

C-7 MUST efficiently transport many attribute messages — YES

C-8 MUST operate efficiently over low-speed links — YES

C-9 MUST support adapting user-visible strings to user's language preferences — YES

Evaluation Against Requirements

C-10 MUST support UTF-8 string encoding

YES

C-11 MUST expose PT limitations to NEA Client and NEA Server

YES

PT-1 MUST NOT interpret contents of PB messages

YES

Evaluation Against Requirements

PT-2 MUST support mutual authentication, integrity, confidentiality, and replay protection of PB messages

YES

PT-3 MUST provide reliable delivery

YES

PT-4 SHOULD be able to run over 802.1X and IKEv2

YES

Evaluation Against Requirements

PT-5 SHOULD be able to run over TCP or UDP

NO

Except with PANA

PT-6 MUST be connection oriented

YES

PT-7 MUST be able to carry binary data

YES

Evaluation Against Requirements

PT-8 MUST provide flow control and
YES congestion control

PT-9 MUST describe capabilities and
YES limitations

Pros of PT-EAP

- EAP method
  - Works with any EAP Tunnel Method
  - No changes to the EAP state machine or to supplicants (if they support adding EAP methods)
- Optional key derivation and export
  - Allows protection against lying endpoints, when used with TPM
- Equivalent to TCG's EAP-TNC
  - Open standard with many implementations
  - Years of experience and security reviews
- No external dependencies
  - Easy to move to Proposed Standard
- Scalable
  - Supports PB-TNC messages up to 2^32 – 1 bytes via fragmentation

Cons of PT-EAP

- Key derivation and export adds complexity
  - But it's optional with no cost if not used

Questions?

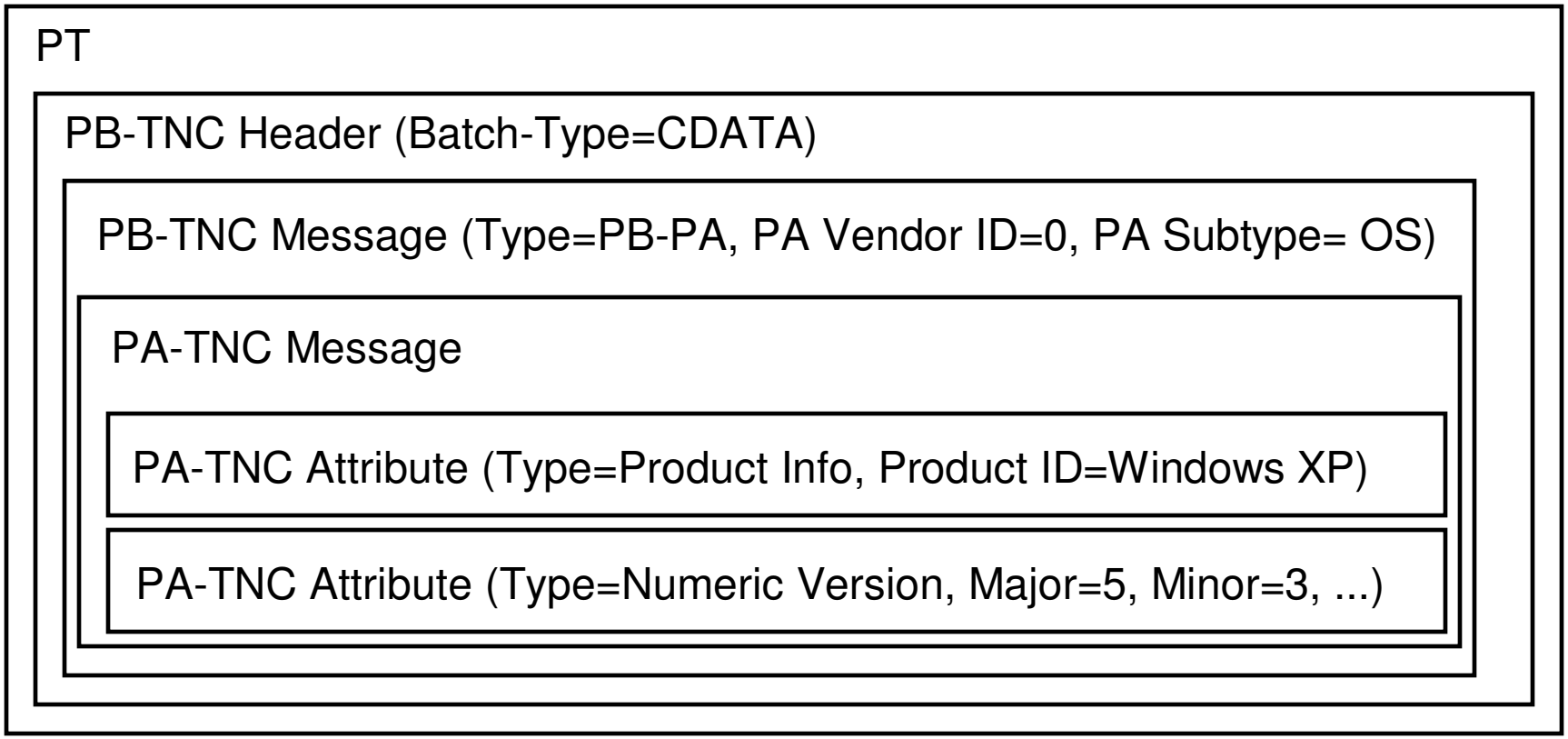
EAP-NEA-TLV Evaluation

Nancy Cam-Winget ncamwing@cisco.com
Hao Zhou hzhou@cisco.com

Outline

- NEA Encapsulations
- EAP Tunneled Encapsulation
- EAP TLV container
- EAP NEA TLV container
- PT Requirements

PA-TNC Within PB-TNC Within PT



EAP TLV Overview

Proposal

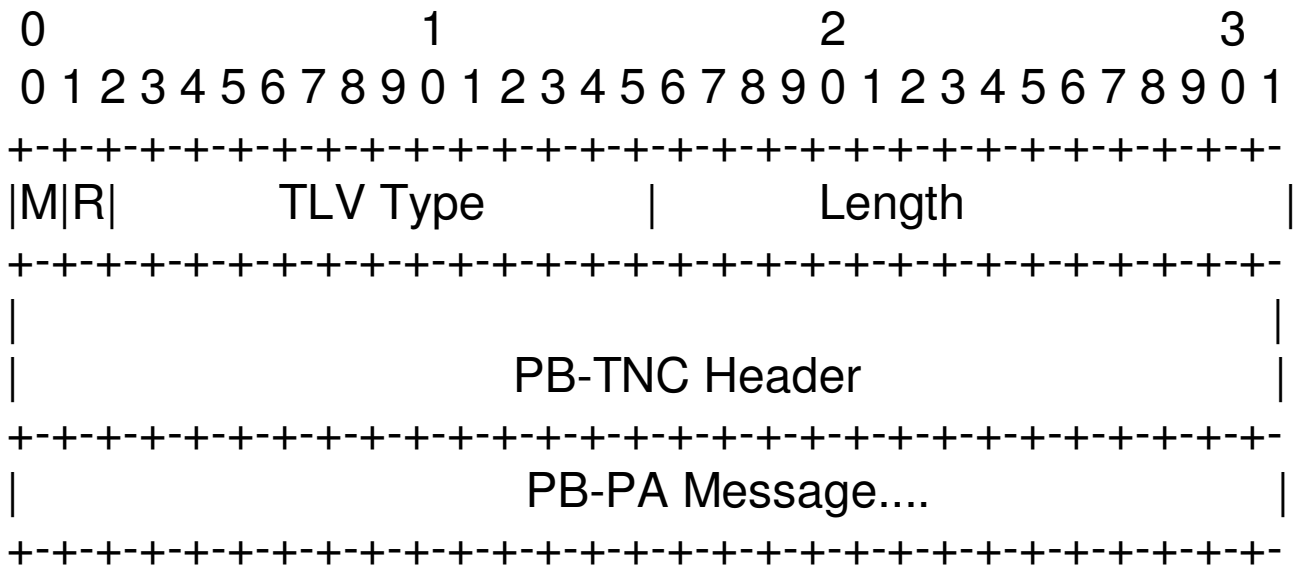
- Facilitate the use of an EAP Tunnel Based Method to carry PB-TNC messages
- EAP Tunnel Based Method provides:
  - Server authentication MUST be enforced
  - Mutual authentication SHOULD occur between NEA Client and NEA Server
  - Protected tunnel to transport PB-TNC messages

What is EAP TLV?

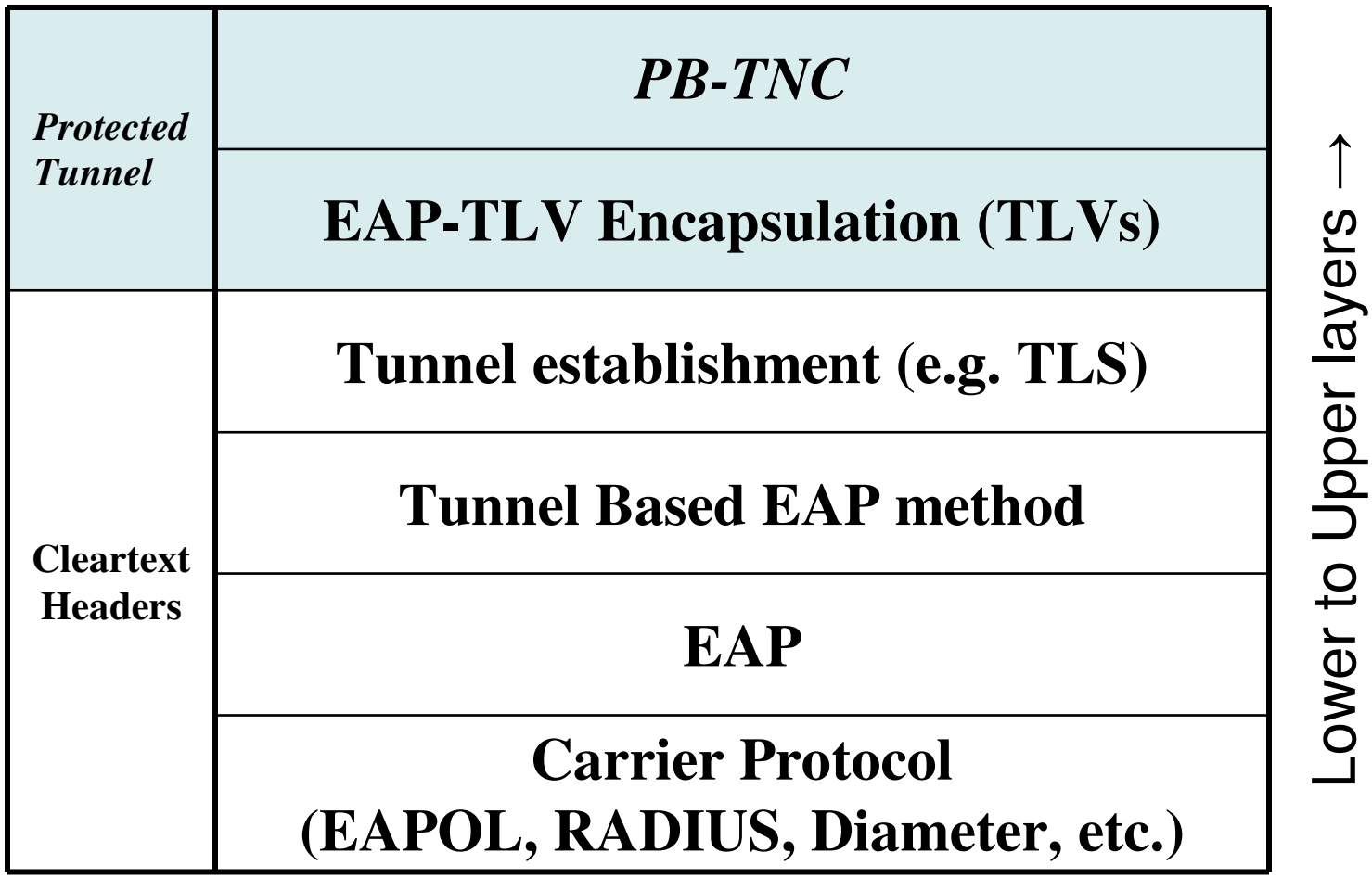
- General container format to facilitate transport of any data (like channel and crypto binding) inside an EAP Tunnel Based Method, for NEA it can also transport PB-TNC messages

- NEA Use cases: 802.1X or IKEv2
  - (NEA) posture assessment in network access decision
  - Remediation thru isolation of vulnerable endpoints
  - Quarantine or block infected endpoints

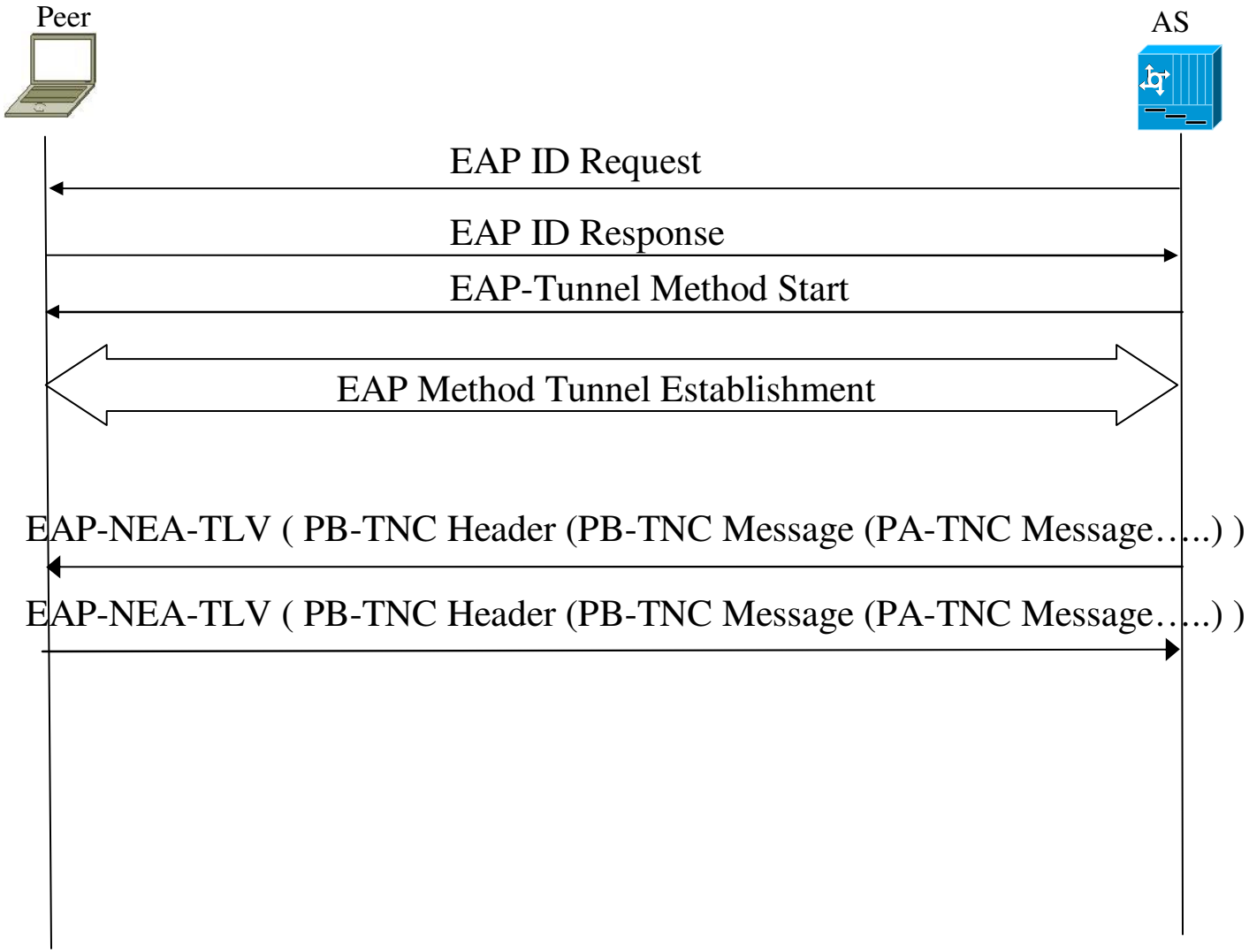
EAP NEA TLV Encapsulation



EAP Tunnel w/ EAP TLV Protocol Layers



EAP + NEA Potential Sequencing



Features of EAP NEA TLV

- EAP NEA TLV:
  - simple construct used inside EAP tunnel
  - flexible and extensible construction to transport NEA messages
- Relies on EAP Tunneled Method to:
  - Provide mutual authentication either during tunnel establishment or through an inner EAP (authentication) method (or both)
  - Provide confidentiality and integrity thru the protected tunnel
- EAP features:
  - Half Duplex (only one packet at a time)
  - Simple congestion control (thru half duplex property)
  - Works in both 802.1X and IKEv2

NEA Protocol Requirements

C-1 NEA protocols MUST support multiple round trips between the NEA Client and NEA Server in a single assessment.

C-2 NEA protocols SHOULD provide a way for both the NEA Client and the NEA Server to initiate a posture assessment or reassessment as needed.

C-3 NEA protocols including security capabilities MUST be capable of protecting against active and passive attacks by intermediaries and endpoints including prevention from replay based attacks.

C-4 The PA and PB protocols MUST be capable of operating over any PT protocol

C-5 The selection process for NEA protocols MUST evaluate and prefer the reuse of existing open standards that meet the requirements before defining new ones. The goal of NEA is not to create additional alternative protocols where acceptable solutions already exist.

C-6 NEA protocols MUST be highly scalable; the protocols MUST support many Posture Collectors on a large number of NEA Clients to be assessed by numerous Posture Validators residing on multiple NEA Servers.

C-7 The protocols MUST support efficient transport of a large number of attribute messages between the NEA Client and the NEA Server.

C-8 NEA protocols MUST operate efficiently over low bandwidth or high latency links.

C-9 For any strings intended for display to a user, the protocols MUST support adapting these strings to the user's language preferences.

C-10 NEA protocols MUST support encoding of strings in UTF-8 format [UTF8].

C-11 Due to the potentially different transport characteristics provided by the underlying candidate PT protocols, the NEA Client and NEA Server MUST be capable of becoming aware of and adapting to the limitations of the available PT protocol

NEA Protocol Requirements

C-Req	Met	Description
C-1	✔	EAP Tunnel Based Methods allow for multiple roundtrips
C-2	–	EAP Tunnel Based Method is intended to be used pre-network admission
C-3	✔	EAP Tunnel Based Method provides tunnel protection against attacks
C-4	✔	The EAP Tunnel Based Method is independent of both PB and PA
C-5	✔	EAP Tunnel Based Method is based on the EAP (RFC 3748) standard
C-6	✔	EAP Tunnel Based Method and EAP TLV container is independent of the NEA collector and validator
C-7	✔	The number or attributes is limited by the EAP transport; though multiple roundtrips can occur
C-8	✔	EAP is designed to work with constrained and low latency links
C-9	–	EAP in general, does not include strings to be displayed; however support for UTF-8 strings if used in EAP-NEA-TLV can be specified
C-10	–	EAP in general, does not include strings, however support for UTF-8 strings if used in EAP-NEA-TLV can be specified
C-11	✔	EAP Tunnel Based Method implementations can expose the constraints to the respective PB Client and PB Broker

PT Requirements

PT-1 The PT protocol MUST NOT interpret the contents of PB messages being transported, i.e., the data it is carrying must be opaque to it.

PT-2 The PT protocol MUST be capable of supporting mutual authentication, integrity, confidentiality, and replay protection of the PB messages between the Posture Transport Client and the Posture Transport Server

PT-3 The PT protocol MUST provide reliable delivery for the PB protocol. This includes the ability to perform fragmentation and reassembly, detect duplicates, and reorder to provide in-sequence delivery, as required.

PT-4 The PT protocol SHOULD be able to run over existing network access protocols such as 802.1X and IKEv2

PT-5 The PT protocol SHOULD be able to run between a NEA Client and NEA Server over TCP or UDP (similar to Lightweight Directory Access Protocol (LDAP))

PT-6 The PT protocol MUST be connection oriented; it MUST support confirmed initiation and close down.

PT-7 The PT protocol MUST be able to carry binary data.

PT-8 The PT protocol MUST provide mechanisms for flow control and congestion control.

PT-9 PT protocol specifications MUST describe the capabilities that they provide for and limitations that they impose on the PB protocol (e.g. half/full duplex, maximum message size).

PT Requirements

PT-Req	Met	Description
PT-1	✔	EAP TLV is a generic container allowing pass thru of NEA data; no EAP interpretation and state machine changes are made
PT-2	✔	EAP Tunnel method supports mutual authentication and tunnel protection
PT-3	✔	EAP (RFC 3748) includes retransmissions; reordering and fragmentation is handled by the EAP Tunnel Based Method
PT-4	✔	EAP is enabled on both 802.1X and IKEv2
PT-5	–	The EAP Tunnel Based Method is intended to be used pre-network access
PT-6	✔	EAP supports initiation and closure
PT-7	✔	EAP TLV is a general container and allows for binary data to be carried
PT-8	✔	EAP being half duplex and MTU size limited, congestion and flow is not an issue
PT-9	✔	EAP is half-duplex with packet size limit as a function of the link

EAP-NEA-TLV Evaluation

Pro's

- Simple Encapsulation
- Can be carried in existing tunnel based methods
- Does not require additional support from tunnel based methods
- Can also be used in TLS

Con's

- Dependent on EAP-TLV
- Assumes no key generation is required

Questions?

Consensus Check Questions

- Do you support work on TLS-based PT?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

- Do you support adoption of PT-TLS as a -00 WG draft?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

Consensus Check Questions

- Do you support work on EAP-based PT?
  - Yes
  - No
  - Defer (decision pending some further action taking place)

- What should we adopt as EAP-based PT?
  - EAP-TNC
  - NEA TLV
  - Other

Next Steps

- Confirm consensus on email list
- Publish -00 WG I-D(s)