IEEE P802.1Xck YANG Instance Document

IEEE 802 Plenary Meeting

Marc Holness

Version 4.0
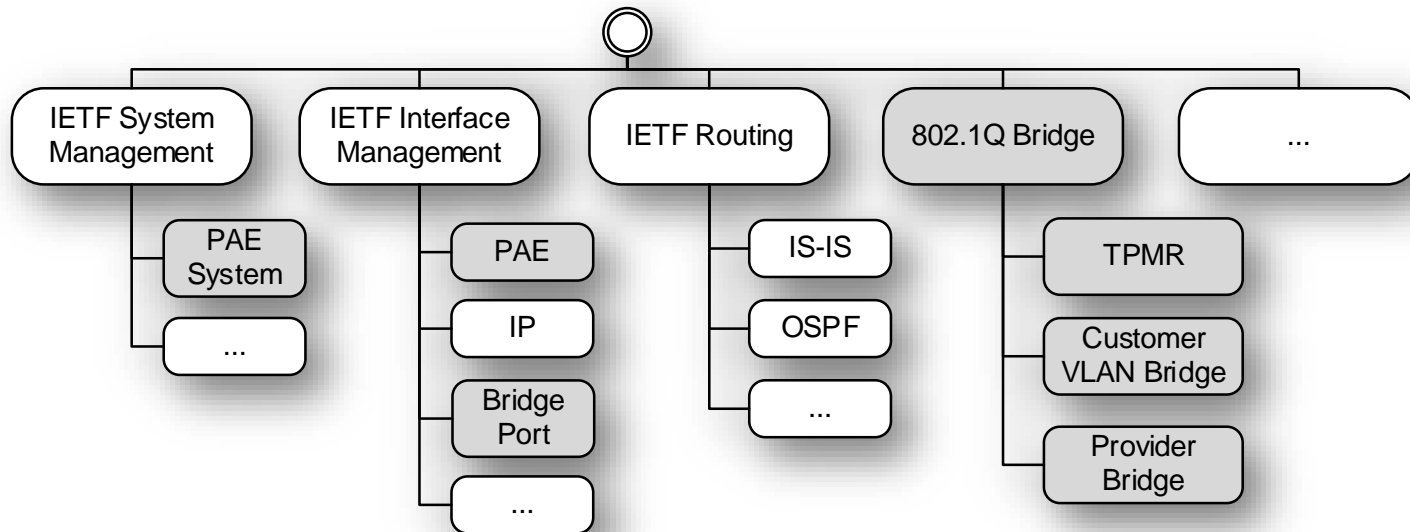
13 March 2017

Introduction

- This package provides "configuration instances" of various aspect of the P802.1Xck version D1.1 YANG modules

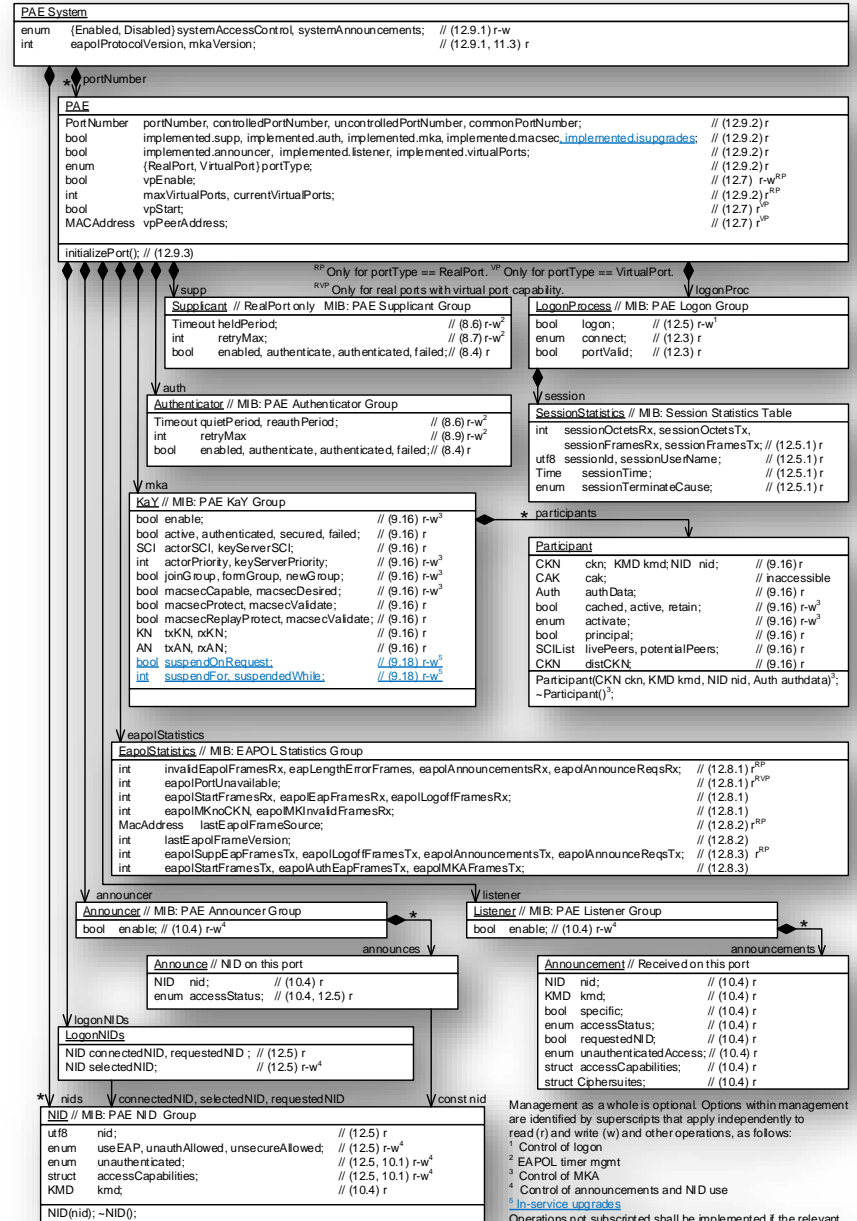# 802.1 YANG Structure and Relationships

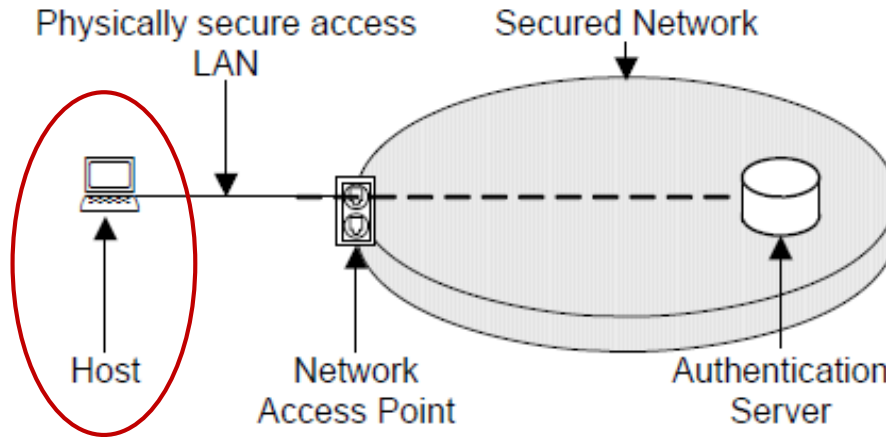- The following hi-level YANG structure and relationships were defined

PAE Management Information Model

- The PAE management process controls and monitors the operation of each PAE's component protocol entities and processes, providing access to operational controls, statistics and diagnostic capabilities

- The management information that provides control over and reporting of these capabilities is summarized in the model to the right

PAE System

enum	{Enabled, Disabled} systemAccessControl, systemAnnouncements; // (12.9.1) r-w
int	eapolProtocolVersion, mkaVersion; // (12.9.1, 11.3) r

* portNumber

PAE

PortNumber	portNumber, controlledPortNumber, uncontrolledPortNumber, commonPortNumber;	// (12.9.2) r
bool	implemented.supp, implemented.auth, implemented.mka, implemented.macsec, implemented.isupgrades;	// (12.9.2) r
bool	implemented.announcer, implemented.listener, implemented.virtualPorts;	// (12.9.2) r
enum	{RealPort, VirtualPort} portType;	// (12.9.2) r
bool	vpEnable;	// (12.7) r-w^{RP}
int	maxVirtualPorts, currentVirtualPorts;	// (12.9.2) r^{RP}
bool	vpStart;	// (12.7) r^{VP}
MACAddress	vpPeerAddress;	// (12.7) r^{VP}

initializePort(); // (12.9.3)

^{RP} Only for portType == RealPort. ^{VP} Only for portType == VirtualPort.
^{RVP} Only for real ports with virtual port capability.

supp / logonProc

Supplicant // RealPort only MIB: PAE Supplicant Group

Timeout	heldPeriod;	// (8.6) r-w^2
int	retryMax;	// (8.7) r-w^2
bool	enabled, authenticate, authenticated, failed;	// (8.4) r

LogonProcess // MIB: PAE Logon Group

bool	logon;	// (12.5) r-w^1
enum	connect;	// (12.3) r
bool	portValid;	// (12.3) r

auth

Authenticator // MIB: PAE Authenticator Group

Timeout	quietPeriod, reauthPeriod;	// (8.6) r-w^2
int	retryMax	// (8.9) r-w^2
bool	enabled, authenticate, authenticated, failed;	// (8.4) r

session

SessionStatistics // MIB: Session Statistics Table

int	sessionOctetsRx, sessionOctetsTx, sessionFramesRx, sessionFramesTx;	// (12.5.1) r
utf8	sessionId, sessionUserName;	// (12.5.1) r
Time	sessionTime;	// (12.5.1) r
enum	sessionTerminateCause;	// (12.5.1) r

mka

KaY // MIB: PAE KaY Group

bool	enable;	// (9.16) r-w^3
bool	active, authenticated, secured, failed;	// (9.16) r
SCI	actorSCI, keyServerSCI;	// (9.16) r
int	actorPriority, keyServerPriority;	// (9.16) r-w^3
bool	joinGroup, formGroup, newGroup;	// (9.16) r-w^3
bool	macsecCapable, macsecDesired;	// (9.16) r-w^3
bool	macsecProtect, macsecValidate;	// (9.16) r
bool	macsecReplayProtect, macsecValidate;	// (9.16) r
KN	txKN, rxKN;	// (9.16) r
AN	txAN, rxAN;	// (9.16) r
bool	suspendOnRequest;	// (9.18) r-w^5
int	suspendFor, suspendedWhile;	// (9.18) r-w^5

* participants

Participant

CKN	ckn; KMD kmd; NID nid;	// (9.16) r
CAK	cak;	// inaccessible
Auth	authData;	// (9.16) r
bool	cached, active, retain;	// (9.16) r-w^3
enum	activate;	// (9.16) r-w^3
bool	principal;	// (9.16) r
SCIList	livePeers, potentialPeers;	// (9.16) r
CKN	distCKN;	// (9.16) r

Participant(CKN ckn, KMD kmd, NID nid, Auth authdata)^3;
~Participant()^3;

eapolStatistics

EapolStatistics // MIB: EAPOL Statistics Group

int	invalidEapolFrames, eapLengthErrorFrames, eapolAnnouncementsRx, eapolAnnounceReqsRx;	// (12.8.1) r^{RP}
int	eapolPortUnavailable;	// (12.8.1) r^{RVP}
int	eapolStartFramesRx, eapolEapFramesRx, eapolLogoffFramesRx;	// (12.8.1)
int	eapolMKNoCKN, eapolMKInvalidFramesRx;	// (12.8.1)
MacAddress	lastEapolFrameSource;	// (12.8.2) r^{RP}
int	lastEapolFrameVersion;	// (12.8.2)
int	eapolSuppEapFramesTx, eapolLogoffFramesTx, eapolAnnouncementsTx, eapolAnnounceReqsTx;	// (12.8.3) r^{RP}
int	eapolStartFramesTx, eapolAuthEapFramesTx, eapolMKAFramesTx;	// (12.8.3)

announcer / listener

Announcer // MIB: PAE Announcer Group

bool	enable; // (10.4) r-w^4

*

Listener // MIB: PAE Listener Group

bool	enable; // (10.4) r-w^4

*

announces / announcements

Announce // NID on this port

NID	nid;	// (10.4) r
enum	accessStatus;	// (10.4, 12.5) r

Announcement // Received on this port

NID	nid;	// (10.4) r
KMD	kmd;	// (10.4) r
bool	specific;	// (10.4) r
enum	accessStatus;	// (10.4) r
bool	requestedNID;	// (10.4) r
enum	unauthenticatedAccess;	// (10.4) r
struct	accessCapabilities;	// (10.4) r
struct	Ciphersuites;	// (10.4) r

logonNIDs

LogonNIDs

NID connectedNID, requestedNID ;	// (12.5) r
NID selectedNID;	// (12.5) r-w^4

* nids / connectedNID, selectedNID, requestedNID / const nid

NID // MIB: PAE NID Group

utf8	nid;	// (12.5) r
enum	useEAP, unauthAllowed, unsecureAllowed;	// (12.5) r-w^4
enum	unauthenticated;	// (12.5, 10.1) r-w^4
struct	accessCapabilities;	// (12.5, 10.1) r-w^4
KMD	kmd;	// (10.4) r

NID(nid); ~NID();

Management as a whole is optional. Options within management are identified by superscripts that apply independently to read (r) and write (w) and other operations, as follows:
^{1} Control of logon
^{2} EAPOL timer mgmt
^{3} Control of MKA
^{4} Control of announcements and NID use
^{5} In-service upgrades
Operations not subscripted shall be implemented if the relevant capability is identified as implemented by the PAE.

Example Host Accessing Network Access Point — Physically secure point-to-point LAN
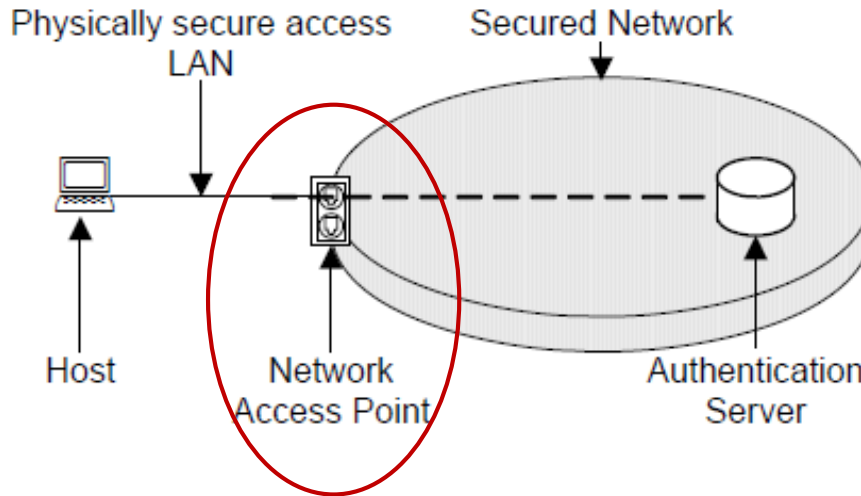

Physically secure access LAN

Secured Network

Host

Network Access Point

Authentication Server

1
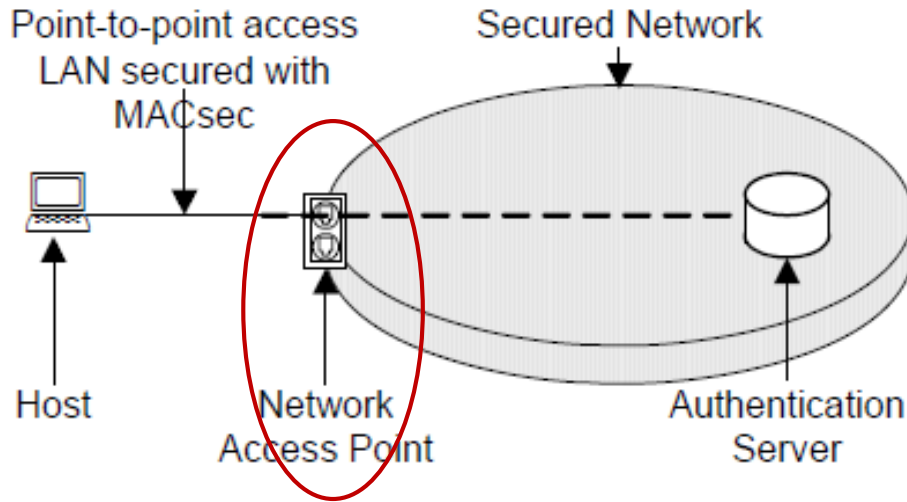
```
<pae-system xc:operation="create">
  <name>aPAESystem</name>
  <system-access-control>enabled</system-access-control>
  <system-announcements>disabled</system-announcements>
</pae-system>
```

2

```
<interfaces xc:operation="create">
  <interface>
    <name>if1</name>
    <type>ethernetCsmacd</type>
    <pae>
      <pae-system>aPAESystem</pae-system>
      <port-type>real-port</port-type>
      <logon-process>
        <logon>true</logon>
      </logon-process>
    </pae>
  </interface>
</interfaces>
```
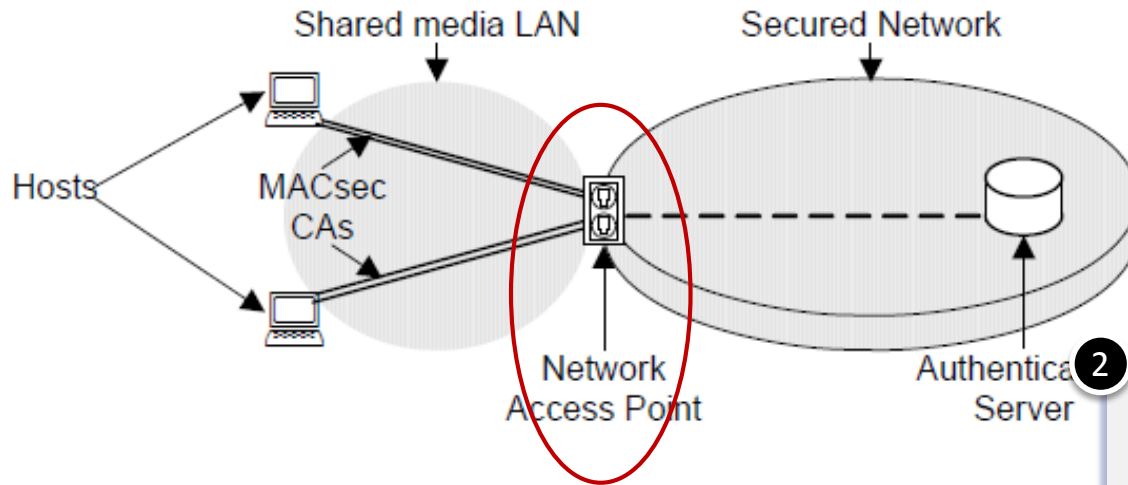
Example Network Access Point supporting Host — Physically secure point-to-point LAN

1

```
<pae-system xc:operation="create">
   <name>aPAESystem</name>
   <system-access-control>enabled</system-access-control>
   <system-announcements>disabled</system-announcements>
</pae-system>
```

2

```
<interfaces xc:operation="create">
   <interface>
     <name>if1</name>
     <type>ethernetCsmacd</type>
     <pae>
       <pae-system>aPAESystem</pae-system>
       <port-type>real-port</port-type>
       <logon-process>
         <logon>true</logon>
       </logon-process>
     </pae>
   </interface>
</interfaces>
```

Example Network Access Point supporting Host — MACsec and point-to-point LAN

Point-to-point access LAN secured with MACsec

Secured Network

Host

Network Access Point

Authentication Server

1

```
<pae-system xc:operation="create">
  <name>aPAESystem</name>
  <system-access-control>enabled</system-access-contro
  <system-announcements>disabled</system-announcements
</pae-system>
```

2

```
<interfaces xc:operation="create">
  <interface>
    <name>if1</name>
    <type>ethernetCsmacd</type>
    <pae>
      <pae-system>aPAESystem</pae-system>
      <port-type>real-port</port-type>
      <kay>
        <enable>true</enable>
        <macsec>
          <capable>true</capable>
        </macsec>
      </kay>
      <listener>
        <enable>true</enable>
      </listener>
      <logon-process>
        <logon>true</logon>
      </logon-process>
    </pae>
  </interface>
</interfaces>
```

Example Network Access Point supporting Host — MACsec and multi-access LAN

Shared media LAN   Secured Network

Hosts

MACsec CAs

Network Access Point

Authentica...
Server

①

```
<pae-system xc:operation="create">
  <name>aPAESystem</name>
  <system-access-control>enabled</system-access-contro...
  <system-announcements>disabled</system-announcements...
</pae-system>
```

②
```
<interfaces xc:operation="create">
  <interface>
    <name>if1</name>
    <type>ethernetCsmacd</type>
    <pae>
      <pae-system>aPAESystem</pae-system>
      <port-type>virtual-port</port-type>
      <vp-enable>true</vp-enable>
      <kay>
        <enable>true</enable>
        <macsec>
          <capable>true</capable>
        </macsec>
      </kay>
      <listener>
        <enable>true</enable>
      </listener>
      <logon-process>
        <logon>true</logon>
      </logon-process>
    </pae>
  </interface>
</interfaces>
```