802.1X / dot1x supplicant support on AOS-CX switches

Presenters

Yash

Technical Marketing Engineer

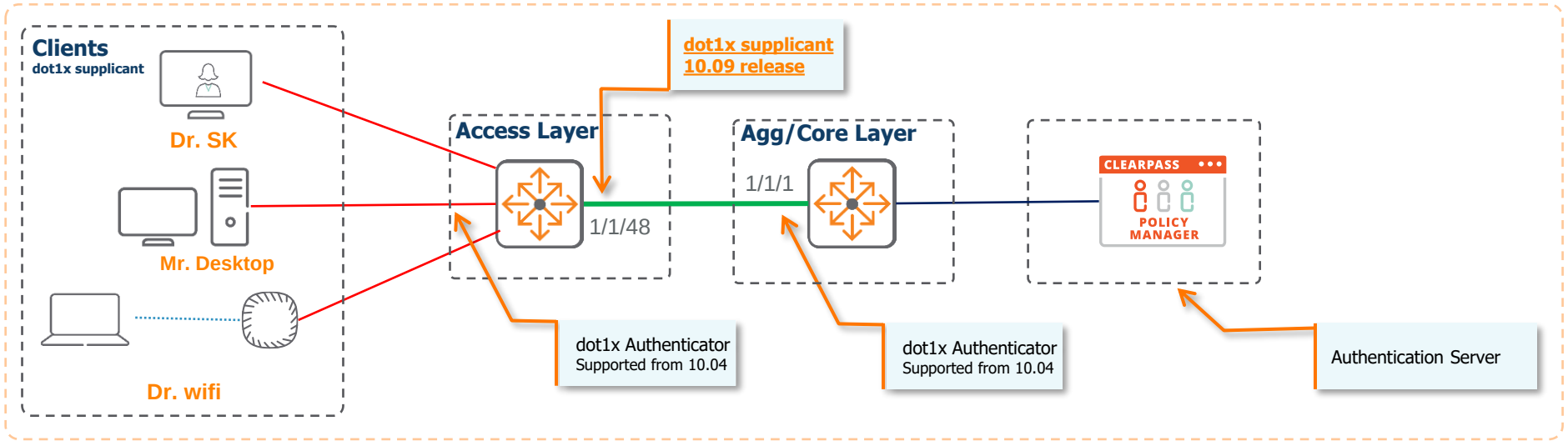
Agenda

1. Overview
2. Details and Caveats
3. Configuration
4. Best Practices
5. Troubleshooting
6. Demo
7. Additional Resources

Overview

AOS-CX 10.09: dot1x supplicant

- dot1x authentication involves three entities:
  - a **supplicant** (PC/AP/Clients/ **Access Switches**)
  - an **authenticator**, (Aruba AOS-CX Switches)
  - **an authentication server** (Aruba ClearPass)
- **dot1x authenticator** feature is supported from AOS-CX 10.04 release.
- To secure network infrastructure**, dot1x supplicant** feature is supported from AOS-CX 10.09 release.



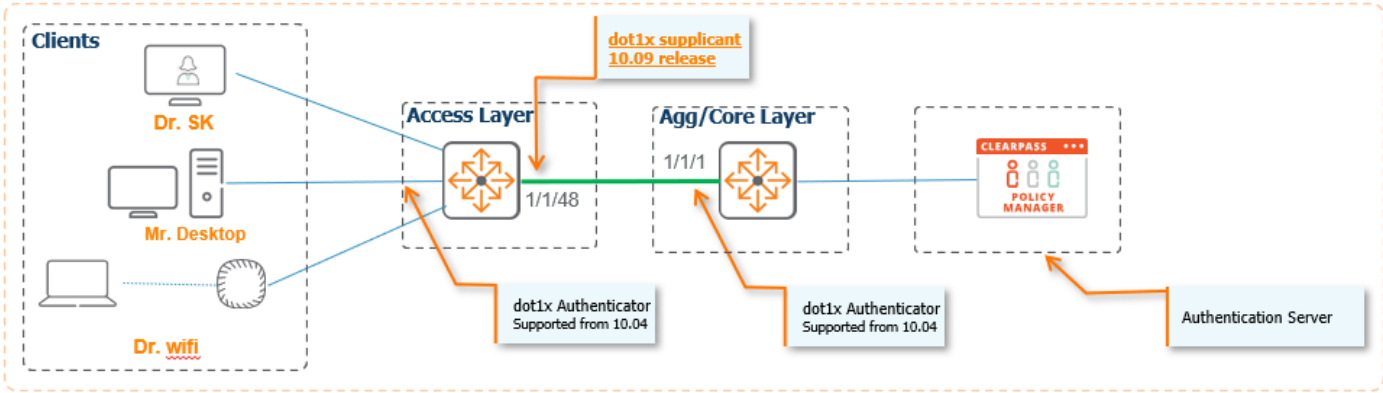
Details and Caveats

dot1x supplicant support on AOS-CX Switches

dot1x Features	10.09 Support	Not Supported
Standard	IEEE 802.1X - 2010	
EAP Methods	EAP-TLS EAP-MD5	EAP-TLS based MACsec (client MACsec)
Certificate	User Defined EST enrollment	IDevID ZTP workflow
Interface Type	Only L2 Physical Interface	L2/L3 LAG, RoP
MIB	NA	dot1x 2010 PAE MIB
AOS-CX platforms	4100i, 6000, 6100 6200, 6300, 6400, 8360	8320, 8325, 8400, 10000
Mutual Exclusion Feature	Same interface support dot1x supplicant and dot1x authenticator	Infrastructure MACsec and dot1x supplicant on same interface not supported

AOS-CX dot1x supplicant sub-features

- eap-method (Default: eap-tls)
- canned-eap-success (Default: disabled)
- eapol-force-multicast (Default: disabled)
- fail-mode (Default: fail-open)
- start-mode (Default: start-open)
- eapol-protocol-version (Default: 3)



dot1x Supplicant- eapol-force-multicast

With force-multicast

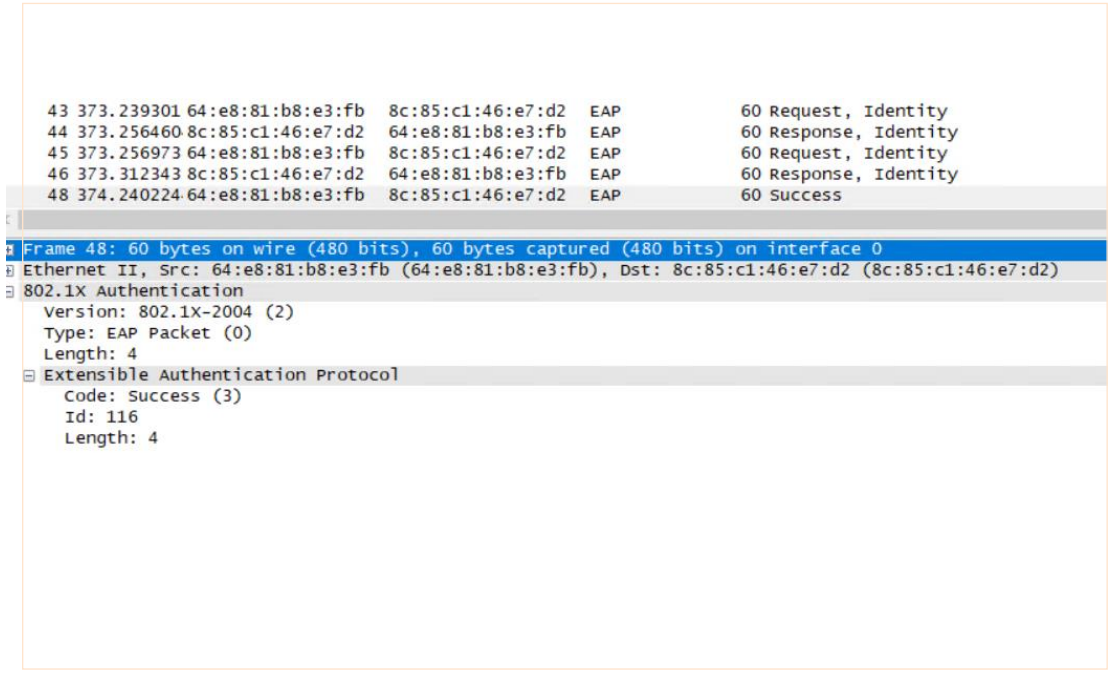
```
    9 20.0133505 8c:85:c1:46:e7:d2  Nearest            EAPOL      60 Start
   10 23.0105443 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Request, Identity
   11 23.0653438 8c:85:c1:46:e7:d2  Nearest            EAP        60 Response, Identity
   12 23.0704217 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Request, TLS EAP (EAP-T
   15 23.1777594 8c:85:c1:46:e7:d2  Nearest            EAP        60 Response, TLS EAP (EAP-
   18 23.2622143 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Request, TLS EAP (EAP-T
   20 23.2920139 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Request, TLS EAP (EAP-T
   21 23.3455545 8c:85:c1:46:e7:d2  Nearest            TLSv1.2    60 Certificate, Client Key
   23 23.5293962 8c:85:c1:46:e7:d2  Nearest            EAP        60 Response, TLS EAP (EAP-
   24 23.5658402 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Success

⊞ Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Ethernet II, Src: 8c:85:c1:46:e7:d2 (8c:85:c1:46:e7:d2), Dst: Nearest (01:80:c2:00:00:03)
  ⊟ Destination: Nearest (01:80:c2:00:00:03)
      Address: Nearest (01:80:c2:00:00:03)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ⊟ Source: 8c:85:c1:46:e7:d2 (8c:85:c1:46:e7:d2)
      Address: 8c:85:c1:46:e7:d2 (8c:85:c1:46:e7:d2)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1X Authentication (0x888e)
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
⊟ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 10
  ⊟ Extensible Authentication Protocol
      Code: Response (2)
      Id: 50
      Length: 10
      Type: Identity (1)
      Identity: cxtme
```

Without force-multicast

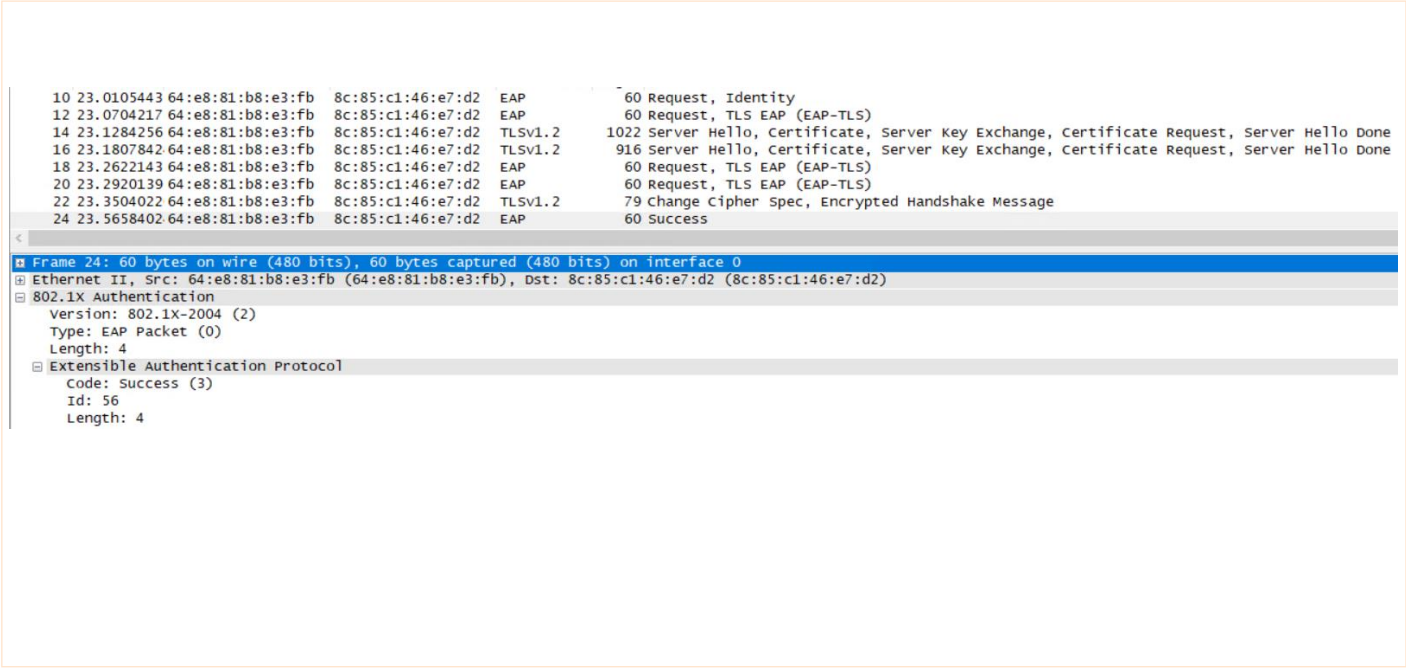
```
 3 2.45342260 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP        60 Response, Identity
 4 2.45721908 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Request, TLS EAP (EAP-TLS)
 5 2.51042288 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2   291 Client Hello
 6 2.51526036 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2  1022 Server Hello, Certificate, Server
 7 2.56544412 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP        60 Response, TLS EAP (EAP-TLS)
 8 2.57167828 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2  1022 Server Hello, Certificate, Server
 9 2.62545024 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP        60 Response, TLS EAP (EAP-TLS)
10 2.62766672 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2    97 Server Hello, Certificate, Server
11 2.69589280 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2  1181 Certificate, Client Key Exchange,
12 2.69960828 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2    79 Change Cipher Spec, Encrypted Han
13 2.74330108 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP        60 Response, TLS EAP (EAP-TLS)
14 2.77665216 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP        60 Success

⊞ [3 EAP-TLS Fragments (2057 bytes): #6(994), #8(994), #10(69)]
⊟ Secure Sockets Layer
  ⊞ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  ⊟ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1566
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1562
        Certificates Length: 1559
      ⊟ Certificates (1559 bytes)
          Certificate Length: 786
        ⊞ Certificate (id-at-commonName=Server)
          Certificate Length: 767
        ⊟ Certificate (id-at-commonName=My CA)
          ⊞ signedCertificate
          ⊞ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted: 90d958d8c52e42a00b9160cda95ddef3a5d442d423860f9eabefc7e1e8cf27279a7d9cbd7ca81c2
```

dot1x Supplicant- canned EAP success

With canned EAP success



Without canned EAP success



Note: Canned EAP success configuration required on both dot1x supplicant and authenticator

dot1x Supplicant EAP-Method: EAP-TLS EST enrollment certificate

```
3 18.3917984 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Request, Identity
9 18.3943937 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, Identity
0 18.3971691 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Request, TLS EAP (EAP-TLS)
1 18.4511413 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2     291 Client Hello
2 18.4543625 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2    1022 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
3 18.5064220 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, TLS EAP (EAP-TLS)
4 18.5088125 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2     916 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
5 18.5858135 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2    1426 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
5 18.5885172 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Request, TLS EAP (EAP-TLS)
7 18.6184155 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2    1422 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
8 18.6212420 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Request, TLS EAP (EAP-TLS)
9 18.6784016 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2      60 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
0 18.6848995 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2      79 Change Cipher Spec, Encrypted Handshake Message
1 18.8826333 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, TLS EAP (EAP-TLS)
2 18.9137312 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Success
```

```
    Type: TLS EAP (EAP-TLS) (13)
  ⊞ EAP-TLS Flags: 0xc0
    EAP-TLS Length: 1882
  ⊞ [2 EAP-TLS Fragments (1882 bytes): #12(994), #14(888)]
  ⊟ Secure Sockets Layer
    ⊞ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    ⊟ TLSv1.2 Record Layer: Handshake Protocol: Certificate
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 1215
      ⊟ Handshake Protocol: Certificate
          Handshake Type: Certificate (11)
          Length: 1211
          Certificates Length: 1208
        ⊟ Certificates (1208 bytes)
            Certificate Length: 691
          ⊞ Certificate (pkcs-9-at-emailAddress=yashavantha.n.n@hpe.com,id-at-commonName=10.5.6.21,id-at-organizationalUnitName=Aruba,id-at-organizationName=HPE,id-at
            Certificate Length: 511
          ⊞ Certificate (pkcs-9-at-emailAddress=yashavantha.n.n@hpe.com,id-at-commonName=danest-int2,id-at-organizationalUnitName=Aruba,id-at-organizationName=HPE,id-
```

EAP-TLS
EST enroll

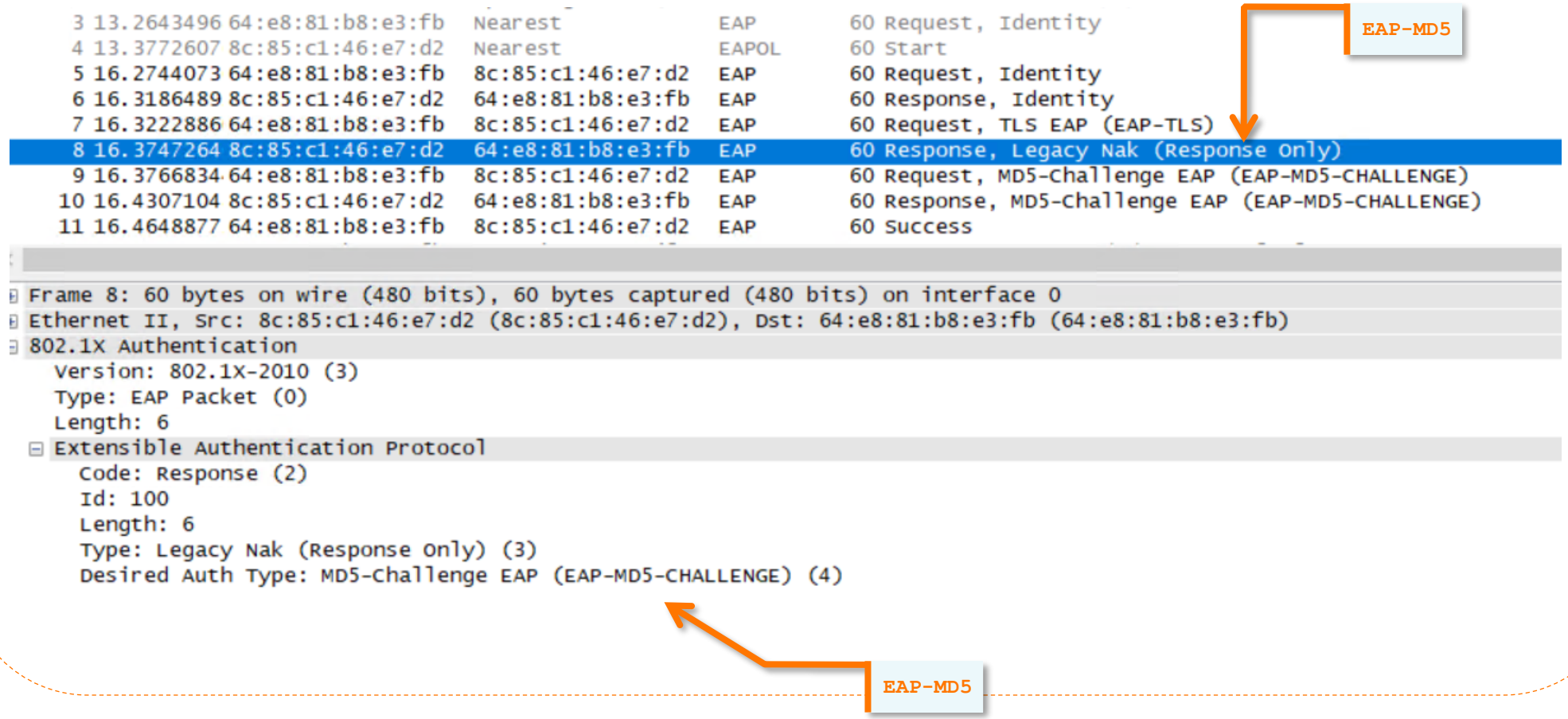
dot1x Supplicant EAP-Method: EAP-TLS - User defined certificate

```
  3 2.45342260 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, Identity
  4 2.45721908 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Request, TLS EAP (EAP-TLS)
  5 2.51042288 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2     291 Client Hello
  6 2.51526036 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2    1022 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  7 2.56544412 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, TLS EAP (EAP-TLS)
  8 2.57167828 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2    1022 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  9 2.62545024 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, TLS EAP (EAP-TLS)
 10 2.62766672 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2      97 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
 11 2.69589280 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  TLSv1.2    1181 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
 12 2.69960828 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  TLSv1.2      79 Change Cipher Spec, Encrypted Handshake Message
 13 2.74330108 8c:85:c1:46:e7:d2  64:e8:81:b8:e3:fb  EAP          60 Response, TLS EAP (EAP-TLS)
 14 2.77665216 64:e8:81:b8:e3:fb  8c:85:c1:46:e7:d2  EAP          60 Success

  EAP-TLS Length: 2057
⊞ [3 EAP-TLS Fragments (2057 bytes): #6(994), #8(994), #10(69)]
⊟ Secure Sockets Layer
  ⊞ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  ⊟ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1566
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1562
        Certificates Length: 1559
      ⊟ Certificates (1559 bytes)
          Certificate Length: 786
        ⊞ Certificate (id-at-commonName=Server)
          Certificate Length: 767
        ⊟ Certificate (id-at-commonName=My CA)
          ⊞ signedCertificate
          ⊞ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted: 90d958d8c52e42a00b9160cda95ddef3a5d442d423860f9eabefc7e1e8cf27279a7d9cbd7ca81c2272adafbff306400bb16b1e5a...
```

EAP-TLS
User defined cert

show crypto pki certificate client | in Issuer

dot1x Supplicant EAP-Method: EAP-MD5



dot1x Supplicant support on AOS-CX CX_SWes

AOS-CX_SW dot1x supplicant	AOS-CX dot1x supplicant
Implements the dot1x 2004 standard.	Implements the dot1x 2010 standard.
Only support EAP-MD5 for authentication.	Supports EAP-TLS and EAP-MD5 for authentication.
Designed to use only CX_SW base mac address	Designed to use only interface MAC address
eapol-protocol-version 2	eapol-protocol-version 2 & 3(default)

Configuration

AOS-CX dot1x supplicant certificate enrollment

- Associates a leaf certificate with a feature (application) on the switch. By default, all features are associated with the default, self-signed certificate local-cert. This certificate is created by the switch the first time it starts.

```
Access-CXSW(config)# crypto pki application

  captive-portal    Captive Portal

  dot1x-supplicant  802.1X supplicant

  est-client        EST Client

  https-server      HTTPS Server

  radsec-client     RadSec Client

  syslog-client     Syslog Client

Access-CXSW(config)# crypto pki application
```

```
Access-CXSW(config)# show crypto pki application

Associated Applications    Certificate Name           Cert Status

-------------------------- -------------------------- ------------------------------

captive-portal                                        not configured, using local-ce

dot1x-supplicant           est_certificate1           valid

est-client                                            not configured, using local-ce

https-server                                          not configured, using local-ce

radsec-client                                         not configured, using local-ce

syslog-client                                         not configured, using local-ce
```

```
Access-CXSW(config)# show crypto pki certificate

Certificate Name                 Cert Status    EST Status        Associated
Applications

-------------------------------- -------------- ----------------- ------------------
-----------

CX_SUP                           installed      n/a               none

client                           installed      n/a               none

local-cert                       installed      n/a               captive-portal,
est-client, https-server, radsec-client, syslog-client

est_certificate1                 installed      enroll success    dot1x-supplicant

device-identity                  installed      n/a               none

Access-CXSW(config)#
```

AOS-CX dot1x supplicant

- Enable dot1x supplicant on the system. **By default, dot1x supplicant is disabled on the system.**

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)#
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# enable
```

- Create a **dot1x supplicant policy**

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_dot1x_supplicant_uplink
CX_SW(config-dot1x-supp-policy)#
```

- eapol-protocol-version:
  - Configure the EAPoL protocol version to use in EAPoL frames

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)#     enable
CX_SW(config-dot1x-supp)#     policy cx_dot1x_supplicant
CX_SW(config-dot1x-supp-policy)# eapol-protocol-version
  <2-3>  Specify the protocol version. (Default: 3)
```

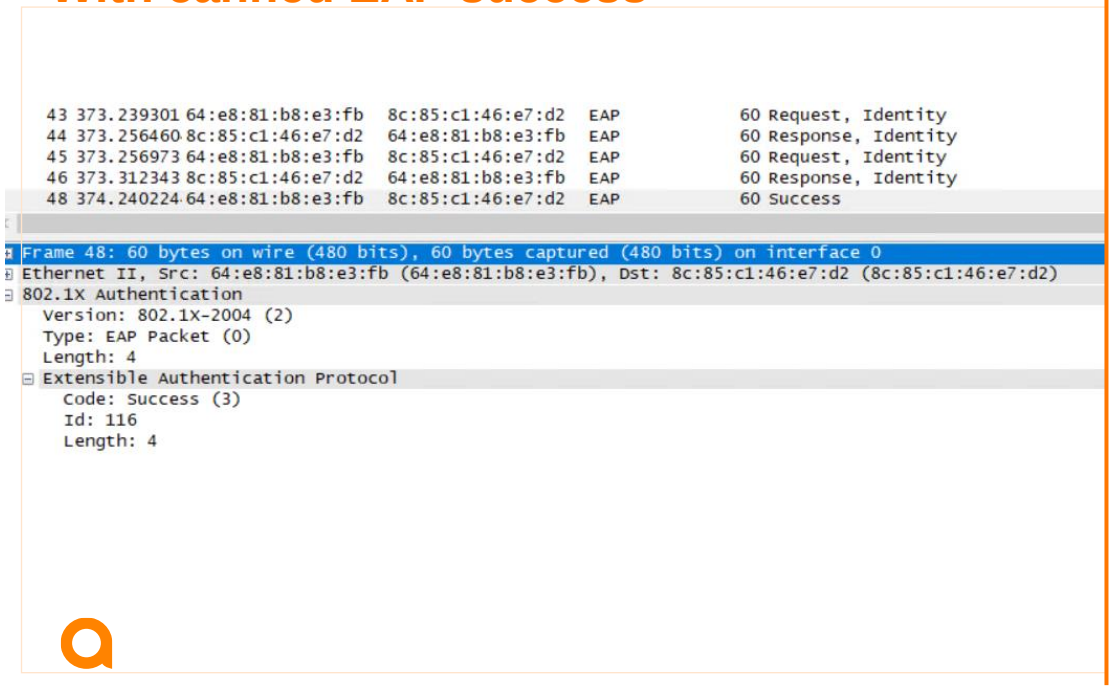
dot1x supplicant- Sub features

- **canned EAP success**: Configure the CX_SW to accept an EAP success from the authenticator without going through the complete authentication cycle.

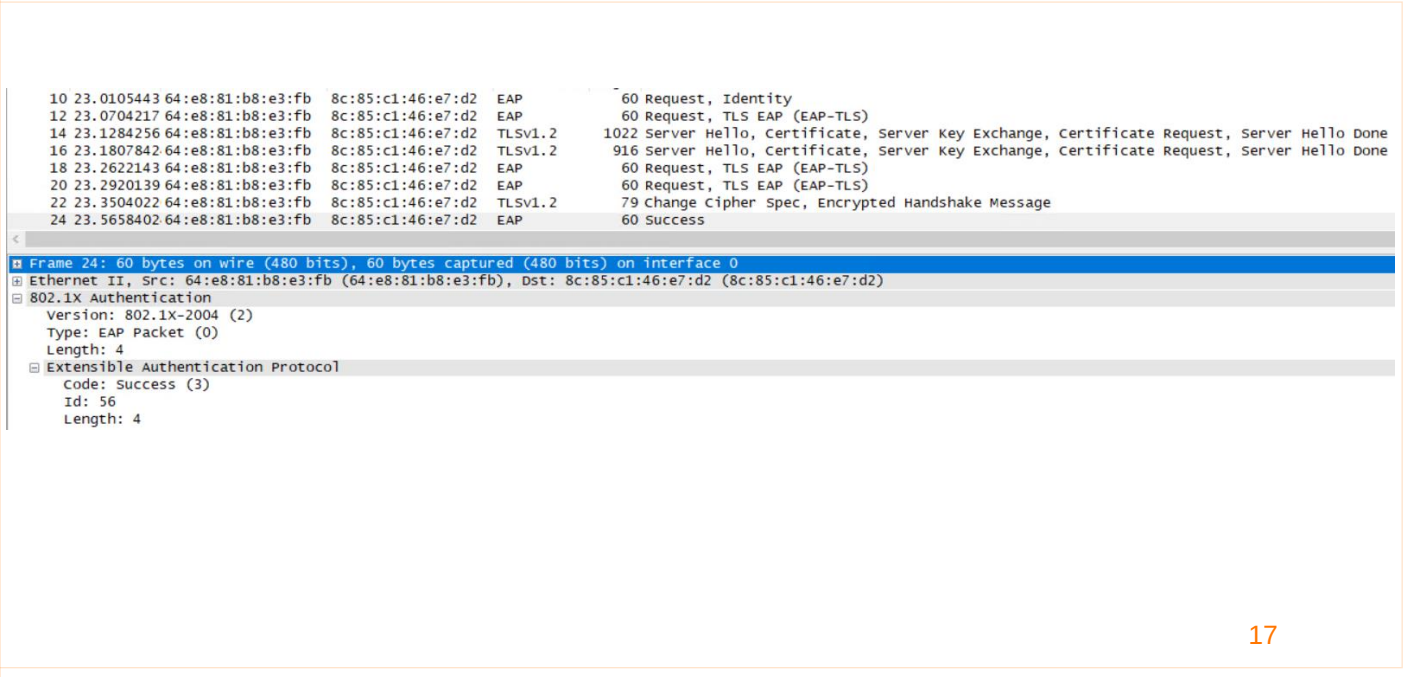
Note: Canned EAP success configuration required on both dot1x supplicant and authenticator

```
CX_SW(config)# aaa authentication port-access dot1x supplicant

CX_SW(config-dot1x-supp)# policy CX_dot1x_supplicant_uplink

CX_SW(config-dot1x-supp-policy)# canned-eap-success

no canned-eap-success (default)
```

With canned EAP success



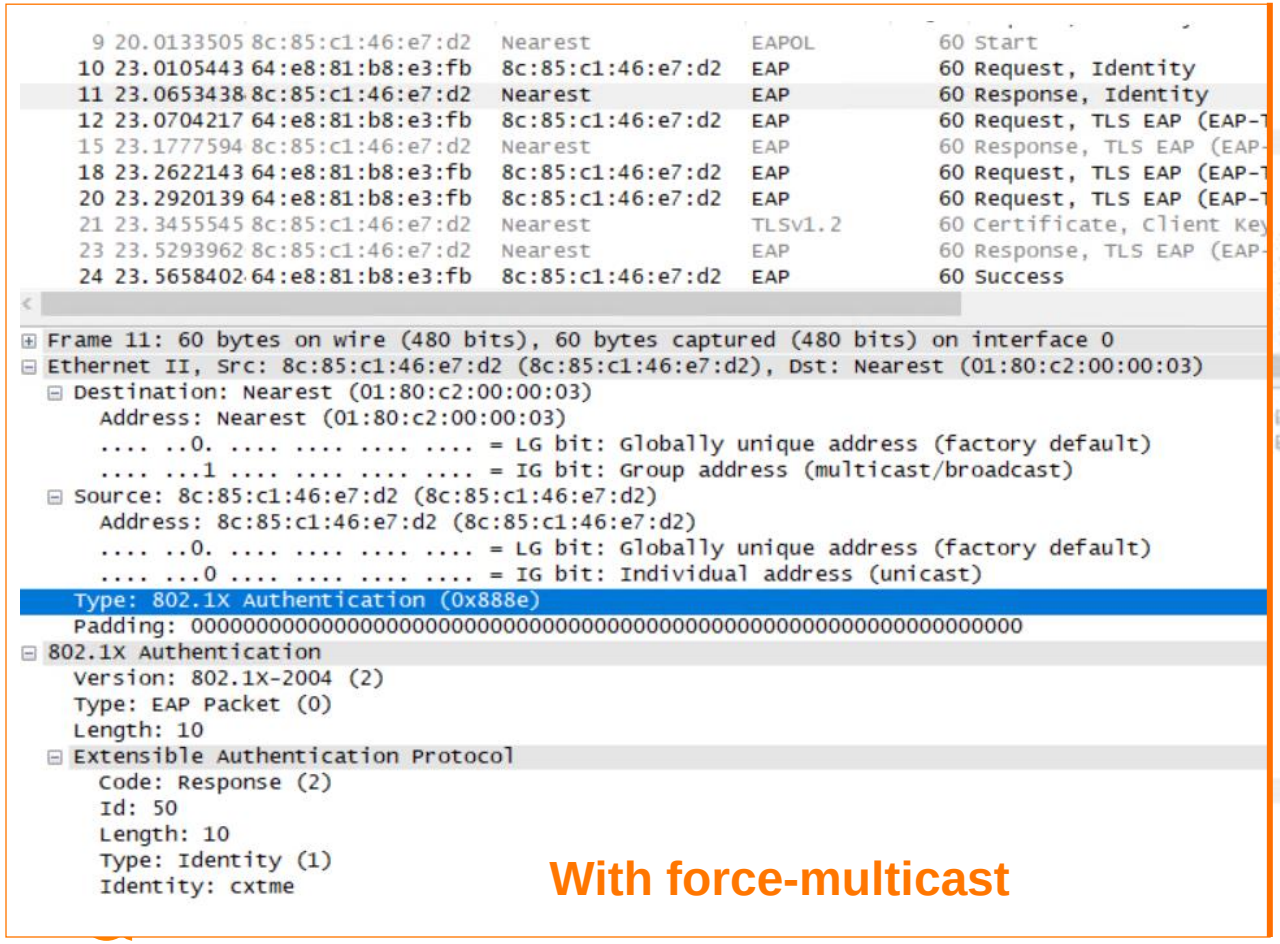
Without canned EAP success



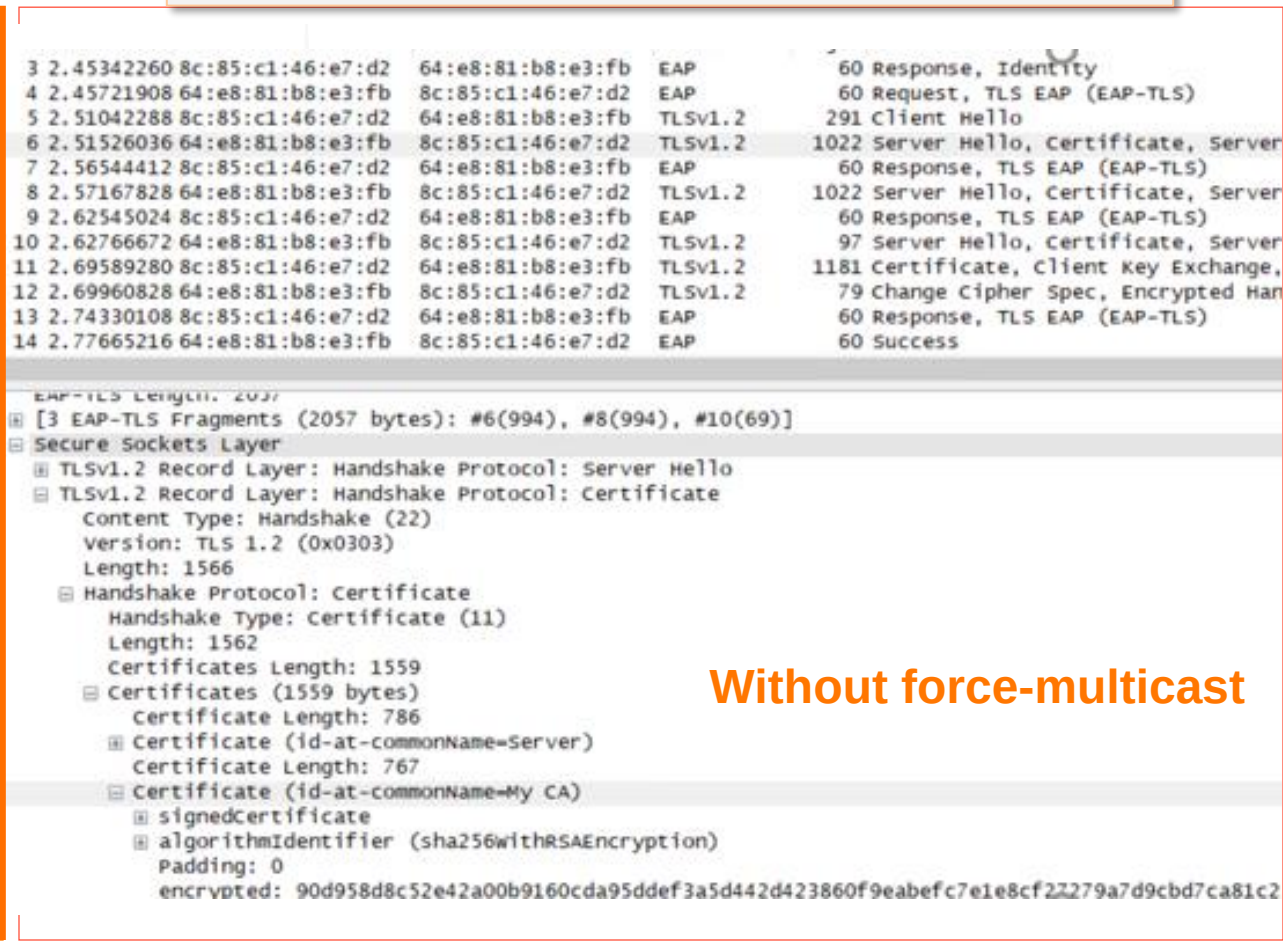
dot1x Supplicant- EAPoL force multicast

EAPoL force multicast: Configure the dot1x supplicant to send only multicast EAPoL packets irrespective of receiving unicast EAPoL packets from the authenticator.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant

CX_SW(config-dot1x-supp)# policy CX_Policy

CX_SW(config-dot1x-supp-policy)# eapol-force-multicast

no eapol-force-multicast (default)
```



With force-multicast



Without force-multicast

dot1x Supplicant- Sub features

- max-retries: Configure the maximum number of authentication attempts before authentication fails.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# max-retries 5
max-retries 2 (default)
```

- eapol-timeout: Configure the time period (in seconds) to wait for a response from an authenticator before reattempting authentication.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# eapol-timeout 10
eapol-timeout 30 (default)
```

- EAP method: Configure the EAP method to use for authentication.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# eap-method eap-md5
eap-method eap-tls (default)
```

dot1x Supplicant- Sub features

- EAP identity: Configure the EAP identity to use for authentication. The information includes an identity string and an optional password.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_Policy
CX_SW(config-dot1x-supp-policy)# eap-identity identity yash
CX_SW(config-dot1x-supp-policy)# eap-identity password plaintext CXTME
```

- discovery-timeout: Configure the time period (in seconds) to wait for a potential dot1x authenticator on the other end before considering the link to be non dot1x capable and opening the interface on the data-plane. On a timeout, the switch will not use the authentication result to determine the forwarding behavior of the interface until a link flap. If not set, the switch will wait for the dot1x authentication cycle to complete before determining the forwarding state of the interface.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_Policy
CX_SW(config-dot1x-supp-policy)# discovery-timeout 15
no discovery-timeout (default)
```

dot1x Supplicant- Sub features

- Held-period: Configure the time period (in seconds) to wait after a failed authentication attempt before another attempt is permitted.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant

CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy

CX_SW(config-dot1x-supp-policy)# held-period 30

 held-period 60 (default)
```

- start mode: Configure the forwarding behavior of the interface on the data-plane when the authentication is in-progress during the first run of the supplicant.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant

CX_SW(config-dot1x-supp)# policy CX_Policy

CX_SW(config-dot1x-supp-policy)# start-mode start-closed

start-mode start-open (default)
```

- fail mode: Configure the forwarding behavior of the interface when the dot1x authentication fails.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant

CX_SW(config-dot1x-supp)# policy CX_Policy

CX_SW(config-dot1x-supp-policy)# fail-mode fail-closed

fail-mode fail-open (default)
```

- **dot1x supplicant restart**: Configure the EAPoL protocol version to use in EAPoL frames

```
CX_SW # port-access dot1x supplicant restart

interface  Restart the 802.1X supplicant for specified interfaces

  <cr>
```

dot1x supplicant show commands

```
CX_SW# show aaa authentication port-access dot1x supplicant status

802.1X Supplicant Status

Interface           Policy              PAE State           Authenticator       EAP Method          Status

----------          ----------------    ----------------    ------------------  -----------         ------- ---

1/1/1               CX_Policy_01        Authenticated       38:21:c7:59:ad:27   EAP-TLS             Secured

1/1/2               CX_Policy_02        Authenticating      38:21:c7:59:ad:28   EAP-MD5             Blocked

1/1/3               CX_Policy_01        Unauthenticated     38:21:c7:59:ad:29   EAP-TLS             Fail-Open

1/1/4               CX_Policy_03        Unauthenticated      --                     --              Open
```

1. show aaa authentication port-access dot1x supplicant policy
2. **show aaa authentication port-access dot1x supplicant status**
    1. show aaa authentication port-access dot1x supplicant status interface 1/1/1 802.1X Supplicant Status
3. show aaa authentication port-access dot1x supplicant statistics
4. diag-dump dot1x-supplicant basic
5. port-access dot1x supplicant restart
6. show tech dot1x-supplicant [local-file]

Best Practices

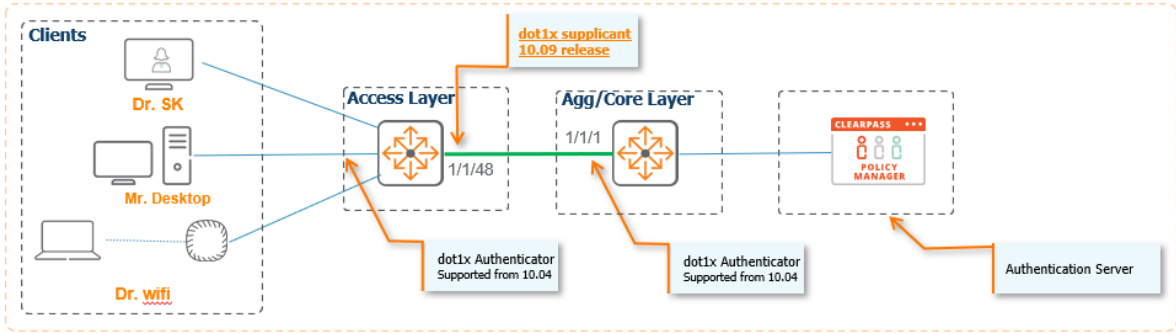
AOS-CX dot1x supplicant configuration

Recommended dot1x supplicant configuration

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant_uplink_1
        eap-identity identity cxtme
        eap-identity password plaintext setpasswd ###(EAP-MD5)
        discovery-timeout 60
        start-mode start-closed
        fail-mode fail-closed
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant_uplink_1
        enable
```

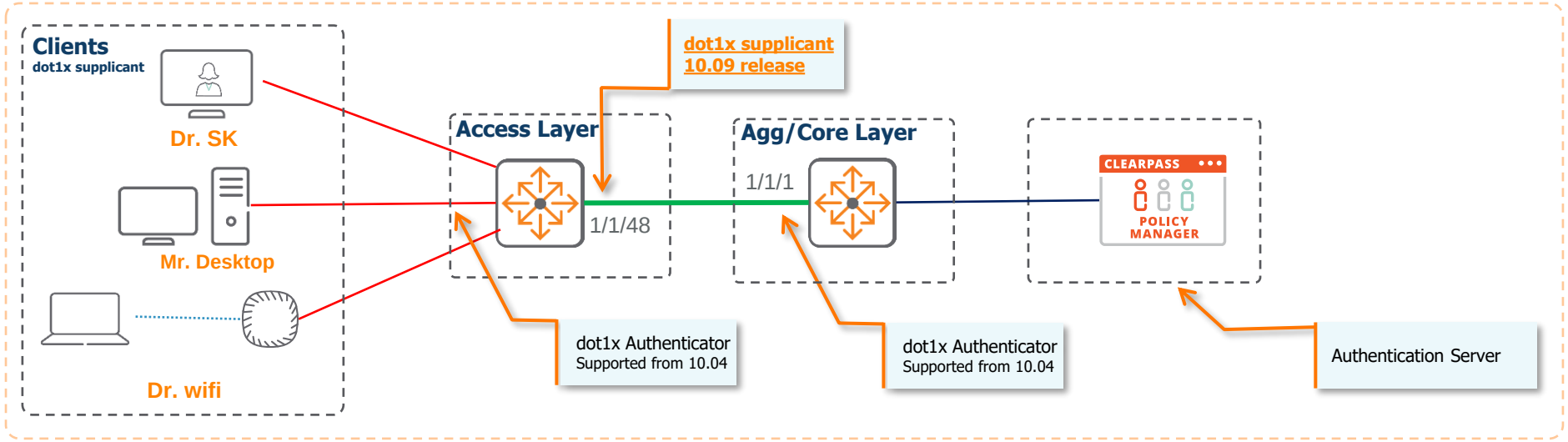
New Show commands

```
show aaa authentication port-access dot1x supplicant status

CXdot1xsupplicant# sh aaa authentication port-access dot1x supplicant status

802.1X supplicant Status

 Interface  Policy           PAE State       Authenticator      EAP Method  Status
 ---------- ---------------- --------------- ------------------ ----------- ----------
 1/1/48     cx_dot1x_supp... Authenticated   64:e8:81:b8:e3:fb  EAP-TLS     Secured

CXdot1xsupplicant#
```



Troubleshooting

Recommended troubleshooting flow



- Have a topology diagram ready
- Ensure IPs, interface details are included
- Check physical cabling and generate “show tech” when opening a TAC case
- Check network: show LLDP neighbor, ensure underlay network works using ping and traceroute between loopbacks and interfaces, fix any issues found

1. Check dot1x supplicant policy configuration
2. Check dot1x supplicant policy is associated to right uplink interface
3. Check dot1x authenticator switch interface eapol is reaching and authenticator has required configuration
4. Check radius server configuration
5. Check required certificate are installed and attached to right application

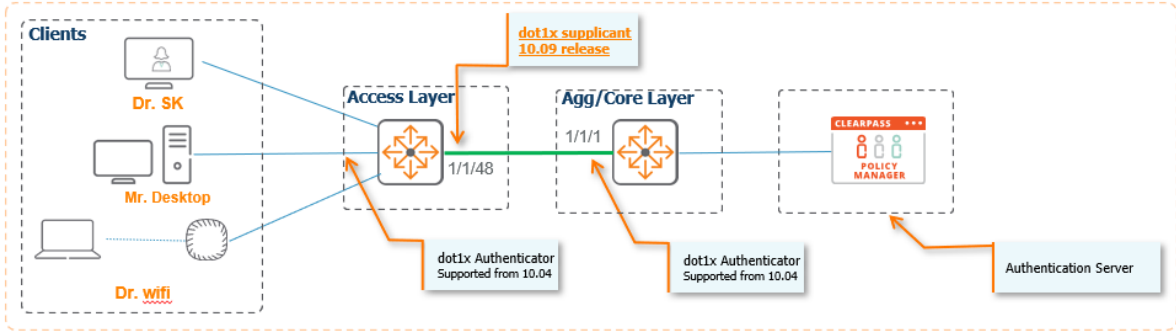
AOS-CX dot1x supplicant configuration

Recommended dot1x supplicant configuration

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant_uplink_1
        eap-identity identity cxtme
        eap-identity password plaintext setpasswd ###(EAP-MD5)
        discovery-timeout 60
        start-mode start-closed
        fail-mode fail-closed
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant_uplink_1
        enable
```

New Show commands

```
show aaa authentication port-access dot1x supplicant status

CXdot1xsupplicant# sh aaa authentication port-access dot1x supplicant status

802.1X supplicant Status

 Interface  Policy           PAE State       Authenticator      EAP Method  Status
 ---------- ---------------- --------------- ------------------ ----------- ----------
 1/1/48     cx_dot1x_supp... Authenticated   64:e8:81:b8:e3:fb  EAP-TLS     Secured

CXdot1xsupplicant#
```



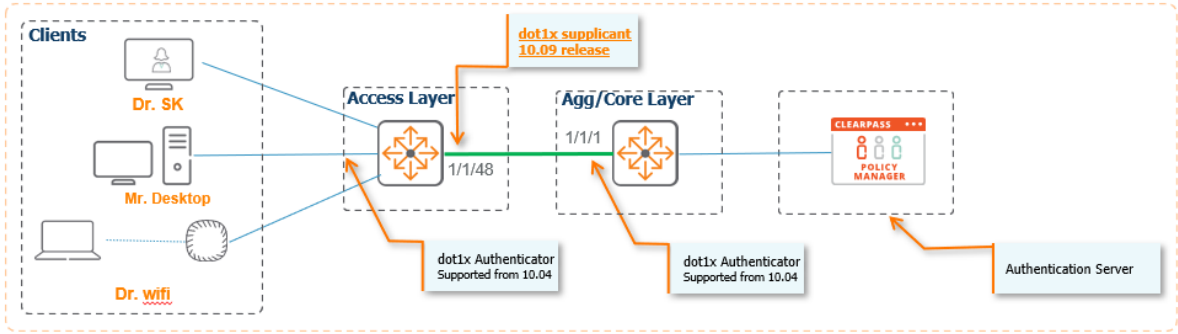
AOS-CX dot1x authenticator configuration

Recommended dot1x supplicant configuration

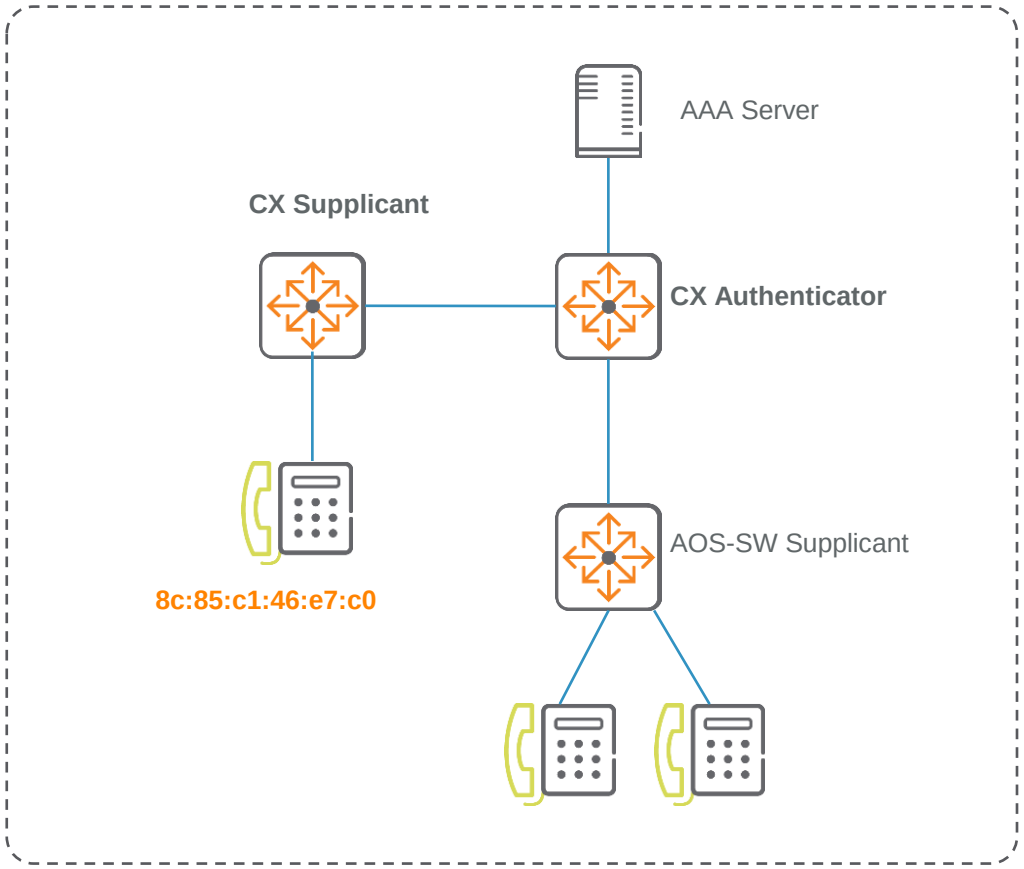
```
interface 1/1/5

aaa authentication port-access client-limit 5

    aaa authentication port-access dot1x authenticator

    enable

    aaa authentication port-access mac-auth

        enable

radius-server tracking interval 60

radius-server tracking retries 2

radius-server host 50.1.1.2 key ciphertext
AQBapdAz4irjSK61Zg/CFArsNYWKbn1LObqDD/v9SH1eMQ6ABQAAADY26li
u tracking enable tracking-mode dead-only
```

New Show commands

```
Agg-Core-CXSW# show port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

--------------------------------------------------------------------------------------------------------

  Port     MAC-Address       Onboarding     Status      Role                              Device Type
                             Method

--------------------------------------------------------------------------------------------------------

c 1/1/5    8c:85:c1:46:e7:d2 dot1x          Success     RADIUS_652982728

c 1/1/5    8c:85:c1:46:e7:c0 mac-auth       Success     RADIUS_652982728

Agg-Core-CXSW#
```

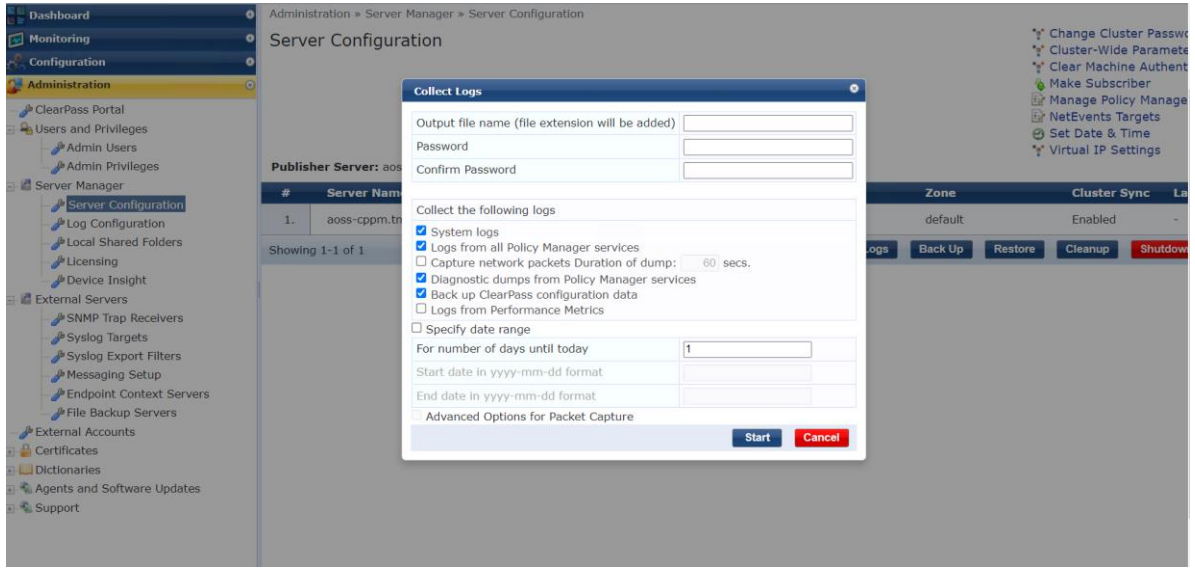


Troubleshooting - Mirror




```
mirror session 1
    enable
    destination interface 1/1/40
    source interface 1/1/51 both
```

```
Mirror session 1
Source interface 1/1/1 both
Destination CPU
enable
diag utilities tshark file
copy tshark-pcap tftp://10.80.2.187/supplicant.pcap vrf mgmt
```



dot1x supplicant Troubleshooting

New Show & Tech Command

```
show crypto pki certificate

show aaa authentication port-access dot1x supplicant policy

show aaa authentication port-access dot1x supplicant status

show aaa authentication port-access dot1x supplicant statistics

show running-config aaa authentication port-access dot1x supplicant

port-access dot1x supplicant restart

diag-dump dot1x-supplicant basic

show tech dot1x-supplicant [local-file]
```

New Event Logs

Daemon	Event ID	Severity	Message	Description
dot1x-suppd	12301	INFO	dot1x supplicant has blocked the interface {iface}.	The dot1x supplicant is blocking the interface on the data-plane.
dot1x-suppd	12302	INFO	dot1x supplicant has unblocked the interface {iface}.	The dot1x supplicant is opening the interface on the data-plane.
dot1x-suppd	12303	INFO	dot1x supplicant PAE restarted on interface {iface} due to change in policy {policy}.	The dot1x supplicant PAE is restarted due to a change in the policy used on the interface.
dot1x-suppd	12304	ERR	dot1x supplicant is not supported on the port {port}.	The dot1x supplicant is enabled on a port that is not supported (Ex: LAG, ROP).

New Debug Logs

Daemon	Severity	Message	Description
dot1x-suppd	INFO	dot1x supplicant FSM for PAE with MAC {mac} transitioned from {old-state} to {new-state}.	The dot1x supplicant PAE’s state machine has changed state.
dot1x-suppd	INFO	dot1x supplicant status on interface {iface} changed from {old-status} to {new-status}.	The dot1x supplicant status changed on the interface.

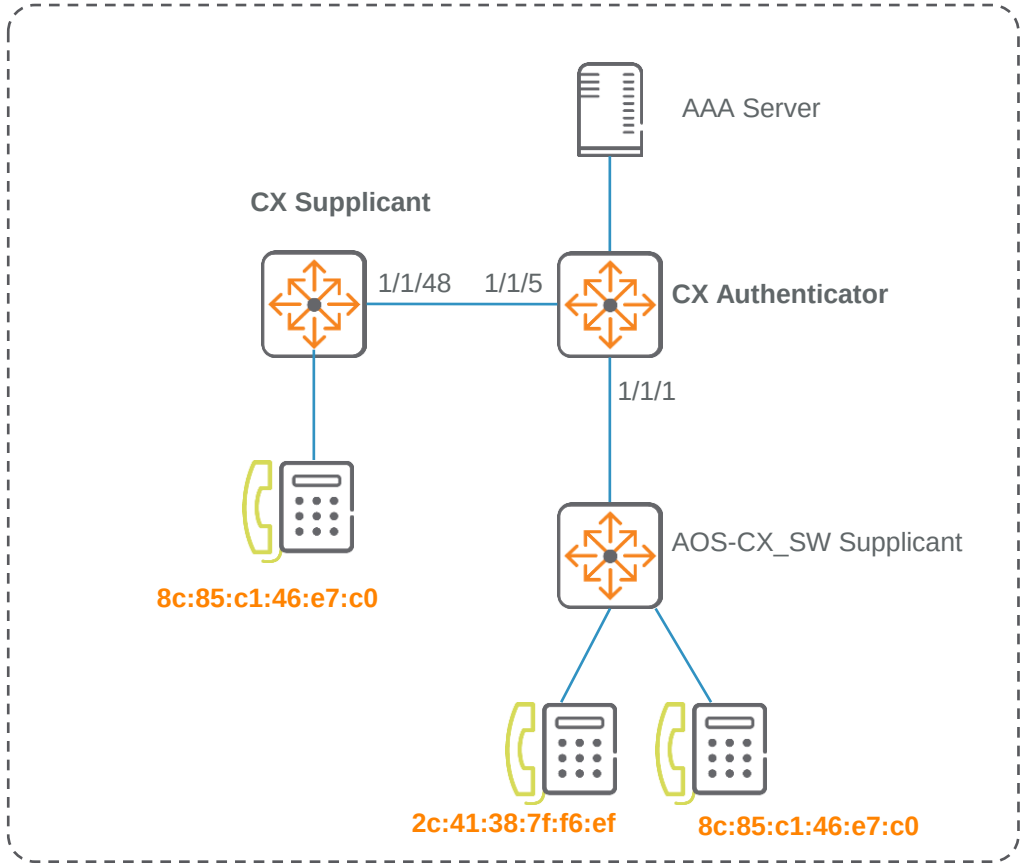
Demo

Demo: dot1x supplicant

- EAP-Method
  - EAP-TLS
    - User-defined Certificate
    - EST enrollment
  - EAP-MD5
- start-mode & fail-mode
- canned eap success
- eapol-force-multicast

dot1x Supplicant: EAP-TLS User defined Certificate

```
crypto pki application dot1x-supplicant certificate client


aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-identity identity cxtme
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant
        enable
```



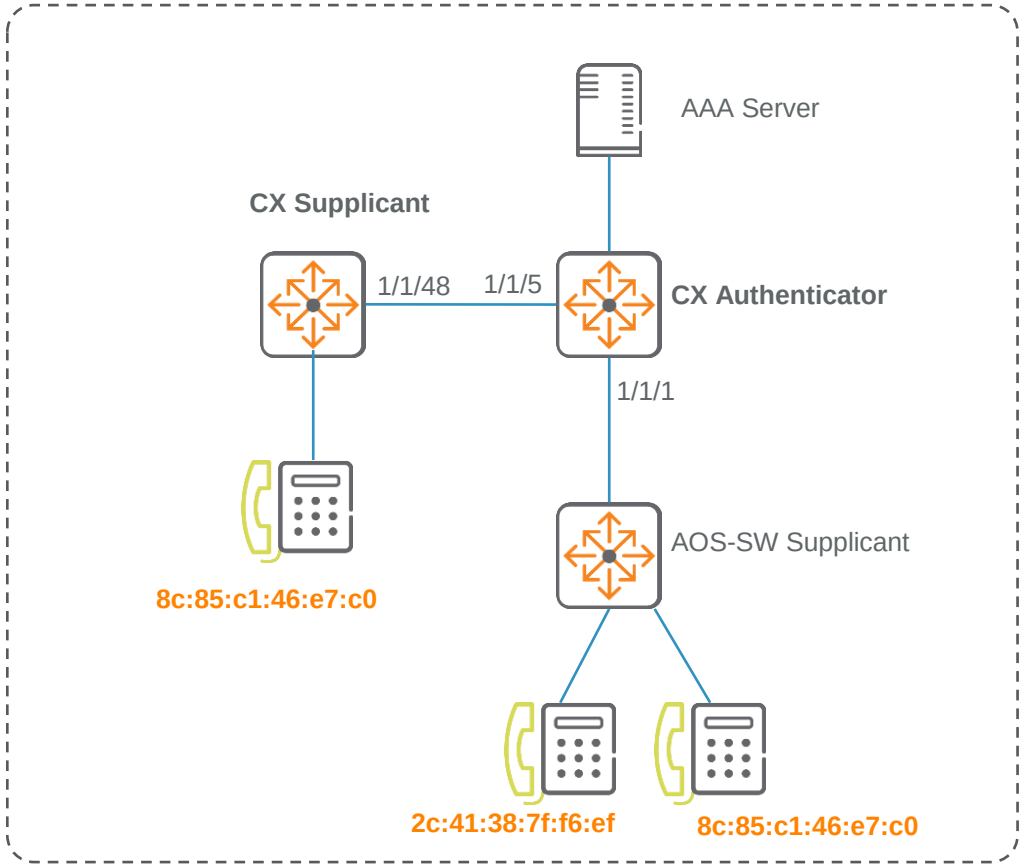
dot1x Supplicant: EAP-TLS User defined Certificate

```
Access-CXSW(config)# crypto pki application dot1x-supplicant certificate client

Access-CXSW(config)# end

Access-CXSW# sh crypto pki certificate

Certificate Name                Cert Status    EST Status        Associated Applications

------------------------------- -------------- ----------------- ------------------------------

client                          installed      n/a               dot1x-supplicant

local-cert                      installed      n/a               captive-portal, est-client, https-server, radsec-
client, syslog-client

est_certificate1                installed      enroll success    none

device-identity                 installed      n/a               none

Access-CXSW#
```

```
Access-CXSW# show crypto pki certificate client pem

  Certificate Name: client

  Associated Applications:

    dot1x-supplicant

  Certificate Status: installed

  EST Status: n/a

  Certificate Type: regular

  Intermediates:

    none
```

dot1x Supplicant: EAP-TLS EST Enrolled Certificate

```
crypto pki application dot1x-supplicant certificate
est_certificate1

aaa authentication port-access dot1x supplicant

    enable

    policy cx_dot1x_supplicant

        eap-identity identity cxtme


interface 1/1/48

    aaa authentication port-access dot1x supplicant

        associate policy cx_dot1x_supplicant

        enable
```



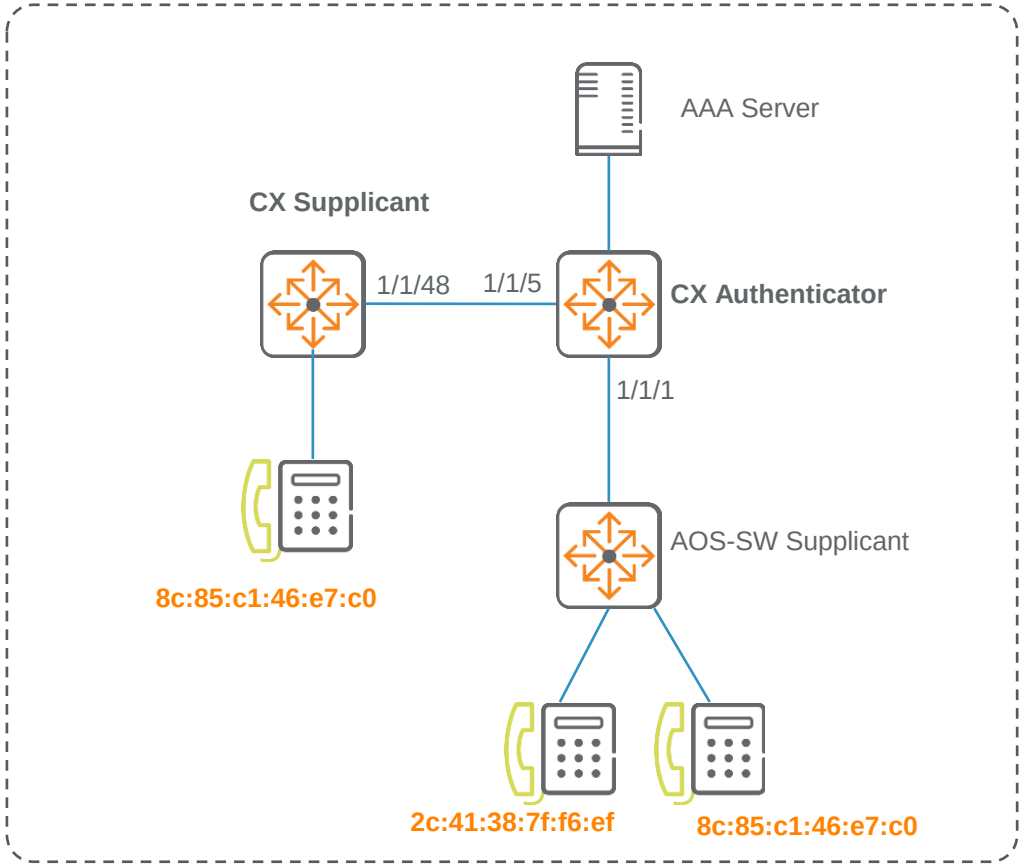
dot1x Supplicant: EAP-TLS User defined Certificate

```
Access-CXSW(config)# crypto pki application dot1x-supplicant certificate est_certificate1

Access-CXSW(config)# end

Access-CXSW# sh crypto pki certificate

Certificate Name                Cert Status    EST Status        Associated Applications

------------------------------- -------------- ----------------- -------------------------------

client                          installed      n/a               none

local-cert                      installed      n/a               captive-portal, est-client, https-server, radsec-
client, syslog-client

est_certificate1                installed      enroll success    dot1x-supplicant

device-identity                 installed      n/a               none

Access-CXSW#
```

```
Access-CXSW# sh crypto pki certificate est_certificate1
pem

  Certificate Name: est_certificate1

  Associated Applications:

    dot1x-supplicant

  Certificate Status: installed

  EST Status: enroll success

  Certificate Type: regular
```

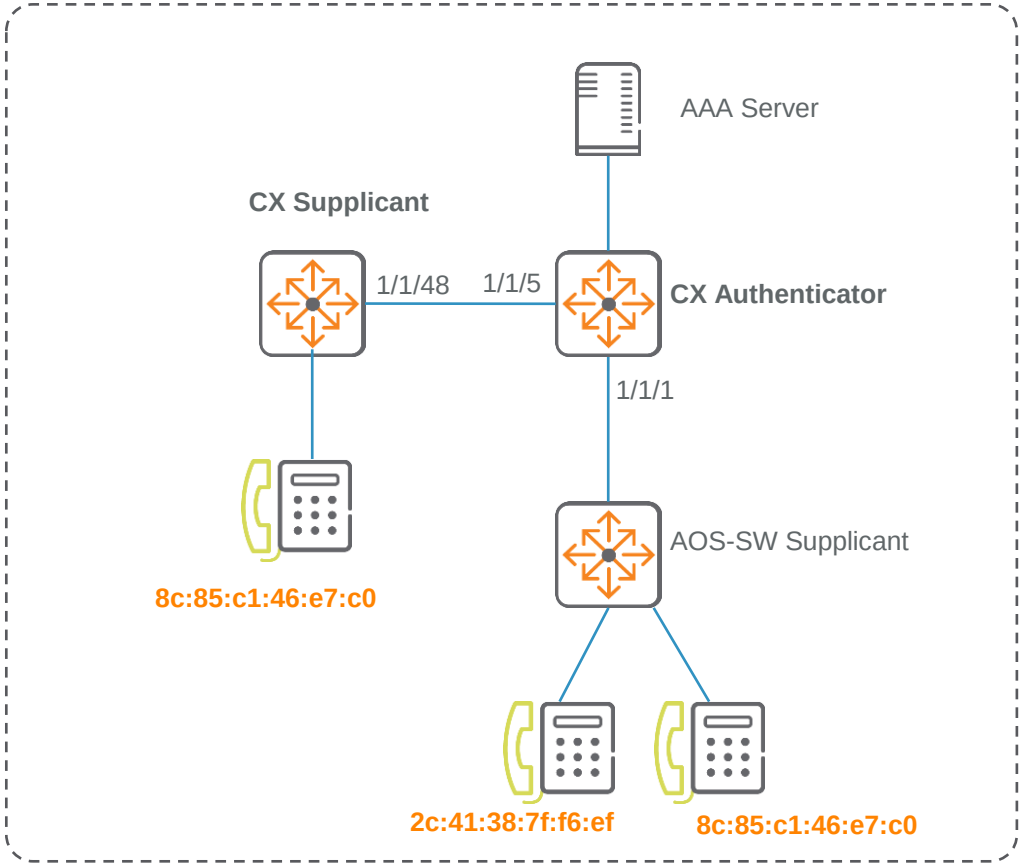
dot1x Supplicant: EAP-MD5

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-method eap-md5
        eap-identity identity cxtme
        eap-identity password ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPijBaqs
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant
        enable
```



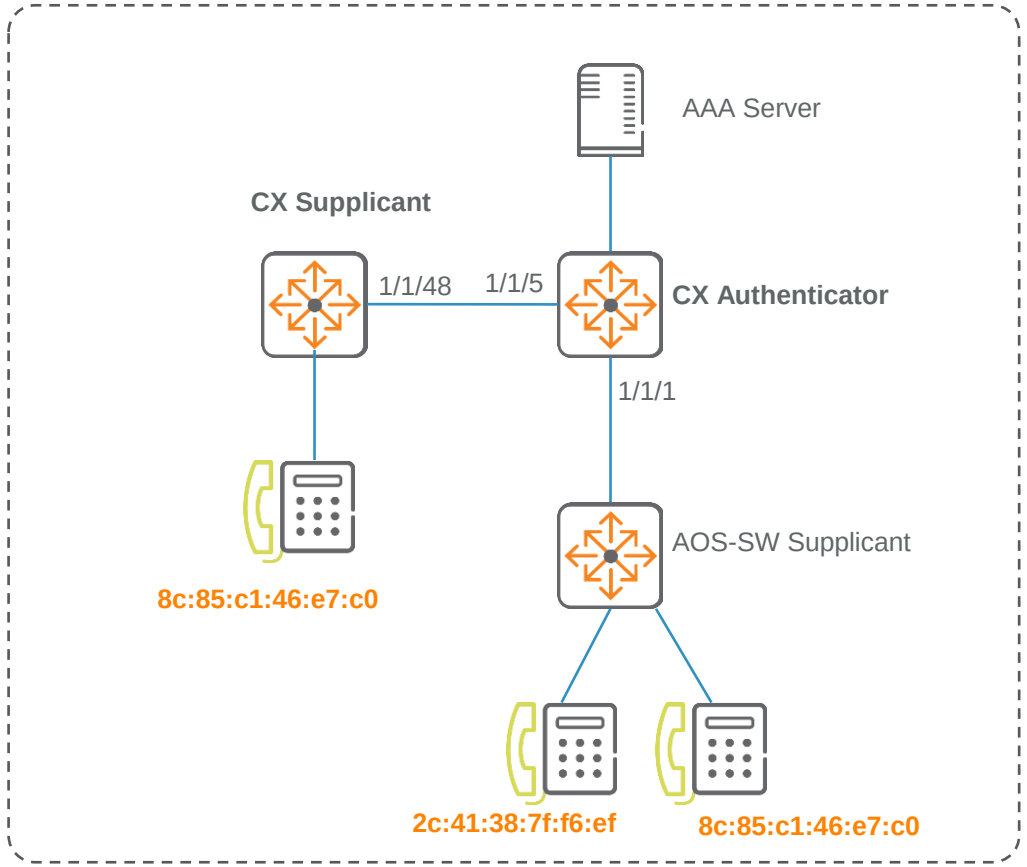
dot1x Supplicant: start-mode and fail-mode

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-method eap-md5
        eap-identity identity cxtme
        eap-identity password ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPi
jBaqs
        start-mode start-closed
        fail-mode fail-closed
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant
        enable
```



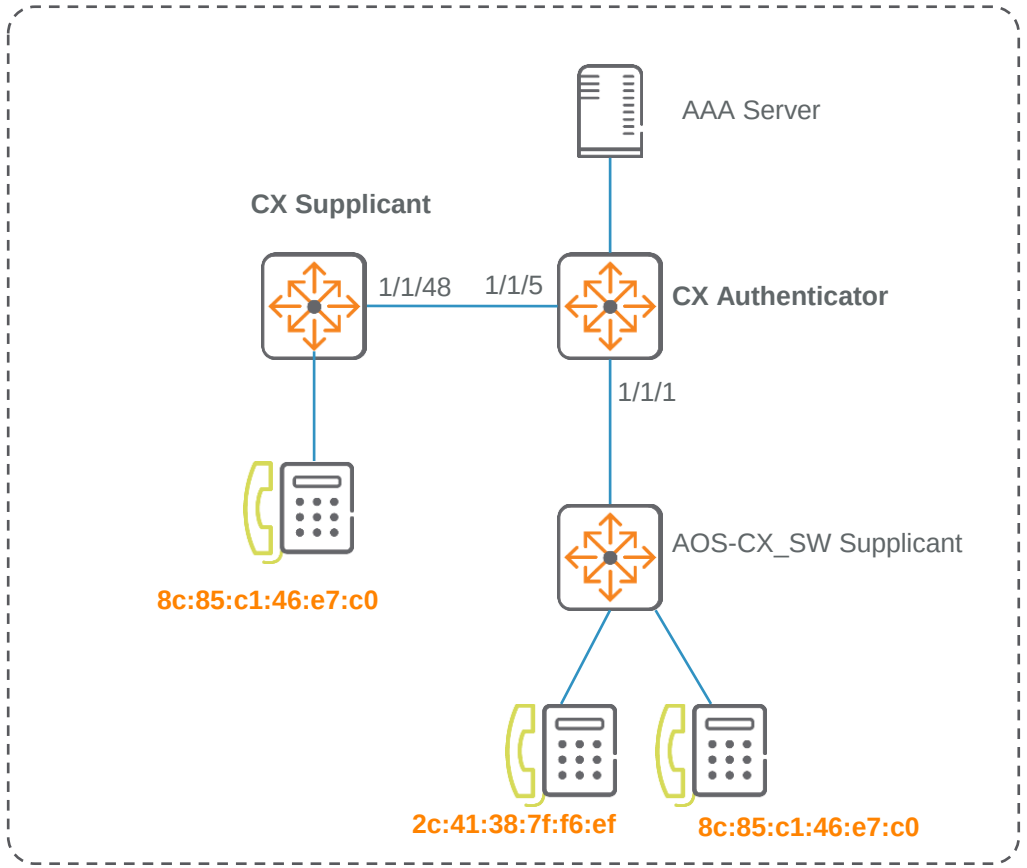
dot1x Supplicant: Canned EAP Success

```
aaa authentication port-access dot1x supplicant

    enable

    policy cx_dot1x_supplicant

        eap-method eap-md5

        eap-identity identity cxtme

        eap-identity password ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPi
jBaqs

canned-eap-success

interface 1/1/48

    aaa authentication port-access dot1x supplicant

        associate policy cx_dot1x_supplicant

        enable
```



dot1x Supplicant: force-multicast

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-method eap-md5
        eap-identity identity cxtme
        eap-identity password ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPi
jBaqs
        eapol-force-multicast
        eapol-protocol-version 2
        canned-eap-success
        discovery-timeout 60
        start-mode start-closed
        fail-mode fail-closed
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant
        enable
```



Additional Information

Additional information (internal)

- Functionality guide dot1x supplicant
- Design guide dot1x supplicant
- IEEE dot1x

aruba
a Hewlett Packard
Enterprise company

Thank you

yashavantha.n.n@hpe.com