AOS-CX Security Update

Speakers:
- Yash N. N.
- Gopala Krishna
- Shobana Nandakumar
Agenda

1. Security Review
2. Concurrent Onboarding
3. Authentication Priority
4. Cache-Reauth
Security Review
AOS-CX Security Classification

MANAGEMENT SECURITY INFRA

NETWORK DEFENCE

PORT-ACCESS

ACL and Classifier Policy

AOS-CX Security external documentation
Port-access and Mgmt Security Infra features
Network defense
ACL and Classifier

Note:
- Above Security Classification is based on our AOS-CX Software features.
- Hardware security and OS Security is not part of this presentation.
AOS-CX Access Security Terminology

- **Authentication**: Identifies users, validates their credentials, and grants port/switch access.

- **Authorization**: controls authenticated users command execution and switch interaction privileges.

- **Accounting**: collects and manages user session activity logs for auditing and reporting purposes.

- Local AAA and Remote AAA

- **TACACS+** (Terminal Access Controller Access-Control System Plus)

- **RADIUS** (Remote Authentication Dial-In User Service)

- **NAC**: Network Access Control

- **Supplicant**:  
  - Client/end-user - PC, AP, IoT Device, Phone.  
  - Device that tries to access the LAN or WLAN.

- **Authenticator**:  
  - Network Access Device  
  - A network device, such as an Ethernet switch that authenticates the supplicant.

- **Authentication Server**:  
  - AAA/Radius Server  
  - Typically a host running software supporting the RADIUS and EAP protocols that provides an authentication service to the authenticator

- **Network Port-Access**:  
  - Auth-precedence or Auth-order  
  - 802.1x or dot1x, mac-auth

- **AAA Onboarding**:  
  - Default AAA highest priority (dot1x, mac-auth)  
  - Device profile
Client <MAC-ADDR>[, <USER-NAME>]

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

Session Details
-----------------

Port : <IFNAME>
Session Time : <SESSION-ALIVE-TIME>
IPv4 Address : <IPv4-ADDRESS>
IPv6 Address : <IPv6-ADDRESS>

Authentication Details
-----------------------

Status : <AUTH-METHOD> <AUTH-STATUS>
Auth Precedence : <AUTH-METHOD-1> - <AUTH-METHOD-STATUS>, <AUTH-METHOD-2> - <AUTH-METHOD-STATUS>

Authorization Details
---------------------

Role : <ROLE-NAME>[, <ROLE-TYPE>]
Status : <ROLE-STATUS>[, <FAILURE-REASON>]

AOS-CX Security internal documentation

Port-access
AOS-CX Simple Steps!
Access Security Simple Steps!

AOS-CX Simple Steps to configure Radius-server
AOS-CX Simple Steps to configure Downloadable User Role
AOS-CX Simple Steps to Local User Role (LUR) simple steps to Configure
AOS-CX Simple Steps to Deploy VOIP
AOS-CX Port-Access Security 10.6 feature introduction

- **Concurrent-onboarding:**
  - Also know as Parallel-Authentication

- **Auth-priority:**
  - To authorize the client based on priority.
  - First download the supplicant software or firmware/OS patches before attempting 802.1x Authentication

- **Cache-reauth**
  - Per user cache-reauth – Port-access role!
  - Interface level cache-reauth is supported in previous release.
Concurrent Onboarding

Auth methods dot1x and mac-auth start concurrently

Advantage: faster onboarding process
Overview and Use cases
Overview Topics

– What is the Feature/Solution
– Why is the Feature/Solution important
– What use cases does the Feature/Solution Solve Well
– If Enhancement
  – How does this enhancement fit into the existing feature.
  – What changes in behavior will be seen from previous releases
– What versions of partner software is this feature dependent on.
  – E.g. Dynamic segmentation and Downloadable User Roles are depending on Mobility Controller SW and Clearpass
Common methods of authentication

- **IEEE 802.1X – EAPoL RFC 3748**
  - Extensible Authentication Protocol
  - Supports bi-directional authentication
  - Usernames/passwords and/or certificates

- **MAC authentication**
  - Requires managing a database of MAC addresses
  - **Subject to spoofing**
  - Can be augmented with device fingerprinting

- **Captive/web portal**
  - Commonly used in guest networks
  - User device uses a web browser to authenticate

- **Dynamic segmentation**
  - Combines authentication with authorization
  - Switch performs the authentication, and a Mobility Controller performs the authorization
802.1x authentication

**EAP over LAN (EAPOL)**

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000 0000</td>
<td>EAP-Packet</td>
<td>Contains an encapsulated EAP frame (this is what majority of EAPOL frames are)</td>
</tr>
<tr>
<td>0000 0001</td>
<td>EAPOL-Start</td>
<td>A supplicant can issue an EAPOL-Start frame instead of waiting for a challenge from the authenticator</td>
</tr>
<tr>
<td>0000 0010</td>
<td>EAPOL-Logoff</td>
<td>Used to return the state of the port to unauthorized when the supplicant is finished using the network</td>
</tr>
<tr>
<td>0000 0011</td>
<td>EAPOL-Key</td>
<td>Used to exchange Cryptographic Keying Information</td>
</tr>
<tr>
<td>0000 0100</td>
<td>EAPOL-Encapsulated-ASF-Alert</td>
<td>Provided as a method of allowing Alerting Standards Forum (ASF) alerts (ex. specific SNMP traps) to be forwarded through a port that is in the Unauthorized state</td>
</tr>
</tbody>
</table>

All other possible values are reserved for future use.
802.1x authentication

- **Access**
- **blocked**

802.1X/EAP Authentication

RADIUS

EAP over LAN (EAPOL)

RADIUS
(encrypts packets)

---

### aaa authentication port-access dot1x authenticator enable
### config-if)

### 6300-1-VSF# show port-access clients

#### Port Access Clients

Status codes: d device-mode

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Address</th>
<th>Onboarding Method</th>
<th>Status</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/3</td>
<td>00:50:56:8e:86:27 dot1x</td>
<td>Success</td>
<td>RADIUS_2811264511</td>
<td></td>
</tr>
</tbody>
</table>

6300-1-VSF#
802.1x authentication

802.1x Client

Access

blocked

802.1X/EAP Authentication

EAP over LAN (EAPOL)

RADIUS server

RADIUS
(encapsulates packets)

aaa authentication port-access dot1x authenticator enable
config-if)#
aaa authentication port-access dot1x authenticator enable

Check radius-server configuration

Mgmt or any vrf reachable to Radius-server
radius-server host 15.136.40.53 key ciphertext
AQBapdA4irjS6K61Zg/CFArsNYWbKn10bqQD/v9S1eMQ6ABQAAADY26liu tracking enable clearpass-username
appadmin clearpass-password ciphertext
AQBap5x6d58BCqtV3fVhkpQltk11bWJeMt1zwCIMH7UK8BoeDQAAB2+e5ytA3XjZwhkVY4= vrf mgmt

Default vrf
radius-server host 15.136.40.53 key ciphertext
AQBapdA4irjS6K61Zg/CFArsNYWbKn10bqQD/v9S1eMQ6ABQAAADY26liu tracking enable clearpass-username
appadmin clearpass-password ciphertext
AQBap5x6d58BCqtV3fVhkpQltk11bWJeMt1zwCIMH7UK8BoeDQAAB2+e5ytA3XjZwhkVY4=

show radius-server detail
802.1x authentication

6300-1-VSF# show aaa authentication port-access dot1x authenticator interface
2/1/3 client-status

Client 00:50:56:8e:86:27, hpn, 2/1/3
========================================= Authentication Details
--------------------------------------
Status : Authenticated
Type : Pass-Through
EAP-Method : MD5
Auth Failure reason :
Time Since Last State Change : 5722s

Authentication Statistics
-------------------------
Authentication : 1
Authentication Timeout : 0
EAP-Start While Authenticating : 0
EAP-Logoff While Authenticating : 0
Successful Authentication : 1
Failed Authentication : 0
Re-Authentication : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
EAP-Start When Authenticated : 0
EAP-Logoff When Authenticated : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0

6300-1-VSF# show aaa authentication port-access interface all client-status

Port Access Client Status Details
Client 00:50:56:8e:86:27, hpn
========================================= Session Details
-------------------------
Port : 2/1/3
Session Time : 20041s
IPv4 Address :
IPv6 Address :

Authentication Details
-----------------------
Status : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted

Authorization Details
---------------------
Role : RADIUS_2811264511
Status : Applied

6300-1-VSF#
802.1x Troubleshooting and Debugging
Polling question

- Factory default AOS-CX switch comes with dot1x and mac-auth enabled?
  - True
  - False
Let's Focus and start very small
Mac-Auth authentication

Client

2c:41:38:7f:27:05

RADIUS server

Mac-Auth

Access blocked

aaa authentication port-access mac-auth enable (config-if)#
aaa authentication port-access mac-auth enable

BLDG02-F1# show port-access clients

Port Access Clients
Status codes: d device-mode

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Address</th>
<th>Onboarding Method</th>
<th>Status</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/5</td>
<td>2c:41:38:7f:27:05</td>
<td>mac-auth</td>
<td>Success</td>
<td>RADIUS_1986087471</td>
</tr>
</tbody>
</table>

BLDG02-F1#
Mac-Auth Authentication

Client
2c:41:38:7f:27:05

RADIUS server

BLDG02-F1# show aaa authentication port-access mac-auth interface all
Client-status mac 2c:41:38:7f:27:05
Port Access Client Status Details
Client 2c:41:38:7f:27:05, 2c41387f2705, 1/1/5

Authentication Details
-----------------------------------------------
Status : Authenticated
Auth-Method : chap
Successful Authentication : 1
Failed Authentication : 0
Re-Authentication : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0

BLDG02-F1#
Mac-Aauth Troubleshooting and Debugging

6300-1- VSF# show debug buffer | in PORTACCESS_MACAUTH_PROTOCOL
logID=1736540 logID=1736540 Handling event 'MAC-Aauth Port State Up' for MACAuthPort '1/1/5' in state 'DOWN'
logID=1736540 logID=1736540 macauthport SM State transition [DOWN] -> [UP] for object with key '1/1/5'
logID=1736540 logID=1736540 Event handler of MACAuthPort '1/1/5' for event 'MAC-Aauth Port State Up' in state 'DOWN' returned 'OK'
logID=1736543 Handling event 'Portclient Auth Start' for MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 in state 'NULL'
logID=1736543 macauthpae SM State transition [INITIALIZED] -> [AUTHENTICATING] for object with key '1/1/5, 08:00:0f:22:c6:e4'
logID=1736543 Mac-auth client send radius auth request on port 1/1/5 for client 08-00-0f-22-c6-e4
logID=1736543 Event handler of MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 for event 'Portclient Auth Start' in state 'NULL' returned 'OK'
logID=1736544 Handling event 'MAC-Aauth RADIUS Auth Response' for MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 in state 'AUTHENTICATING'
logID=1736544 macauthpae SM State transition [AUTHENTICATING] -> [AUTHENTICATED] for object with key '1/1/5, 08:00:0f:22:c6:e4'
logID=1736544 Event handler of MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 for event 'MAC-Aauth RADIUS Auth Response' in state 'AUTHENTICATING' returned 'OK'
logID=1736545 Handling event 'Profile Status For Client' for MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 in state 'AUTHENTICATED'
logID=1736545 Event handler of MACAuthPAE 08:00:0f:22:c6:e4 on port 1/1/5 for event 'Profile Status For Client' in state 'AUTHENTICATED' returned 'OK'
6300-1- VSF#
Mac-Auth Troubleshooting and Debugging

6300-1- VSF# show debug buffer | in transition

**Authentication**
- **PORTACCESS_SERVICES|logID=1733990** secureport SM State transition [DOWN] -> [BLOCKED] for object with key '1/1/5'
- **PORTACCESS_MACAUTH_PROTOCOL|logID=1733991** macauthport SM State transition [UP] -> [DOWN] for object with key '1/1/5'
- **PORTACCESS_SERVICES|logID=1734002** portclientauth SM State transition [NO AUTH] -> [AUTH IN PROGRESS] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_MACAUTH_PROTOCOL|logID=1734002** macauthpae SM State transition [INITIALIZED] -> [AUTHENTICATING] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_MACAUTH_PROTOCOL|logID=1734003** macauthpae SM State transition [AUTHENTICATING] -> [AUTHENTICATED] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_SERVICES|logID=1734003** portclientauth SM State transition [AUTH IN PROGRESS] -> [FINAL AUTH SUCCESS] for object with key '1/1/5, 08:00:0f:22:c6:e4'

**Authorization**
- **PORTACCESS_SERVICES|logID=1734003** portclientprofile SM State transition [NULL] -> [PROFILE APPLY IN PROGRESS] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_SERVICES|logID=1734003** securevlan SM State transition [INACTIVE] -> [ACTIVE] for object with key '1/1/5'
- **PORTACCESS_SERVICES|logID=1734004** portclientattr SM State transition [APPLY IN PROGRESS] -> [APPLIED] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_SERVICES|logID=1734004** portclientprofile SM State transition [PROFILE APPLY IN PROGRESS] -> [PROFILE APPLIED] for object with key '1/1/5, 08:00:0f:22:c6:e4'
- **PORTACCESS_SERVICES|logID=1734004** securereport SM State transition [BLOCKED] -> [CLIENT MODE SECURE] for object with key '1/1/5'
Demo
Polling Question!

What is default authentication precedence (auth-precedence or auth-order) on CX Access Switches?

– mac-authentication then dot1x.
– dot1x then mac-auth
802.1x & Mac-Auth authentication

**EAP over LAN (EAPOL)**

```plaintext
aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable

(config-if)#
aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable

aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
```
AOS-CX 802.1x timer configuration

aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable

(config-if)#

aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable

Default Values
- Max-eapol-Requests = 5
- Max-eap-retries = 2
- Eapol Timeout = 0 - Based on Jitter Algorithm
- Discovery Period 30s

(config-if)#

aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
aaa authentication port-access auth-precedence Specify authentication precedence.
(Default: dot1x mac-auth)
PC Behind Phone Use Case

802.1x Client  →  Mac-Auth Client  →  RADIUS server

802.1X/EAP Authentication

EAP over LAN (EAPOL)

RADIUS
(encapsulates packets)

aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable

(config-if)#
  vlan trunk native 10
  vlan trunk allowed 10,112
  aaa authentication port-access dot1x authenticator
eapol-timeout 30
  max-eapol-requests 1
  max-retries 1
  reauth
  enable
  aaa authentication port-access mac-auth
cached-reauth
  cached-reauth-period 86400
  quiet-period 30
  enable
Demo
Delay in Mac authentication

```
aaa authentication port-access mac-auth enable
(config-if)#
aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable
```

**Note**
- With default precedence, it takes **162 sec to onboard the mac-auth clients**.
- Dot1x timers can be tuned to reduce this time
Concurrent onboarding from 10.6

- Enabling AAA authentication on Port, takes order of precedence, that will introduce some delay (162 secs in worst/default) to authenticate mac-auth client.
- Enables all methods to start concurrently for faster onboarding process
Concurrent onboarding from 10.6

1- Faster onboarding
- With default precedence, it takes 162 sec to onboard the mac-auth clients.
- Dot1x timers can be tuned to reduce this time but still it takes 60sec to start mac-auth with below recommended config.
- Reducing the eapol-timeout to aggressive value further makes dot1x to fail in some cases.

With concurrent onboarding mac-auth clients can be onboarded quickly.

2- Clients like PXE to download supplicant
The PXE clients expect the IP address to be assigned within 15-20 sec to continue further with PXE process to connect to server to download and install the images and supplicants. With concurrent onboarding, this can be achieved as mac-auth gets authenticated quickly that gives access to PXE network and continues the process.

Once supplicant is downloaded, PXE client will reboot and start dot1x!

```
(config-if)#
aaa authentication port-access dot1x authenticator enable
  aaa authentication port-access mac-auth enable

eapol-timeout 30
max-retires 1
max-eapol-request 1
```
Concurrent onboarding from 10.6

```
(config-if)#
port-access onboarding-method concurrent enable
  aaa authentication port-access dot1x authenticator enable
  aaa authentication port-access mac-auth enable
```

---

**EAP over LAN (EAPOL)**

**802.1X/EAP Authentication**

---

**Access blocked**

---

**Access**

---

**Mac-Auth**

---

**RADIUS server**

---

**RADIUS server**

---
Concurrent Onboarding from 10.6

802.1x Client

Mac-Auth Client

Access blocked

802.1X/EAP Authentication

RADIUS server

EAP over LAN (EAPOL)

RADIUS (encapsulates packets)

(config-if)#

!aaa authentication port-access auth-precedence mac-auth dot1x
  port-access onboarding-method concurrent enable
  aaa authentication port-access dot1x authenticator enable
  aaa authentication port-access mac-auth enable
Concurrent onboarding from 10.6 – Show CLI

6300-1- VSF# show aaa authentication port-access dot1x authenticator interface 2/1/3 client-status

Client 00:50:56:8e:86:27, hpn, 2/1/3
-----------------------------------------

Authentication Details
----------------------
Status : Authenticated
Type : Pass-Through
EAP-Method : MD5
Auth Failure reason :
Time Since Last State Change : 5722s

Authentication Statistics
-------------------------
Authentication : 1
Authentication Timeout : 0
EAP-Start While Authenticating : 0
EAP-Logoff While Authenticating : 0
Successful Authentication : 1
Failed Authentication : 0
Re-Authentication : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
EAP-Start When Authenticated : 0
EAP-Logoff When Authenticated : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0

6300-1- VSF# show aaa authentication port-access interface all client-status

Port Access Client Status Details
--------------------------------
Client 00:50:56:8e:86:27, hpn

Session Details
---------------
Port : 2/1/3
Session Time : 20041s
IPv4 Address :
IPv6 Address :

Authentication Details
----------------------
Status : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted

Authorization Details
---------------------
Role : RADIUS_2811264511
Status : Applied

6300-1- VSF#
Concurrent Onboarding

Note: It’s not a limitation, but good to aware!

- Consider RADIUS server blocks the client if it receives two requests (mac-auth and dot1x) from the same client, then concurrent onboarding is not feasible for such kind of deployment, because radius server allowing only one authentication request. In such cases solution is auth precedence with auth-priority.
Demo
Best Practices
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>CX 10.5</th>
<th>10.6 – Concurrent Onboarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>CX_6xxxx# show running-config interface 1/1/12</td>
<td>CX_6xxxx# show running-config interface 1/1/12</td>
<td></td>
</tr>
<tr>
<td>interface 1/1/12</td>
<td>interface 1/1/12</td>
<td></td>
</tr>
<tr>
<td>no shutdown</td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>no routing</td>
<td>no routing</td>
<td></td>
</tr>
<tr>
<td>vlan access 1</td>
<td>vlan access 1</td>
<td></td>
</tr>
<tr>
<td>spanning-tree bpdu-guard</td>
<td>spanning-tree bpdu-guard</td>
<td></td>
</tr>
<tr>
<td>spanning-tree root-guard</td>
<td>spanning-tree root-guard</td>
<td></td>
</tr>
<tr>
<td>spanning-tree tcn-guard</td>
<td>spanning-tree tcn-guard</td>
<td></td>
</tr>
<tr>
<td>spanning-tree port-type admin-edge</td>
<td>spanning-tree port-type admin-edge</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access allow-cdp-bpdu</td>
<td>aaa authentication port-access allow-cdp-bpdu</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access allow-lldp-bpdu</td>
<td>aaa authentication port-access allow-lldp-bpdu</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access client-limit 2</td>
<td>aaa authentication port-access client-limit 2</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access critical-role CriticalRole</td>
<td>aaa authentication port-access critical-role CriticalRole</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access preauth-role PreauthRole</td>
<td>aaa authentication port-access preauth-role PreauthRole</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access reject-role RejectRole</td>
<td>aaa authentication port-access critical-role CriticalRole</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access auth-role AuthRole</td>
<td>aaa authentication port-access auth-role AuthRole</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access dot1x authenticator</td>
<td>aaa authentication port-access dot1x authenticator</td>
<td></td>
</tr>
<tr>
<td>reauth enable</td>
<td>reauth enable</td>
<td></td>
</tr>
<tr>
<td>aaa authentication port-access mac-auth</td>
<td>aaa authentication port-access mac-auth</td>
<td></td>
</tr>
<tr>
<td>cached-reauth</td>
<td>cached-reauth</td>
<td></td>
</tr>
<tr>
<td>cached-reauth-period 86400</td>
<td>cached-reauth-period 86400</td>
<td></td>
</tr>
<tr>
<td>eapol-timeout 30</td>
<td>eapol-timeout 30</td>
<td></td>
</tr>
<tr>
<td>max-eapol-requests 1</td>
<td>max-eapol-requests 1</td>
<td></td>
</tr>
<tr>
<td>max-retries 1</td>
<td>max-retries 1</td>
<td></td>
</tr>
<tr>
<td>reauth enable</td>
<td>reauth enable</td>
<td></td>
</tr>
<tr>
<td>client track ip enable</td>
<td>client track ip enable</td>
<td></td>
</tr>
<tr>
<td>client track ip update-interval 60</td>
<td>client track ip update-interval 60</td>
<td></td>
</tr>
<tr>
<td>loop-protect</td>
<td>loop-protect</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>CX_6xxxx#</td>
<td>CX_6xxxx#</td>
<td></td>
</tr>
<tr>
<td>AOS-Switch</td>
<td>10.6 – Concurrent Onboarding</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Interface 2/15</td>
<td>CX_6xxx# show running-config interface 1/1/12</td>
<td></td>
</tr>
<tr>
<td>untagged vlan 1</td>
<td>interface 1/1/12</td>
<td></td>
</tr>
<tr>
<td>aaa port-access authenticator</td>
<td>no shutdown</td>
<td></td>
</tr>
<tr>
<td>aaa port-access authenticator reauth-period 3600</td>
<td>no routing</td>
<td></td>
</tr>
<tr>
<td>aaa port-access authenticator client-limit 2</td>
<td>spanning-tree bpdu-guard</td>
<td></td>
</tr>
<tr>
<td>aaa port-access authenticated cached-reauth-period 86400</td>
<td>spanning-tree root-guard</td>
<td></td>
</tr>
<tr>
<td>aaa port-access mac-based</td>
<td>spanning-tree tcn-guard</td>
<td></td>
</tr>
<tr>
<td>aaa port-access mac-based addr-limit 2</td>
<td>spanning-tree port-type admin-edge</td>
<td></td>
</tr>
<tr>
<td>aaa port-access mac-based quiet-period 30</td>
<td>port-access onboarding-method concurrent enable</td>
<td></td>
</tr>
<tr>
<td>aaa port-access mac-based reauth-period 3600</td>
<td>aaa authentication port-access allow-cdp-bpdu</td>
<td></td>
</tr>
<tr>
<td>aaa port-access mac-based cached-reauth-period 86400</td>
<td>aaa authentication port-access allow-lldp-bpdu</td>
<td></td>
</tr>
<tr>
<td>aaa port-access critical-auth user-role &quot;CriticalRole&quot;</td>
<td>aaa authentication port-access client-limit 2</td>
<td></td>
</tr>
<tr>
<td>aaa port-access open-auth user-role &quot;OpenauthRole&quot;</td>
<td>aaa authentication port-access critical-role CriticalRole</td>
<td></td>
</tr>
<tr>
<td>aaa port-access initial-role &quot;InitialRole&quot;</td>
<td>aaa authentication port-access preauth-role PreauthRole</td>
<td></td>
</tr>
<tr>
<td>spanning-tree admin-edge-port</td>
<td>aaa authentication port-access reject-role RejectRole</td>
<td></td>
</tr>
<tr>
<td>spanning-tree root-guard tcn-guard bpdu-protection</td>
<td>aaa authentication port-access auth-role AuthRole</td>
<td></td>
</tr>
<tr>
<td>loop-protect</td>
<td>aaa authentication port-access dot1x authenticator</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>cached-reauth</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cached-reauth-period 86400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>eapol-timeout 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>max-eapol-requests 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>max-retries 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reauth enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>aaa authentication port-access mac-auth</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cached-reauth</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cached-reauth-period 86400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>quiet-period 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reauth enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>client track ip enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>client track ip update-interval 60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>loop-protect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CX_6xxx#</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting
Feature/Solution Troubleshooting
Basic level

6300-1-VSF#
- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x
  authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

6300-1-VSF# show events
6300-1-VSF# terminal-monitor (only on ssh)
Feature/Solution Troubleshooting
Entry level

6300-1-VSF#
- show mac-address-table detail
- show 1ldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

- Debugs
6300-1-VSF#
dep bug radius all
dep bug port access all
dep bug destination buffer
6300-1-VSF#
show debug buffer

- Daigdump
6300-1-VSF# diagnostics
diag dump port-access basic
diag dump dot1x-authenticator basic
diag dump mac-auth basic
Feature/Solution Troubleshooting
Advance level

- **start-shell** - Are you ready 😊!

```
6300-1-VSF# start-shell
6300-1-VSF:$ pwd
/home/admin
6300-1-VSF:$ sudo bash
6300-1-VSF:/home/admin#
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd fastlog show
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd port-access/role/dump_data
6300-1-VSF:/home/admin# ovsdb-client dump Port_Access_Role -flist
```

```
6300:$ cd /var/log/
6300:/var/log$ ls -l
6300:/var/log$ journalctl -n 100 | grep lldpd
```
Demo
Auth-Priority

To authorize the client based on priority!
Overview and Use Cases
Overview Topics

– What is the Feature/Solution
– Why is the Feature/Solution important
– What use cases does the Feature/Solution Solve Well
– If Enhancement
  – How does this enhancement fit into the existing feature.
  – What changes in behavior will be seen from previous releases
– What versions of partner software is this feature dependent on.
  – E.g. Dynamic segmentation and Downloadable User Roles are depending on Mobility Controller SW and Clearpass
Auth-precedence Current Challenge

Client

00:50:56:8e:86:27

RADIUS server

Supplicant

Download

802.1X/EAP Authentication

EAP over LAN (EAPOL)

RADIUS server

Mac-Auth

RADIUS (encapsulates packets)
Clients [like wireless access-points (APs), or phones or laptops] without-pre-loaded-suppliant-software, can first download the required supplicant Software and then attempt 802.1x Authentication.

Set MAC Authentication as the primary authentication method followed by 802.1x for the Authentication order.

Set the Authentication priority with primary as 802.1x and secondary as MAC Authentication to enforce the access based on 802.1x.

- Auth-precedence: mac-auth dot1x
- Auth-priority: dot1x mac-auth

Thus the client will initially get authenticated by MAC Authentication, and then install the required supplicant-software to achieve subsequent 802.1x Authentication.

Authentication is started based on the precedence order and even after successful authentication by an auth-method, authentication continues till enabled highest priority method gives the response.
Authentication will be triggered based on precedence.

**Concurrent** - If concurrent-onboarding is enabled, precedence is ignored.

**Legacy** - If auth precedence and auth priority are configured as same, it behaves same as legacy auth-precedence behavior.

**Default** - By default the order of auth-priority will be equal to the order of auth-precedence.

**Enabling** - Auth-priority is considered as enabled when the order of auth-precedence and auth-priority are different.

**Completion of authentication** - Authentication process is not completed until highest priority enabled auth method gives the response.

**Configuration update** - If order of auth-precedence/auth-priority configured or updated or even if auth methods are enabled/disabled, the existing clients will be deleted.

**Highest priority method fails** - If highest priority method fails, then the client is given access by successful secondary priority method.

**Critical/Reject** - If authentication by all the auth-method fails then reject/critical role of highest priority method is assigned.
Auth-precedence + Auth-priority

- First download the supplicant software or certificate/firmware/OS patches using mac-authentication because of auth-precedence

Mac-Auth

Client 00:50:56:8e:86:27

Supplicant Download

802.1X/EAP Authentication

Client

EAP over LAN (EAPOL)

RADIUS server

aaa authentication port-access dot1x authenticator enable
aaa authentication port-access mac-auth enable
(config-if)#
  aaa authentication port-access auth-precedence mac-auth dot1x
    aaa authentication port-access auth-priority dot1x mac-auth
    aaa authentication port-access dot1x authenticator enable
    aaa authentication port-access mac-auth enable

RADIUS server

RADIUS

(encapsulates packets)
Concurrent onboarding + Auth-priority

- First download the supplicant software or firmware/OS patches before attempting 802.1x Authentication

```
(config-if) #
!aaa authentication port-access auth-precedence mac-auth dot1x
    port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-access mac-auth
        enable
```
Best Practices
<table>
<thead>
<tr>
<th>CX 10.5</th>
<th>10.6 – Auth precedence + priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>CX_6xxx# show running-config interface 1/1/12</td>
<td>CX_6xxx# show running-config interface 1/1/12</td>
</tr>
<tr>
<td>interface 1/1/12</td>
<td>interface 1/1/12</td>
</tr>
<tr>
<td>no shutdown</td>
<td>no shutdown</td>
</tr>
<tr>
<td>no routing</td>
<td>no routing</td>
</tr>
<tr>
<td>vlan access 1</td>
<td>vlan access 1</td>
</tr>
<tr>
<td>spanning-tree bpdu-guard</td>
<td>spanning-tree bpdu-guard</td>
</tr>
<tr>
<td>spanning-tree root-guard</td>
<td>spanning-tree root-guard</td>
</tr>
<tr>
<td>spanning-tree tcn-guard</td>
<td>spanning-tree tcn-guard</td>
</tr>
<tr>
<td>spanning-tree port-type admin-edge</td>
<td>spanning-tree port-type admin-edge</td>
</tr>
<tr>
<td>aaa authentication port-access allow-cdp-bpdu</td>
<td>aaa authentication port-access allow-cdp-bpdu</td>
</tr>
<tr>
<td>aaa authentication port-access allow-lldp-bpdu</td>
<td>aaa authentication port-access allow-lldp-bpdu</td>
</tr>
<tr>
<td>aaa authentication port-access client-limit 2</td>
<td>aaa authentication port-access client-limit 2</td>
</tr>
<tr>
<td>aaa authentication port-access critical-role CriticalRole</td>
<td>aaa authentication port-access critical-role CriticalRole</td>
</tr>
<tr>
<td>aaa authentication port-access preauth-role PreauthRole</td>
<td>aaa authentication port-access preauth-role PreauthRole</td>
</tr>
<tr>
<td>aaa authentication port-access reject-role RejectRole</td>
<td>aaa authentication port-access reject-role RejectRole</td>
</tr>
<tr>
<td>aaa authentication port-access auth-role AuthRole</td>
<td>aaa authentication port-access auth-role AuthRole</td>
</tr>
<tr>
<td>aaa authentication port-access dot1x authenticator</td>
<td>aaa authentication port-access dot1x authenticator</td>
</tr>
<tr>
<td>cached-reauth</td>
<td>cached-reauth</td>
</tr>
<tr>
<td>cached-reauth-period 86400</td>
<td>cached-reauth-period 86400</td>
</tr>
<tr>
<td>eapol-timeout 30</td>
<td>eapol-timeout 30</td>
</tr>
<tr>
<td>max-eapol-requests 1</td>
<td>max-eapol-requests 1</td>
</tr>
<tr>
<td>max-retries 1</td>
<td>max-retries 1</td>
</tr>
<tr>
<td>reauth</td>
<td>reauth</td>
</tr>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>aaa authentication port-access mac-auth</td>
<td>aaa authentication port-access mac-auth</td>
</tr>
<tr>
<td>cached-reauth</td>
<td>cached-reauth</td>
</tr>
<tr>
<td>cached-reauth-period 86400</td>
<td>cached-reauth-period 86400</td>
</tr>
<tr>
<td>quiet-period 30</td>
<td>quiet-period 30</td>
</tr>
<tr>
<td>reauth</td>
<td>reauth</td>
</tr>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>client track ip enable</td>
<td>client track ip enable</td>
</tr>
<tr>
<td>client track ip update-interval 60</td>
<td>client track ip update-interval 60</td>
</tr>
<tr>
<td>loop-protect</td>
<td>loop-protect</td>
</tr>
<tr>
<td>exit</td>
<td>exit</td>
</tr>
</tbody>
</table>

---

```bash
exit
```
<table>
<thead>
<tr>
<th>AOS-Switch</th>
<th>10.6 – Auth priority + Precedence</th>
</tr>
</thead>
</table>
| interface 2/15  
untagged vlan 1  
aaa port-access authenticator  
aaa port-access authenticator reauth-period 3600  
aaa port-access authenticator client-limit 2  
aaa port-access authenticator cached-reauth-period 86400  
aaa port-access mac-based  
aaa port-access mac-based addr-limit 2  
aaa port-access mac-based quiet-period 30  
aaa port-access mac-based reauth-period 3600  
aaa port-access mac-based cached-reauth-period 86400  
aaa port-access critical-auth user-role "CriticalRole"  
aaa port-access open-auth user-role "OpenauthRole"  
aaa port-access initial-role "InitialRole"  
aaa port-access auth-order mac-based authenticator  
aaa port-access auth-priority authenticator mac-based  
spanning-tree admin-edge-port  
spanning-tree root-guard tcn-guard bpdud-protection  
loop-protect  
exit | CX_6xxx# show running-config interface 1/1/12  
interface 1/1/12  
no shutdown  
no routing  
no spanning-tree bpdu-guard  
spanning-tree root-guard  
spanning-tree tcn-guard  
spanning-tree port-type admin-edge  
aaa authentication port-access allow-cdp-bpdu  
aaa authentication port-access allow-ldp-bpdu  
aaa authentication port-access client-limit 2  
aaa authentication port-access critical-role CriticalRole  
aaa authentication port-access critical-role "OpenauthRole"  
aaa authentication port-access preauth-role PreauthRole  
aaa authentication port-access reject-role RejectRole  
aaa authentication port-access auth-role AuthRole  
aaa authentication port-access auth-precedence mac-auth dot1x  
aaa authentication port-access auth-priority dot1x mac-auth  
aaa authentication port-access dot1x authenticator  
reauth enable  
reauth cached-reauth-period 86400  
eapol-timeout 30  
max-eapol-requests 1  
max-retries 1  
reauth enable  
aaa authentication port-access mac-auth  
reauth enable  
reauth cached-reauth-period 86400  
quiet-period 30  
reauth enable  
client track ip enable  
client track ip update-interval 60  
loop-protect  
exit |
Troubleshooting
Feature/Solution Troubleshooting
Basic level

6300-1-VSF#
- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x
  authenticator interface all client-status
- show aaa authentication port-access mac-
  auth interface all client-status
- show aaa authentication port-access
  interface all client-status

6300-1-VSF# show events
6300-1-VSF# terminal-monitor (only on ssh)
Feature/Solution Troubleshooting
Entry level

6300-1-VSF#
- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

- Debugs

6300-1-VSF#
debug radius all
debug port access all
debug destination buffer

6300-1-VSF#
show debug buffer

- Daigdump

6300-1-VSF# diagnostics
diag-dump port-access basic
diag-dump dot1x-authenticator basic
diag-dump mac-auth basic
Feature/Solution Troubleshooting
Advance level

- start-shell - Are you ready 😎!

6300-1-VSF# start-shell
6300-1-VSF:~$ pwd
/home/admin
6300-1-VSF:~$ sudo bash
6300-1-VSF:/home/admin#
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd fastlog show
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd port-access/role/dump_data
6300-1-VSF:/home/admin# ovsdb-client dump Port_Access_Role -flist

6300:~$ cd /var/log/
6300:/var/log$ ls -l
6300:/var/log$ journalctl -n 100 | grep lldpd
Cache-Reauth

Client authentication continue because Cached Re-Authentication (due to AAA server being unreachable)!
Overview and Use case
Overview Port-access Role

– Port-access Role is a feature that allows administrators to **assign network access to clients**.
– The network admin can create configuration profiles(roles), associate them to clients – LUR or DUR.

```
6xxx(config)# port-access role
ROLE-NAME The name of the role

6300-1- VSF# show running-config port-access
port-access role Critical
port-access role Reject
port-access role allpara
    mtu 1800
port-access role authrole
port-access role dot1x_access
    reauth-period 100
    vlan access 110
port-access role patch_download
    description test_lur
    mtu 1700
    vlan access 210
```
Cache-Reauth
Cached-Re-Authenticated

– Client authentication completed via Cached Re-Authentication due to AAA server being unreachable.

```conf
6xxx(config)# port-access role <role-name>
6xxx(config-pa-role)# cached-reauth-period 200
6xxx(config-pa-role)# no cached-reauth-period
 cached-reauth-period [period <30-4294967295>

port-access role patch_download
description test_lur
mtu 1700
reauth-period 5
cached-reauth-period 150
vlan access 210
```
## Port-access Role Parameters!

<table>
<thead>
<tr>
<th>Sl.No</th>
<th>Parameters</th>
<th>Roles</th>
<th>Device-Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MTU</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>auth-mode</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>reauth-period</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><strong>cached-reauth-period</strong></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>session-timeout</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>trust-mode</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>7</td>
<td>stp-admin-edge-port</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>associate policy</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>9</td>
<td>associate captive-portal-profile</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>poe-priority</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>11</td>
<td>client-inactivity timeout</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>
## Port-access Role Parameters!

<table>
<thead>
<tr>
<th>Sl.No</th>
<th>Parameters</th>
<th>Roles</th>
<th>Device-Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>vlan access</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>13</td>
<td>vlan access name</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>vlan trunk allowed</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>15</td>
<td>vlan trunk allowed name</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>vlan trunk native</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>17</td>
<td>vlan trunk native name</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>18</td>
<td>gateway-zone zone</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>gateway-zone gateway-role</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting
Feature/Solution Troubleshooting
Basic level

6300-1-VSF#
- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

6300-1-VSF# show events
6300-1-VSF# terminal-monitor (only on ssh)
Feature/Solution Troubleshooting
Entry level

6300-1-VSF#
- show mac-address-table detail
- show lldp neighbor-info
- show cdp neighbor-info
- show radius-server detail
- show port-access clients detail
- show aaa authentication port-access dot1x authenticator interface all client-status
- show aaa authentication port-access mac-auth interface all client-status
- show aaa authentication port-access interface all client-status

- Debugs

6300-1-VSF#
debug radius all
debug port access all
debug destination buffer

6300-1-VSF#
show debug buffer

- Daigdump

6300-1-VSF# diagnostics
diag-dump port-access basic
diag-dump dot1x-authenticator basic
diag-dump mac-auth basic
Feature/Solution Troubleshooting
Advance level

- **start-shell** - Are you ready 😊!

6300-1-VSF# start-shell
6300-1-VSF:$ pwd
/home/admin
6300-1-VSF:$ sudo bash
6300-1-VSF:/home/admin#
6300-1-VSF:/home/admin# ovs-appctl -t port-accessd fastlog show

6300:$ cd /var/log/
6300:/var/log$ ls -l
6300:/var/log$ journalctl -n 100 | grep lldpd
Thank You