

CX Port-Access Security Update

Presenters
Yash – Technical Marketing Engineer

aruba
a Hewlett Packard
Enterprise company



CX 10.6 Port-Access Security Enhancement

– **Auth-priority:**

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

– **Cache-reauth**

- Port-access role based Per user cache-reauth

The background is a dark blue gradient. In the top-left corner, there is a large, solid red circle. A large, irregular shape in the center-right of the image is filled with a pattern of small, light red dots.

Introduction Auth-Priority

AOS-CX 10.6 Auth-priority

- Clients like wireless access-points (APs), or phones or laptops comes without pre-loaded-suppllicant or software or certificate.
- Those client will initially get authenticated by MAC Authentication, and then install the required suppllicant-software to achieve subsequent dot1x Authentication.
- First clients can download the required suppllicant Software with mac-based authentication and then attempt dot1x Authentication.
- To achieve, set MAC Authentication as the auth-precedence method followed by dot1x for the Authentication precedence.
- Set the Authentication priority with primary as dot1x and secondary as MAC Authentication to enforce the access based on dot1x once after the suppllicant/software/certificate is downloaded as below:
 - Auth-precedence: mac-auth dot1x
 - Auth-priority: dot1x mac-auth
- Authentication get started based on the auth-precedence order and even after successful authentication by an auth-method, authentication continues till enabled highest auth-priority method gives the response.
- Reauthentication will be triggered for all high priority methods and not just the final successful authentication method

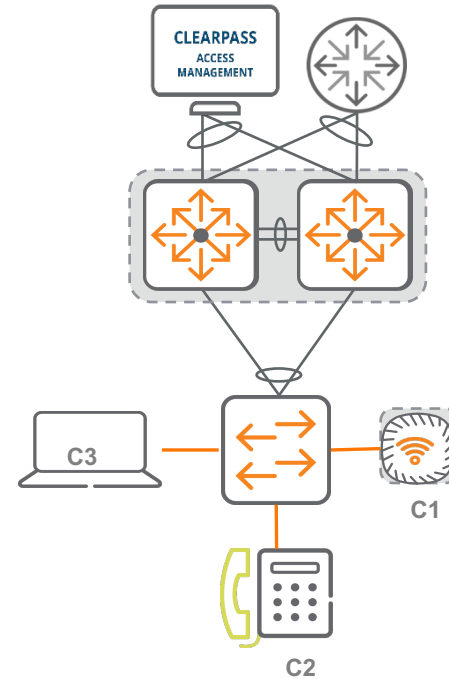
AOS-CX 10.6 Auth-priority

CX 10.5

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

Manually IT/network admin must change the precedence

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



CX 10.6

```
(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
```

Recommendation

CX 10.5	10.6 – Auth precedence + priority
<pre>CX_6xxx# show running-config interface 1/1/12 interface 1/1/12 no shutdown no routing vlan access 1 spanning-tree bpdu-guard spanning-tree root-guard spanning-tree tcu-guard spanning-tree port-type admin-edge aaa authentication port-access allow-cdp-bpdu aaa authentication port-access allow-lldp-bpdu aaa authentication port-access client-limit 2 aaa authentication port-access critical-role CriticalRole 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 dot1x authenticator cached-reauth cached-reauth-period 86400 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 reauth enable client track ip enable client track ip update-interval 60 loop-protect exit</pre>	<pre>CX_6xxx# show running-config interface 1/1/12 interface 1/1/12 no shutdown no routing vlan access 1 spanning-tree bpdu-guard spanning-tree root-guard spanning-tree tcu-guard spanning-tree port-type admin-edge aaa authentication port-access allow-cdp-bpdu aaa authentication port-access allow-lldp-bpdu aaa authentication port-access client-limit 2 aaa authentication port-access critical-role CriticalRole 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 cached-reauth cached-reauth-period 86400 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 reauth enable client track ip enable client track ip update-interval 60 loop-protect exit</pre>

Recommendation

AOS-Switch	10.6 – Auth priority + Precedence
<pre>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 bpdu-protection loop-protect exit</pre>	<pre>CX_6xxx# show running-config interface 1/1/12 interface 1/1/12 no shutdown no routing vlan access 1 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-lldp-bpdu aaa authentication port-access client-limit 2 aaa authentication port-access critical-role CriticalRole 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 cached-reauth cached-reauth-period 86400 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 reauth enable client track ip enable client track ip update-interval 60 loop-protect exit</pre>

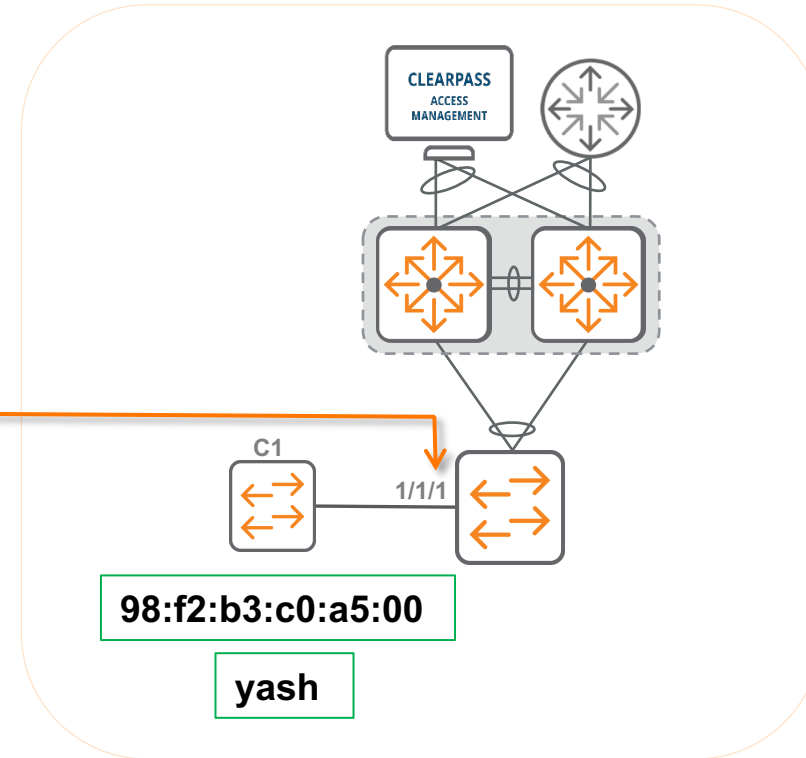
The background features a solid dark blue field. In the top-left corner, a large red circle is partially visible. A large, irregular shape in the center-right is filled with a pattern of small, light blue dots, creating a halftone effect. The word "Demo" is written in white, bold, sans-serif font, positioned over the red circle.

Demo

Demo: port-access auth-priority

Download supplicant and then attempt dot1x

```
aaa authentication port-access auth-precedence mac-auth dot1x
aaa authentication port-access auth-priority dot1x mac-auth
aaa authentication port-access allow-cdp-bpdu
aaa authentication port-access allow-lldp-bpdu
aaa authentication port-access dot1x authenticator
    enable
aaa authentication port-access mac-auth
    enable
```



The background is a dark blue gradient. In the top-left corner, there is a large, solid red circle. A large, irregular shape in the center-right of the image is filled with a pattern of small, light red dots.

Introduction Cache-Reauth

Cache-Reauth

Cached-Re-Authenticated

- 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.
- Admin now can configure cache-reauth inside a port-access role.
- Client authentication completed via Cached Re-Authentication due to AAA server being unreachable.

```
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>
```

```
Example:
port-access role CS_student
description test_lur
mtu 1700
reauth-period 5
cached-reauth-period 150
vlan access 210
```

Port Access Clients
Status codes: d device-mode

Port	MAC-Address	Onboarding Method	Status	VLAN	Role
1/1/5	08:00:0f:22:c6:e4	mac-auth	Success	210	CS_student

Cache-Reauth

```
6300-1-VSF# show radius-server detail
***** Global RADIUS Configuration *****
Shared-Secret: None
Timeout: 1
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 3
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name           : 15.136.40.53
Auth-Port             : 1812
Accounting-Port       : 1813
VRF                   : mgmt
TLS Enabled           : No
Shared-Secret         : AQBapdAz4irjSK61Zg/CFArsNYWKbn1LObqDD/v9SH1eMQ6ABQAAADY26liu
Timeout               : 1
Retries               : 1
Auth-Type             : pap
Server-Group          : radius
Default-Priority      : 1
ClearPass-Username    : appadmin
ClearPass-Password    :
AQBapSx6d58BCqtVJfVhkp1tk1IbWJeMtIzwCIMH7UKB8oeDQAAAB2+E5ytA3XjZwhkVY4=
Tracking              : enabled
Tracking-Mode         : any
Reachability-Status   : unreachable, Since Wed Oct 21 15:28:35 UTC 2020
Tracking-Last-Attempted : Wed Oct 21 15:28:31 UTC 2020
Next-Tracking-Request : 46 seconds
6300-1-VSF#
```

Port Access Client Status Details

Client 08:00:0f:22:c6:e4

=====

Session Details

Port : 1/1/5
Session Time : 241s
IPv4 Address :
IPv6 Address :

Authentication Details

Status : Authenticated
Auth Precedence : dot1x - Authenticating, **mac-auth - Cached-Re-Authenticated**

Authorization Details

Role : CS_student
Status : Applied

The background features a solid dark blue field. In the top-left corner, a large red circle is partially visible. A large, irregular shape in the center-right is filled with a pattern of small, light blue dots, creating a halftone effect. The word "Demo" is written in white, bold, sans-serif font, positioned over the red circle.

Demo

Additional Resources

Feature/Solution References

- AOS-CX 10.06 Security Guide

- <https://www.arubanetworks.com/techdocs/AOS-CX/10.06/HTML/5200-7723/index.html>
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00108360en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00108317en_us&docLocale=en_US

Thank you