CX Port-Access Concurrent Onboarding

aruba
a Hewlett Packard Enterprise company

Presenters
Yash – Aruba Technical Marketing Engineer

Agenda

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

Overview

Port-access Concurrent Onboarding

Concurrent Onboarding = Faster Clients onboarding

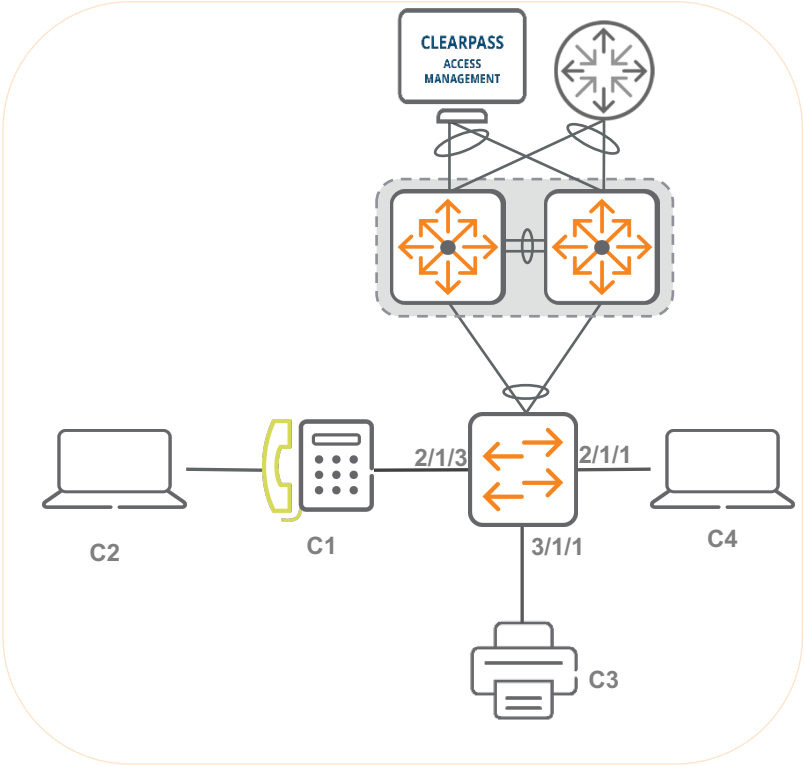
Clients	Without Concurrent Onboarding Enabled or 10.5	10.6 Concurrent Onboarding Enabled
dot1x client 	Same time onboarding	Same time onboarding
Mac-auth client 	As per default auth-precedence, dot1x authentication will be attempted first and then Mac-authentication will be trigger, means mac-auth clients need to wait!	Onboarding will be faster because all auth methods will be trigger concurrently.
PC behind Phone 	As started above, for every client first dot1x authentication will be trigger followed by mac-authentication.	Both auth methods, dot1x and mac-auth access-request will be triggered at same time/concurrently. Hence onboarding clients becomes faster

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

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

Use cases

Concurrent onboarding from 10.6



1- Faster onboarding Mac authentication Clients

- 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 with in 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!**

Details and Caveats

Concurrent Onboarding

Details

- Default priority for concurrent onboarding is 802.1x followed by mac-auth and device-profile.
- When the authentication method with the highest priority fails, the profile of the next successful authentication method is applied.
- Once after the authentication, authorization profile for the client is applied based on the auth-priority order configured on the port.
- When enabling concurrent onboarding on the port, existing clients will be de-authenticated and freshly onboarded concurrently.
- When concurrent onboarding is enabled, then auth-precedence will be ignored.
- If all methods fail, the reject or critical role is applied based on the 802.1X authentication failure reason and continues to reauthenticate with the 802.1X method.
- If concurrent onboarding is configured, the client will stay in pre-auth role till it gets succeeded by one authentication method or gets failed by all the authentication methods.
- Reauthentication will be triggered for all high priority methods and not just the final successful authentication method.

Concurrent Onboarding

Faster Clients onboarding process

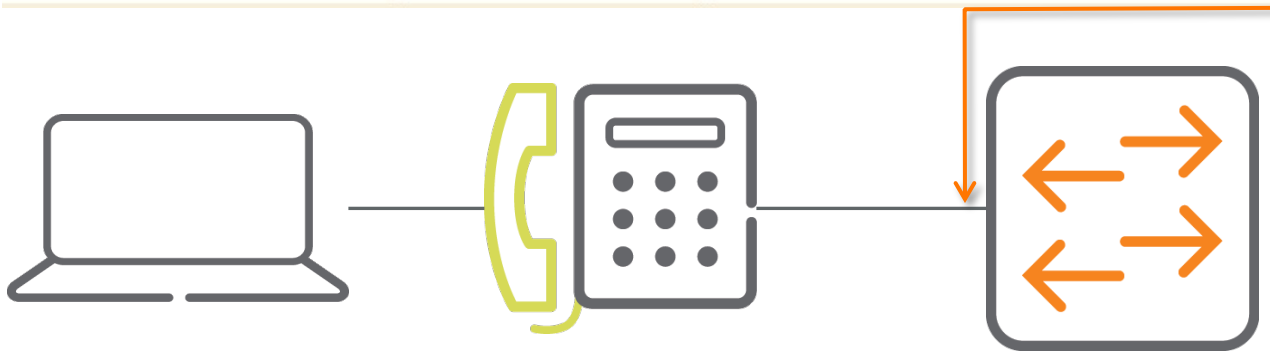
– Some RADIUS server may block the client when it receives two requests, mac-auth and 802.1X, from the same client at the same time.

– This is because the RADIUS server allows only one authentication request. In such cases, concurrent onboarding is not feasible. To prevent such scenarios, configure auth-precedence with auth-priority.

Concurrent Onboarding

concurrent onboarding enables all authentication methods to start concurrently for **faster onboarding the clients!**

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60 Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177 Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146 Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60 Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236 Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211 Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Success



240	85.354920	192.168.2.200	192.168.2.21	RADIUS	211 Access-Request id=35
241	85.408514	192.168.2.21	192.168.2.200	RADIUS	195 Access-Accept id=35

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

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

dot1x EAP Identity Request from Switch to Client

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> Frame 621: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: ArubaaHe_b8:e3:ff (64:e8:81:b8:e3:ff), Dst: HewlettP_c0:a5:00 (98:f2:b3:c0:a5:00)
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 5
v Extensible Authentication Protocol
    Code: Request (1)
    Id: 217
    Length: 5
    Type: Identity (1)
```

Dot1x EAP Identity Response from Client to Switch

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> Frame 622: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: HewlettP_c0:a5:00 (98:f2:b3:c0:a5:00), Dst: Nearest-non-TPMR-bridge (01:80:c2:00:00:03)
v 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 9
v Extensible Authentication Protocol
    Code: Response (2)
    Id: 217
    Length: 9
    Type: Identity (1)
    Identity: yash
```

Radius Access-Request from Switch to Radius-Server

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
Packet identifier: 0xbb (187)
Length: 135
Authenticator: d837900c07bf49d066999e9df4e76ad4
[The response to this request is in frame 624]
Attribute Value Pairs
  AVP: t=User-Name(1) l=6 val=yash
  AVP: t=Calling-Station-Id(31) l=19 val=98-F2-B3-C0-A5-00
  AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
  AVP: t=NAS-Port-Id(87) l=7 val=1/1/1
  AVP: t=NAS-Port(5) l=6 val=1
  AVP: t=Service-Type(6) l=6 val=Framed(2)
  AVP: t=EAP-Message(79) l=11 Last Segment[1]
    Type: 79
    Length: 11
    EAP fragment: 02d900090179617368
    Extensible Authentication Protocol
      Code: Response (2)
      Id: 217
      Length: 9
      Type: Identity (1)
      Identity: yash
  AVP: t=Message-Authenticator(80) l=18 val=a34928342f97bbfcd5d53d192cce32a3
  AVP: t=Called-Station-Id(30) l=19 val=64-E8-81-B8-E3-C0
  AVP: t=NAS-Identifier(32) l=11 val=Yash-6300
  AVP: t=NAS-IP-Address(4) l=6 val=192.168.2.200
```

Radius Access-Challenge from Radius-Server to Switch

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60 Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177 Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146 Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60 Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236 Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211 Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60 Success

```
RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0xbb (187)
    Length: 104
    Authenticator: ca7d45bad65c4b479d04af67d15ed43b
    [This is a response to a request in frame 623]
    [Time from request: 0.027505000 seconds]
    Attribute Value Pairs
        AVP: t=EAP-Message(79) l=24 Last Segment[1]
            Type: 79
            Length: 24
            EAP fragment: 01da00160410af1f5002c748b5ce1f6664cfae31dd37
            Extensible Authentication Protocol
                Code: Request (1)
                Id: 218
                Length: 22
                Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
                    [Expert Info (Warning/Security): Vulnerable to MITM attacks. If possible, change EAP type.]
                        [Vulnerable to MITM attacks. If possible, change EAP type.]
                        [Severity level: Warning]
                        [Group: Security]
                EAP-MD5 Value-Size: 16
                EAP-MD5 Value: af1f5002c748b5ce1f6664cfae31dd37
        AVP: t=Message-Authenticator(80) l=18 val=cd66153f89b76d959bc62745aa692895
        AVP: t=State(24) l=42 val=414367415267446b41496c48585155414b377232524b5252567479626262 7a634b45444b…
```

dot1x EAP-Challenge Request sent from Switch to Client

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> Frame 625: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: ArubaaHe_b8:e3:ff (64:e8:81:b8:e3:ff), Dst: HewlettP_c0:a5:00 (98:f2:b3:c0:a5:00)
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 22
v Extensible Authentication Protocol
    Code: Request (1)
    Id: 218
    Length: 22
  v Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
    v [Expert Info (Warning/Security): Vulnerable to MITM attacks. If possible, change EAP type.]
          [Vulnerable to MITM attacks. If possible, change EAP type.]
          [Severity level: Warning]
          [Group: Security]
    EAP-MD5 Value-Size: 16
    EAP-MD5 Value: af1f5002c748b5ce1f6664cfae31dd37
```

dot1x EAP Challenge Response from Client to Switch

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> Frame 626: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: HewlettP_c0:a5:00 (98:f2:b3:c0:a5:00), Dst: Nearest-non-TPMR-bridge (01:80:c2:00:00:03)
v 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: EAP Packet (0)
    Length: 26
v Extensible Authentication Protocol
    Code: Response (2)
    Id: 218
    Length: 26
  v Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
    v [Expert Info (Warning/Security): Vulnerable to MITM attacks. If possible, change EAP type.]
          [Vulnerable to MITM attacks. If possible, change EAP type.]
          [Severity level: Warning]
          [Group: Security]
    EAP-MD5 Value-Size: 16
    EAP-MD5 Value: 3de99e2c804a36bb19464f0502d494ef
    EAP-MD5 Extra Data: 79617368
```

dot1x Access-Request from Switch to Radius-Server

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
> AVP: t=NAS-Port-Id(87) l=7 val=1/1/1
> AVP: t=NAS-Port(5) l=6 val=1
> AVP: t=Service-Type(6) l=6 val=Framed(2)
v AVP: t=EAP-Message(79) l=28 Last Segment[1]
    Type: 79
    Length: 28
    EAP fragment: 02da001a04103de99e2c804a36bb19464f0502d494ef79617368
  v Extensible Authentication Protocol
      Code: Response (2)
      Id: 218
      Length: 26
    v Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
      v [Expert Info (Warning/Security): Vulnerable to MITM attacks. If possible, change EAP type.]
            [Vulnerable to MITM attacks. If possible, change EAP type.]
            [Severity level: Warning]
            [Group: Security]
      EAP-MD5 Value-Size: 16
      EAP-MD5 Value: 3de99e2c804a36bb19464f0502d494ef
      EAP-MD5 Extra Data: 79617368
> AVP: t=State(24) l=42 val=414367415267446b41496c48585155414b377232524b52525674796262627a634b45444b…
> AVP: t=Message-Authenticator(80) l=18 val=beb963885863f8bfb170adfdbae19457
> AVP: t=Called-Station-Id(30) l=19 val=64-E8-81-B8-E3-C0
> AVP: t=NAS-Identifier(32) l=11 val=Yash-6300
> AVP: t=NAS-IP-Address(4) l=6 val=192.168.2.200
```

dot1x Access-Accept from Radius to Switch

```
621 47.292431   ArubaaHe_b8:e3:ff   HewlettP_c0:a5:00   EAP      60 Request, Identity
622 47.292494   HewlettP_c0:a5:00   Nearest-non-TPMR-br… EAP      60 Response, Identity
623 47.295635   192.168.2.200       192.168.2.21        RADIUS  177 Access-Request id=187
624 47.323140   192.168.2.21        192.168.2.200       RADIUS  146 Access-Challenge id=187
625 47.325454   ArubaaHe_b8:e3:ff   HewlettP_c0:a5:00   EAP      60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626 47.325454   HewlettP_c0:a5:00   Nearest-non-TPMR-br… EAP      60 Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627 47.326506   192.168.2.200       192.168.2.21        RADIUS  236 Access-Request id=188
628 47.365227   192.168.2.21        192.168.2.200       RADIUS  211 Access-Accept id=188
629 47.374838   ArubaaHe_b8:e3:ff   HewlettP_c0:a5:00   EAP      60 Success
```

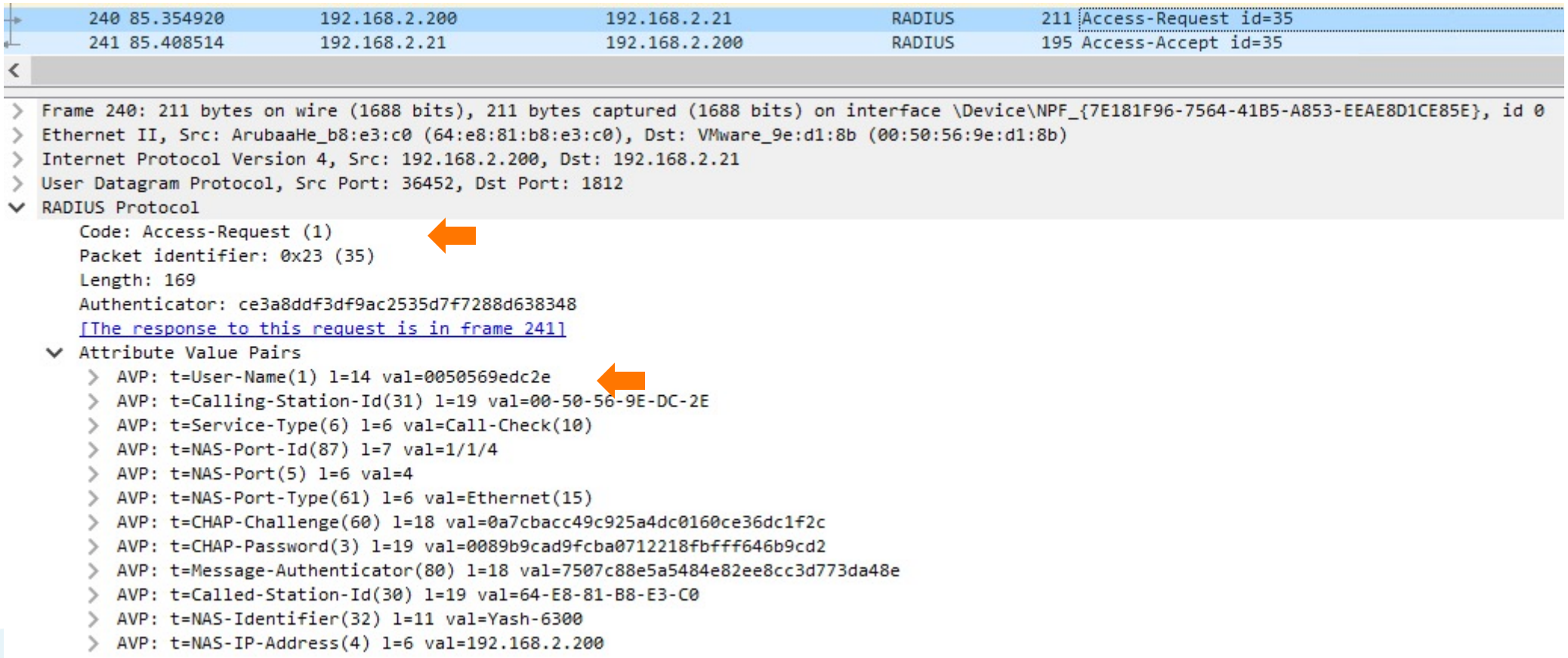
```
Internet Protocol Version 4, Src: 192.168.2.21, Dst: 192.168.2.200
User Datagram Protocol, Src Port: 1812, Dst Port: 38089
RADIUS Protocol
   Code: Access-Accept (2)
   Packet identifier: 0xbc (188)
   Length: 169
   Authenticator: 73231fc20659ad2d5b6b84de138af4e7
   [This is a response to a request in frame 627]
   [Time from request: 0.038721000 seconds]
 ▾ Attribute Value Pairs
   ▸ AVP: t=Vendor-Specific(26) l=17 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
   ▸ AVP: t=Vendor-Specific(26) l=26 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
   ▸ AVP: t=Vendor-Specific(26) l=12 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
   ▸ AVP: t=Egress-VLANID(56) l=6 val=Tagged, Vlan ID: 23
   ▾ AVP: t=EAP-Message(79) l=6 Last Segment[1]
        Type: 79
        Length: 6
        EAP fragment: 03da0004
      ▾ Extensible Authentication Protocol
           Code: Success (3)
           Id: 218
           Length: 4
   ▸ AVP: t=Message-Authenticator(80) l=18 val=410e1ad803fa9455fcd9d48789a606d4
   ▸ AVP: t=User-Name(1) l=6 val=yash
   ▸ AVP: t=Class(25) l=58 val=f18bbe3fbca54374b91fcb8575e22502bb0b0000000000005230303035323436632d3031…
```

dot1x EAP Success from Switch to Client

621	47.292431	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, Identity
622	47.292494	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, Identity
623	47.295635	192.168.2.200	192.168.2.21	RADIUS	177	Access-Request id=187
624	47.323140	192.168.2.21	192.168.2.200	RADIUS	146	Access-Challenge id=187
625	47.325454	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
626	47.325454	HewlettP_c0:a5:00	Nearest-non-TPMR-br…	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
627	47.326506	192.168.2.200	192.168.2.21	RADIUS	236	Access-Request id=188
628	47.365227	192.168.2.21	192.168.2.200	RADIUS	211	Access-Accept id=188
629	47.374838	ArubaaHe_b8:e3:ff	HewlettP_c0:a5:00	EAP	60	Success

```
> Frame 629: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: ArubaaHe_b8:e3:ff (64:e8:81:b8:e3:ff), Dst: HewlettP_c0:a5:00 (98:f2:b3:c0:a5:00)
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 4
v Extensible Authentication Protocol
    Code: Success (3)
    Id: 218
    Length: 4
```

Mac-auth Radius Access-Request



Mac-auth Radius Access-Accept

```
    240 85.354920    192.168.2.200    192.168.2.21     RADIUS    211 Access-Request id=35
    241 85.408514    192.168.2.21     192.168.2.200    RADIUS    195 Access-Accept id=35
```

```
> Frame 241: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface \Device\NPF_{7E181F96-7564-41B5-A853-EEAE8D1CE85E}, id 0
> Ethernet II, Src: VMware_9e:d1:8b (00:50:56:9e:d1:8b), Dst: ArubaaHe_b8:e3:c0 (64:e8:81:b8:e3:c0)
> Internet Protocol Version 4, Src: 192.168.2.21, Dst: 192.168.2.200
> User Datagram Protocol, Src Port: 1812, Dst Port: 36452
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x23 (35)
    Length: 153
    Authenticator: e79d2cadccb448486c6159b4c9428e4e
    [This is a response to a request in frame 240]
    [Time from request: 0.053594000 seconds]
  v Attribute Value Pairs
    v AVP: t=User-Name(1) l=14 val=0050569edc2e
        Type: 1
        Length: 14
        User-Name: 0050569edc2e
    > AVP: t=Vendor-Specific(26) l=17 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
    > AVP: t=Vendor-Specific(26) l=26 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
    > AVP: t=Vendor-Specific(26) l=12 vnd=Aruba, a Hewlett Packard Enterprise company(14823)
    > AVP: t=Egress-VLANID(56) l=6 val=Tagged, Vlan ID: 23
    > AVP: t=Class(25) l=58 val=f18bbe3fbca54374b91fcb8575e22502cb0b0000000000052303030373839363432d3031…
```

Configuration and Supported Platforms

Concurrent onboarding Configuration and supported CX platforms

– **Enabling or Disabling concurrent onboarding on a port:**

```
switch(config)# interface 1/1/1 switch(config-if)# port-access onboarding-method concurrent enable / disable
```

– **Auth-precedence will be ignored as below:**

```
interface 1/1/1
no shutdown
no routing
vlan access 999
!aaa authentication port-access auth-precedence mac-auth dot1x
port-access onboarding-method concurrent enable
```

Platform	6200	6300	6400	8320	8325	8360	8400	Simulator
Concurrent onboarding	**Yes**	**Yes**	**Yes**	NA	NA	NA	NA	**Yes**

Best Practices/Configuration

Recommendation

CX 10.5	10.6 – Concurrent Onboarding
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 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 CX_6xxx#	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 **port-access onboarding-method concurrent enable** 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 CX_6xxx#

AOS-Switch vs AOS-CX

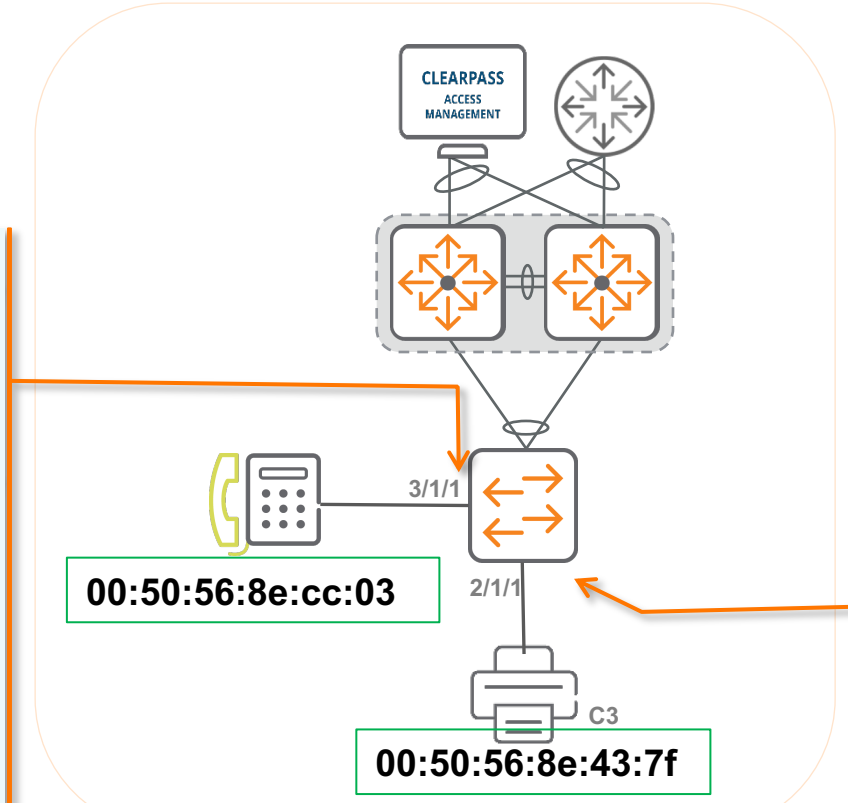
AOS-Switch	10.6 – Concurrent Onboarding
interface 2/15 untagged vlan 1 aaa port-access authenticator aaa port-access authenticator reauth-period 3600 aaa port-access authenticator client-limit 2 aaa port-access authenticator cached-reauth-period 86400 aaa port-access mac-based aaa port-access mac-based 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" spanning-tree admin-edge-port spanning-tree root-guard tcn-guard bpdu-protection loop-protect exit	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 **port-access onboarding-method concurrent enable** 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 CX_6xxx#

Demo

Demo1: Concurrent onboarding

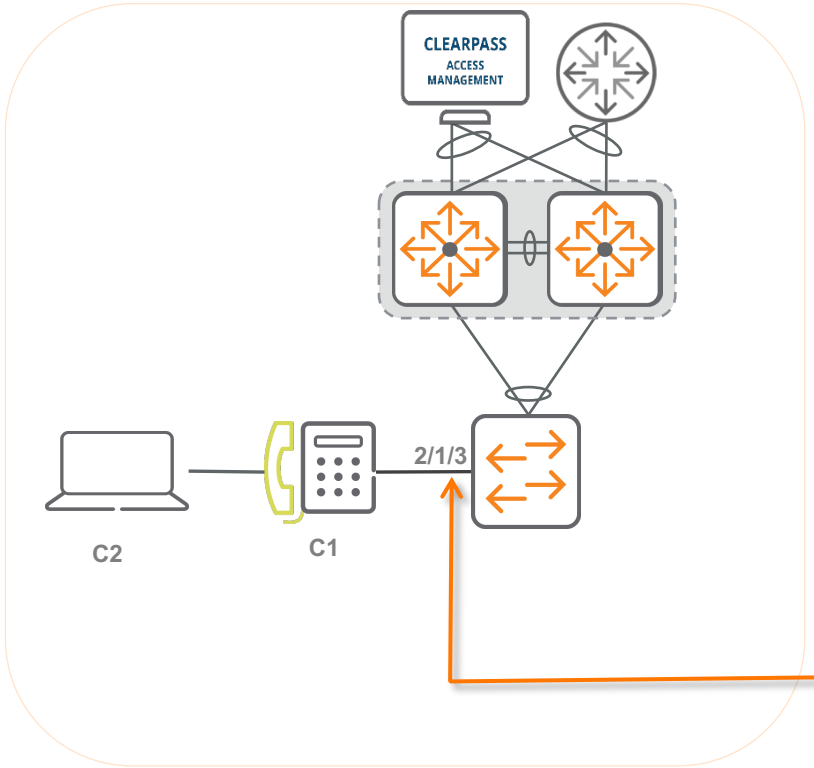
Client onboarding will be faster

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

(config-if)#
description Phone_mac-auth
aaa authentication port-access dot1x authenticator
        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
```




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

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

Demo2: Concurrent onboarding




```
(config-if)#
port-access onboarding-method concurrent enable
description pc behind IP_phone
    no routing
    vlan trunk native 10
    vlan trunk allowed 10,112
    no sflow
    aaa authentication port-access client-limit 2
    aaa authentication port-access dot1x authenticator
        reauth
        enable
    aaa authentication port-access mac-auth
        enable
```

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 -r -d port-accessd

- **Daigdump**

6300-1-VSF# diagnostics

diag-dump port-access basic

diag-dump dot1x-authenticator basic

diag-dump mac-auth basic

- **Debugs**

6300-1-VSF#

debug radius all

debug port access all

debug destination buffer

6300-1-VSF#

show debug buffer

Troubleshooting – CX Mirroring

Mirror session 1

Source interface 1/1/1 both

Destination CPU

enable

diag utilities tshark file

copy tshark-pcap tftp://10.80.2.187/djky.pcap vrf mgmt

Mirror session 1

Source interface 1/1/1 both

Source interface 1/1/48 both

Destination interface 1/1/3

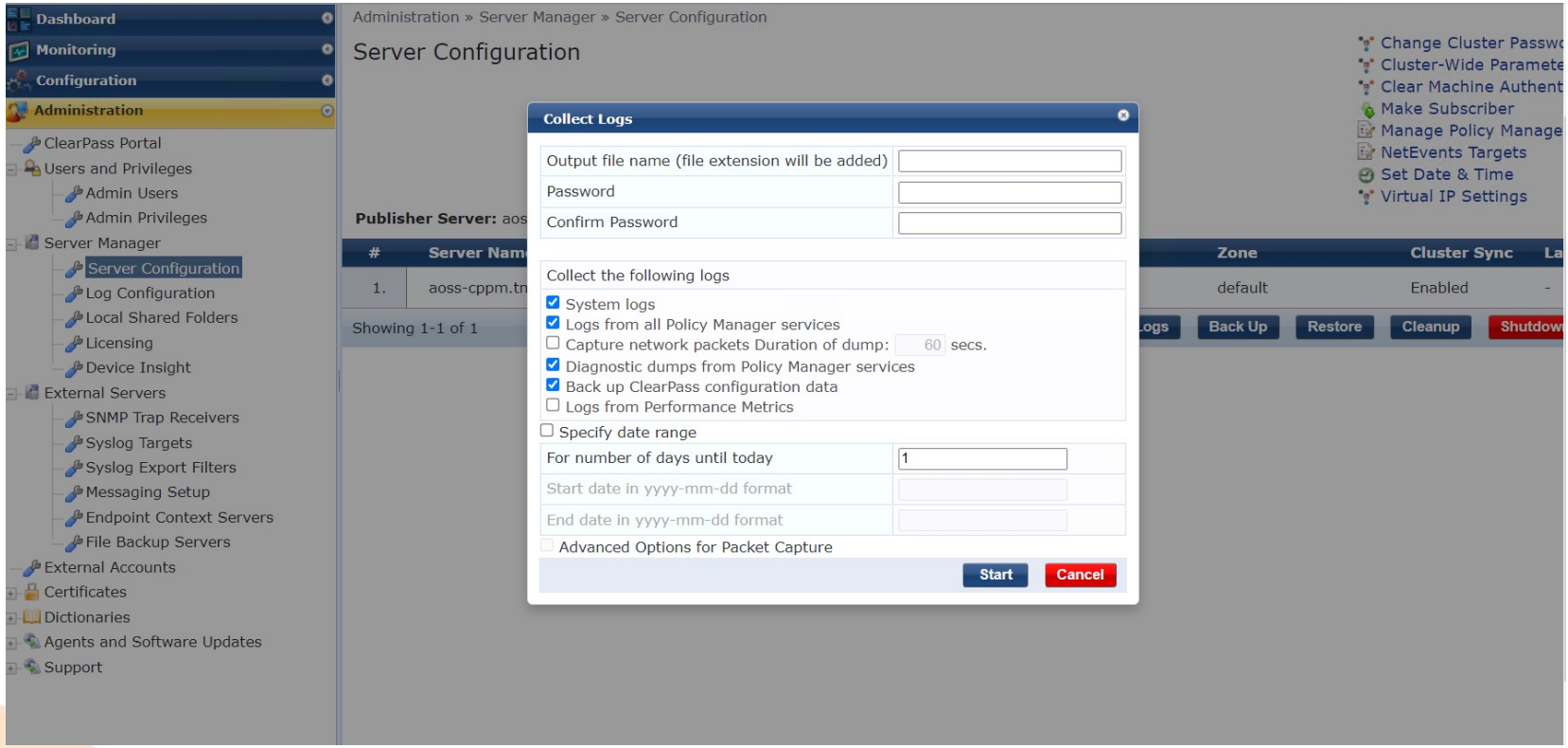
enable

Note:

- Disable enabled mirroring once work is done. You must disable one for destination CPU.
- Source vlan is also supported
- Destination CPU or interface or Tunnel is supported

aruba
a Hewlett Packard Enterprise company

ClearPass Packet Capture



Feature/Solution Troubleshooting

Advance level

```
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
```

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

aruba
a Hewlett Packard
Enterprise company

Thank you

yashavanth.n.n@hpe.com