Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: Enable Colorless port for Dual Port APs

Shobana Nandakumar , Technical Marketing Engineer

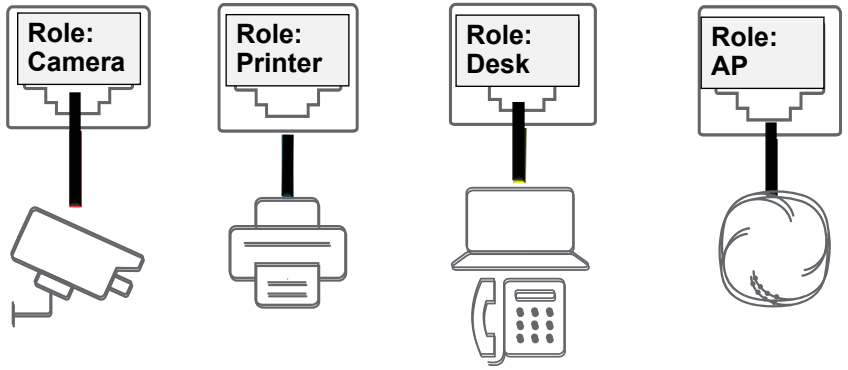
Nov 2nd, 2023

Overview

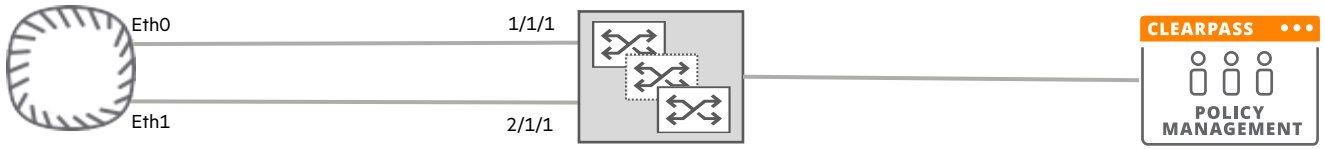
Colored versus Colorless Ports

```
interface 1/1/1
    description Colorless-Port
    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 dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    loop-protect action tx-disable
```

– We no longer care what gets plugged in; ports **are now colorless**



Prior to 10.13 – Colored Dual Port APs



- AOS-CX switches uses **Chassis MAC** of LLDP packet for MAC/Device-Profile Authentication by default.
- As Chassis MAC of LLDP Packets from the Dual Port APs remains the same, results in **MAC Move**.

No.	Time	Source	Destination	Protocol
16	20:49:24.35268…	ArubaaHe_c4:81:1b	LLDP_Multicast	LLDP

```
Frame 16: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on ir
Ethernet II, Src: ArubaaHe_c4:81:1b (d0:15:a6:c4:81:1b), Dst: LLDP_Multicast
Link Layer Discovery Protocol
  Chassis Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  Port Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  Time To Live = 120 sec
  System Name = Bldg1-AP-555
  System Description = ArubaOS (MODEL: 555), Version Aruba IAP
```

Chassis-ID MAC

Eth0 Source MAC

No.	Time	Source	Destination	Protocol
7	20:49:17.84484…	ArubaaHe_c4:81:1c	LLDP_Multicast	LLDP

```
Frame 7: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on int
Ethernet II, Src: ArubaaHe_c4:81:1c (d0:15:a6:c4:81:1c), Dst: LLDP_Multicast
Link Layer Discovery Protocol
  Chassis Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  Port Subtype = MAC address, Id: d0:15:a6:c4:81:1c
  Time To Live = 120 sec
  System Name = Bldg1-AP-555
  System Description = ArubaOS (MODEL: 555), Version Aruba IAP
```

Chassis-ID MAC

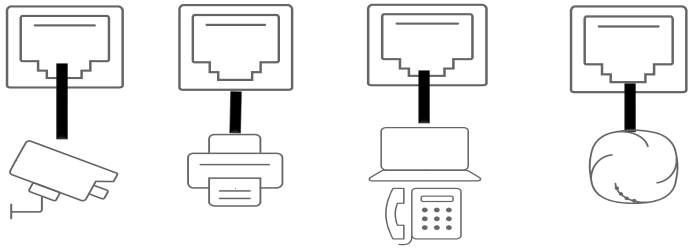
Eth1 Source MAC

- Therefore, Colorless port configuration becomes inappropriate for Dual Port APs and **LLDP Authentication is disabled in Dual Port AP** connected ports to overcome MAC moves.

```
interface <Dual-Port-AP>
no aaa authentication port-access allow-lldp-auth
```

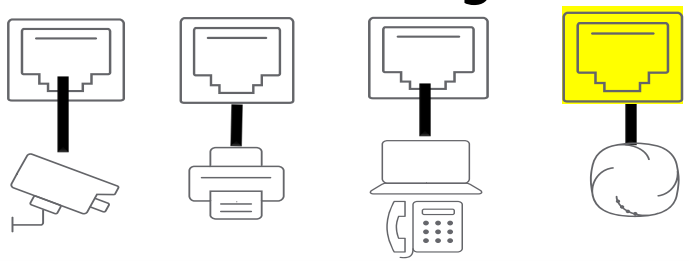
Prior to 10.13

Colorless Port Config



```
interface 1/1/1
    description Colorless-Port
    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 dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    loop-protect action tx-disable
```

Colored – Dual Port AP Config



```
interface 1/1/1
    description Dual-Port-AP
    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
    no aaa authentication port-access allow-lldp-auth
    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 dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    loop-protect action tx-disable
```

Enhancement in 10.13 – Colorless Dual Port APs

- Enhancement to source MAC address in LLDP packet for triggering MAC/Device-Profile Authentication to onboard Dual port APs.

No.	Time	Source	Destination	Protocol
16	20:49:24.35268…	ArubaaHe_c4:81:1b	LLDP_Multicast	LLDP

```
> Frame 16: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits) on ir
> Ethernet II, Src: ArubaaHe_c4:81:1b (d0:15:a6:c4:81:1b), Dst: LLDP_Multicast
v Link Layer Discovery Protocol
  > Chassis Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  > Port Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  > Time To Live = 120 sec
  > System Name = Bldg1-AP-555
  > System Description = ArubaOS (MODEL: 555), Version Aruba IAP
```

Chassis-ID MAC

Eth0 Source MAC

No.	Time	Source	Destination	Protocol
7	20:49:17.84484…	ArubaaHe_c4:81:1c	LLDP_Multicast	LLDP

```
> Frame 7: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on int
> Ethernet II, Src: ArubaaHe_c4:81:1c (d0:15:a6:c4:81:1c), Dst: LLDP_Multicast
v Link Layer Discovery Protocol
  > Chassis Subtype = MAC address, Id: d0:15:a6:c4:81:1b
  > Port Subtype = MAC address, Id: d0:15:a6:c4:81:1c
  > Time To Live = 120 sec
  > System Name = Bldg1-AP-555
  > System Description = ArubaOS (MODEL: 555), Version Aruba IAP
```

Chassis-ID MAC

Eth1 Source MAC

- Retain existing configuration and new configurable CLI sub-option to select the MAC address type used for triggering authentication from LLDP Packets.

```
6300(config)# interface 1/1/1
6300(config-if)# aaa authentication port-access allow-lldp-auth mac
  chassis-mac   Configure LLDP authentication-mac type to chassis mac.
  source-mac    Configure LLDP authentication-mac type to interface mac.
```

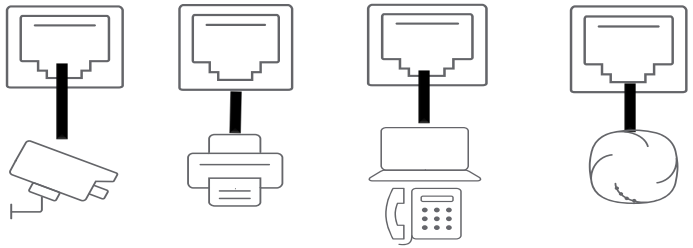
Chassis-ID MAC

Source MAC

- Supported Platforms – 10000,8360,8325,8100,6400,6300,6200,6100 and 4100i

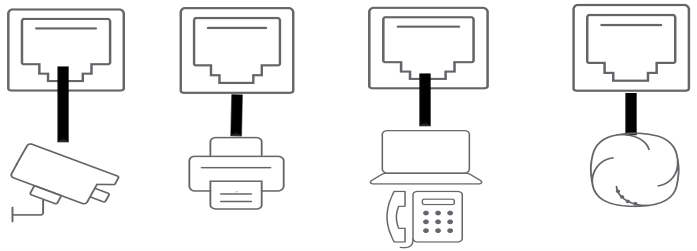
Enhancement from 10.13

Existing Colorless Port Config



```
interface 1/1/1
    description Colorless-Port
    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 dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    loop-protect action tx-disable
```

New Colorless Port Config – To Support Dual Port APs

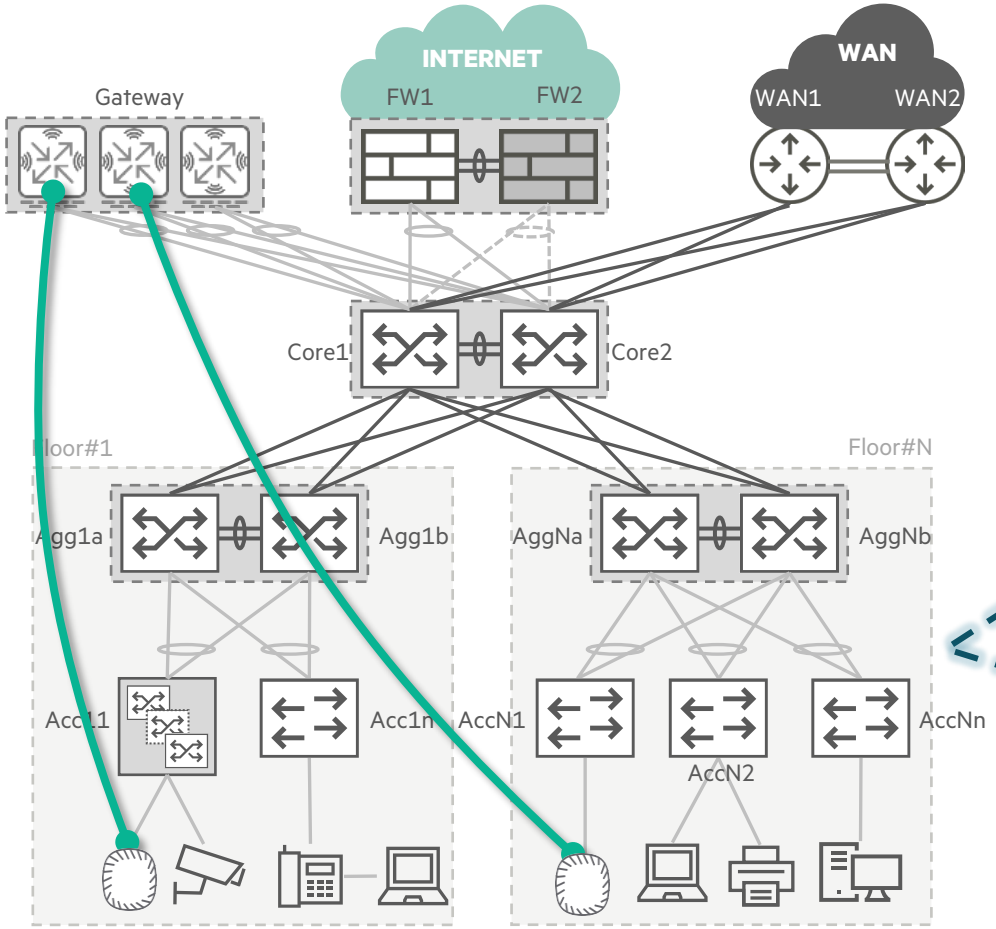


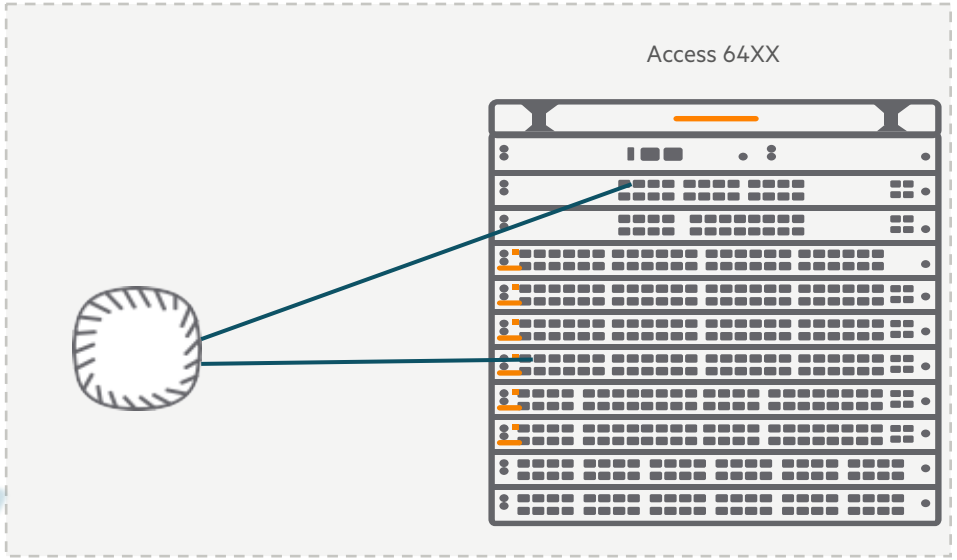
```
interface 1/1/1
    description Colorless-Port
    no shutdown
    no routing
    vlan access 1
    spanning-tree bpdu-guard
    spanning-tree root-guard
    spanning-tree tcn-guard
    spanning-tree port-type admin-edge
    port-access onboarding-method concurrent enable
    aaa authentication port-access allow-lldp-auth mac source-mac
    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 dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    loop-protect action tx-disable
```

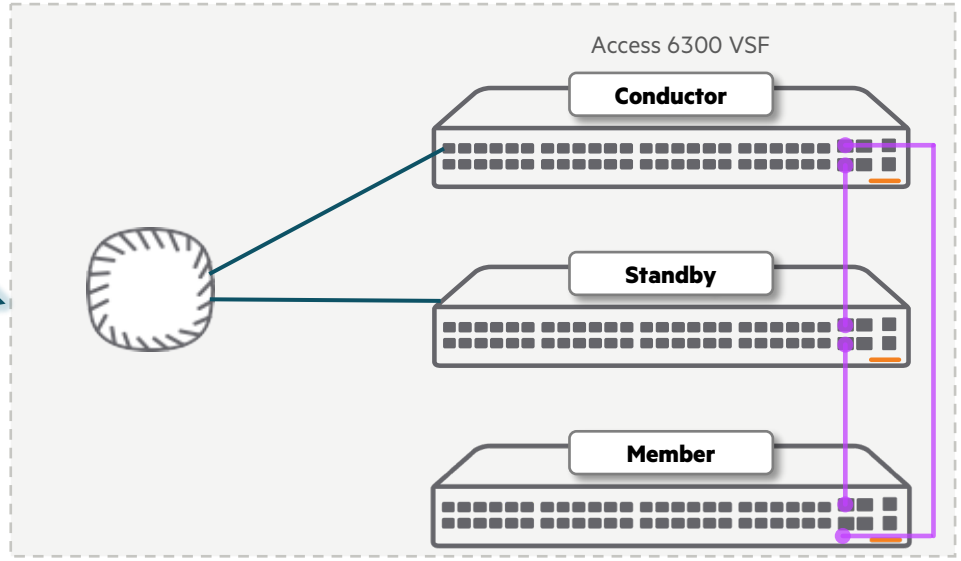
Use Cases

Dual Port AP

Enterprise Campus



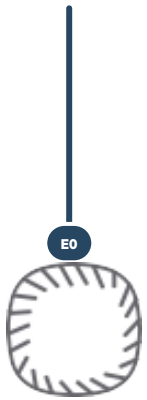
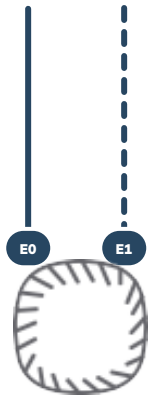
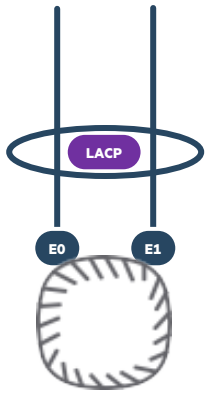




L2
L3

Intra-Zone GRE Overlay Tunnel

Better Wireless Service Reliability and Performance

Single Uplink	Active / Standby	Active / Active
		
802.1x/MAC/Device Profile Authentication	802.1x/MAC/Device Profile Authentication	Device Profile
✗ PoE Redundancy	✓ PoE Redundancy	✓ PoE Redundancy
✗ Path Redundancy	✓ Path Redundancy	✓ Path Redundancy
✗ Aggregated Throughput	✗ Aggregated Throughput	✓ Aggregated Throughput

Configuration

CLI

- To configure the MAC address type to be used for LLDP MAC Authentication –

```
6300(config)# interface 1/1/1
6300(config-if)# aaa authentication port-access allow-lldp-auth
  mac   Specify LLDP authentication-mac type. (Default: chassis-mac)
  <cr>
6300(config-if)# aaa authentication port-access allow-lldp-auth mac
  chassis-mac  Configure LLDP authentication-mac type to chassis mac.
  source-mac   Configure LLDP authentication-mac type to interface mac.
```

- To view the configuration -

```
6300(config)# show run interface <> | in allow-lldp-auth
    aaa authentication port-access allow-lldp-auth mac source-mac
```

REST API - POST

POST /system/interfaces

Parameters | Try it out

No parameters

Request body | application/json

Example Value | Schema


```
  "port_access_enable_client_auto_logoff": {
    "final_authentication_failure_enable": true
  },
  "port_access_fallback_role": "Unknown Type: URI",
  "port_access_lldp_authentication_mac": "chassis-mac",
  "port_access_mda_data_clients_limit": 0,
  "port_access_onboarding_precedence": {
    "integer": "aaa"
  },
```

REST API - GET

GET /system/interfaces/{Interface.name}

Parameters

Cancel

Name	Description
Interface.name * required string *(path)*	Reference Resource: Interface The interface name. For non-bonded ports, the interface name is the same as the associated port name. The name must otherwise be unique across all ports and interfaces of the system. 1/1/3
attributes array[string] *(query)*	Columns to display. port_access_enable_client_auto_logon port_access_extended_access_vlans port_access_fallback_role port_access_lldp_authentication_mac port_access_mda_data_clients_limit
depth integer *(query)*	Depth to traverse. 2

Curl

```
curl -X GET "https://10.6.8.6/rest/v10.13/system/interfaces/1%2F1%2F3?attributes=port_access_lldp_authentication_mac&depth=2" -H "accept: application/json" -H "x-csrf-token: SIPHm64DMNGGRVCo9OMYIw=="
```

Request URL

https://10.6.8.6/rest/v10.13/system/interfaces/1%2F1%2F3?attributes=port_access_lldp_authentication_mac&depth=2

Server response

Code	Details

200	Response body
	{
	"port_access_lldp_authentication_mac": "source-mac"
	}
	Download

Troubleshooting

Debugging

- To enable debugging -

```
Debug destination <buffer | console | file | syslog>
Debug portaccess all
```

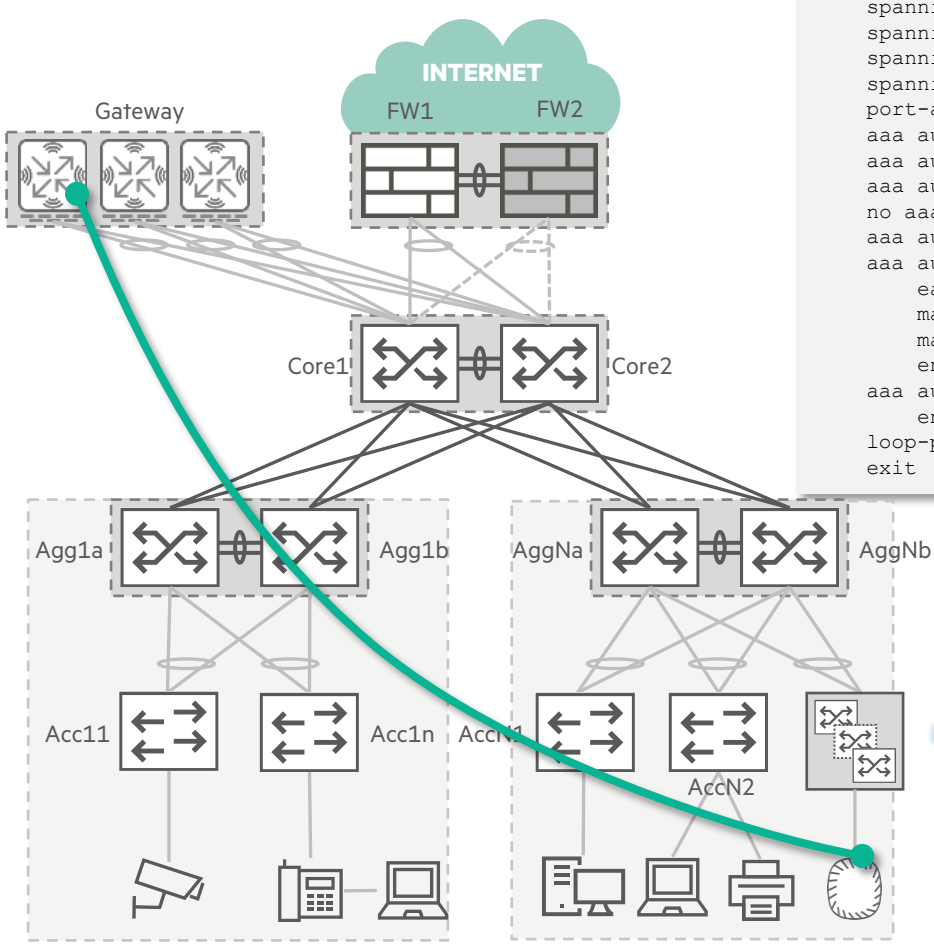
```
Show debug buffer module portaccess reverse
2023-12-04:01:15:07.603605|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5579010 Handling event Packet Rx for Client d0:15:a6:c4:81:1b on port 1/1/3 in state
SECURE MOVE.
2023-12-04:01:15:06.609932|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5579008 Handling event Packet Received for port 2/1/3 in state DEVICE MODE SECURE
2023-12-04:01:15:06.609876|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5579008 Client d0:15:a6:c4:81:1b updated in Client Move Manager on port 2/1/3.
2023-12-04:01:15:06.609841|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5579008 Client d0:15:a6:c4:81:1b moved from port 1/1/3 -> 2/1/3.
2023-12-04:01:15:06.609703|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5579008 Handling event Packet Rx for Client d0:15:a6:c4:81:1b on port 1/1/3 in state
AVAILABLE.
2023-12-04:01:14:58.110179|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5578995 Handling event Packet Received for port 2/1/3 in state DEVICE MODE SECURE
2023-12-04:01:14:58.110099|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5578995 Handling event Packet Rx for Client d0:15:a6:c4:81:1c on port 2/1/3 in state
AVAILABLE.
2023-12-04:01:14:58.109970|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_DEVICEPROFILE|logID=5578994 Handling event 'Neighbor Detected' in state 'SECURE PROFILE NONE' for port
'2/1/3'
2023-12-04:01:14:58.109914|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_DEVICEPROFILE|logID=5578994 Neighbor SM State transition [NEIGHBOR NOT MATCHED] -> [NEIGHBOR NOT
MATCHED] for MAC d0:15:a6:c4:81:1c on port 2/1/3.
2023-12-04:01:14:58.109884|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_DEVICEPROFILE|logID=5578994 Neighbor data updated for neighbor with MAC d0:15:a6:c4:81:1c on port
2/1/3 for neighbor type LLDP.
2023-12-04:01:14:58.109836|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_DEVICEPROFILE|logID=5578994 Handling event Neighbor Updated for MAC d0:15:a6:c4:81:1c on port 2/1/3 in
state NEIGHBOR NOT MATCHED.
2023-12-04:01:14:58.104546|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5578993 Handling event Packet Received for port 1/1/3 in state DEVICE MODE SECURE
2023-12-04:01:14:58.104463|port-accessd|LOG_DEBUG|CDTR|1|PORTACCESS|PORTACCESS_SERVICES|logID=5578993 Handling event Packet Rx for Client d0:15:a6:c4:81:1b on port 1/1/3 in state
AVAILABLE.
```

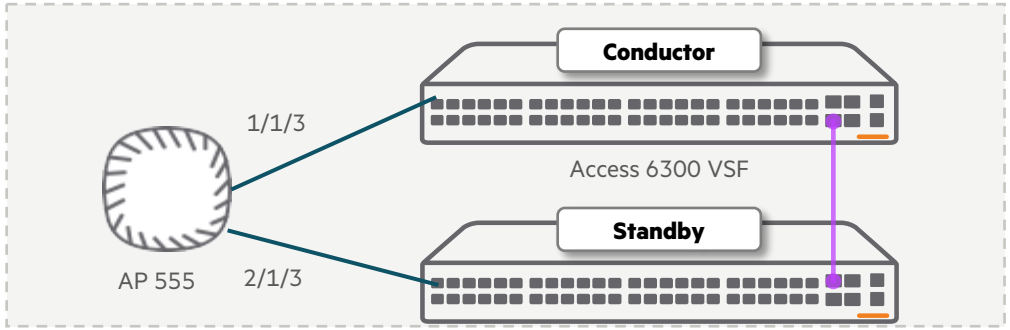
Demo

Dual Port AP

```
6300-VSF(config)# show run interface 1/1/3
interface 1/1/3
    description Colorless-Port
    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 allow-lldp-auth mac source-mac
    no aaa authentication port-access allow-lldp-auth
    aaa authentication port-access client-limit 2
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    exit
```

```
6300-VSF(config)# show run interface 2/1/3
interface 1/1/3
    description Colorless-Port
    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 allow-lldp-auth mac source-mac
    no aaa authentication port-access allow-lldp-auth
    aaa authentication port-access client-limit 2
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
    loop-protect
    exit
```





L2
L3

Intra-Zone GRE Overlay Tunnel

```
Port-access role Dual-Port-AP
    auth-mode device-mode
exit
```

Thank you

© 2023 Hewlett Packard Enterprise Development LP