Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: Device Profile Over LAG

Shobana Nandakumar , Technical Marketing Engineer

Nov 2nd, 2023

Agenda

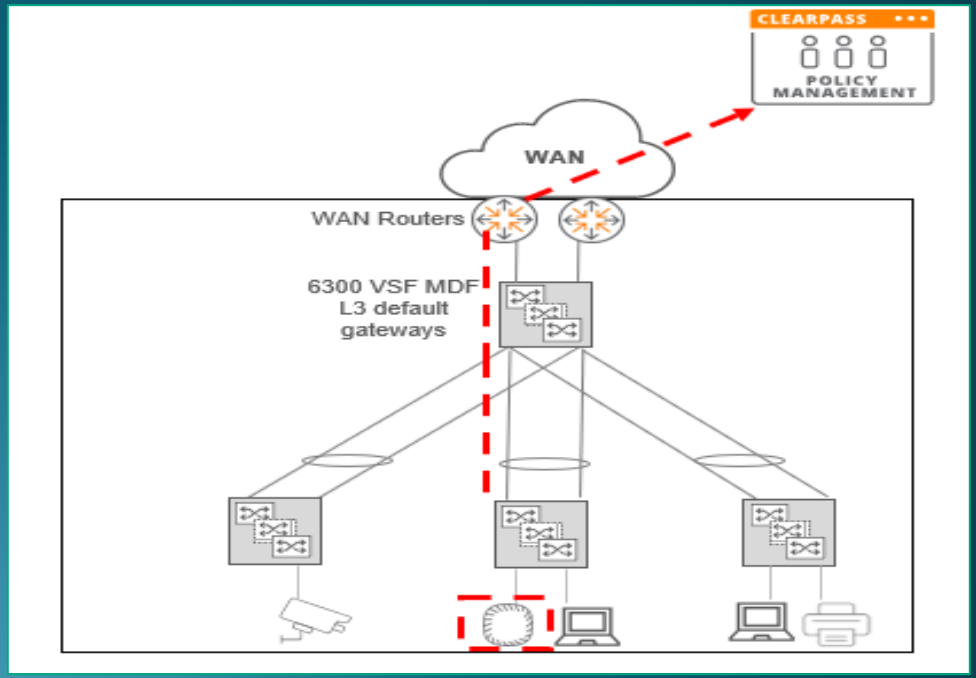
1	Overview
2	Use Cases
3	Configuration
4	Details
5	Best Practices
6	Demo

Overview

Current Challenges

Device Visibility

Onboarding Latency



Device Profile Overview

Device Profiles are used to **dynamically** assign port attributes based on the type of devices connected, **without RADIUS infrastructure**.

Device Profiles are mapped to Device Groups

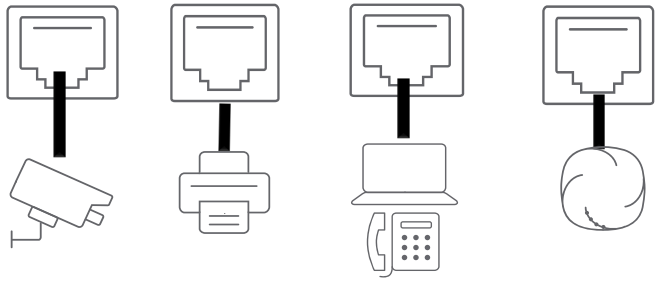
Device group contains various match criteria from following sources

- LLDP
- CDP
- Local Mac Match

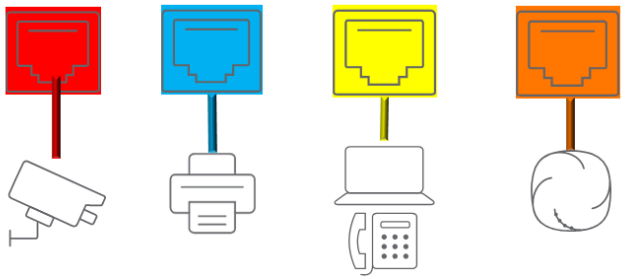
Prior to 10.13, Device Profile can be applied only on **Physical L2 Ports**

Secure - Device Profile

- Colorless Deployment



- Colored Deployment



- Using – 802.1x/Mac Authentication

```
Interface <>
    no shutdown
    vlan access 1
    port-access onboarding-method precedence device-profile aaa
    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
        enable
    aaa authentication port-access mac-auth
        enable
```

- Using – Block until Profile Applied

```
Interface <>
            vlan access 1
            aaa authentication port-access allow-cdp-bpdu
            aaa authentication port-access allow-lldp-bpdu
            port-access device-profile
                        mode block-until-profile-applied
```

Enhancement in Device Profile

Device Profile Over LAG

Link aggregation group (LAG) bundles multiple physical Ethernet links into one logical link

Benefits

- Increased Bandwidth
- Improved Link Reliability

Device Profile Clients are supported over L2 LAG Interface

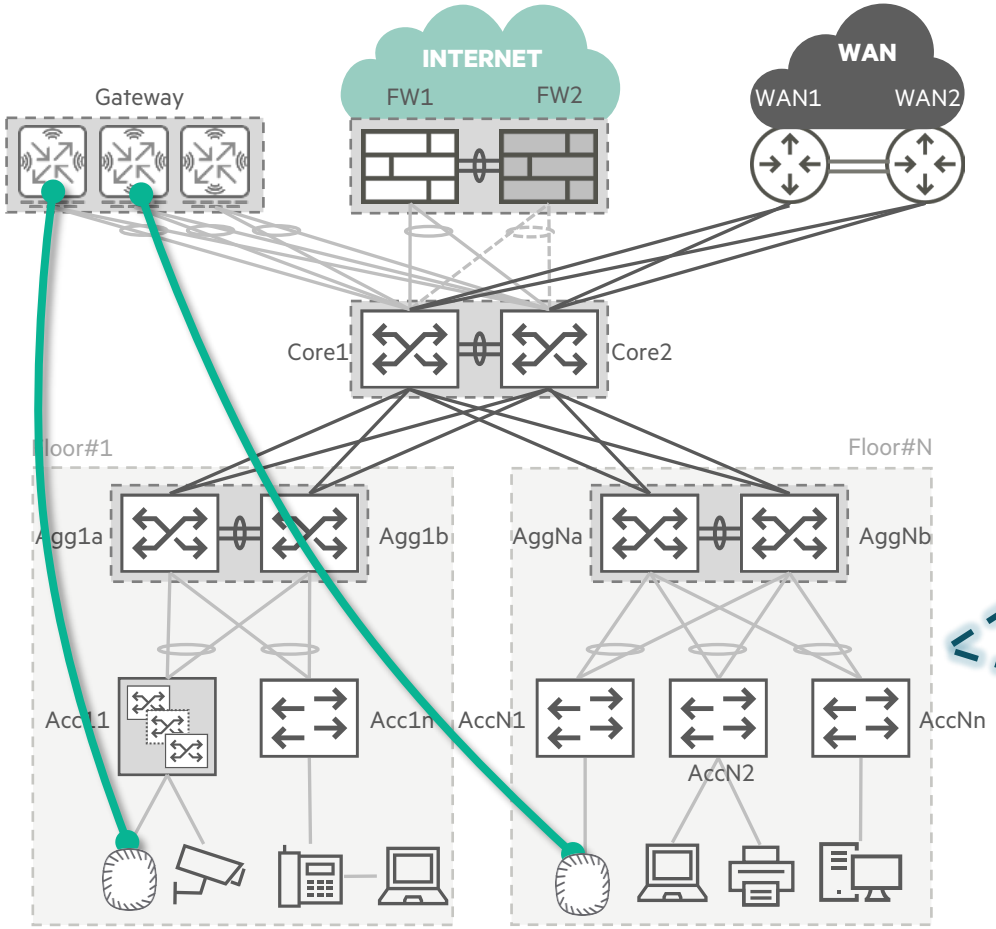
Roles are mapped to configured device groups (LLDP/CDP/MAC) and applied on the whole LAG, if the device connected to LAG port matches the group match criteria.

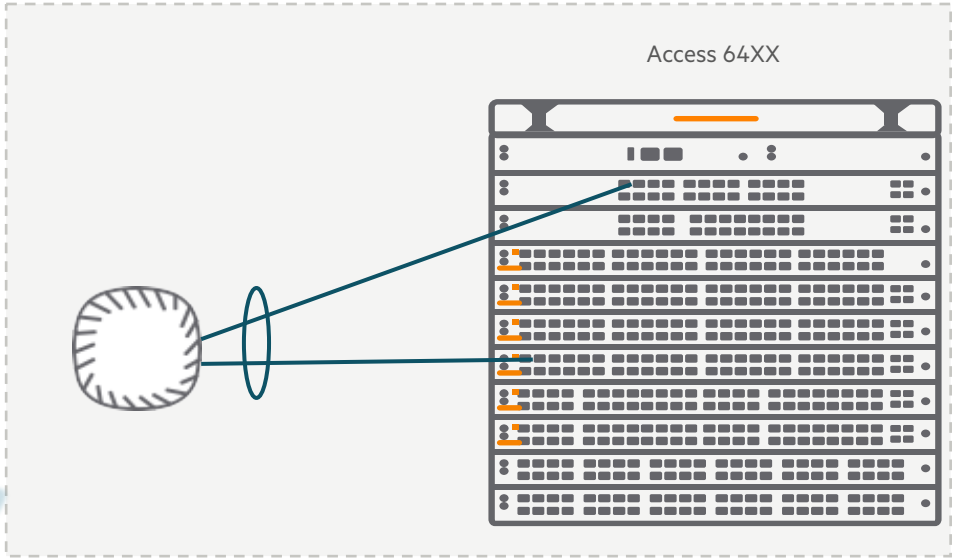
Supported Platforms – 4100i,6XXX,8100 and 8360

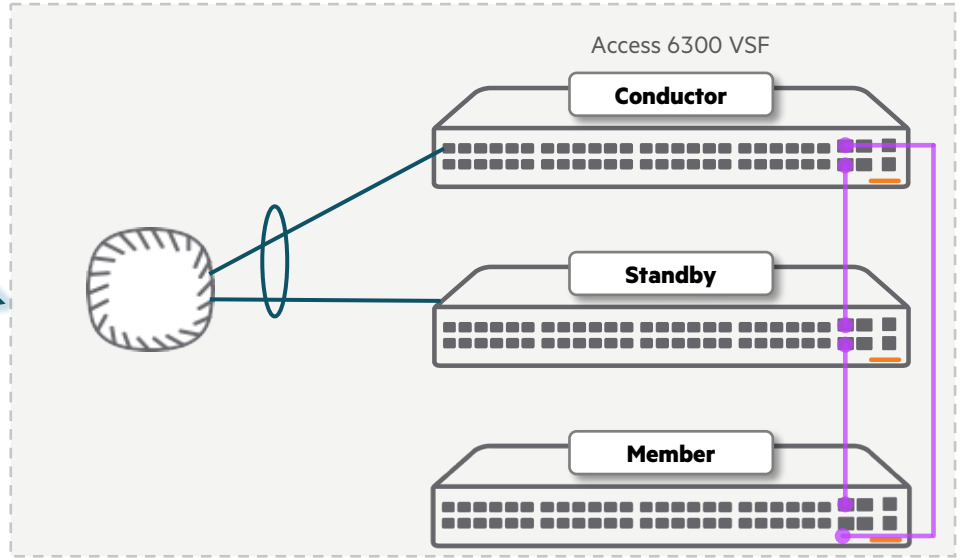
Use Cases

Dual Port AP

Enterprise Campus



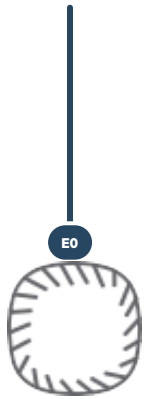
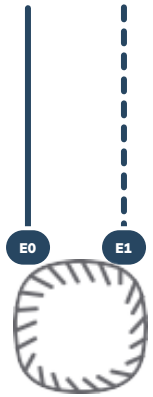
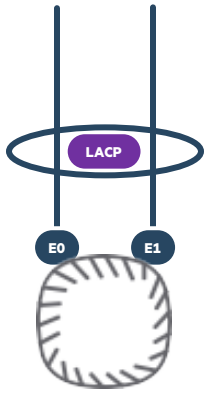




L2
L3

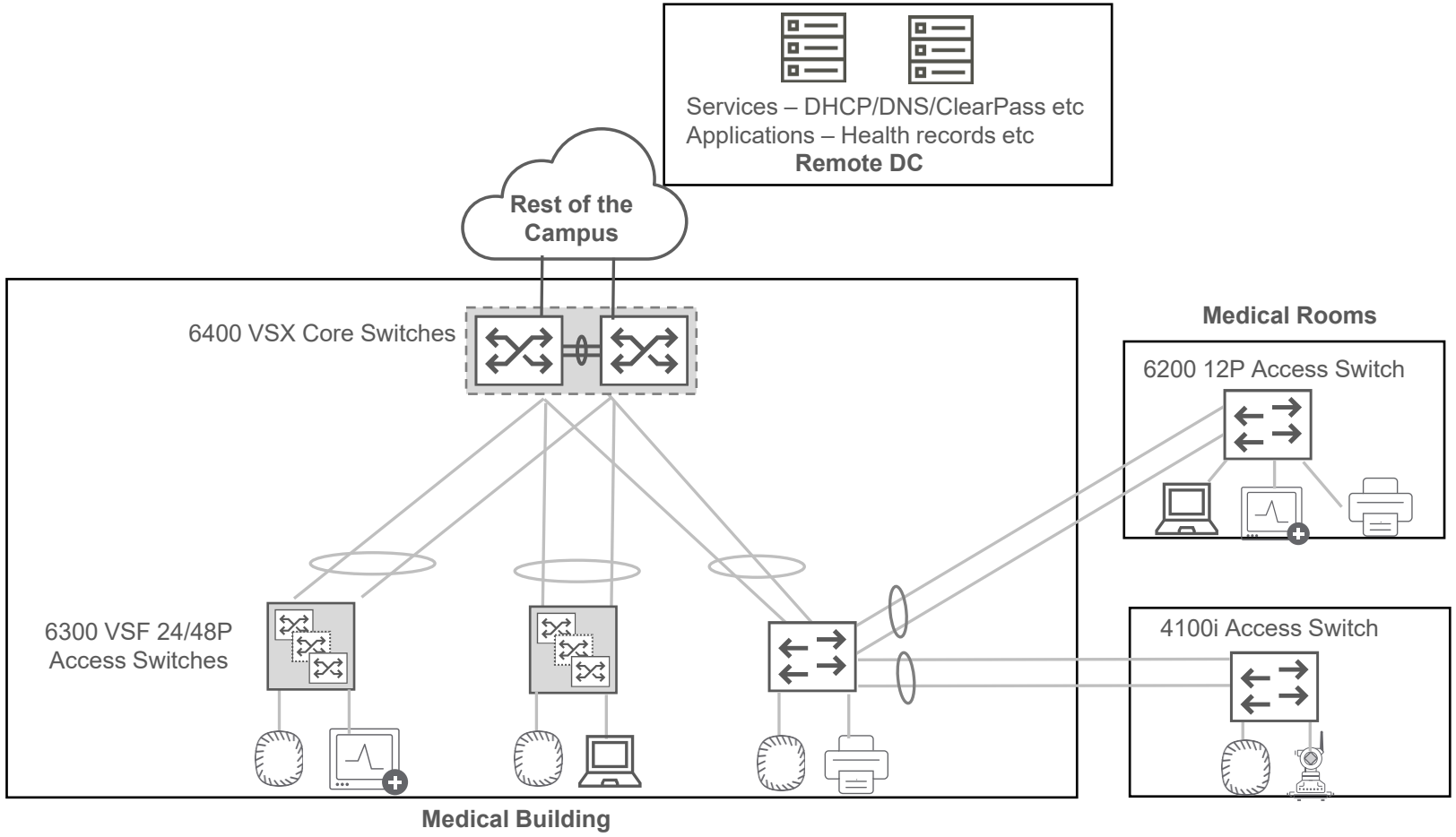
Intra-Zone GRE Overlay Tunnel

Better Wireless Service Reliability and Performance

Single Uplink	Active / Standby	Active / Active
		
✗ PoE Redundancy	✓ PoE Redundancy	✓ PoE Redundancy
✗ Path Redundancy	✓ Path Redundancy	✓ Path Redundancy
✗ Aggregated Throughput	✗ Aggregated Throughput	✓ Aggregated Throughput

Secure Access Extension

- To securely onboard Mini Access Switches in Cruises, Hospitality and Manufacturing Verticals as 802.1x/Mac Auth is not supported over LAG currently.

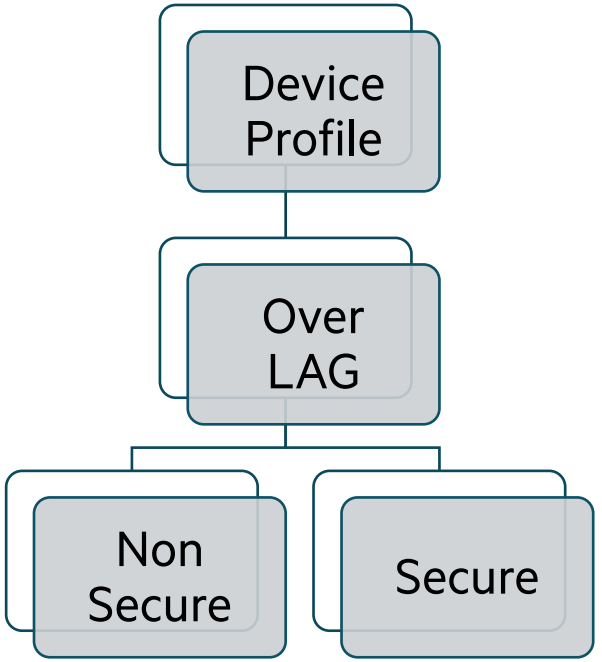


Configuration

Configuration

- To Configure Device Profile Over LAG -

```
port-access lldp-group <group-name>
  match [sys-desc | sys-name | vendor-oui] <value>
exit
port-access cdp-group <group-name>
  match [platform | sw-version | voice-vlan] <value>
exit
mac-group <group-name>
  match [mac | mac-mask | mac-oui]
exit
port-access role <role-name>
  <role-parameters>
exit
port-access device-profile <profile-name>
  associate [lldp-group | cdp-group | mac-group] <group-name>
  associate role <role-name>
  enable
exit
```




```
interface lag <>
   no shutdown
   vlan access 1
exit
```

```
interface lag <>
    no shutdown
    vlan access 1
    aaa authentication port-access allow-lldp-bpdu
    aaa authentication port-access allow-cdp-bpdu
    aaa authentication port-access client-limit <>
    port-access device-profile
        mode block-until-profile-applied
exit
```

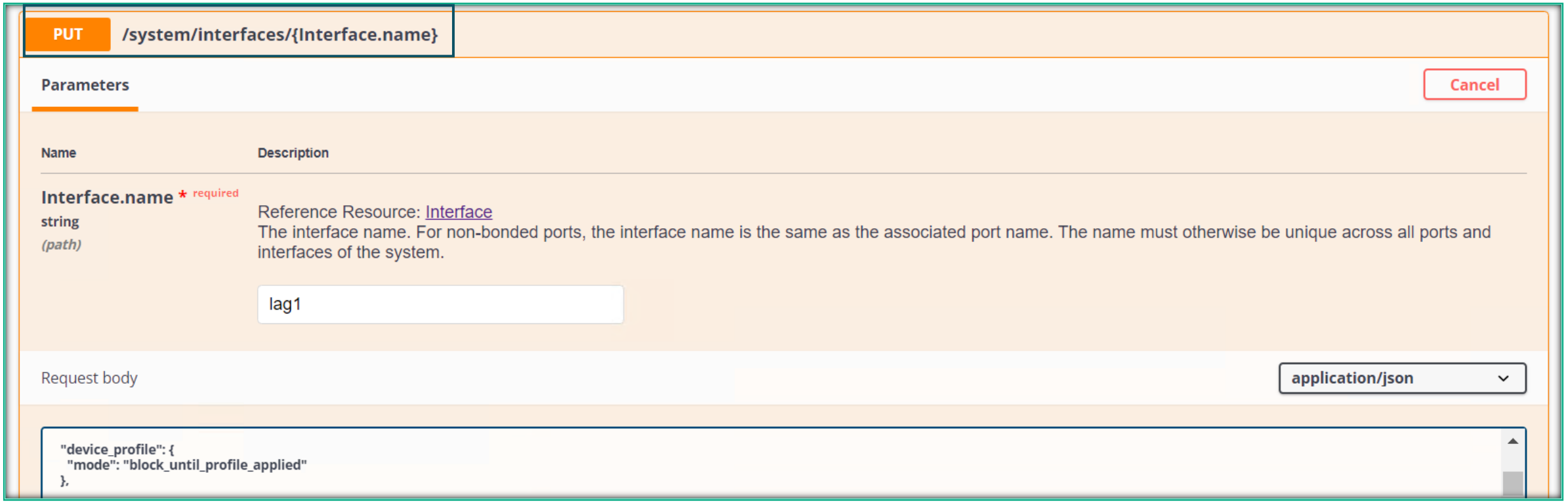
Configuration

- List of Port-Access CLIs supported in LAG -

```
interface lag <>
aaa authentication port-access allow-cdp-auth
aaa authentication port-access allow-cdp-bpdu
aaa authentication port-access allow-cdp-proxy-logoff
aaa authentication port-access allow-lldp-auth
aaa authentication port-access allow-lldp-bpdu
aaa authentication port-access auth-mode [Client-mode | device-mode]
aaa authentication port-access client-limit <platform-specific-limit>
port-access allow-flood-traffic [enable | disable]
port-access device-profile mode block-until-profile-applied
exit
```

Configuration - REST

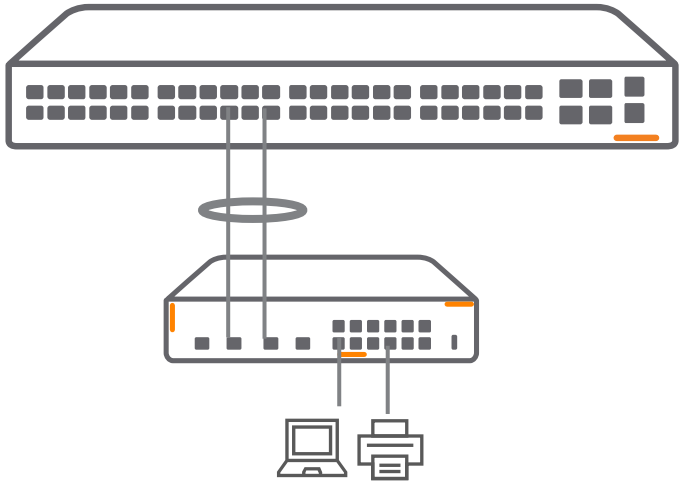
- To enable device-profile mode through REST API



Details

Device Profile - Modes

- Client Mode

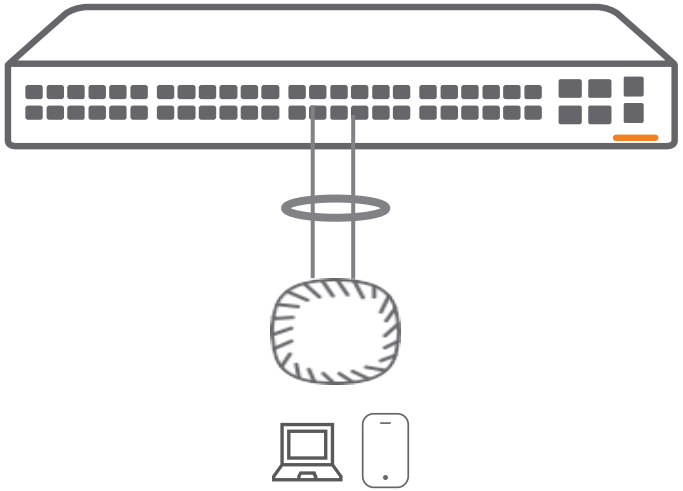


```
show po
-------
Port
-------
lag1
lag1
lag1
```

```
port-access device-profile "Switch"
associate lldp-group "Switch-group"
associate role "Switch"
exit
port-access device-profile "PC"
associate mac-group "PC-group"
associate role "PC"
exit
port-access device-profile "Printer"
associate mac-group "Printer-group"
associate role "Printer"
exit
```

```
------------------------
le   VLAN    Flags
------------------------
     (u)600   dp|c|-|s
     (u)700   dp|c|-|s
     (u)800   dp|c|-|s
```

- Device Mode



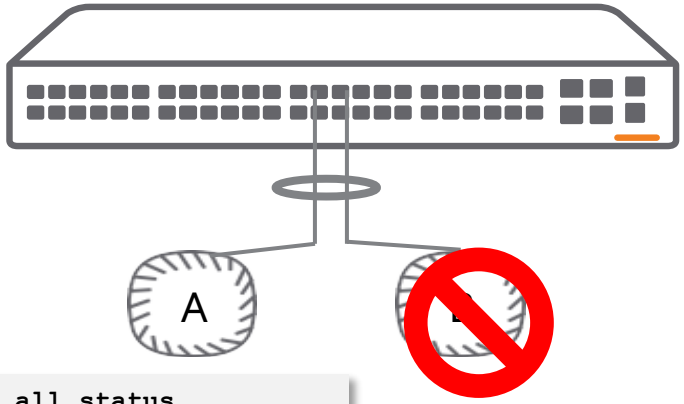
```
show port-access clients interface lag1

-------------------------------------------------------------------------
Port      Client-Name         IPv4-Address    User-Role    VLAN      Flags
-------------------------------------------------------------------------
lag1      bc:9f:e4:cb:54:be   60.1.83.65      Dual-Port-AP (u)600    dp|d|-|s
```

```
show mac-address-table interface lag1
MAC Address          VLAN     Type                        Interface
-------------------------------------------------------------------
bc:9f:e4:cb:54:be    600      port-access-security        lag1
bc:9f:e4:cb:54:bf    600      port-access-security        lag1
ac:7b:dc:76:34:af    700      port-access-security        lag1
fc:6b:ac:b4:3e:ba    800      port-access-security        lag1
```

Secure Device Onboarding over LAG

Blocks different device Onboarding in same LAG

```
port-access lldp-group "Dual-AP-group"
  match sys-desc "ArubaOS (MODEL: 325)"
exit
port-access device-profile "Dual-Homed-AP"
  associate lldp-group "Dual-AP-group"
  associate role "Dual-AP"
exit
```




```
interface lag <>
  no shutdown
  vlan access 1
  aaa authentication port-access allow-lldp-bpdu
  aaa authentication port-access allow-cdp-bpdu
  aaa authentication port-access auth-mode device-mode
    port-access device-profile
        mode block-until-profile-applied
exit
```

```
show port-access interface all status
Port       Interface   St
---------  ----------  --
lag1       1/1/3       Se
lag1       1/1/4       Bl
```

```
show port-access interface all status
Port       Interface   Status
---------  ----------  -------
lag1       1/1/3       Secured
lag1       1/1/4       Down
```

```
> Frame 68: 190 bytes on wire (                                  t, id 0
> Ethernet II, Src: ArubaaHe_ca:59:98 (f0:5c:19:ca:59:98), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
v Link Layer Discovery Protocol
  v Chassis Subtype = MAC address, Id: f0:5c:19:ca:59:98
      0000 001. .... .... = TLV Type: Chassis Id (1)
      .... ...0 0000 0111 = TLV Length: 7
      Chassis Id Subtype: MAC address (4)
      Chassis Id: ArubaaHe_ca:59:98 (f0:5c:19:ca:59:98)
  > Port Subtype = MAC address, Id: f0:5c:19:ca:59:98
  > Time To Live = 120 sec
  > System Name = f0:5c:19:ca:59:98
  > System Description = ArubaOS (MODEL: 325), Version 6.4.4.3-4.2.2.0 (53034)
  > Capabilities
  > Management Address
  > Port Description = eth0
```

```
> Frame 79: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface MirrorRxNet, id 0
> Ethernet II, Src: ArubaaHe_ca:59:7a (f0:5c:19:ca:59:7a), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
v Link Layer Discovery Protocol
  v Chassis Subtype = MAC address, Id: f0:5c:19:ca:59:7a
      0000 001. .... .... = TLV Type: Chassis Id (1)
      .... ...0 0000 0111 = TLV Length: 7
      Chassis Id Subtype: MAC address (4)
      Chassis Id: ArubaaHe_ca:59:7a (f0:5c:19:ca:59:7a)
  > Port Subtype = MAC address, Id: f0:5c:19:ca:59:7a
  > Time To Live = 120 sec
  > System Name = f0:5c:19:ca:59:7a
  > System Description = ArubaOS (MODEL: 325), Version 6.4.4.3-4.2.2.0 (53034)
  > Capabilities
  > Management Address
  > Port Description = eth0
```

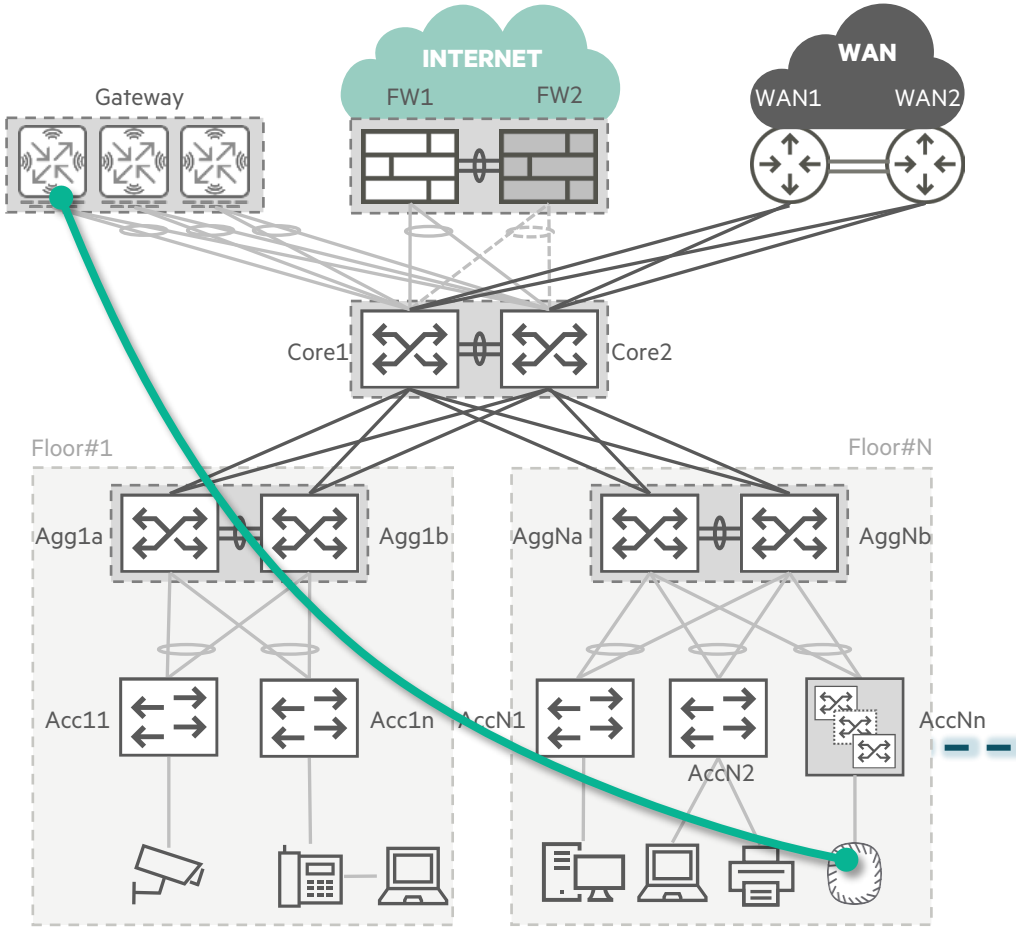
Best Practices

Best Practices

- Device mode should be used on LAGs connected to Dual Homed APs for best results.
- If there are multiple device profiles matching the onboarding clients on LAG interface, configurations should be such that same role should be applied on the LAG.
- Avoid adding pre-configured interfaces to LAG , as existing port-access configurations will be cleared.
- Device Profile enabled by default in all the L2 and L2 LAG interfaces , advisable to configure appropriate role assignment based on device type.
- Client-limit should be configured as per the number of interfaces in the LAG.
- Enable “port-access allow-flood-traffic” in case of silent clients connected in secure mode.

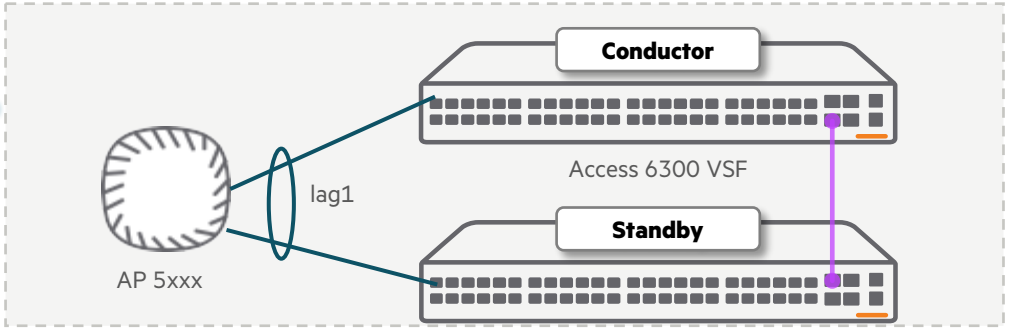
Demo

Dual Port AP




```
port-access lldp-group "Dual-Homed-AP-Group"
  match sysname "Bldg1-AP-555"
exit
port-access role "Dual-Homed-AP"
  vlan trunk native <>
  vlan trunk allowed <>
  auth-mode device-mode
exit
port-access device-profile "Dual-Homed-AP"
  associate lldp-group "Dual-AP-group"
  associate role "Dual-AP"
exit
```

```
interface lag 1
  no shutdown
  vlan access 1
  aaa authentication port-access allow-lldp-bpdu
  aaa authentication port-access allow-cdp-bpdu
  port-access device-profile
        mode block-until-profile-applied
exit
```



L2
L3

Intra-Zone GRE Overlay Tunnel

Thank you

© 2023 Hewlett Packard Enterprise Development LP