Device Profiles with Aruba 6200/6300/6400 CX Switches

Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
01 Jul 2020	0.1	Ariya Parsamanesh	Final version

1.2 Introduction

The aim of this solution is to automatically discover the key devices that are connected to the switch port using LLDP and/or CDP, and to apply device profiles to enable automatic configuration of the switch ports in which they are connected.

Device profiles which we had in AOS-S switches like Aruba 2930F/Ms are also available in CX switches that enable predefined configuration settings to be applied to an interface based on the type of devices that are connected to the interface. When a device of a configured type is connected to an interface, the switch automatically applies the corresponding device profile.

Generally the Device profiles are used for devices such as access points, IP phones, security cameras, and printers. Obviously it is always much more secure to use ClearPass for device profiling.

In this guide we'll demonstrate this functionality for connecting Aruba APs.

We need to create a device-profile and associate to it, couple of other profiles namely

1. Role profile
2. LLDP-group profile.

LLDP profile is used to match on some specific LLDP info from the AP and the Role profile is used to assign a number of attributes such as VLANs, QoS and PoE priority to name a few.

I have tested this feature with CX switch running CX version 10.04.2000 and 10.04.3000.

1.3 Role Profile

Here is our role profile in which we want the AP to be on native VLAN of 11 and its various WLANs on VLANs 12 and 13. So the switch port needs to be a trunk port. We'll also assign PoE priority and QoS trust.

```
!
port-access role Lab-IAP-role
    description Aruba IAP
    poe-priority high
    trust-mode dscp
    vlan trunk native 11
    vlan trunk allowed 11-13
!
```

1.4 LLDP-Group Profile

LLDP group is the main profile that matches on type of device which gets connected to any of the switch ports. The options for your match criterion are

- sys-desc Configure LLDP system description.
- sysname Configure LLDP system name.
- vendor-oui Configure LLDP vendor OUI.

Note that vendor OUI is not a MAC OUI for the most of Aruba APs it is 000b86 and by default LLDP is enabled on all the Instant APs, so you don't need to do anything to enable it.

Sysname is the name of that AP. For example you can configure the APs to have a name that would identify their location, then you could use that as a match criteria.

You can also match on sys-desc which is mainly is the description of the AP model

This is the LLDP neighbour info from AP-515, the chassis-name is the "sysname" and Chassis-Description is sys-desc.

```
6300-1# sh lldp nei de

LLDP Neighbor Information
=========================
Total Neighbor Entries          : 0
Total Neighbor Entries Deleted  : 6
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 3
--------------------------------------------------------------------------------
Port                           : 1/1/1
Neighbor Entries               : 0
Neighbor Entries Deleted       : 6
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 3
Neighbor Chassis-Name          : 9c:8c:d8:c9:3e:ae
Neighbor Chassis-Description   : ArubaOS (MODEL: 515), Version Aruba IAP
Neighbor Chassis-ID            : 9c:8c:d8:c9:3e:ae
Neighbor Management-Address    :
Chassis Capabilities Available : Bridge, WLAN
Chassis Capabilities Enabled   :
Neighbor Port-ID               : 9c:8c:d8:c9:3e:ae
Neighbor Port-Desc             : eth0
Neighbor Port VLAN ID          :
TTL                            : 120
```

```
Neighbor Mac-Phy details
Neighbor Auto-neg Supported    : true
Neighbor Auto-Neg Enabled      : true
Neighbor Auto-Neg Advertised   : 1000 BASE_TFD, 1000 BASE_T, 100 BASE_TXFD, 100
BASE_TX, Other
Neighbor MAU type              : 1000 BASETFD

6300-1#
```

This is the LLDP neighbour info from an old AP-205H

```
6300-1# sh lldp nei det

LLDP Neighbor Information
=========================
Total Neighbor Entries          : 1
Total Neighbor Entries Deleted  : 4
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 1
--------------------------------------------------------------------------------
Port                            : 1/1/1
Neighbor Entries                : 1
Neighbor Entries Deleted        : 4
Neighbor Entries Dropped        : 0
Neighbor Entries Aged-Out       : 1
Neighbor Chassis-Name           :
Neighbor Chassis-Description    : ArubaOS (MODEL: 205H), Version Aruba AP
Neighbor Chassis-ID             : 00:0b:86:fd:c4:0e
Neighbor Management-Address     :
Chassis Capabilities Available : Bridge, WLAN
Chassis Capabilities Enabled    :
Neighbor Port-ID                : 00:0b:86:fd:c4:0e
Neighbor Port-Desc              : eth0
Neighbor Port VLAN ID           :
TTL                             : 120

6300-1#
```

And this is from IAP-205

```
6300-1# sh lldp nei de

LLDP Neighbor Information
=========================
Total Neighbor Entries          : 1
Total Neighbor Entries Deleted  : 5
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 2
--------------------------------------------------------------------------------
Port                            : 1/1/1
Neighbor Entries                : 1
Neighbor Entries Deleted        : 5
Neighbor Entries Dropped        : 0
Neighbor Entries Aged-Out       : 2
Neighbor Chassis-Name           : ac:a3:1e:c1:bb:0c
Neighbor Chassis-Description    : ArubaOS (MODEL: 205), Version Aruba IAP
Neighbor Chassis-ID             : ac:a3:1e:c1:bb:0c
Neighbor Management-Address     :
Chassis Capabilities Available : Bridge, WLAN
```

```
Chassis Capabilities Enabled   :
Neighbor Port-ID               : ac:a3:1e:c1:bb:0c
Neighbor Port-Desc             : bond0
Neighbor Port VLAN ID          :
TTL                            : 120

Neighbor PoE information       : DOT3
Neighbor Power Type            : Type 2 PD
Neighbor Power Priority        : Unknown
Neighbor Power Source          : PSE
PD Requested Power Value       : 12.5 W
PSE Allocated Power Value      : 12.5 W
Neighbor Power Supported       : No
Neighbor Power Enabled         : No
Neighbor Power Class           : Class4
Neighbor Power Paircontrol     : No
PSE Power Pairs                : SIGNAL

Neighbor Mac-Phy details
Neighbor Auto-neg Supported    : true
Neighbor Auto-Neg Enabled      : true
Neighbor Auto-Neg Advertised   : 1000 BASE_TFD, 100 BASE_TXFD, 100 BASE_TX, 10
BASET_FD, 10 BASE_T
Neighbor MAU type              : 1000 BASETFD

6300-1#
```

So sys-desc becomes handy as a match criteria if you have specific VLAN requirement for certain AP model.

Here are the config snippets for the three criteria types that you can use.

```
!
port-access lldp-group Lab-IAP-group1
     seq 20 match vendor-oui 000b86
!
port-access lldp-group Lab-IAP-group2
     seq 10 match sysname Lab
!
port-access lldp-group Lab-IAP-group3
     seq 10 match sys-desc 303H
!
```

Note that if you have two match criteria in one LLDP group profile, the operation is OR.

1.5 Device Profile

So now that we have configured the LLDP group and Role profiles, we need to associate it with our device profile as shown below.

```
!
port-access lldp-group Lab-IAP-group
     seq 30 match vendor-oui 204c03
!
port-access role Lab-IAP-role
    description Aruba IAP
    poe-priority high
    trust-mode dscp
    vlan trunk native 11
    vlan trunk allowed 11-13
!
```

```
port-access device-profile Lab-IAP-prof
    enable
    associate role Lab-IAP-role
    associate lldp-group Lab-IAP-group
!
```

And here is the partial running configuration for this switch.

```
6300-1# sh run
Current configuration:
!
!Version ArubaOS-CX FL.10.04.3000
!export-password: default
hostname 6300-1
clock timezone australia/melbourne
aruba-central
    disable
ntp server 216.239.35.12 iburst
ntp enable
ntp vrf mgmt
cli-session
    timeout 0
!
ssh server vrf default
ssh server vrf mgmt
vsf secondary-member 2
vsf member 1
    type jl666a
    link 1 1/1/27-1/1/28
vsf member 2
    type jl666a
    link 1 2/1/27-2/1/28
!
!
vlan 1,11-12
spanning-tree
interface mgmt
    no shutdown
    ip static 192.168.1.23/24
    default-gateway 192.168.1.249

port-access lldp-group Lab-IAP-group
     seq 30 match vendor-oui 204c03

port-access role Lab-IAP-role
    description Aruba IAP
    poe-priority high
    trust-mode dscp
    vlan trunk native 11
    vlan trunk allowed 11-13

port-access device-profile Lab-IAP-prof
    enable
    associate role Lab-IAP-role
    associate lldp-group Lab-IAP-group

interface 1/1/1
    no shutdown
    no routing
```

```
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan access 11

<removed the rest of the interface config>

interface 2/1/26
    no shutdown
    no routing
    vlan access 1
interface 2/1/27
    no shutdown
interface 2/1/28
    no shutdown
interface vlan1
    ip dhcp
interface vlan11
    ip address 10.10.11.1/24
interface vlan12
    ip address 10.10.12.1/24
https-server vrf default
https-server vrf mgmt.
!
dhcp-server vrf default
    pool IAP
        range 10.10.11.5 10.10.11.9 prefix-len 24
        dns-server 8.8.8.8
        default-router 10.10.11.1
        lease 00:02:00
        exit
    pool VLAN12
        range 10.10.12.5 10.10.12.9 prefix-len 24
        default-router 10.10.12.1
        dns-server 8.8.8.8
        lease 00:02:00
        exit
    no authoritative
    enable
6300-1#
```

1.6 Testing

Now we'll connect an AP-303H to port 1/1/1 to test our configuration. First we'll check the status of the interfaces, 1/1/1 and it is up and has the default VLAN

```
6300-1# sh int b
-------------------------------------------------------------------------------------
Port      Native  Mode   Type           Enabled Status  Reason                Speed
          VLAN                                                                (Mb/s)
-------------------------------------------------------------------------------------
1/1/1     1       access 1GbT           yes     up                            1000
1/1/2     11      access 1GbT           yes     down    Waiting for link      --
1/1/3     1       access 1GbT           yes     down    Waiting for link      --
1/1/4     1       access 1GbT           yes     down    Waiting for link      --
```

Checking if the device profile is enabled.

```
6300-1# sh port-access device-profile

    Profile Name             : Lab-IAP-prof
    LLDP Groups              : Lab-IAP-group3
    CDP Groups               :
    Role                     : Lab-IAP-role
    State                    : Enabled
6300-1#
```

Checking if the IAP has booted up by seeing the LLDP info.

```
6300-1# sh lldp nei

LLDP Neighbor Information
=========================
Total Neighbor Entries          : 1
Total Neighbor Entries Deleted  : 10
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 5

LOCAL-PORT  CHASSIS-ID         PORT-ID          PORT-DESC               TTL      SYS-NAME
-------------------------------------------------------------------------------------
1/1/1       20:4c:03:23:a7:c0  20:4c:03:23:...  eth0                    120      Lab-IAP1

6300-1#
```

And now checking if the device profile is “applied”

```
6300-1# sh port-access device-profile interface all
  Port 1/1/1, Neighbor-Mac  20:4c:03:23:a7:c0
    Profile Name:            : Lab-IAP-prof
    LLDP Group:              : Lab-IAP-group3
    CDP Group:               :
    Role:                    : Lab-IAP-role
    State:                   : application-failed
    Failure Reason:          :
6300-1#
```

Note the state. The reason for it is that in the Role profile we have allowed VLANs 11-13 but VLAN 13 is not configured. Now we’ll configure it and test again.

```
6300-1# conf t
6300-1(config)# vlan 13
6300-1(config-vlan-13)# ^Z

6300-1#
```

As soon as we do that, we’ll again check the status of the device profile

```
6300-1# sh port-access device-profile interface all
  Port 1/1/1, Neighbor-Mac  20:4c:03:23:a7:c0
    Profile Name:            : Lab-IAP-prof
    LLDP Group:              : Lab-IAP-group3
    CDP Group:               :
    Role:                    : Lab-IAP-role
    State:                   : applied
```

```
    Failure Reason:          :
6300-1#
```

This is without rebooting of the AP. And finally the interface information

```
6300-1# sh int br
--------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason                Speed
          VLAN                                                               (Mb/s)
--------------------------------------------------------------------------------
1/1/1     11      trunk  1GbT          yes     up                            1000
1/1/2     11      access 1GbT          yes     down    Waiting for link      --
1/1/3     1       access 1GbT          yes     down    Waiting for link      --
```

Note that the port is in Trunk mode and the native vlan is VLAN 11 as specified in the Role profile. Now checking the PoE priority.

```
6300-1# sh power-over-ethernet  brief

  Member 1 Power Status
    Available: 370.00 W  Reserved: 4.34 W  Remaining: 365.66 W
    Always-on PoE Enabled:1/1

PoE      Pwr Power    Pre-std Alloc PSE Pwr PD Pwr PoE Port     PD     Cls Type
Port     Ena Priority Detect  Act   Rsrvd   Draw   Status       Sign
-------- --- -------- ------- ----- ------- ------ ------------ ------ --- ----
1/1/1    Yes high     Off     lldp  4.3 W   4.2 W  delivering*  N/A    4   2
1/1/2    Yes low      Off     usage 0.0 W   0.0 W  searching    N/A    N/A N/A
1/1/3    Yes low      Off     usage 0.0 W   0.0 W  searching    N/A    N/A N/A
```

And the QoS DSCP trust.

```
6300-1# sh int 1/1/1

Interface 1/1/1 is up
 Admin state is up
 Link transitions: 43
 Description:
 Hardware: Ethernet, MAC Address: 88:3a:30:ad:66:67
 MTU 1500
 Type 1GbT
 Full-duplex
 qos trust dscp
 Speed 1000 Mb/s
 Auto-negotiation is on
 Flow-control: off
 Error-control: off
 MDI mode: MDI
 VLAN Mode: access
 Access VLAN: 1
 Rx
          728 packets                96364 bytes
            0 errors                     0 dropped
            0 CRC/FCS
 Tx
         2053 packets               293406 bytes
            0 errors                     0 dropped
            0 collision
6300-1#
```