Policy Based Automation Auto-vlan 11.08.09

Contents

Đào Lý Trân
01/02/2024 09:16:34

Version Information.

Version	Comments	Date	Author
0.1	Initial content	31st Aug 2020	Vijay

Feature overview.

The PBA Auto-vlan feature enables cnMatrix switch to dynamically learn the vlan id's advertised by cnPilot Ap's as part of LLDP control packet. The received LLDP control packets are first authenticated by cnMatrix and then parses the received vlan ids and allows them on the directly connected interface.

This feature is intended to support zero-touch detection of cnPilot access point on cnMatrix switch and dynamically configure the port on which the LLDP packet is received. The support for PBA Auto-vlan feature starts from cnPilot firmware version 4.1 and cnMatrix firmware release 3.1.1-r3

Functional Details about the PBA Auto-vlan.

New Cambium vendor-specific LLDP TLVs is introduced to support "pushing vlan ids from Cambium cnPilot to cnMatrix switch.

The PBA TLVs are implemented as an extension to the LLDP standard, using its flexible extension mechanism.

They are implemented as vendor-specific (Cambium OUI: 58-C1-7A) TLVs using TLV type 127 as described in the 802.1ab (LLDP) standard.

Two new TLVs have been defined:

PBA Authentication TLV – used by cnMatrix switch to export current authentication-related data and settings for use by attached cnPilot devices

PBA Device Settings TLV – used by cnPilot devices leveraging PBA to export required PBA device settings like the vlan id's to cnMatrix.

By default, the cnMatrix regularly generates LLDP authentication TLV on all the ports. The below criteria decide whether the LLDP PBA Authentication TLV is included in the LLDP packet generated by cnMatrix switch or not.

- Enable/Disable Port operational status
- Enabled/Disabled PBA authentication TLV setting on the port . On port execute "no lldp pba-tlv-select authentication"
- Enabled/Disabled Auto-Attach policy globally. Execute "no auto-attach". TLV transmission is stopped on all ports when PBA is disabled globally.

Upon receipt of this LLDP authentication tlv, cnPilot AP responds by sending Device setting tlv (which basically includes the list of vlan ids allowed on the trunk interface of the AP). The expectation is the native vlan on the AP's ethernet interface to be untagged. However, when AP Ethernet is in Trunk Mode with Native VLAN Tagged, then Native VLAN ID must be present in 'Allowed vlans on the interface so that it is allowed by the switch on the port.

On cnPilot AP, PBA device setting TLV is included in LLDP packet if the ethernet port is in trunk mode. It is not generated if it is in Access mode. LLDP is enabled by default globally on the cnPilot AP. The cnMatrix switch authenticates the received LLDP

packet from the cnPilot AP . From the device setting tlv, the switch reads the component (VLAN list, state flags) and creates a dynamic policy that is applied to the port on which the tlv was received.

The policy remains in effect until the LLDP port status changes (e.g., downstream neighbor LLDP data expires, PBA disabled on the port, link-down event), the policy data being pushed by the downstream neighbor changes (e.g., the VLAN list is updated) or a higher precedence PBA is determined to be applicable to the port.

Functional Details about PBA TLV extension.

Cambium PBA Authentication tlv

- This is Proprietary tlv generated by cnMatrix to convey authentication related data and setting. If this tlv is included in the LLDP packet, then it notifies the cnPilot devices that PBA based data path configuration is supported by the cnMatrix. If the tlv is absent, then this feature is not supported.
- The PBA Authentication TLV exports current authentication-related settings and data that is required to support secure communication between the device generating authenticated PBA TLVs and cnMatrix. It sends the following information in the tlv.
    - Source mac address: mac address of the device generating the tlv
    - Authentication state flag:
        - Flag = 1 : indicates PBA authentication is enabled. The device setting tlv received on this port in ingress direction will be authenticated before processing. If the authentication fails, the packet will be dropped, and no policy will be applied.
        - Flag= 0 : indicates the LLDP packed will not authenticated when processing the tlv.
    - Authentication challenge:
- The cnPilot uses this information when connecting to cnMatrix to leverage PBA functionality and automatically configure datapath characteristics (e.g., VLAN settings) in a secure communication mode.

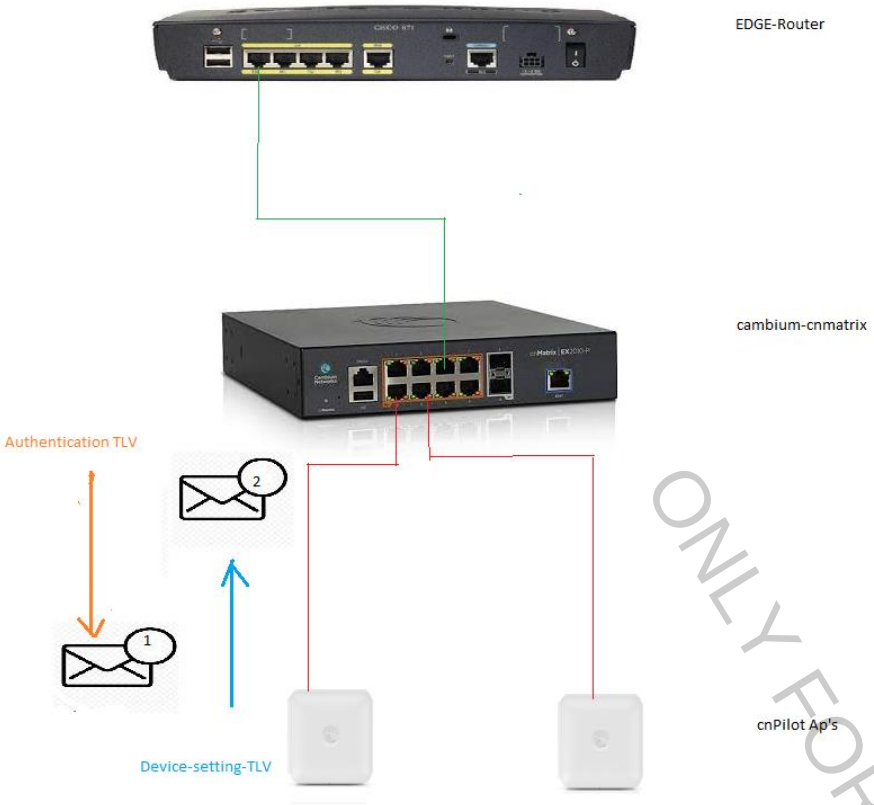
Cambium PBA Device setting tlv

- This proprietary tlv is generated by the cnPilot Ap's to update PBA enabled uplink switch about the interface configuration requirement.
- It is only generated following the receipt of a PBA Authentication TLV on the interface.
- PBA Device Settings TLV data integrity and source validation is supported using the HMAC-SHA256 message authentication algorithm. The HMAC-SHA256 generated digest size is 32 octets and the PBA Device Settings TLV includes a field to support the digest exchange between source and destination parties. Symmetric (shared) private keys are used for digest generation.
- The Digest is computed by passing the below data to the HMAC-SHA256.
    - Authentication challenge value: received from most recent incoming lldp packet from switch
    - Source mac address: MAC address of the device formulating the PBA Device Settings TLV
    - Destination mac address: derived from the Source MAC address from the most recently received PBA Authentication TLV
    - Port-id: – derived from the value of the LLDP standard (mandatory) Port ID TLV exported by the upstream cnMatrix device
- This data, along with the message authentication key, is passed through the standard HMAC-SHA256 algorithm to produce the associated message digest. The digest is then placed in the HMAC-SHA256 Digest field in the TLV prior to transmission. Upon receipt, the digest is again computed, and the resulting digest is compared against the received digest. If the received digest is the same as the newly computed digest, the TLV is considered authentic and processing can commence. If the comparison fails, the TLV is discarded and processing is terminated.
- PBA Device Settings TLV authentication can be bypassed to support Cambium devices that do not support the required authentication procedure. Disabling PBA message authentication means that PBA Device Settings TLV authentication is not performed.
- The primary use of the PBA Device Settings TLV is to pass desired VLAN settings from the source to the destination device to facilitate automatic configuration of datapath settings. This effectively pushes policy action data from the source downstream device to the destination upstream device. Settings are applied to the port through which the TLV was received (i.e., the ingress port). The following VLAN settings can be specified.

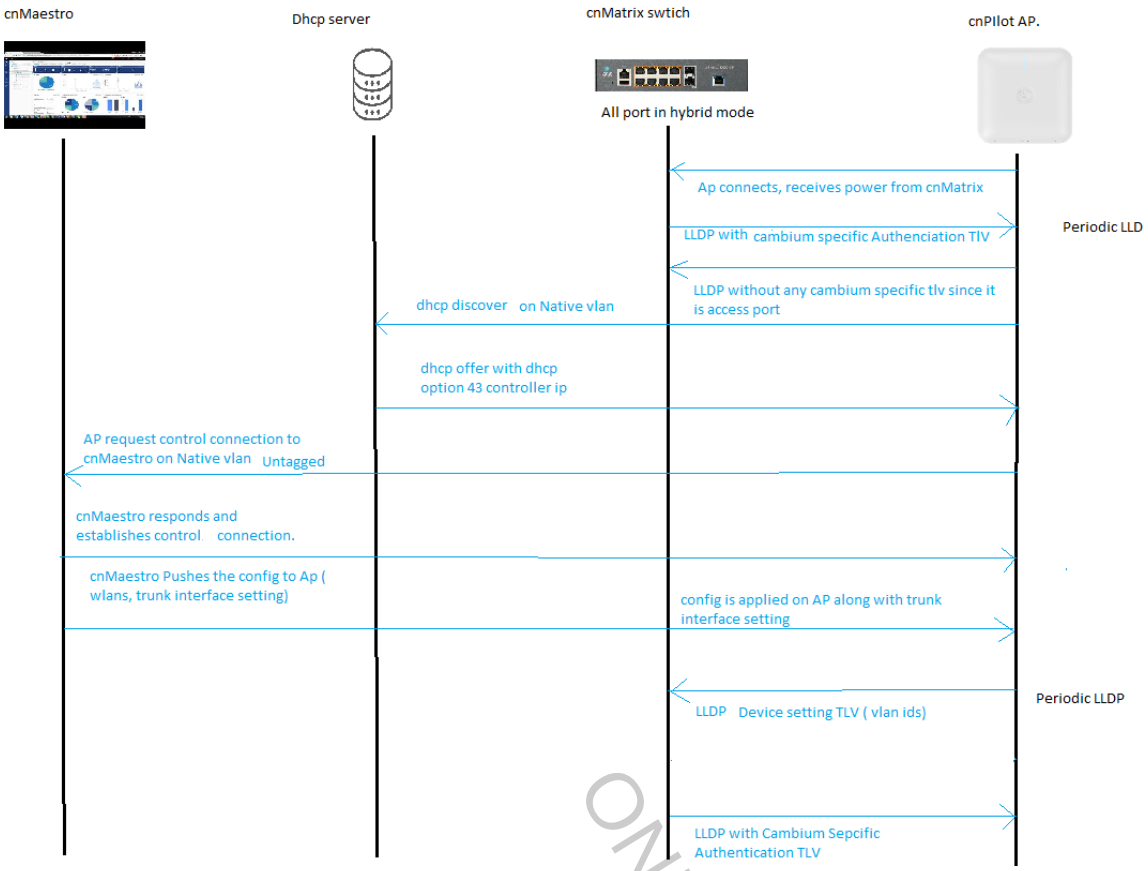
- Native VLAN – native vlan is always send as “0”. This is to avoid cnMatrix from updating the port based on received tlv from cnPilot.

- VLAN List – identifies a list of VLANs that are to be created and applied to the ingress port of the switch. The VLAN list specified is either comma separated or range (5-10). A maximum of 20 VLANs may be specified on the ethernet port.

Toplogy diagram



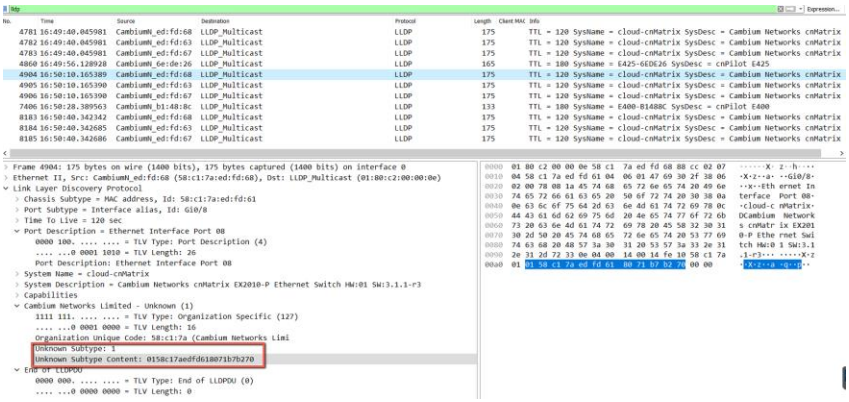
LLDP Work Flow.



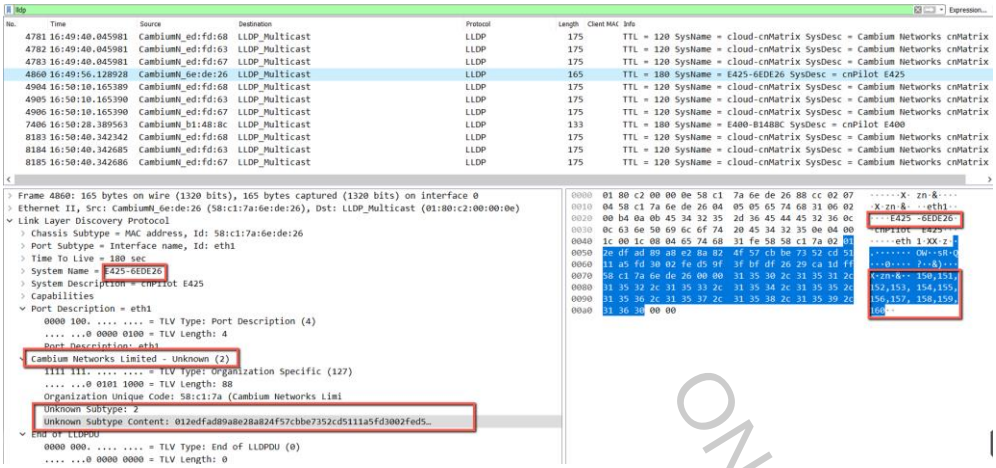
LLDP packet capture

LLDP packet originated from cnMatrix switch port (Hybrid mode)

It has authentication TLV

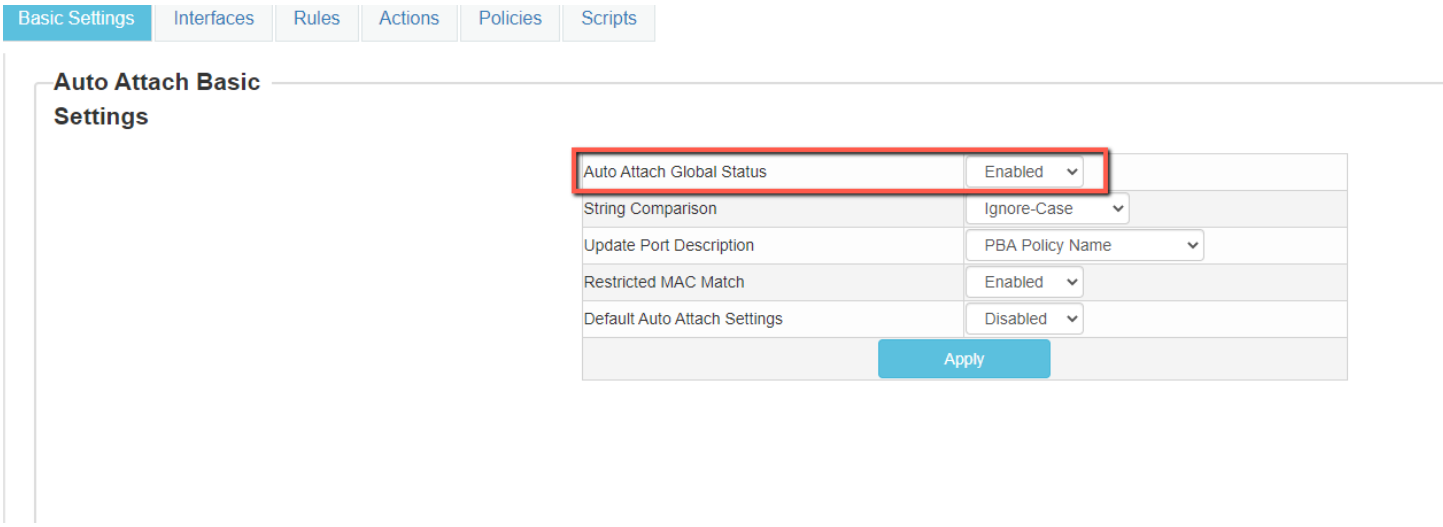


LLDP packet originated from cnPIlot AP. It has the device setting TLV.



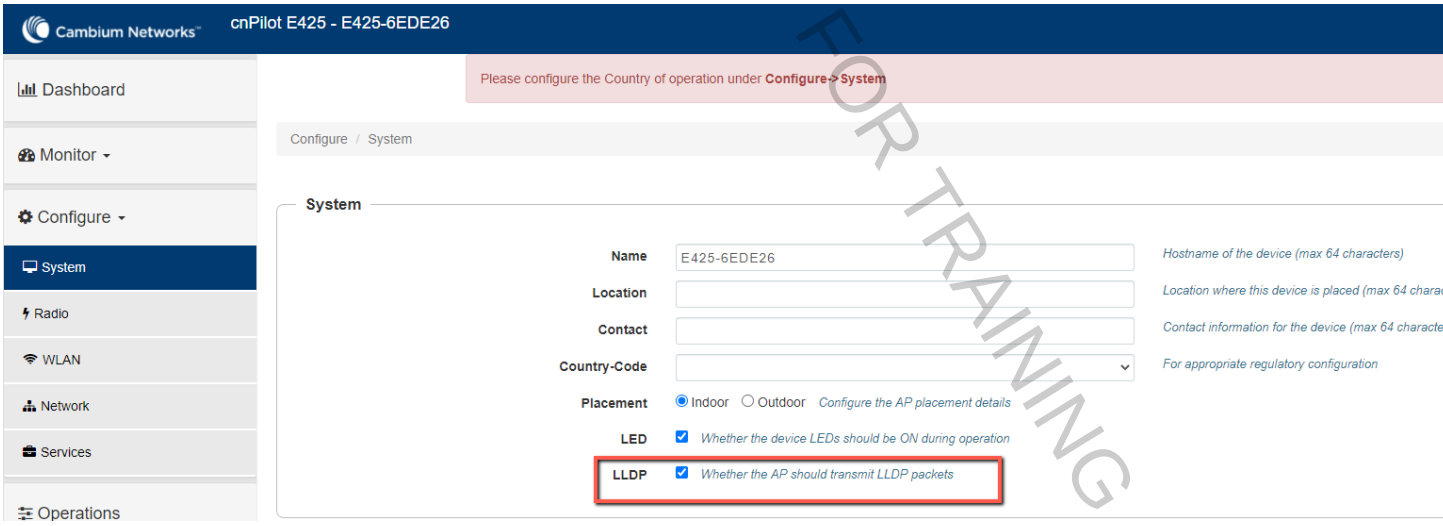
Configuration on cnMatrix switch

By default, Auto-Attach policy is enabled by default on cnMatrix Switch.



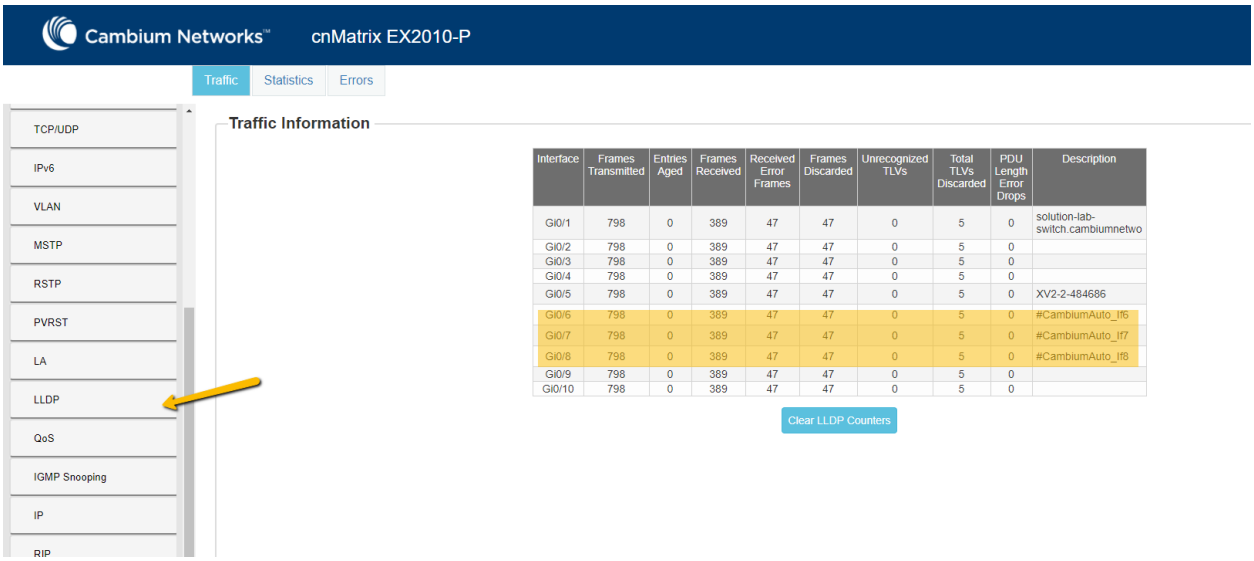
Configuration on cnPilot Access point.

LLDP is enabled by default on cnPilot AP.



.

Stats command on cnMatrix switch



To check the LLDP neighbor's

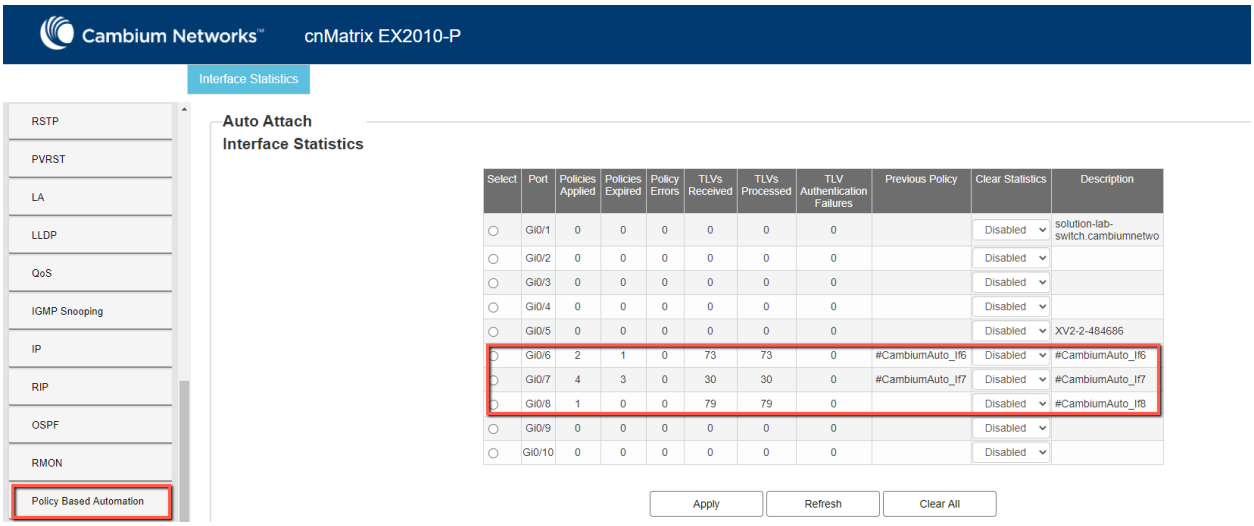
```
cloud-cnMatrix# show lldp neighbors

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID            Local Intf     Hold-time   Capability      Port Id
----------            ----------     ---------   ----------      -------
f8:0b:cb:98:a5:00     Gi0/1          120         B,R             Gi1/0/22
XV2-2-484686          Gi0/5          480         B,W,R,S         bc:e6:7c:48:46:86
58:c1:7a:6e:de:26     Gi0/7          180         B,W,R           eth1
00:04:56:b1:48:8c     Gi0/8          180         B,W,R           eth1
00:04:56:95:98:28     Gi0/6          180         B,W,R           eth1

Total Entries Displayed : 5
cloud-cnMatrix#
```

To check the vlan's learned from LLDP neighbors

```
cloud-cnMatrix#
cloud-cnMatrix# show lldp neighbors gigabitethernet 0/6 detail

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other


>>>> Local Interface : Gi0/6 <<<<

Chassis Id SubType              : Mac Address
Chassis Id                      : 00:04:56:95:98:28
Port Id SubType                 : Interface Name
Port Id                         : eth1
Port Description                : eth1
System Name                     : E410-959828
System Desc                     : cnPilot E410
Time Remaining                  : 165 Seconds
System Capabilities Supported : B,W,R
System Capabilities Enabled   : B,W,R
Management Addresses            : Not Advertised

Extended 802.3 TLV Info

Extended 802.1 TLV Info
-Port VLAN Id                   : 0




Cambium TLV Info
PBA Device Settings TLV Info
- Version                       : 1
- Non-Zero Digest               : True
- Flags                         : 0x00
- Source MAC Address            : 00:04:56:95:98:28
- Native VLAN                   : 0
- VLAN List                     : 800,900,1000

------------------------------------------------------------

Total Entries Displayed : 1
```

```
cloud-cnMatrix#
cloud-cnMatrix# show lldp neighbors gigabitethernet 0/7 detail

Capability Codes    :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other


>>>> Local Interface : Gi0/7 <<<<

Chassis Id SubType              : Mac Address
Chassis Id                      : 58:c1:7a:6e:de:26
Port Id SubType                 : Interface Name
Port Id                         : eth1
Port Description                : eth1
System Name                     : E425-6EDE26
System Desc                     : cnPilot E425
Time Remaining                  : 155 Seconds
System Capabilities Supported : B,W,R
System Capabilities Enabled   : B,W,R
Management Addresses            : Not Advertised

Extended 802.3 TLV Info

Extended 802.1 TLV Info
-Port VLAN Id                   : 0




Cambium TLV Info
PBA Device Settings TLV Info
- Version                       : 1
- Non-Zero Digest               : True
- Flags                         : 0x00
- Source MAC Address            : 58:c1:7a:6e:de:26
- Native VLAN                   : 0
- VLAN List                     : 150,151,152,153,154,155,156,157,158,159,160

------------------------------------------------------------

Total Entries Displayed : 1
```

To view the Auto-Attach policy Attached




```
cloud-cnMatrix#
cloud-cnMatrix# show auto-attach policy

Policy Name:              #CambiumAuto_If6
Policy Precedence:        80
Policy Status:            enabled

**************************************************

Policy Name:              #CambiumAuto_If7
Policy Precedence:        80
Policy Status:            enabled

**************************************************

Policy Name:              #CambiumAuto_If8
Policy Precedence:        80
Policy Status:            enabled
```

To view the policy applied on the interface.

```
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix# show auto-attach interface

                AA        Msg Auth
Interface     Status      Status     Auth TLV   Active Policy
---------   --------    --------   --------   --------------------
Gi0/1       enabled     enabled    enabled
Gi0/2       enabled     enabled    enabled
Gi0/3       enabled     enabled    enabled
Gi0/4       enabled     enabled    enabled
Gi0/5       enabled     enabled    enabled
Gi0/6       enabled     enabled    enabled    #CambiumAuto_If6
Gi0/7       enabled     enabled    enabled    #CambiumAuto_If7
Gi0/8       enabled     enabled    enabled    #CambiumAuto_If8
Gi0/9       enabled     enabled    enabled
Gi0/10      enabled     enabled    enabled

cloud-cnMatrix#
```

To view the Auto Attach policy applied on the interface from cli.

```
cloud-cnMatrix# show auto-attach policy detail

Policy Name:              #CambiumAuto_If6
Policy Precedence:        80
Policy Status:            enabled
------
Rule Name:                n/a
Rule Type:                SYSTEM-LLDP-PUSH
Rule Device ID Data:      <Cambium Device Auto Generated Pushed Policy>
------
Action Name:              n/a
Action PVID:              n/a
Action Port Mode:         hybrid
Action VLAN List:         800,900,1000

**************************************************

Policy Name:              #CambiumAuto_If7
Policy Precedence:        80
Policy Status:            enabled
------
Rule Name:                n/a
Rule Type:                SYSTEM-LLDP-PUSH
Rule Device ID Data:      <Cambium Device Auto Generated Pushed Policy>
------
Action Name:              n/a
Action PVID:              n/a
Action Port Mode:         hybrid
Action VLAN List:         150,151,152,153,154,155,156,157,158,159,160

**************************************************

Policy Name:              #CambiumAuto_If8
Policy Precedence:        80
Policy Status:            enabled
------
Rule Name:                n/a
Rule Type:                SYSTEM-LLDP-PUSH
Rule Device ID Data:      <Cambium Device Auto Generated Pushed Policy>
------
Action Name:              n/a
Action PVID:              n/a
Action Port Mode:         hybrid
Action VLAN List:         400,600,700
```

To view the status of TLV processed or Failed.

```
cloud-cnMatrix#   show auto-attach interface statistics

           Policies  Policies   Policy     TLVs      TLVs     TLV Auth
Interface  Applied   Expired    Errors   Received  Processed  Failures
---------  --------  --------  --------  --------  ---------  --------
Gi0/1      0         0         0         0         0          0
Gi0/2      0         0         0         0         0          0
Gi0/3      0         0         0         0         0          0
Gi0/4      0         0         0         0         0          0
Gi0/5      0         0         0         0         0          0
Gi0/6      2         1         0         66        66         0
Gi0/7      4         3         0         23        23         0
Gi0/8      1         0         0         72        72         0
Gi0/9      0         0         0         0         0          0
Gi0/10     0         0         0         0         0          0
```

To view the policy statics on the port.

```
cloud-cnMatrix# show auto-attach policy statistics

Name: #CambiumAuto_If6
Applied: 1          Expired: 0          Errors: 0

Interface  Applied    Expired    Errors
---------  ---------- ---------- ----------
Gi0/1      0          0          0
Gi0/2      0          0          0
Gi0/3      0          0          0
Gi0/4      0          0          0
Gi0/5      0          0          0
Gi0/6      1          0          0
Gi0/7      0          0          0
Gi0/8      0          0          0
Gi0/9      0          0          0
Gi0/10     0          0          0

**********************************************************

Name: #CambiumAuto_If7
Applied: 1          Expired: 0          Errors: 0

Interface  Applied    Expired    Errors
---------  ---------- ---------- ----------
Gi0/1      0          0          0
Gi0/2      0          0          0
Gi0/3      0          0          0
Gi0/4      0          0          0
Gi0/5      0          0          0
Gi0/6      0          0          0
Gi0/7      1          0          0
Gi0/8      0          0          0
Gi0/9      0          0          0
Gi0/10     0          0          0

**********************************************************

Name: #CambiumAuto_If8
Applied: 1          Expired: 0          Errors: 0

Interface  Applied    Expired    Errors
---------  ---------- ---------- ----------
Gi0/1      0          0          0
Gi0/2      0          0          0
Gi0/3      0          0          0
Gi0/4      0          0          0
Gi0/5      0          0          0
Gi0/6      0          0          0
Gi0/7      0          0          0
Gi0/8      1          0          0
Gi0/9      0          0          0
Gi0/10     0          0          0

cloud-cnMatrix#
```

To view the LLDP counters globally.

```
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix#
cloud-cnMatrix# show lldp traffic
Total Frames Out                        : 127426
Total Tagged Frames Out                 : 0
Total Entries Aged                      : 0
Total Frames In                         : 64030
Total Frames Received In Error          : 7291
Total Frames Discarded                  : 65
Total TLVS Unrecognized                 : 0
Total TLVs Discarded                    : 7291
Total PDU length error Drops            : 0
Total LLDP-MED Frames Out               : 28830
Total LLDP-MED Frames In                : 7226
Total LLDP-MED Frames Discarded         : 0
Total LLDP-MED TLVs Discarded           : 0
Total Media Capability TLVs Discarded   : 0
Total Network Policy TLVs Discarded     : 0
Total Inventory TLVs Discarded          : 0
Total Location TLVs Discarded           : 0
Total Ex-PowerViaMDI TLVs Discarded     : 0
Med-Capability TLV Discard Reason       : Not Applicable
Nw-Policy TLV Discard Reason            : Not Applicable
Inventory TLV Discard Reason            : Not Applicable
Location-ID TLV Discard Reason          : Not Applicable
Ex-PowerViaMDI TLV Discard Reason       : Not Applicable
Total Device Settings TLVs Discarded    : 0
Total Device Settings TLVs Auth Fails   : 22
```

To change the Authentication key on cnMatrix and cnPIlot.

If the user wants to change the default shared authentication key, then can use the below cli on cnMatrix and cnPilot . Ensure it is same on both the devices, else the authentication of lldp packet will fail.

On cnPilot

```
E425-6EDE26(config)# lldp-pba-auth-key

  <ENTER>
```