cnMatrix Policy Based Automation

Using Auto Attach

Auto Attach Functional Description

Auto Attach functionality is enabled by default. Out of the box, the AA agent is ready to accept device detection and action configuration and process incoming traffic accordingly. AA operation can be disabled globally if the administrator does not want automatic port/data path conditioning based on device discovery to occur. When globally disabled, any defined AA policies are not applied to incoming traffic and AA policy data that was previously applied is cleared (i.e., dynamic AA settings are deleted and previously configured static settings are restored).

AA operation can also be controlled on a per-port basis. By default, AA is enabled on all access ports. AA operation can be disabled on an individual port if the administrator does not want automatic port/data path conditioning based on device discovery on that port to occur. When disabled, any defined AA policies are not applied to incoming traffic on the specified port and AA policy data that was previously applied is cleared (i.e., port-specific dynamic AA settings are deleted and previously configured port-specific static settings are restored).

Device Detection Rules

LLDP TLV-Based Device Detection

LLDP-capable network devices must export the mandatory core LLDP Chassis ID and Port ID TLVs. Additionally, most LLDP-capable devices also advertise the optional core LLDP TLVs Port Description, System Name and System Description TLVS. These TLVs contain string data values. AA can be configured to match this string data. If AA detects a LLDP-capable device and identification data in an AA policy is present in the target device data, AA applies the actions associated with the AA policy.

AA performs substring matching, such that the user-specified target string is searched for WITHIN the LLDP string data. The entire LLDP data string doesn't need to be matched. The user can match as little or as much data as they wish to perform very general to very specific device identification. String comparison is case-sensitive by default. The user can choose to ignore case for greater flexibility by updating the global Auto-Attach string comparison setting.

For example, Cambium APs send LLDP frames containing the System Description TLV, which specifies the product and model number in a string format, such as "**cnPilot E430W**". The user can use this data to identify cnPilot devices in general (target device ID data: "cnPilot") or specific cnPilot models (target device ID data: "cnPilot E430").

Device identification based on advertised **System Capabilities** (TLV Type 7) can also be performed. Network devices can advertise their supported and enabled capabilities: Repeater, Bridge, WLAN AP, Router, Telephone, etc. This is a more generic way to detect devices and is vendor-independent. Utilizing this mechanism, for example, an administrator can detect WLAN Access Points (APs) from different vendors with just one matching rule.

For clarity, the user specifies capabilities using capability keywords (i.e., **repeater, bridge, wlan, router, phone, docsis, station, other**) in a comma-separated list (e.g., "bridge,wlan,phone"). AA examines a device's exported enabled capabilities data and, if ANY advertised capabilities match ANY of the specified target capabilities, a policy match occurs. All of the user-specified target data (e.g., "bridge,router,wlan") doesn't need to match all of the advertised capabilities.

Continuing with the previous example, the user may want to identify all APs attached to the switch and not just cnPIlot devices. This is easily accomplished by leveraging advertised capabilities data to identify all wireless LAN devices (target device capability: "wlan").

Certain TLVs, namely the **Chassis ID** and the **Port ID** export different types of data with the type of data indicated using a TLV subtype value. Not all types of data are string-based and therefore will not support strings matches. Non-string data that is potentially useful for AA, such as MAC address and network address data, is converted to a string format to support matching.

Many devices, including cnPilot, uniquely identify themselves using MAC address data advertised through LLDP using the Chassis ID. Received MAC address data is converted to a standard format (xx:xx:xx:xx:xx:xx) for comparison purposes. A user can match Chassis ID data to target a specific device (target device ID data: “00:04:56:9a:7b:fe”) or devices from a specific vendor (target device ID data: “00:04:56” MAC OUI).

Device Detection Actions

Each AA policy identifies a set of actions that are initiated when a device matching the policy device detection criteria is discovered. One or more actions are associated with an AA policy. Actions are initiated in an all-or-none fashion, i.e., all actions are applied or none are if an issue is detected, to condition the discovered device’s ingress port/data path. Potential actions include:

- Create VLANs and assign VLANs to the device ingress port.
- Change device ingress port PVID.
- Update switch port mode (Access/Hybrid/Trunk) for device ingress port.

Actions in general are optional in that the user doesn’t need to specify a certain set of actions. Actions that are not specified indicate that the related settings are left unchanged. Administrator operations may supersede AA-associated (i.e., dynamic) actions. For example, an administrator can manually update dynamic VLAN associations or update a PVID if required. AA will not block administrator requests.

VLAN Creation and Port Association Action

The VLAN creation/port assignment action creates dynamic VLANs and assigns them to the port on which the matching device was detected. These VLAN settings are incremental, meaning that the previously statically configured VLANs will remain assigned to the device port. At this point a combination of static and dynamic VLANs may be associated with the discovered device’s ingress port.

The dynamic VLAN settings are removed and the device ingress port is left with the initial static VLAN configuration when the detected device ceases to be “present”. This detected device cleanup phase includes deletion of dynamically created VLANs that are no longer referenced. Refer to the Dynamic Settings Cleanup section for additional details.

Traffic associated with automatically created VLANs egresses the switch as tagged traffic for the initial release.

Native VLAN (PVID) Update Action

The native VLAN (PVID) update action overwrites the existing statically configured PVID setting for the detected device’s ingress port. The PVID setting is restored to the previous statically configured value during the detected device cleanup phase.

This action is tightly coupled with the aforementioned VLAN update action. A PVID update can only be requested if the VLAN update action is specified and the PVID is a member of the VLAN update action set. Traffic associated with the PVID egresses the switch as tagged traffic for the initial release.

Switch Port Mode Update

The ability to update the switch port mode (Access/Hybrid/Trunk) based on device discovery is available.

Attention: Updating the switch port mode is a static operation for release 2.0.1, meaning that the switch port mode remains in effect after the detected device is no longer present.

For the initial release, the only accepted setting for this action is Hybrid switch port mode.

Auto Attach Policy Definition

A policy is an association of device identification criteria and actions. A policy is comprised of:

- Policy name: used for policy identification.
- Policy match data: one rule identifying device match criteria is associated with a policy. Rule data can be specified directly in the policy or indirectly through the rule table (using the rule name).
- Action data: multiple actions can be initiated when a policy match occurs. All policy actions are performed or none are if an issue is detected during action execution. Limited action data can be specified directly in the policy or indirectly through the action table (using the action name).
- Policy precedence: an optional precedence (1..100, with 1 being the highest and 100 being the lowest precedence) is provided by the administrator to address the issue of multiple policies matching the same device. All policies with the same precedence are applied in the order they were defined. A default precedence (50) is used if one is not provided during policy definition.
- Administrative status: a policy can be enabled or disabled by the administrator. A policy is enabled by default.

A policy can be created, deleted and displayed from the management interfaces. Policy rule (match) and action (set) criteria can't be modified (i.e., delete/create operations are required) but the policy status (enable/disable) and precedence of an existing policy can be modified. Rule and action table data must be defined to be referenced in a policy and can't be deleted when referenced. Policies associated with a interface (i.e., an active policy) can't be deleted. Policy data, as well as rule and action table data, is persistent (saved in NVRAM) and is restored following a device reset.

Note: AA policies are applicable to all network access ports. The Out Of Band (OOB) port doesn't support AA operations.

Dynamic Settings Cleanup

AA operation updates configuration settings based on actions defined through an AA policy. Some actions are incremental (e.g., VLAN creation/assignment) while others overwrite the current statically configured settings (e.g., PVID update, egress tagging mode update, default port QoS setting). All dynamic AA settings are cleared, with the previously configured static settings restored, when the detected device is no longer deemed "present".

Dynamic settings cleanup on the discovered devices port is triggered in the following scenarios:

- Link down event on device ingress port.
- LLDP neighbor data expiration on device ingress port. This can be triggered by LLDP traffic stopping for a period of time.
- LLDP neighbor data change on device ingress port. This can be triggered by administratively configured LLDP data (e.g., System Name) being changed.
- System reboot. All settings applied by Auto Attach are dynamic, i.e. not saved in NVRAM. At system reboot, the initial static settings are restored.

Auto Attach Ancillary Components

Statistics

Port-based counters are maintained for each AA policy providing statistics related to usage on a per-port basis:

- Policies Applied (device match).
- Policies Expired (LLDP timeout/neighbor data change, link down).
- Policy Errors (issues detected during policy application/expiration processing).

Logging

Log messages are generated for core AA events including:

- Global enable/disable.
- Interface enable/disable.
- Policy applied to an interface based on device detection.
- Policy cleared from an interface due to device expiration.

Auto Attach Feature Management

All AA configuration data is maintained in non-volatile storage. Configuration data is restored following a device reset. If incremental auto-save is not enabled, AA configuration data is volatile until explicitly committed to non-volatile store using the appropriate CLI command.

CLI Management

Overview

CLI commands introduced in support of AA can be grouped into three buckets:

Feature Control

(Config Mode) auto-attach

(Config Mode) clear auto-attach

(Interface Config Mode) auto-attach

(Interface Config Mode) clear auto-attach

Operational Configuration

(Config Mode) auto-attach rule

(Config Mode) auto-attach action

(Config Mode) auto-attach policy

Status Monitoring

(User EXEC Mode) show auto-attach global

(User EXEC Mode) show auto-attach interface

(User EXEC Mode) show auto-attach rule

(User EXEC Mode) show auto-attach action

(User EXEC Mode) show auto-attach policy

(User EXEC Mode) show auto-attach policy interface

(User EXEC Mode) show auto-attach policy detail

(User EXEC Mode) show auto-attach policy statistics

Global Configuration Mode

Auto Attach Global Feature Control

When AA is disabled globally, none of the AA policy matching criteria will be invoked. When disabling AA, all dynamic configuration created/updated through AA operation will be deleted/reset based on previous static values. Global AA operation is enabled by default.

```
(config)# [no] auto-attach
```

The ability to globally (and per-policy) clear AA policy statistics is also supported:

```
(config)# clear auto-attach policy statistics [policy-name]
```

AA Policy, Rule and Action Configuration

An AA policy defines a named collection of device identification criteria and actions that are performed following device discovery. An optional policy precedence to resolve multiple match issues can be specified. Simple policy enable/disable is supported as well.

Command syntax: `auto-attach policy <policy name> ([match <rule data> set <action data>] [precedence <1..100>] [enable|disable])`

where:

```
<policy name> =     string (1..20)
<rule data> =      { rule <rule name> | <rule type> <device data> }
<action data> =     { action <action name> | vlan <vlan list> [pvid <vlan>] [switch-
                    port-mode hybrid] }
<rule name> =        string (1..20)
<rule type> =        LLDP field identifiers
```

```
<device data> =     string (1..60)
<action name> =     string (1..20)
```

LLDP field identifiers:

Match Type	Description
LLDP-ANY	Match LLDP System Name, System Description and Chassis ID fields.
LLDP-CAP	Match LLDP Enabled System Capabilities flags.
LLDP-SYS-NAME	Match LLDP System Name field data.
LLDP-SYS-DESC	Match LLDP System Description field data.
LLDP-CHASSIS	Match LLDP Chassis ID field data.
LLDP-PORT	Match LLDP Port ID field data.
LLDP-PORT-DESC	Match LLDP Port Description field data.

AA policy semantics:

- All names (policy, rule, action) are limited to 1..20 characters.
- Device identification strings are limited to 1..60 characters.
- A VLAN list is comprised of 1..20 comma separated VLANs.
- Specifying a PVID update action requires a VLAN list containing the PVID VLAN be specified.
- Policies that are associated with an interface (i.e., an active policy) can't be deleted.

The 'no' form of the command supports deleting a single policy by name:

```
no auto-attach policy <policy name>
```

An AA rule defines a named tuple that specifies the rule type, which identifies where to search for device identification data, and the target device identification data. Command syntax:

```
auto-attach rule <rule name> <rule type> <device data>
```

where:

```
<rule name> =     string (1..20)
<rule type> =     LLDP field identifier
<device data> =   string (1..60)
```

AA rule semantics:

- Rule name limited to 1..20 printable ASCII characters. Must be unique.
- Device identification string limited to 1..60 printable ASCII characters.
- Rules that are referenced by a policy can't be deleted.

The ‘no’ form of the command supports deleting a single rule by name:

```
no auto-attach rule <rule name>
```

An AA action defines a named set of action criteria. Command syntax:

```
auto-attach action <action name> ( [vlan <vlan list>] [pvid <vlan>] [switch-port-mode
hybrid] )

where

<action name> = string (1..20)
```

AA action semantics:

- Action name limited to 1..20 characters.
- A VLAN list is comprised of 1..20 comma separated VLANs.
- Specifying a PVID update action requires a VLAN list containing the PVID VLAN be specified.
- Actions that are referenced by a policy can’t be deleted.

The ‘no’ form of the command supports deleting a single action by name:

```
no auto-attach action <action name>
```

Examples:

- Create a rule matching all devices that advertise bridging or wireless LAN capabilities:

```
cnMatrix(config)# auto-attach rule “Bridge_WLANs” LLDP-CAP bridge,wlan
```

- Create a rule to identify devices with “AXIS” in the LLDP System Description field:

```
cnMatrix(config)# auto-attach rule “AXIS_Cameras” LLDP-SYS-DESC AXIS
```

- Create a rule to identify devices with a Cambium MAC address prefix:

```
cnMatrix(config)# auto-attach rule “Cambium OUI” LLDP-CHASSIS “00:04:56”
```

- Create a rule targeting ‘cnPilot’ identifier in System Name, System Description or Chassis ID field:

```
cnMatrix(config)# auto-attach rule cnPilots LLDP-ANY cnPilot
```

- Create an action creating VLANs and updating the native VLAN:

```
cnMatrix(config)# auto-attach action “Surveillance Data Path”

vlan 20,21,22 pvid 21
```

- Configure a policy to identify devices that advertise wireless LAN capabilities and update VLAN, native VLAN and switchport mode on the port through which the device is detected. Policy is enabled with default precedence:

```
cnMatrix(config)# auto-attach policy “APs” match LLDP-CAP “wlan”

set vlan 10,11,12 pvid 12 switch-port-mode hybrid
```

- Configure a policy to identify Cambium cnPilot devices and update VLAN data on the port through which the device is detected. Policy is disabled and given a high evaluation precedence:

```
cnMatrix(config)# auto-attach policy “Cambium APs” match LLDP-ANY “cnPilot”

set vlan 100,101,102 precedence 5 disable
```

- Configure a policy to identify video surveillance gear installed in the warehouse and to segment traffic generated by the equipment to the appropriate VLANs. Predefined action data is referenced and a non-default precedence assigned:

```
cnMatrix(config)# auto-attach policy “Video Surveillance 1”

match LLDP-SYS-NAME “Warehouse Floor Video Devices”

set action “Surveillance Data Path” precedence 30
```

- Configure a policy to identify Axis surveillance cameras and to segment traffic generated by the equipment to the appropriate VLANs. Custom action data is defined and a high precedence assigned:

```
cnMatrix(config)# auto-attach policy “Video Surveillance 2”

match rule “AXIS Cameras”

set vlan 25 pvid 25 switch-port-mode hybrid precedence 10
```

Interface Configuration Mode

When AA is disabled on an interface, no AA policy comparisons occur for traffic received on the interface. When disabling AA on an interface, all dynamic configuration created/updated through AA operation on the interface will be deleted/reset based on previous static values. AA operation is enabled by default on all network access ports. AA operations are not applicable to the OOB management port.

```
(config-if)# [no] auto-attach
```

The ability to clear AA statistics on a per-interface basis is also supported:

```
(config-if)# clear auto-attach statistics
```

Display Commands

```
cnMatrix# show auto-attach global


Auto-Attach: enabled

String Comparison: case-sensitive
```

Command syntax: `show auto-attach policy [name <policy name>] [detail | interface | statistics]`

```
cnMatrix# show auto-attach policy

Policy Name:        Cambium_APs
Policy Precedence:  5
Policy Status:      Disabled

cnMatrix# show auto-attach policy detail
Policy Name:         Cambium APs
Policy Precedence:   5
Policy Status:       disabled
Rule Name:           n/a
Rule Type:           LLDP-ANY
Rule Device ID Data: cnPilot
Action Name:         n/a
Action PVID:         n/a
Action Port Mode:    n/a
Action VLAN List:    100,101,102

Policy Name:         Video Surveillance 2
Policy Precedence:   10
Policy Status:       enabled
Rule Name:           AXIS Cameras
Rule Type:            n/a
Rule Device ID Data:  n/a
Action Name:          n/a
Action PVID:          25
Action Port Mode:     hybrid
Action VLAN List:     25


cnMatrix# show auto-attach policy interface

Auto Attach Policy Interface
```

```
Interface  Policy
---------  --------------------
Gi0/5      Cambium_APs



cnMatrix# show auto-attach policy statistics

Auto Attach Policy Statistics

Name: Cambium_APs  Applied: 23     Expired: 22      Errors: 0

Interface   Applied     Expired     Errors
---------  ----------  ----------  ----------
Gi0/5      20          19          0
Gi0/8      3           3           0
```

Command syntax: `show auto-attach rule [name <rule name>]`

```
cnMatrix# show auto-attach rule

Rule Name:                 AXIS_Cameras
Rule Type:                 LLDP-SYS-DESC
Device ID Data:            AXIS

Rule Name:                 Bridge_WLANs
Rule Type:                 LLDP-CAP
Device ID Data:            bridge,wlan
```

Command syntax: `show auto-attach action [name <action name>]`

```
cnMatrix# show auto-attach action
```

```
Auto Attach Action Data

Action Name:        Surveillance-Data-Path
PVID:               21
Port Mode:                 Hybrid
VLAN List:                 20,21,22
```

Command syntax: `show auto-attach interface [<interface type> <interface ID>]`

```
cnMatrix# show auto-attach interface

Auto Attach Interface Status

             AA      Policies   Policies   Policy
Interface  Status    Applied    Expired    Errors     Active Policy
--------- --------  ---------- ---------- ---------- --------------------
Gi0/1     enabled   6          5          0          Cambium_APs
Gi0/2     enabled   0          0          0
Gi0/3     disabled  0          0          0
Gi0/4     disabled  18         18         0
```

Wizard

Device-specific policy/rule/action configuration using a single command is provided through the AA “wizard”. Initial support is provided for Cambium cnPilot devices that will configure a policy based on administrator input specified using a single CLI command:

```
auto-attach script cnPilot vlan <vlan list> pvid <vlan>

cnMatrix(config)# auto-attach script cnPilot vlan 10,11,12 pvid 12
```

which expands to:

```
cnMatrix(config)# auto-attach policy “#cnPilot-script”
                    match LLDP-ANY “cnPilot”
                    set vlan 10,11,12 pvid 12 switch-port-mode hybrid
                    precedence 50 enable
```