”Tech Con 2025- Aruba CNX-Client Provisioning using Aruba CNX”

Tech Con 2025 Abstract 645

HPE Edge;

Restoring network connectivity for PoE devices after completing Client Profiling using Aruba Next Generation Central.

Abstract

With the increasing number of IoT devices, the number of Power over Ethernet (PoE)devices connected to the networking switch is increasing day by day. This necessitates more sophisticated methods to classify and manage the devices. Aruba Next Generation Central supports predefined and user-defined tags that filter devices based on conditions related to the device profile. A matching device profile is applied on the connected switch port to appropriately route the device traffic with required access/access restrictions. Many scenarios include the device being put into a guest VLAN initially after successful mac-authentication and then further device profiling steps move them into a more privileged user role VLAN. This is achieved by sending a Disconnect Message(DM) from the Radius server. DM forces a port toggle and reauthentication of the end device. The network IP address has to be changed for the end device in this scenario since the port is moved from guest VLAN to user role VLAN. Some devices do not respond to this port drop gracefully and continue to use its previous IP address making it disconnected from the logical network. In this paper, we propose a sequence of messages and actions to fix this problem, and to restore the connectivity for the client device connected.

Problem statement

Let's take a scenario where an IoT device - a phone or a camera or a sensor or any such device - which is PoE capable, is getting connected to a network. The ethernet port of the client device is connected to a switch port which supplies power to the device. Once it boots, it starts sending discovery messages or DHCP requests which is used to authenticate the device and place the port into the guest VLAN. The device gets an IP address, allowing the device to communicate with the network with limited access.

As a preliminary authentication step, the switch port will be assigned to the guest VLAN, with limited access for the device to proceed. The DHCP requests from the device will be responded to in this stage, and an IP address will be assigned. Every piece of information from the device is being used by Next Generation Aruba Central to profile the device and assign the access policy appropriately. Packets from the device are inspected, MAC OUI is used to classify the device manufacturer and the device type by looking up the device database present in Aruba Central. Once the device is profiled completely, a more relevant user role is assigned to the port. This changes the default VLAN to a different profiled VLAN resulting in a re-assignment of IP address in the profiled VLAN. The current IP address of the default/guest VLAN will not be useful to communicate anymore. Radius server will get a notification about the profile change from Aruba Central and issue a Disconnect Message to toggle the port connected to the device. The radius server now applies the profiled user role to the switch port which results in VLAN change. This will demand the client device to send a DHCP request/renewal to obtain IP address in the new profiled VLAN. This DM message does indeed bounce the port but the device stays powered on since the ethernet cable continues delivering power to the device during port bounce. Many IoT devices, IP Phones, Cameras, and Sensors don't handle the port drop gracefully by not sending a DHCP request/renewal. This will result in such devices continuing with old IP addresses making it impossible for the devices to communicate further.

We propose a solution to this problem, by monitoring and analyzing the client information available in Aruba Central. This will either disable/enable the power to the switch port or disable/enable the port, clearing the network stack, and with proper assignment of IP address and other parameters.

Our solution

This problem is an existing issue, where our Support team is asked for a solution from customer deployments. It is observed that, once the device which is connected to the network is powered up, it is not reachable. The solution often followed is, disconnect the device by pulling the ethernet cable and connecting it back.. This assigns a more privileged user role VLAN, and better access rights. For the devices that do not respond to the Disconnect Message gracefully issued by the Radius server, the connectivity is lost as the device does not refresh its IP address.

If the device is disconnected and connected back to the same port, the first packet will classify the already profiled device into the correct VLAN, and the IP address assigned will be from the privileged user role VLAN only. This will restore the connectivity of the device to the network.

There are scenarios where the devices are not easily accessible for a technician to reconnect them to the network.

Large enterprise customer environments will have thousands of such devices which is impractical to disconnect and connect back.

The above scenarios make it difficult to follow this solution. So, we need another solution to avoid this manual intervention.

This manual intervention can be automated by toggling the Power supply to the device by disabling and enabling the PoE configuration on the port where the PoE device is connected. For PoE devices that are not drawing power from the switch port, “shut down” and “no shutdown” with a longer wait time is performed though this is not a common option for PoE devices and is hardly seen in the field.

This solution primarily focuses on scenarios where the PoE device is drawing power from the Switch port.

Aruba Next Generation Central has client information, such as VLAN and IP Address, which is the primary data used for decision-making in our solution.

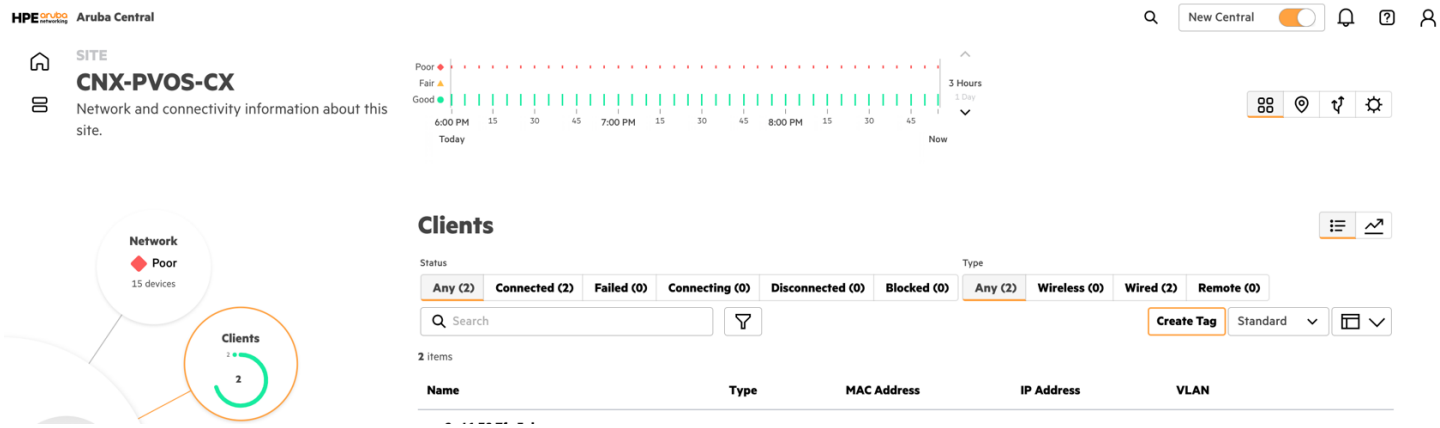


Figure-1 Aruba Next Generation (CNX) Client TAB

We will also use the switch face plate information from Aruba Central to identify whether the connected device is drawing power from the switch port.

Our solution workflow starts with identifying the authentication method as mac-authentication.

The agent deployed on Aruba Central will then record the authenticated device’s initial client IP address,

Initial client VLAN and device/client authenticated switch interface ID.

The agent waits for N sec before it compares the VLAN on the switch interface.

If the initial VLAN is different from the current VLAN, it proceeds to the device IP address comparison else the process ends.

If the initial IP address and current client IP are the same, it is evident that the device must get a new IP Address else it is isolated from the network.

The agent now verifies whether the device/client is drawing power from the switch.

If the device is drawing power from the switch, the agent takes the action to disable power (PoE) on the connected interface using an API call from Aruba Central to the switch.

After a wait time of N sec, the agent sends the enable power(PoE) using the API call.

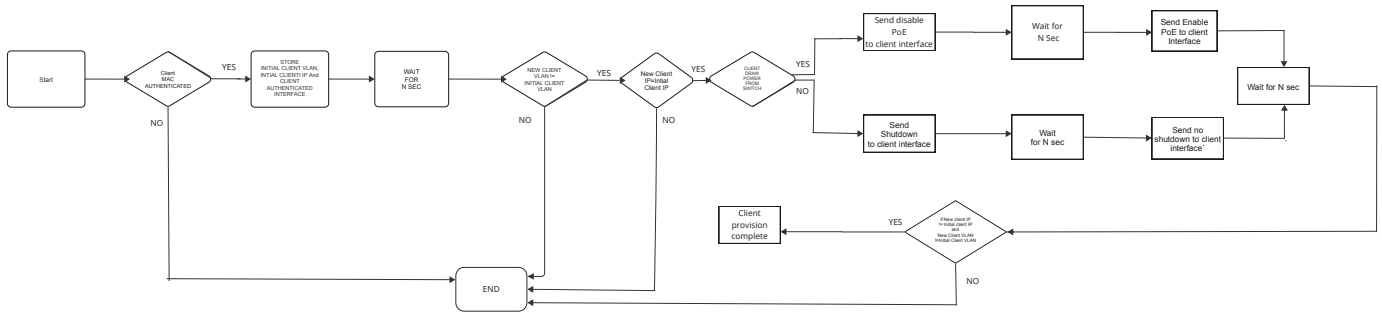
This will force the device to go for a reboot and authentication process again.

Since the device is already profiled by Aruba Central, the device will be directly put into the privileged user role VLAN.

In the next step, the agent will verify that the initial client VLAN is not the same as the current client VLAN and initial client IP address is not the same as the current client IP address.

If the above condition is met, device/client provisioning is successful, and the device will be able to access the network.

FLOW DIAGRAM



On the other hand, though it is not in the scope of our solution, if the device is not drawing power from the switch agent will send shutdown to the port using API and wait for N sec.

Sending no shutdown to enable the port depends on the wait time required which may be defined by capturing the

Device/client DHCP lease time.

In the next step, the agent will verify that the initial client VLAN is not the same as the current client VLAN and initial client IP address is not the same as the current client IP address.

Device/client provisioning is complete if the above condition is met.

Evidence the solution works

Aruba CNX is in the development phase, and we have validated API testing mentioned in the workflow manually.

All information required to follow the workflow is currently available in CNX. We need to develop the agent to follow the workflow that we tested manually to automate our solution.

Competitive approaches

This solution is unique for HPE Aruba Central Next Generation(CNX), and our competitors rely on Radius Disconnect Message(DM) to achieve the profiling issue which is not an ideal solution as we have experienced from customer-filed defects.

Current status

Validated API testing manually by following the above workflow.

Our manual testing was successful by analyzing device/client data and switch data during the testing.

Next steps

The next step is to develop the Aruba Central agent and automate the workflow by collaborating with CNX development team to demonstrate PoC for our solution.

API testing References

Customer defect CN-262530

This ticket is filed against Aruba Central CloudAuth Radius server , but not dependent on specific Radius server.

https://jira.arubanetworks.com/browse/CN-262530