Hewlett Packard
Enterprise

Silent Client Support – AOS-CX

Port Access Security Client Types

Probability of being Silent Client

Device Profile

- Device profile is widely used for APs/ VOIP Phones / Switches for faster onboarding without need for radius infrastructure . These clients send LLDP/CDP packets in regular interval.

802.1x

- Majority of 802.1x clients will be chatty as they perform 802.1x control packet exchange and after successful 802.1x authentication they will start dhcp/dns/arp data packet exchange. Few static clients could be silent.

MAC Auth

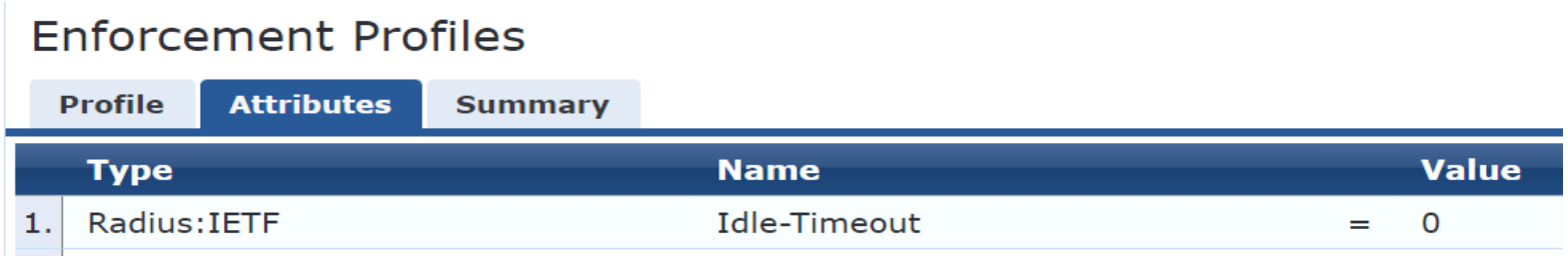
- Mac Authentication is used for onboarding following clients
  - Supplicant Capable – to download the supplicant software . Mac Auth is used for only initial onboarding, later they will be performing 802.1x. So typically, chatty.
  - Non Supplicant Capable – IOT Devices are generally silent in nature.

Client-inactivity/idle timeout

- **Use case** – Ideal for already onboarded clients and clients will not be ageing out until this timer expires because of inactivity.
- **Recommended for Client Types** - MAC Auth and 802.1x.
- **Configuration** – Can be applied per client level using LUR/DUR or Radius IETF attribute.
  - LUR/DUR – client-inactivity-timeout
    – Supported values :- 300-4294967295s and none (never ageout)

```
6300-VSF(config)# port-access role silent
6300-VSF(config-pa-role)# client-inactivity timeout
  <300-4294967295>  Set client inactivity timeout value in seconds.
  none              Configure to not to remove the client due to inactivity.
```

  - Radius IETF – idle-timeout
    – Supported values :- 300-4294967295s and 0 (never ageout)



- **Caveats**
  - Timer restarts after client interface/session toggle and switch reboot.
  - Advisable to refrain the use of “never ageout” value in deployments using intermediate L1 devices . As in such cases the client will never ageout even after being unplugged from the intermediate L1 device. Results in withholding of the client limit and policy resources.

Allow-Flood-Traffic

- **Use case** – To help silent clients to trigger authentication request and onboard successfully. By default, port-access security enabled port will be in blocked state (Ingress and Egress) until successful client authentication. Enabling this feature opens the egress direction of the port-access security enabled port. So the broadcast/wol packets in the associated port vlan can wake up the silent end clients and their response will trigger fresh authentication. After successful onboarding, client can be applied with client-inactivity-timeout/idle-timeout using role assignment.
- **Recommended for Client Types**- Interface level configuration , hence need to be enabled on possible silent client connected ports.
- **Configuration** -

```
6300-VSF(config)# interface 1/1/1
6300-VSF(config-if)# port-access allow-flood-traffic enable
6300-VSF(config-if)# exit
```

- **Caveat**
  - Custom Port vlan membership , as the admin must configure the right broadcast/wol server vlan in the silent end client connected ports even before authentication.

```
6300-VSF(config)# interface 1/1/1
6300-VSF(config-if)# vlan access <>
6300-VSF(config-if)# exit
```

  - Not suitable for colorless port deployments.

Client IP Tracker

- **Use Case** – Ideal for already onboarded clients , as this feature can perform ARP Probe if there are no packets received from the silent clients.
- **Recommended for Client Types** – All client types

```
6300-VSF(config)# client track ip
6300-VSF(config)# client track ip all-vlans
Or
6300-VSF(config)# vlan 2
6300-VSF(config-vlan-2)# client track ip
6300-VSF(config-vlan-2)# exit

6300-VSF(config)# interface 1/1/1
6300-VSF(config-if)#client track ip update-interval <60-28000s>(Default: 1800)
6300-VSF(config-if)#exit
```

- **Workflow** –
  - First , client IP must be learnt once in switch.

```
6300-VSF(config)# show client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------
 00:50:56:9e:0a:e7         1/1/1            9                192.168.9.30
```

  - After the configured update interval , switch will start sniffing for packets from the client mac-address for 15s.
  - If there are no packets received after 15s, it will start the ARP probe – 3 times with each 3s delay
  - Client will respond back to arp probe and it will not age out.

UBT Silent Client – “wol-enable vlan”

- **Use case** – Ideal for UBT Clients in vlan-extended-mode (UBT 1.0). Allows user-based tunnels to stay initiated for devices that may go silent and not send out any packets. To onboard new clients, “port-access allow-flood-traffic” feature must be used in conjunction
- **Recommended for Client Types** – 802.1x and Mac Auth UBT Clients
- **Configuration**

```
6300-VSF(config)# ubt zone zone1 vrf default
6300-VSF(config-ubt-zone1)# wol-enable vlan 10,20
6300-VSF(config-ubt-zone1)# exit
```

- **Workflow** –
  - Using the Wake-on-LAN VLAN feature, you can configure silent client VLANs.
  - This VLAN information will be shared by the switch to the gateway through a new PAPI message after the initial switch bootstrap message handshake is completed and the multicast tunnel is created.
  - Then, the gateway will add this VLAN list to its multicast tunnel so that BUM traffic on these VLANs is allowed from the gateway to be sent to the switch through the existing broadcast/multicast tunnel. This VLAN list is shared with both active and standby SACs.

Additional Resources

Security Guide - https://www.arubanetworks.com/techdocs/AOS-CX/10.13/PDF/security_6200-6300-6400.pdf

UBT Silent Client TOI Session - https://www.youtube.com/watch?v=_QXYN27KRgE

Thank You