technical white paper

MAC Pinning

arubaos-switch version 16.05

purpose

The ArubaOS-Switch MAC Pinning feature overrides the traditional port-access log-off period functionality of Local Mac Authentication (LMA)/MAC-based authentication methods. With MAC Pinning feature enabled, LMA/MAC-based authenticated clients will remain authenticated in the switch even during the client’s inactivity throughout the log-off period. LMA based client’s MAC address is configured manually in the switch whereas MAC-based authenticated client’s MAC address is dynamically obtained from the RADIUS server. This new option pins the authenticated mac addresses permanently even when some clients are quiet (sleep mode) throughout the log-off period expiry.

During port flaps/switch reboots, the mac-pinned based authenticated client entries are retained by the switch, and the authentication services for those clients are restored. MAC Pinning feature is only supported for Local MAC and MAC-based authenticated client. Figure 1 shows the typical implementation of MAC Pinning in ArubaOS-Switches.


Figure 1. MAC Pinning example diagram

As shown in figure 1, the edge clients are pinned to the MAC Table permanently to ensure connectivity to the network. This feature is mainly implemented for legacy devices. Administrators can configure either Local MAC or MAC-based MAC Pinning in their ArubaOS-Switch environment as follow.

[no] aaa port-access local-mac < PORT-LIST> mac-pin

[no] aaa port-access mac-based < PORT-LIST> mac-pin

configuration

MAC Pinning can be simply configured in ArubaOS-Switch with the commands shown above; however, in addition to those commands, there is a need for RADIUS Server to be configured in order to authenticate the devices in the first place. The RADIUS server configuration is shown in the figure 2 below.

|  |
| --- |
| radius-server host 10.5.8.17 key "admin"radius-server host 10.5.8.17 dyn-authorizationradius-server host 10.5.8.17 time-window 0aaa authentication port-access eap-radiusaaa port-access authenticator active |

Figure 2. RADIUS server configuration

Figure 2 shows the typical configuration of RADIUS server in ArubaOS-Switch. Figure 3 shows the MAC Pinning configuration for this scenario.

|  |
| --- |
| aaa port-access mac-based 9aaa port-access mac-based 9 mac-pin |

Figure 3. MAC Pinning configuration

Figure 3 commands indicates that interface number 9 of the switch is configured for MAC Pinning. In addition, the top command of figure 3 indicates the authentication type for the switch is mac-based rather than 802.1X. The next figure 4 shows the output of the switch when the client loses connectivity with the RADIUS Server.

|  |
| --- |
|  |

Figure 4. MAC Pinning output example

Figure 4 above shows the output of the client connected on interface 9 when that client connectivity with the RADIUS server is disable. As shown above, the client still remains authenticated on the network. This exercise proves that with MAC Pinning configuration for legacy devices in ArubaOS-Switch, the devices always maintains its connectivity on the network.

**SUPPORTED PLATFORMS**

MAC Pinning is supported on the following ArubaOS-Switch software version 16.05.

* Aruba 2920 Series Switch
* Aruba 2530 Series Switch
* Aruba 2930M/F Series Switch
* Aruba 3810M Series Switch
* Aruba 5400R Series Switch