technical white paper

per-port initial role

arubaos-switch version 16.05

purpose

ArubaOS-Switches supports initial role where the clients that are rejected by radius server or clients that fails authentication due to radius unreachability will be applied with this initial role. Initial role is enabled with the configuration of user roles and a default initial role is present. Any user role can be designated as initial role using existing CLI commands. Initial role can be tweaked to provide limited access to download supplicant or be used for Wired Guest access solution.

This new feature provides configuration command to add an initial role per port. Per-Port Initial Role when configured will override the default initial role or the global user role that is designated as initial role.

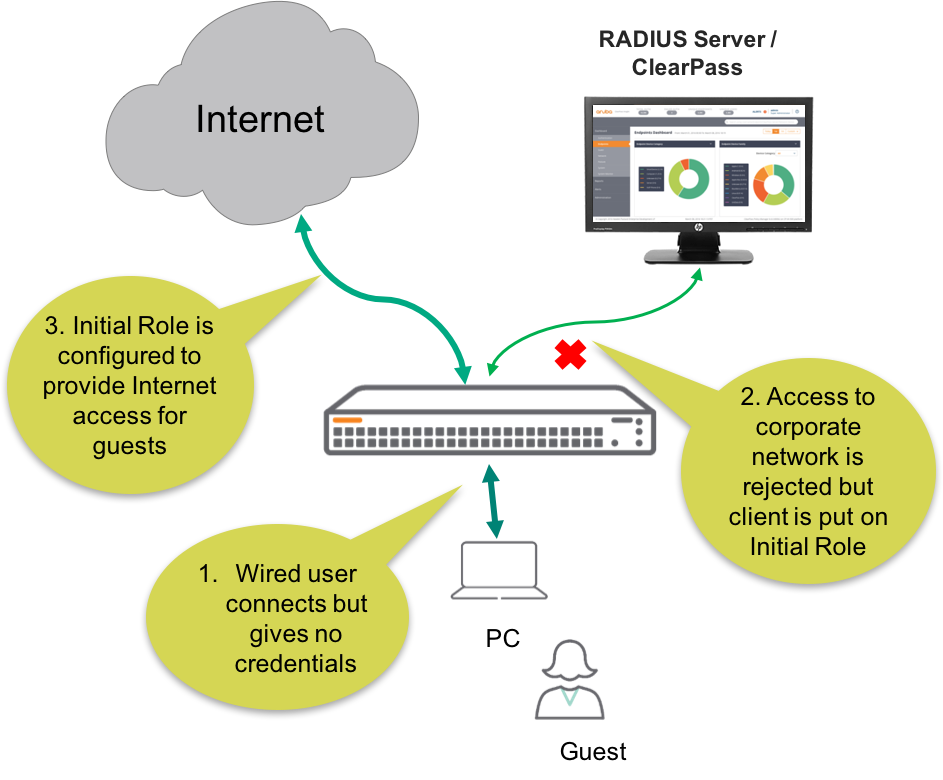


Figure 1. Per-Port Initial Role Example

Figure 1 shows the typical implementation of Per-Port Initial Role in ArubaOS-Switches. In this scenario, the guest is assigned an untagged Per-Port Initial Role VLAN to allow limited network access.

Administrators can configure Per-Port Initial Role in their ArubaOS-Switch environment as follow.

[no] aaa port-access <PORT-LIST> initial-role <ROLE-NAME>

Configuration

Although there is no need to configure RADIUS Server for this feature, because the Per-Port Initial Role can be implemented in ArubaOS-Switch for temporary clients (guest clients) which requires no RADIUS authentication. However, the typical RADIUS server configuration for ArubaOS-Switch is shown in figure 2 below.

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

Figure 2. RADIUS server configuration

In this feature guide example, the RADIUS server is not configured, because the test is to verify whether the guest client can obtain network access through the initial role configured in this example on a specified port. For this feature guide, there are two user-roles configured in ArubaOS-Switch, and they are the “Wired-User” user-role for the clients which has the RADIUS authentication enabled and provide valid credentials, and secondly, the “Guest” user-role for the guest clients who do not provide valid credentials to obtain network access. Figure 3 shows the Per-Port Initial Role configuration executed on ArubaOS-Switch to test this feature.

|  |
| --- |
| aaa authorization user-role name "Guest"  vlan-id 150  exit  aaa authorization user-role name "Wired-User"  vlan-id 200  exit  aaa authorization user-role enable  aaa authentication port-access eap-radius  aaa port-access authenticator 9  aaa port-access authenticator 9 client-limit 5  aaa port-access authenticator active  aaa port-access 9 initial-role "Guest" |

Figure 3. Per-Port Initial Role configuration

As shown in figure 3, the two user-roles are configured to separate the authenticated and non-authenticated clients on a separate VLAN. In addition, the command highlighted in green above is for configuring the Per-Port Initial Role in ArubaOS-Switch. As per the configuration commands above, the client (Windows 7) connected to interface 9 of the switch is configured for Per-Port Initial Role. The next CLI output shows the port access client status for an interface of the switch configured for Per-Port Initial Role.

Aruba-3810M-24G-PoEP-1-slot(config)# show port-access clients

Port Access Client Status

Port Client Name MAC Address IP Address User Role Type VLAN

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

9 admin 705ab6-aee46c n/a Guest 8021X 150

Aruba-3810M-24G-PoEP-1-slot(config)# show port-a cli de

Port Access Client Status Detail

Client Base Details :

Port : 9 Authentication Type : 802.1x

Client Status : initial role Session Time : 89 seconds

Client name : admin Session Timeout : 0 seconds

MAC Address : 705ab6-aee46c

IP : n/a

User Role Information

Name : Guest

Type : local

Reauthentication Period (seconds) : 0

Untagged VLAN : 150

Tagged VLANs :

Captive Portal Profile :

Policy :

Tunnelednode Server Redirect : Disabled

Secondary Role Name :

As shown above, the client is under Untagged VLAN 150 as configured under “Guest” user-role in figure 3. In addition, the client status is “Initial Role”, because the client is authenticated on the network through an Initial Role to allow limited access on the network.

**SUPPORTED PLATFORMS**

Configuration restore without reboot feature is supported on the following ArubaOS-Switch software version 16.05.

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