technical white paper

Open authentication role

arubaos-switch version 16.05

purpose

Prior to ArubaOS version 16.04, ArubaOS Switches did not allow network access until the device is fully authenticated when the authentication is enabled on an interface.

The devices connected to the ArubaOS switch can be broadly divided into two categories:

1. Devices that send voice traffic i.e. IP phones.
2. Devices that send data traffic i.e. PCs, IP cameras etc.

In order to provide network connectivity to these devices connected to a port, they must be assigned a VLAN. Two new VLANs are created for OpenAuth functionality, one for voice traffic and another for data traffic. These VLANs can be configured on the switch individually or they can also be configured within a user-role, in which case, that user-role is called “OpenAuth” role. Both OpenAuth VLAN (voice and/or data) and OpenAuth user-role VLAN cannot co-exist for an interface. Initial traffic on the port is restricted only by ACLs configured for the port or for VLANs or ACLs in the user role. This feature is configurable per-port and only applies to RADIUS based authentication mechanisms.

  
Figure 1. Open Authentication Role example diagram

Figure 1 shows the typical implementation of Open Authentication Role in ArubaOS Switches. In this scenario, the phone and PC will respectively be assigned tagged and untagged Open VLAN.

Administrators can configure either one of three Open Authentication Role in their ArubaOS Switch environment as follow.

[no] aaa port-access <PORT-LIST> open-auth user-role <ROLE-NAME>

[no] aaa port-access <PORT-LIST> open-auth voice-vlan <VLAN-ID>

radius-server host 10.5.9.1 key "admin"

radius-server timeout 15

radius-server retransmit 5

[no] aaa port-access <PORT-LIST> open-auth data-vlan <VLAN-ID>

configuration

For OpenAuth, the RADIUS server configuration is needed for the client to look out for the RADIUS server (even if it is a dummy IP). In the example configuration below, the RADIUS server IP is the default gateway IP of the switch. In addition to the RADIUS server IP, the RADIUS server ‘timeout’ and ‘retransmit’ are also important part of the configuration as well, because through that it is described how long the OpenAuth is configured for the clients on ArubaOS Switch. In the example configuration below, Open Authentication Role last for 90 seconds ([timeout 15 x retransmit 5] + 15 seconds for the first time = 90 seconds) while the device request for authentication is being processed in the background. The RADIUS server related configuration is shown in figure 2 below.

|  |
| --- |
| radius-server host 10.5.9.1 key "admin"  radius-server timeout 15  radius-server retransmit 5 |

Figure 2. RADIUS server configuration

Figure 3 shows the Open Authentication Role configuration in this example.

|  |
| --- |
| aaa port-access mac-based 9  aaa port-access 9 open-auth data-vlan 100 |

Figure 3. Open Authentication Role configuration

Figure 3 commands indicates that interface number 9 of the switch is configured for Open Authentication Role. In addition, the top command of figure 3 indicates the authentication type for the switch is mac-based, because there is no 802.1X based authentication allowed in Open Authentication Role. In this example scenario, Open Authentication Role is shown with “data-vlan” configuration. The next figure 4 shows the output of the switch when the client obtains network connectivity in the absence of a RADIUS server in the network.

|  |
| --- |
|  |

Figure 4. The client obtaining network access through Open Authentication Role

Figure 4 on the previous page shows an output of a client as soon as that client attempts to connect to the network. As expected, the client receives network access through VLAN 100, as configured in the switch, without the RADIUS server interaction. This feature allows any device to obtain instant network access while that particular device is authenticating in the background. As a result, the device always has network connectivity even during the authenticating process. This same type of configuration steps can be taken for Voice-VLAN and UserRole-VLAN. This exercise proves that with Open Authentication Role enabled on ArubaOS allows devices to be on the network in the environment where there is no authentication service.

**SUPPORTED PLATFORMS**

Open Authentication Role is supported on the following ArubaOS-Switch software version 16.05.

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