technical white paper

critical authentication role

arubaos-switch version 16.05

purpose

Typical authentication features do not differentiate between an authentication failure due to a “radius-reject” and “radius-not-being-unreachable”. This feature enhancement is to support a “Critical VLAN” concept, where in a remote authentication scenario such as MAC-Auth or 802.1X starts for a client, but the authentication server is not reachable then, the client will be placed in a “Critical VLAN”.

The Critical VLAN feature can be configured as tagged (Ex. voice) or untagged (Ex. data) VLAN. For clients sending tagged or untagged traffic, this feature will put them in Critical Tagged-VLAN and Critical Untagged-VLAN respectively. This feature supports one tagged or untagged VLAN membership either through direct VLAN configuration or via user-roles. Critical Role can also be configured within a user-role, in which case, that user-role is called “Critical Role”. Therefore, when Critical-Role is configured, any client which fails authentication due to authentication server not being reachable, will be applied with the Critical-Role. This feature is configurable per-port and only applies to RADIUS based authentication mechanisms.

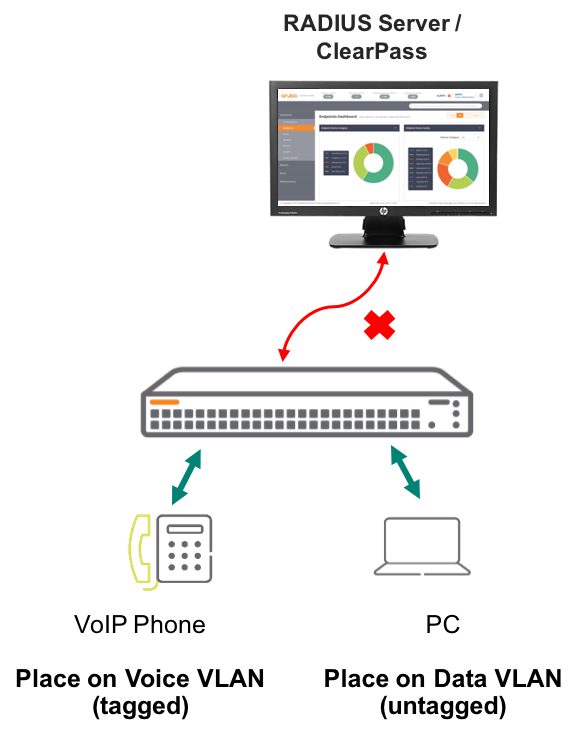
  
Figure 1. Critical Authentication Role example diagram

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

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

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

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

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

configuration

Although there is no need to configure RADIUS Server for this feature, because the Critical Authentication Role can be implemented in ArubaOS Switch as a failsafe mechanism. However, the typical RADIUS server configuration for ArubaOS Switch is shown in figure 2 below. Figure 2 RADIUS server configuration is not implemented in the switch while testing this feature.

|  |
| --- |
| 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

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

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

Figure 3. Critical Authentication Role configuration

Figure 3 commands indicates that interface number 9 of the switch is configured for Critical Authentication Role. In addition, the top command of figure 3 indicates the authentication type for the switch is mac-based rather than 802.1X. In this example scenario, Open Authentication Role is shown with “data-vlan” configuration. The next figure 4 shows the authentication status when the client link to the RADIUS server is up and running.

|  |
| --- |
|  |

Figure 4. The client and RADIUS server link is up

As shown in figure 4, the client is authenticated on the network through MAC-based authentication type. The client is currently under default untagged VLAN 1. The next figure 5 shows the output of the switch when the client loses connectivity to the RADIUS server.

|  |
| --- |
|  |

Figure 5. The client and the RADIUS server link is down

Figure 5 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. The Client Status has changed to “Critical-Auth” and the client’s VLAN has changed to Untagged VLAN 100 as shown in figure 3 of this feature guide. The same type of configuration steps can be taken for Voice-VLAN and UserRole-VLAN. This exercise proves that with Critical Authentication Role enabled on ArubaOS switch can keep any device on the network.

**SUPPORTED PLATFORMS**

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

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