Verify Radius Server Connectivity with Test AAA Radius Command

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[How The Feature Works](#)
[Command Syntax](#)
[Scenario 1. Passed Authentication Attempt](#)
[Scenario 2: Failed Authentication Attempt](#)
[Scenario 3: Communication Failed Between WLC and Radius Server](#)
[Scenario 4: Radius Fallback](#)
[Caveats](#)

Introduction

This document describes how the **test aaa radius** command on the Cisco WLC can be used to identify radius server connectivity and client authentication issues without the use of a wireless client.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Wireless LAN Controller (WLC) code 8.2 and above.

Components Used

This document is not restricted to specific software and hardware versions.

Background Information

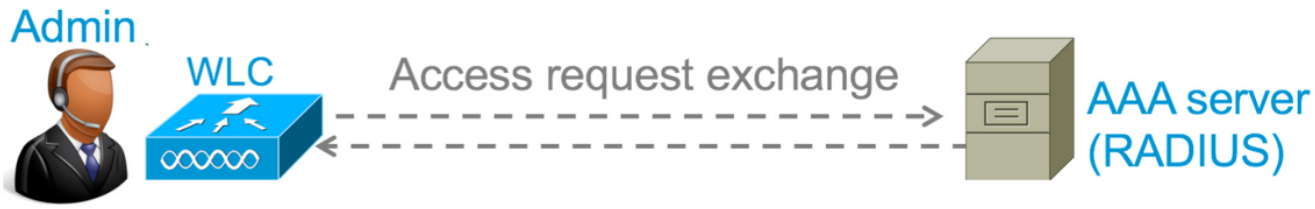
Wireless client authentication issues are one of the most challenging problems that wireless network engineers face. In order to troubleshoot this, it often requires to get hold of the problematic client, work with the end users who may not have the best knowledge of wireless networks and to collect debugs and captures. In an increasingly critical wireless network, this can cause significant downtime.

Up until now there was no easy way to identify if an authentication failure was caused by the

radius server which rejects the client, or just simply a reachability issue. The **test aaa radius** command lets you do just that. You can now remotely verify if the WLC-Radius server communication fails or if the credentials for the client results in a passed or failed authentication.

How The Feature Works

This is a basic workflow when you use the command **test aaa radius**, as shown in the image.



Step 1. The WLC sends an access request message to the radius server along with the parameters that is mentioned in the **test aaa radius** command.

For ex: **test aaa radius username admin password cisco123 wlan-id 1 apgroup default-group server-index 2**

Step 2. The radius server validates the credentials provided and provides the results of the authentication request.

Command Syntax

These parameters need to be provided to execute the command:

(Cisco Controller) > **test aaa radius username <user name> password <password> wlan-id <wlan-id> ap-group <apgroup-name> server-index <server-index>**

```
<username>                      ---> Username that you are testing.
<password>                      ---> Password that you are testing
<wlan-id>                       ---> WLAN ID of the SSID that you are testing.
<apgroup-name>  (optional)      ---> AP group name. This will be default-group if there is no AP
group configured.
<server-index>      (optional)  ---> The server index configured for the radius server that you
are trying to test. This can be found under Security > Authentication tab.
```

Scenario 1. Passed Authentication Attempt

Let's have a look at how the command works and the outputs are seen when the **test aaa radius** command results in a passed authentication. When the command is executed, WLC displays the parameters with which it sends out the access request:

```
(Cisco Controller) >test aaa radius username admin password cisco123 wlan-id 1 apgroup default-
group server-index 2
Radius Test Request
  Wlan-id..................................... 1
```

```
  ApGroup Name..................................... default-group
  Attributes                      Values
  ----------                      ------
  User-Name                       admin
  Called-Station-Id               00:00:00:00:00:00:WLC5508
  Calling-Station-Id              00:11:22:33:44:55
  Nas-Port                        0x0000000d (13)
  Nas-Ip-Address                  10.20.227.39
  NAS-Identifier                  WLC_5508
  Airespace / WLAN-Identifier     0x00000001 (1)
  User-Password                   cisco123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (81)
  Cisco / Audit-Session-Id        ad14e327000000c466191e23
  Acct-Session-Id                 56131b33/00:11:22:33:44:55/210
test radius auth request successfully sent. Execute 'test aaa show radius' for response
```

In order to view the results of the authentication request, you need to execute the command **test aaa show radius**. The command can take some time to show the output if a radius server is unreachable and the WLC needs to retry or fallback to a different radius server.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id.......................................... 1
  ApGroup Name..................................... default-group
  Server Index..................................... 2
Radius Test Response
Radius Server         Retry Status
-------------         ----- ------
10.20.227.52            1   Success
Authentication Response:
  Result Code: Success
  Attributes                      Values
  ----------                      ------
  User-Name                       admin
  Class                           CACS:rs-acs5-6-0-22/230677882/20313
  Session-Timeout                 0x0000001e (30)
  Termination-Action              0x00000000 (0)
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x00000051 (81)
```

The extremely useful aspect of this command is that it shows the attributes which are returned by the radius server. This can be redirect URL and Access Control List (ACL). For example, in the case of Central Web Authentication (CWA) or VLAN info when you use VLAN override.

> **Caution**: The username/password in the access request are sent in clear text to the radius server, so you need to use it with caution if traffic flows over an unsecured network.

Scenario 2: Failed Authentication Attempt

Let's see how the output appears when a username/password entry results in a failed authentication.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.52            1     Success
Authentication Response:
  Result Code: Authentication failed  ------>This indicates that the user authentication will
fail.
  No AVPs in Response
```

In this case, you can see that the connectivity test resulted in a 'Success', however the radius server sent an access-reject for the username/password combination used.

Scenario 3: Communication Failed Between WLC and Radius Server

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.52            1     Success
Authentication Response:
  Result Code: Authentication failed  ------>This indicates that the user authentication will
fail.
  No AVPs in Response
```

You need to wait for the WLC to finish it's retries before it displays the output. The time can vary based on the retry thresholds configured.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.52            1     Success
Authentication Response:
  Result Code: Authentication failed  ------>This indicates that the user authentication will
fail.
  No AVPs in Response
```

In the above output you can see that the WLC tried to contact the radius server 6 times and when there was no response it marked the radius server as unreachable.

Scenario 4: Radius Fallback

When you have multiple radius servers configured under the Service Set Identifier (SSID) and the

primary radius server does not respond, then the WLC tries with the secondary radius server configured. This is shown very clearly in the output where the first radius server does not respond and the WLC then tries the second radius server which responds immediately.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.52            1     Success
Authentication Response:
  Result Code: Authentication failed  ------>This indicates that the user authentication will
fail.
  No AVPs in Response
```

Caveats

- There is currently no GUI support. It is only a command that can be executed from the WLC.
- The verification is only for radius. It cannot be used for TACACS authentication.
- Flexconnect local authentication cannot be tested with this method.