Configure the RADIUS Server Fallback Feature on Wireless LAN Controllers

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[RADIUS Server Fallback Feature](#)
[Fallback Modes](#)
[Active Mode](#)
[Passive Mode](#)
[Off Mode](#)
[Configure](#)
[Configure the RADIUS Server Fallback Feature with the CLI](#)
[Configure the RADIUS Server Fallback Feature with the GUI](#)
[Verify](#)
[Troubleshoot](#)
[Related Information](#)

Introduction

This document describes how to configure the RADIUS server fallback feature with Wireless LAN Controllers (WLCs).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of the configuration of Lightweight Access Points (LAPs) and Cisco WLCs
- Basic knowledge of Control and Provisioning of Wireless Access Point Protocol (CAPWAP)
- Basic knowledge of Wireless Security Solutions

Components Used

The information in this document is based on a Cisco 5508/5520 controller.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

RADIUS Server Fallback Feature

WLC software versions earlier than 5.0 do not support the RADIUS server fallback mechanism. When the primary RADIUS server becomes unavailable, the WLC will failover to the next active-backup RADIUS server. The WLC will continue to use the secondary RADIUS server forever even if the primary server is available. Usually, the primary server is high performance and the preferred server.

In WLC 5.0 and later versions, the WLC supports the RADIUS server fallback feature. With this feature, the WLC can be configured to check if the primary server is available and switches back to the primary RADIUS server once it is available. In order to do this, the WLC supports two new modes, passive and active, in order to check the status of the RADIUS server. The WLC comes back to the most preferable server after the specified timeout value.

Fallback Modes

Active Mode

In active mode, when a server does not respond to the WLC authentication request, the WLC marks the server as dead and then moves the server to the non-active server pool and starts to send probe messages periodically until that server responds. If the server responds, then the WLC moves the dead server to the active pool and stops sending probe messages. In this mode, when an authentication request comes, the WLC always picks the lowest index (highest priority) server from the active pool of RADIUS servers.

The WLC sends a probe packet after timeout (the default is 300 seconds) in order to determine server status in case the server was unresponsive earlier.

Passive Mode

In passive mode, if a server does not respond to the WLC authentication request, the WLC moves the server to the inactive queue and sets a timer. When the timer expires, the WLC moves the server to active queue irrespective of the server's actual status. When an authentication request comes, the WLC picks the lowest index (highest priority) server from the active queue (which might include the non-active server). If the server does not respond then the WLC marks it as inactive, sets the timer, and moves to the next highest priority server. This process continues until the WLC finds an active RADIUS server or the active server pool is exhausted.

The WLC assumes the server is active after timeout (the default is 300 seconds) in case the server was unresponsive earlier. If it is still unresponsive, the WLC waits for another timeout and tries again when an authentication request comes in.

Off Mode

In off mode, the WLC supports failover only. In other words, fallback is disabled. When the primary RADIUS server goes down, the WLC will failover to the next active-backup RADIUS server. The WLC continues to use the secondary RADIUS server forever, even if the primary server is available.

Configure

Configure the RADIUS Server Fallback Feature with the CLI

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Use these commands from the WLC CLI in order to enable the RADIUS server fallback feature on the WLC.

The first step is to select the mode of RADIUS server fallback. As mentioned earlier, the WLC supports active and passive modes of fallback.

In order to select the mode of fallback, enter this command:

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- active - Sends probes to dead servers to test the status.
- passive - Sets server-status based on the last transaction.
- off - Disables the server fallback test (default).

The next step is to select the interval which specifies the probe interval for active mode or the inactive time for the passive modes of operation.

In order to set the interval, enter this command:

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180 to 3600> - Enter the probe interval or inactive time in seconds (the default is 300 seconds).

The interval specifies the probe interval in the case of active mode fallback or inactive time in the case of passive mode fallback.

For the active mode of operation, you need to configure a username which will be used in the probe request sent to the RADIUS server.

In order to configure the username, enter this command:

```
WLC1 >config radius fallback-test username {username}
```

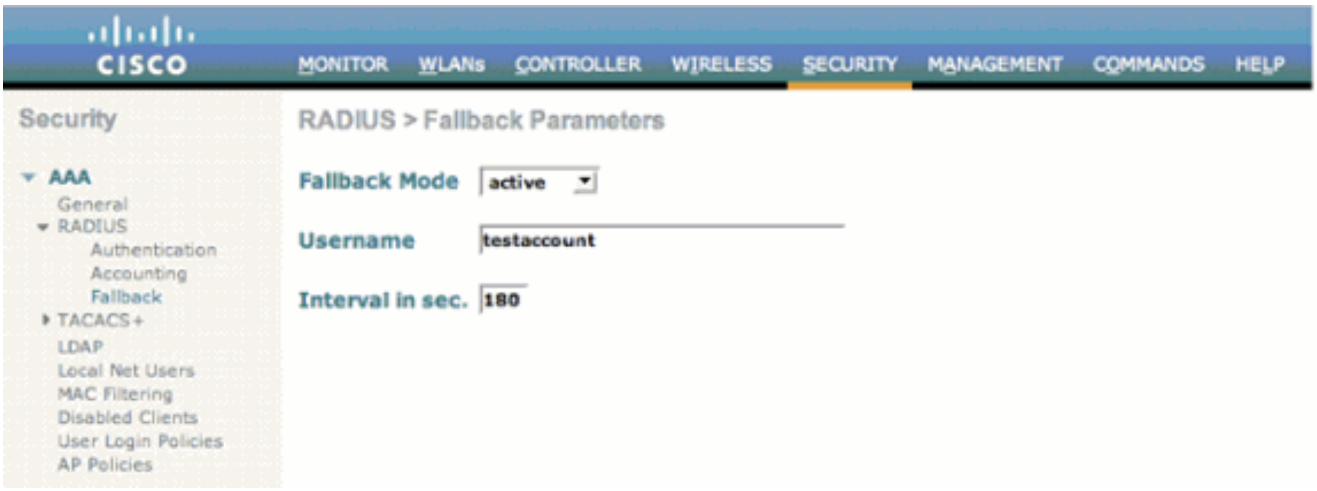
<username> - Enter a name up to 16 alphanumeric characters (the default is cisco-probe).

> **Note**: You can enter your own username or leave it with the default. The default username is "cisco-probe". Because this username is used to send probe messages, you do not need to configure a password.

Configure the RADIUS Server Fallback Feature with the GUI

Complete these steps in order to configure the WLC with the GUI:

1. Configure the mode of RADIUS server fallback. In order to do this, select **Security > RADIUS > Fallback** from the WLC GUI. The **RADIUS > Fallback Parameters** page appears.
2. From the **Fallback Mode** drop-down list, select the mode of fallback. The available options include active, passive, and off.Here is an example screenshot for the configuration of active fallback mode as shown in the image.



3. For active mode of operation, enter the username in the username field.
4. Enter the probe interval value in the Interval in sec. field.
5. Click **Apply**.

If the aggressive failover feature is enabled in the WLC, the WLC is too aggressive to mark the AAA server as "not responding". However, this should not be done because the AAA server is possibly not responsive only to that particular client if you do silent discard. It can be a response to other valid clients with valid certificates. The WLC can still mark the AAA server as "not responding" and "not functional".

In order to overcome this, disable the aggressive failover feature. Enter the **config radius aggressive-failover disable** command from the controller GUI in order to perform this. If this is disabled, then the controller only fails over to the next AAA server if there are three consecutive clients that fail to receive a response from the RADIUS server.

> **Note**: Functionality change introduced in Release 8.5.140,8.8.100,8.10.105 and later: When RADIUS aggressive failover for the controller is disabled: Packet is retried for six times unless there is an abort from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after three timeout events (18 consecutive retries) from multiple clients (previously, from exactly three clients). When RADIUS aggressive failover for the controller is enabled: Packet is retried for six times unless there is an abort from clients. The RADIUS server (both AUTH and ACCT) is marked unreachable after one timeout event (6 consecutive retries) from multiple clients (previously, from exactly one client). It means 18 consecutive retries per RADIUS server (either AUTH or ACCT) can be from multiple clients. Therefore, it is not always guaranteed that each packet will be retried for six times.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

Enter the **show radius summary** command in order to verify your fallback configuration. Here is an example:

```
WLC1 >show radius summary

Vendor Id Backward Compatibility..................... Disabled
Call Station Id Type................................. IP Address
Aggressive Failover.................................. Enabled
Keywrap.............................................. Disabled

Fallback Test:
Test Mode.................................... Active
Probe User Name.............................. testaccount
Interval (in seconds)........................ 180

Authentication Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------------
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none

Accounting Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug dot1x events enable** - Configures debugs of 802.1X events.
- **debug aaa events enable -** Configures debugs of all AAA events.

Related Information

- **EAP Authentication with WLAN Controllers (WLC) Configuration Example**
- **Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)**
- **Configuring Security Solutions**
- **Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller Configuration Example**
- **Technical Support & Documentation - Cisco Systems**