Contents

Introduction

This document explains how to set up multiple wireless LAN (WLAN) controllers (WLCs) for a failover condition. A failover condition occurs when a primary controller goes down or fails for any reason. Then, a second controller takes over the operation. Failover is also called controller redundancy.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of the configuration of lightweight access points (APs) and Cisco WLCs
- Basic knowledge of Lightweight AP Protocol (LWAPP)
- Knowledge of the configuration of an external DHCP server

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Aironet 1000 Series Lightweight AP
- Two Cisco 2000 Series WLCs that run firmware 3.2.78.0
- Microsoft Windows Server 2003 Enterprise DHCP server

This configuration works with any other Cisco WLC and any lightweight AP.

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.

Conventions

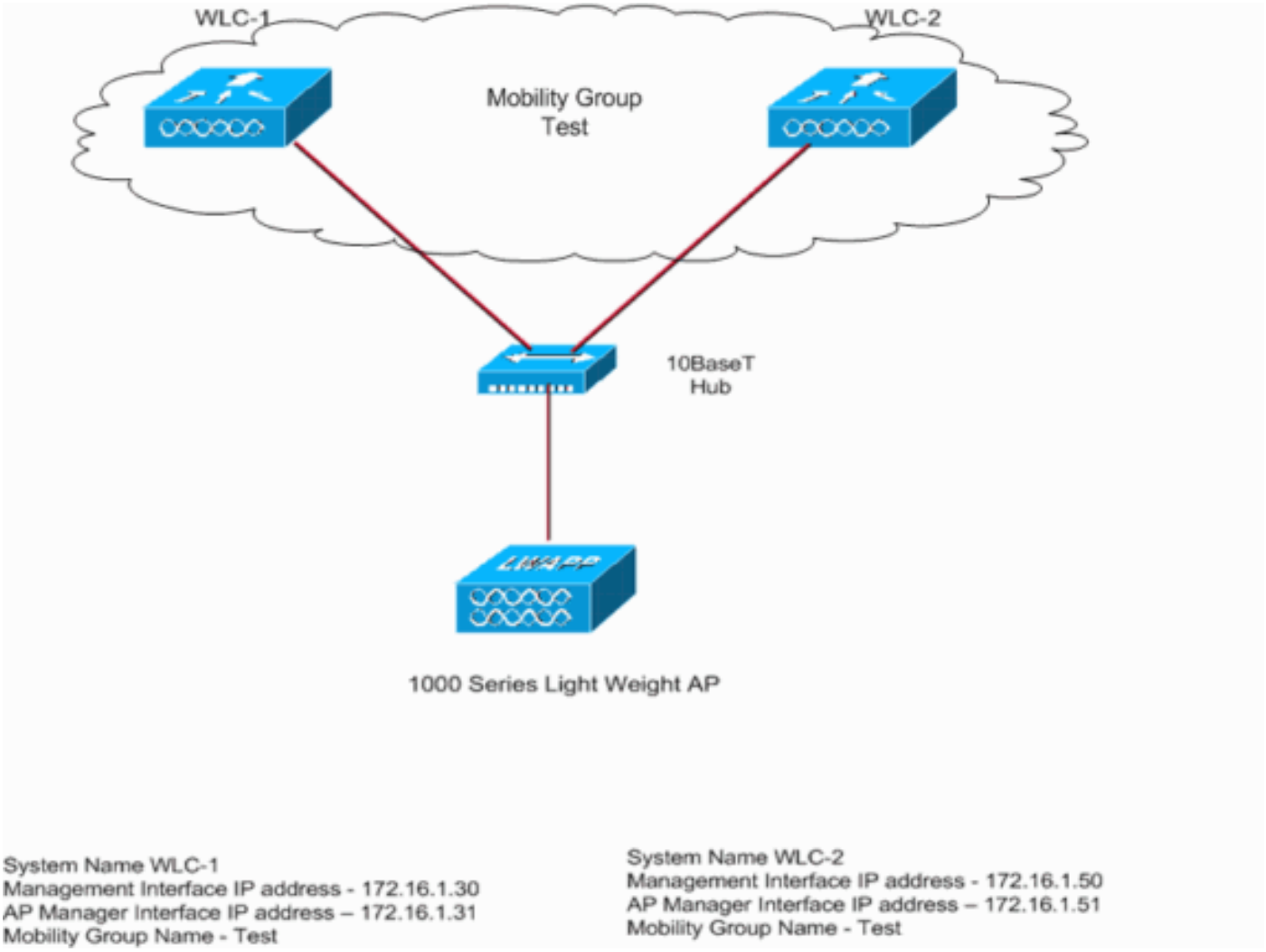
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Network Diagram

This document uses this network setup.

Two Cisco 2006 WLCs and a lightweight AP are connected through a hub. An external DHCP server is also connected to the same hub. All the devices are in the same subnet. The AP is initially registered to the primary controller. You must configure the lightweight AP and the WLC so that the AP automatically switches to the secondary controller if the primary controller goes down. You also must ensure that the AP registers back to the primary controller after the AP is back on line. In order to ensure that the AP registers back to the primary controller, you should use the mobility groups and the AP fallback features of the WLCs.

Note: Before you configure the controller for failover of access points, you must configure the WLC for basic operation and register the LAPs to the WLC. This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user and need to register a LAP with a controller, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).



Configure

In order to configure the devices for WLC failover (or redundancy), you must complete these steps:

1. Configure mobility groups for the WLCs.
2. Assign primary, secondary, and tertiary controllers for the lightweight AP .
3. Configure the Fallback feature on WLC.

Configure Mobility Groups for the WLCs

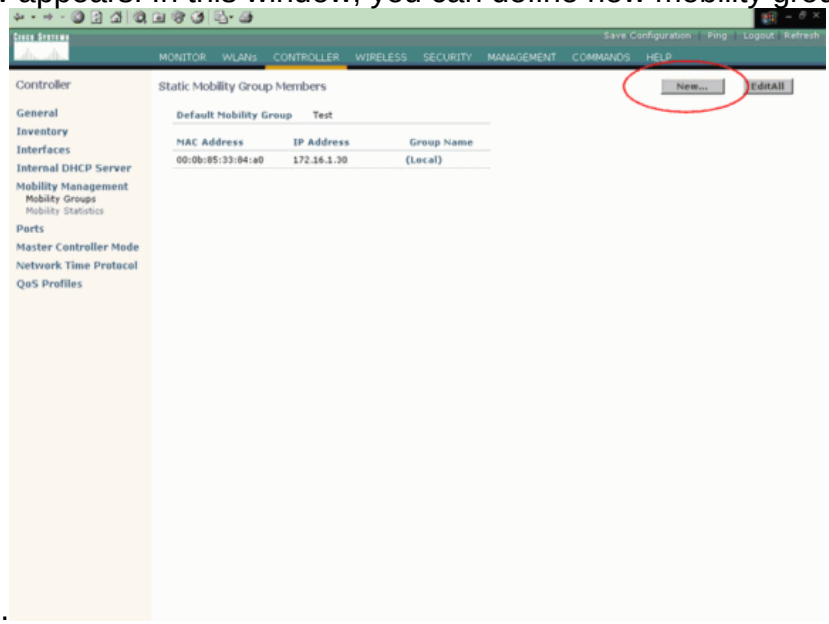
You can configure a set of WLCs as a mobility group in order to allow seamless client roaming within a group of WLCs. If you create a mobility group, you can enable multiple WLCs in a network in order to provide redundancy in the event that a WLC goes down. If a WLC goes down, all the APs that are registered to that WLC automatically switch to the other WLCs in the mobility group. When the primary controller comes back on, the APs fall back to it. However, this operation takes 30 seconds. During this period of time, the service to the APs is interrupted as the APs rejoin the primary WLC.

Note: The mobility group name configured must be the same on all the controllers that belong to a particular mobility group. The mobility group name is also case sensitive. Also, the mobility group members list configured on each controller should contain all the controllers of that particular mobility group. These configurations ensure that the failover occurs seamlessly. These configurations also ensure that when the primary controller comes back on, the previously registered APs fall back to it.

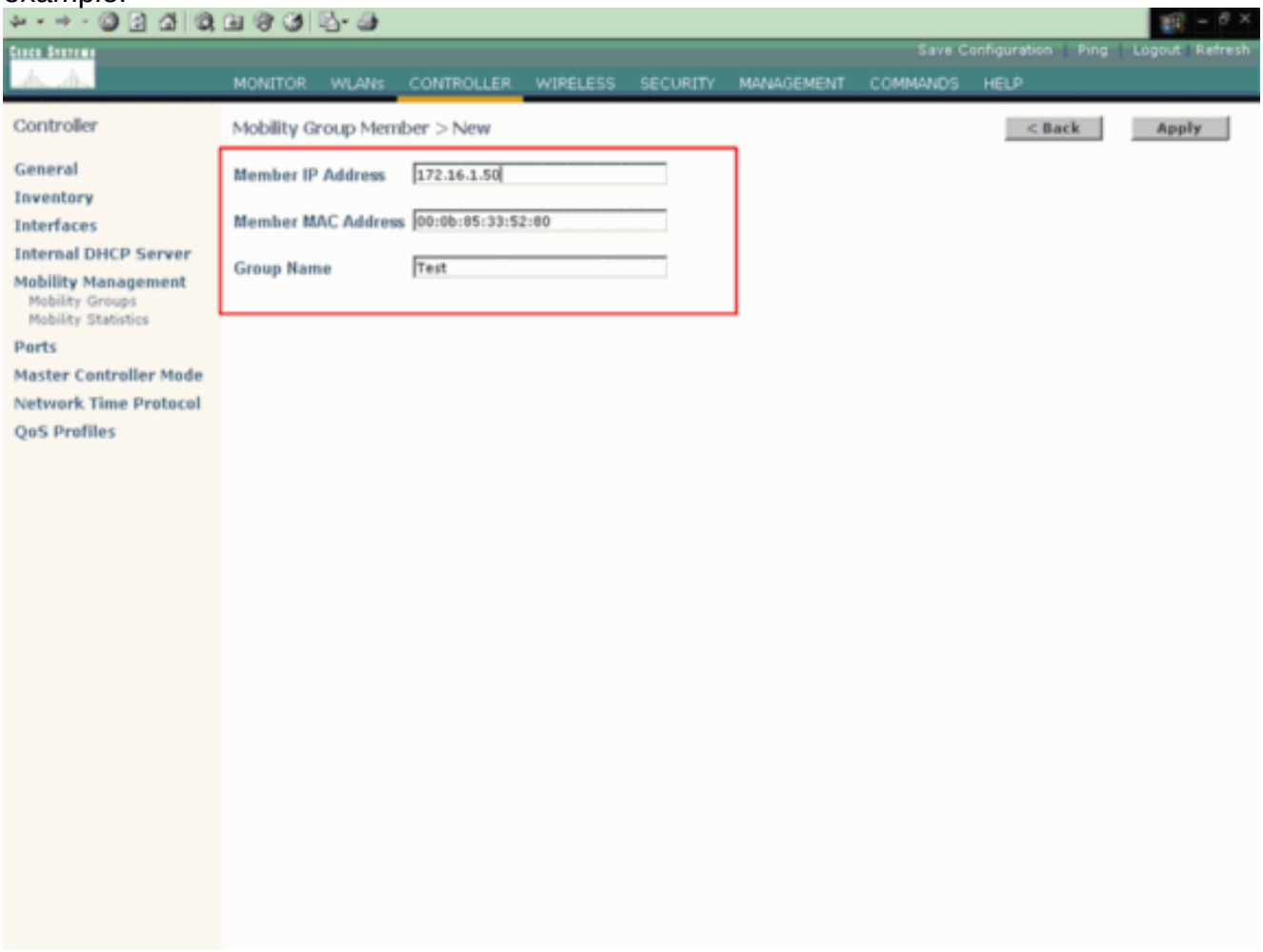
Note: In addition, make sure that the wireless (WLAN) configurations are similiar on both the primary and secondary WLCs so that the client roaming is seamless.

This setup configures the two WLCs to form a mobility group. In order to configure mobility groups, complete these steps:

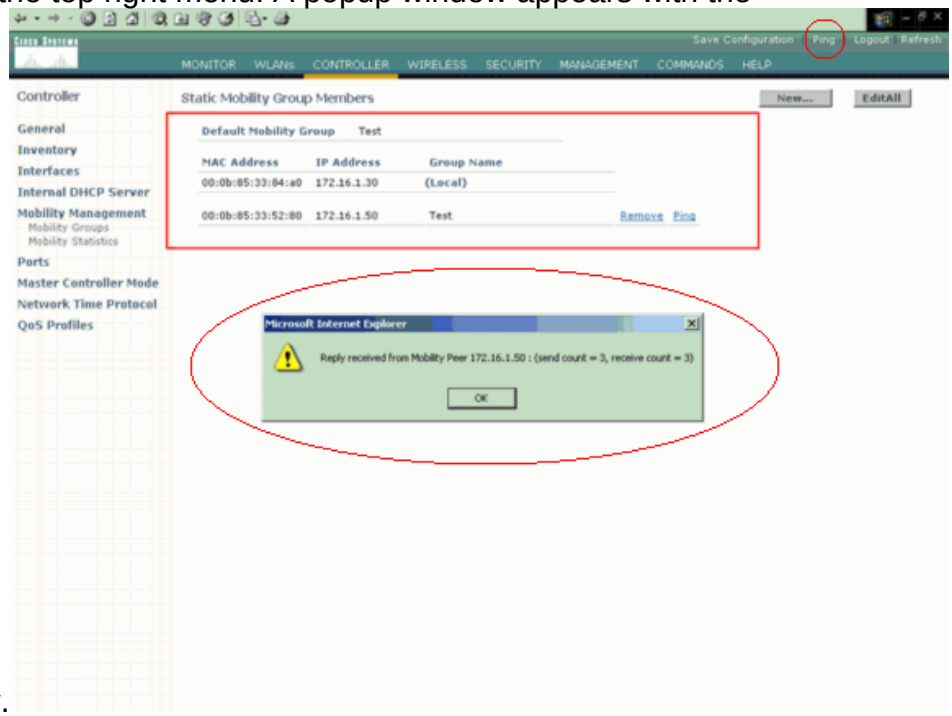
1. From the GUI, click the **Controller** tab in the menu at the top of the window, and then choose **Mobility Groups** from the menu on the left.The Static Mobility Group Members window appears. In this window, you can define new mobility groups or edit existing mobility groups.



2. Create a new mobility group for the WLCs that you have in your network.This example has only two WLCs.Click **New**.Define the mobility group member IP and MAC addresses, and the group name.This example provides the IP address 172.16.1.50 and the MAC address of the second WLC, 00:0b:85:33:52:80, and defines the mobility group name as Test.Click **Apply**.Here is an example:



3. Ping from the GUI in order to check the reachability of the group members.The ping function is in the top right menu. A popup window appears with the reply.

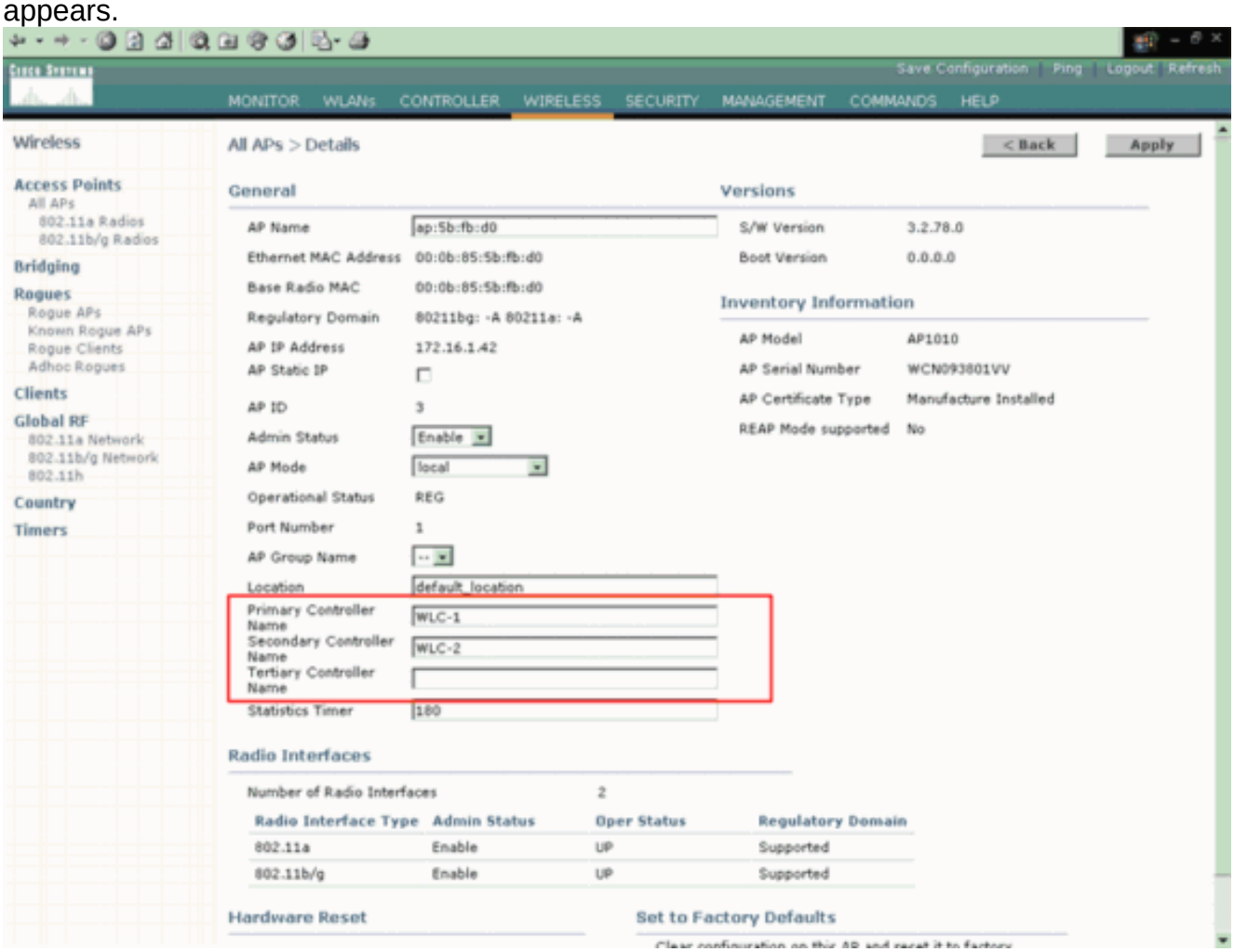


Repeat these steps on the second WLC in order to configure the mobility group. The mobility group name must be the same on both WLCs, and it is case sensitive. Mobility groups are useful for features such as intercontroller roaming and intracontroller roaming. For more information on these features, refer to the *Overview of Mobility Groups* section of Configuring Mobility Groups.

Assign Primary, Secondary, and Tertiary Controllers for the Lightweight AP

Next step in this configuration is to define the primary, secondary, and tertiary controllers on the lightweight AP. This assignment decides the order in which the APs choose the controllers. Complete these steps:

1. From the GUI, click the **Wireless** tab in the menu at the top of the window, select the AP from the list of APs that are registered to the WLC, and click **Detail** beside the AP.The All APs > Details window
   appears.

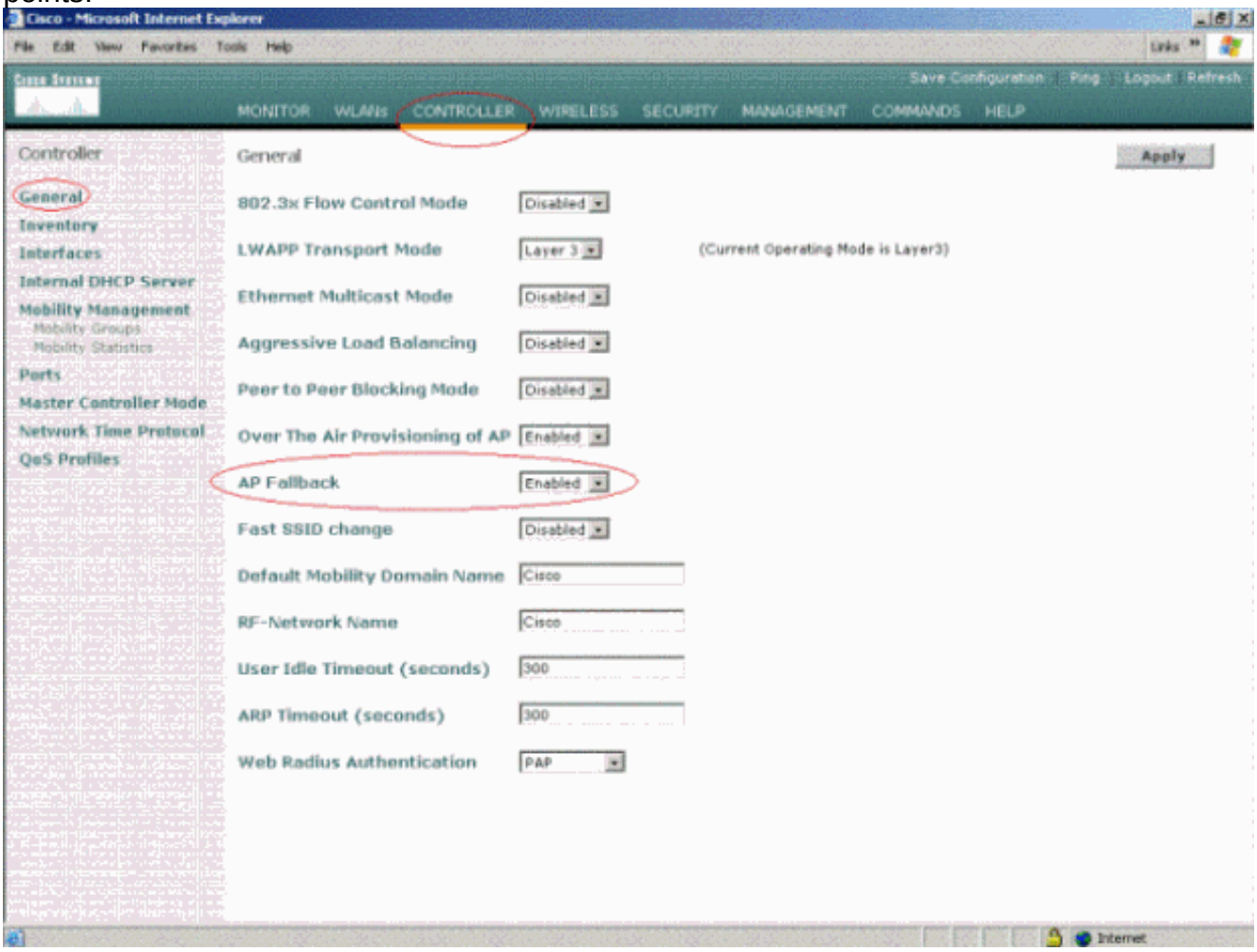


2. In this window, define the primary, secondary, and tertiary controllers.**Note:** Define only system names under the primary, secondary, and tertiary controller name fields. Do not enter the IP address or the MAC address of the controller in these fields.**Note:** This example does not add a tertiary controller name because there are only two controllers.

Configure the Fallback Feature on WLC

The last step is to configure the Fallback feature on the controller. This feature ensures that the AP switches return to the first WLC when the WLC that comes back on line. Complete these steps:

1. From the GUI, choose **Controller > General**.A list of options appears on the General screen.
2. For the AP Fallback option, choose **Enabled** from the drop-down menu.
3. Click **Apply**.**Note:** It is sufficient to enable the Fallback feature on the secondary controller alone. But it is recommended to configure it on the primary WLC as well because it can be configured as a secondary controller for other access points.



After you complete these steps, the setup is configured for WLC failover. When the primary controller (WLC-1, in this case) goes down, the APs automatically get registered with the secondary controller (WLC-2). The APs register back to the primary controller when the primary controller comes back on line. AP switching between the primary and secondary controllers also affects the wireless clients associated with these APs.

In controller software release 5.1.151.0, you can configure the wireless network so that the backup controller recognizes a join request from a higher-priority access point and, if necessary, disassociates a lower-priority access point as a means to provide an available port. In order to configure this feature, failover priority must be enabled on the network and assign priorities to the individual access points. By default, all access points are set to priority level 1, which is the lowest priority level.

Note: Be aware that Failover priority takes effect only if there are more association requests after a controller failure than there are available backup controller ports.

Wireless LAN Controller Failover Priority

During installation, Cisco recommends you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures

each lightweight access point for a primary, secondary, and tertiary controller and allows it to store the configured mobility group information. When sufficient controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, which allows the client device to immediately reassociate and reauthenticate.

Verify

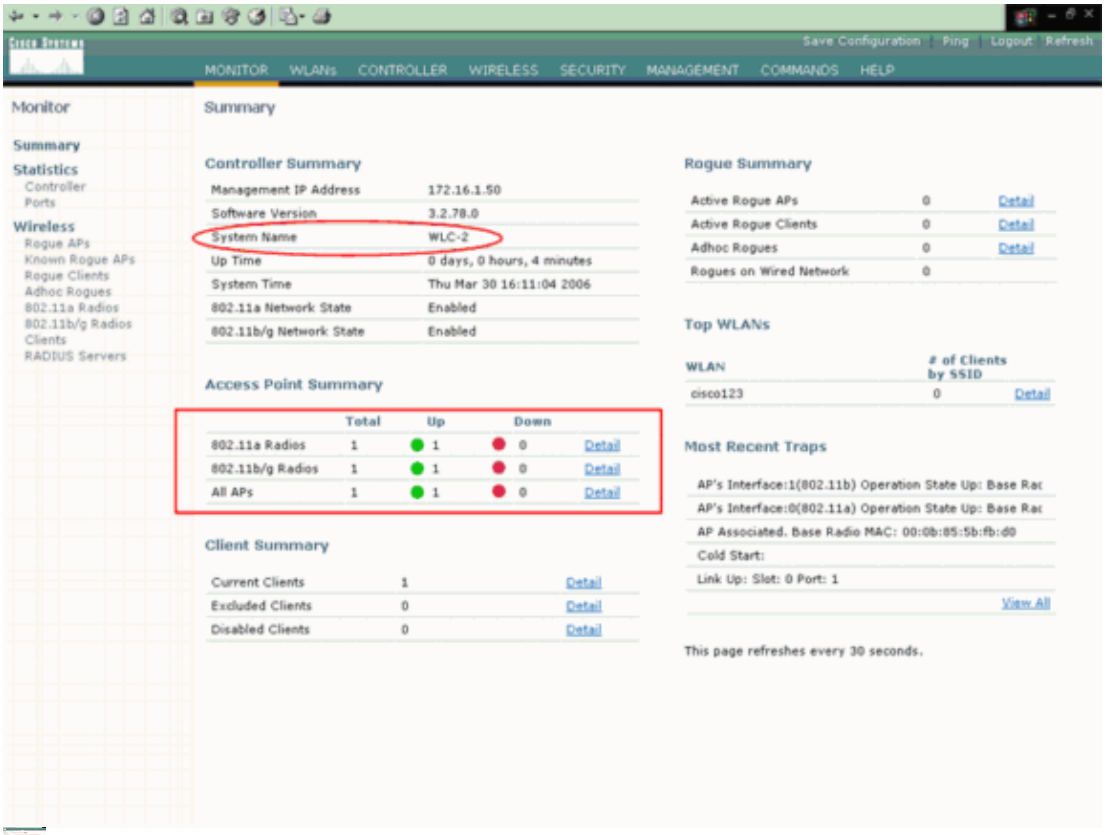
Use this section to confirm that your configuration works properly.

The Cisco CLI Analyzer (registered customers only) supports certain **show** commands. Use the Cisco CLI Analyzer to view an analysis of **show** command output.

You can verify if the configuration works as expected. Power down the primary controller to which the AP is currently registered. The AP waits for the heartbeat time set, which is 30 seconds by default, to detect the failure of the primary WLC. After this period of time, the AP sends heartbeat messages seven more times, one per second, in efforts to find the primary WLC. If the AP does not hear from the primary WLC, the AP registers to an available WLC via the default process. Therefore, the process to detect the primary WLC failure and register to the secondary WLC takes approximately 80 seconds. Once the access point joins the secondary controller, it continues to send the discovery request to the primary controller in order to determine if the primary controller is back in operation. This can be determined with the help of the **debug lwapp client packet** command.

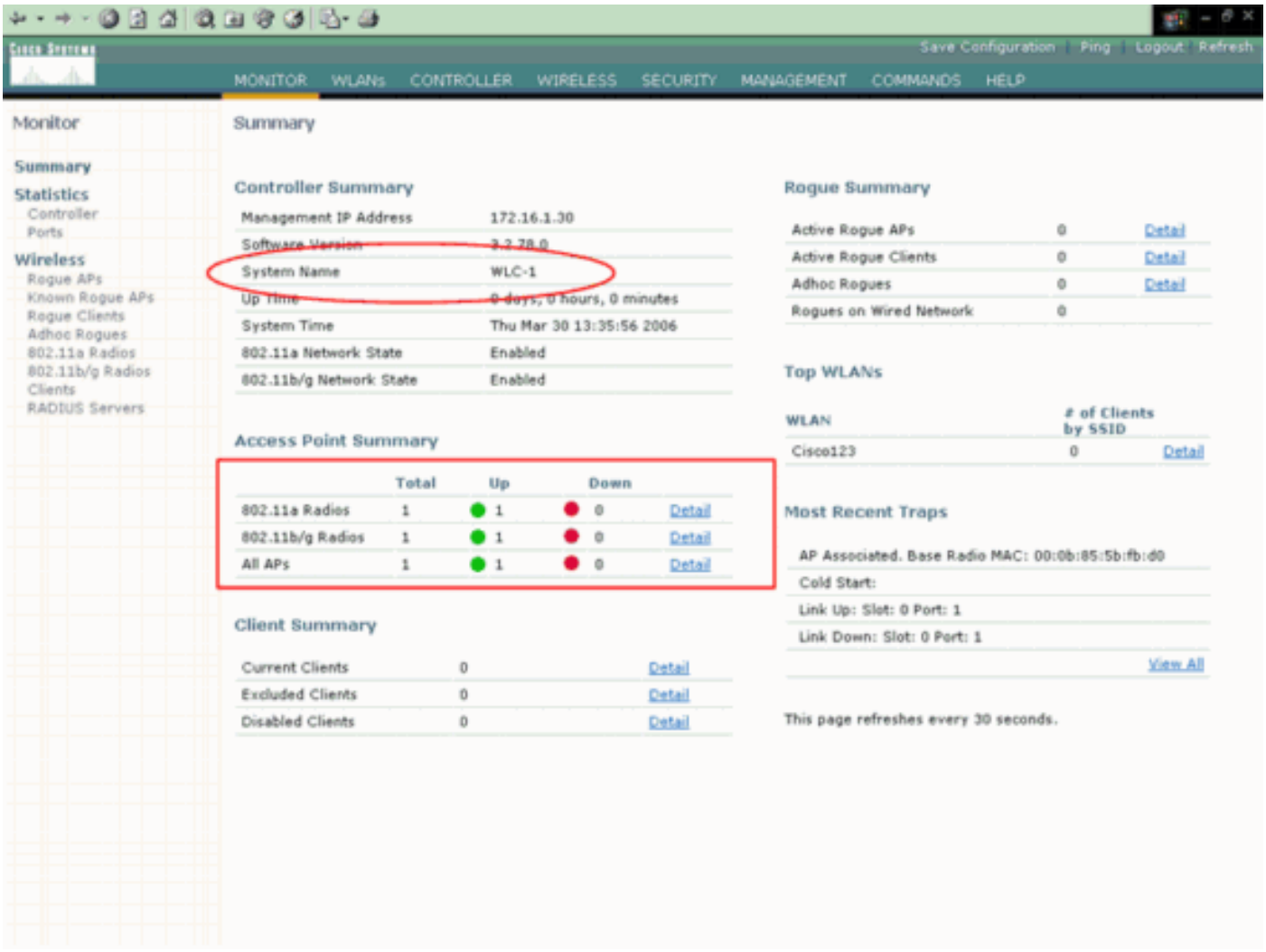
Note: The heartbeat message is similar to a keepalive message. The AP heartbeat is set to 30 seconds by default. You can adjust this heartbeat time, down to 1 second. However, if you have not made this adjustment since the last time that the AP heard from the WLC, 30 seconds pass before the AP realizes that it cannot reach the WLC.

This example shows that the AP gets registered to the secondary controller:



When the primary controller (WLC-1) comes back on line, the AP again switches back to the

primary controller. Here is an example:



You can also use the **show ap summary** command on the WLC in order to view the APs that are registered to the WLC. Here is an example:

```
(Cisco Controller) >show ap summary

AP Name          Slots  AP Model         Ethernet MAC      Location
   Port
-----------------  -----  ------------------  ----------------  ----------------
ap:5b:fb:d0      2    AP1010           00:0b:85:5b:fb:d0
default_location
```

Note: If the global 802.11g configuration between the controllers does not match (enable versus disable), when you run 5.2 code or later on WLCs and set up AP high availability, it can cause AP join issues when a failover event occurs. Make sure that all WLC settings are identical between primary/secondary/tertiary WLCs.

Troubleshoot

Use this section to troubleshoot your configuration.

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

The **debug lwapp client packet** command output shows the discovery request sent by the access point to the primary controller:

```
Cisco Controller) > debug lwapp client packet
*Feb 25 02:12:55.743: Sent Msg Type    :   ECHO_REQUEST

*Feb 25 02:12:55.743: Msg Length      :   12

*Feb 25 02:12:55.743: Msg SeqNum      :   48

*Feb 25 02:12:55.744: Sent Msg Type    :   PRIMARY_DISCOVERY_REQ

*Feb 25 02:12:55.744: Msg Length      :   27

*Feb 25 02:12:55.744: Msg SeqNum      :   0

*Feb 25 02:12:55.744: Recd Msg Type    :   ECHO_RESPONSE

*Feb 25 02:12:55.744: Msg Length      :   0

*Feb 25 02:12:55.745: Msg SeqNum      :   48

*Feb 25 02:12:55.745: LWAPP_CLIENT_PACKET_DEBUG: SPAM received ECHO_RESPONSE

*Feb 25 02:12:55.745: Recd Msg Type    :   PRIMARY_DISCOVERY_RES

*Feb 25 02:12:55.746: Msg Length      :   27

*Feb 25 02:12:55.746: Msg SeqNum      :   0

*Feb 25 02:12:55.746: LWAPP_CLIENT_PACKET_DEBUG:  SPAM received PRIMARY_DISCOVERY_RES
```

You can use these additional **debug** commands in order to troubleshoot your configuration:

- **debug lwapp events enable -** Shows the series of steps involved when lightweight access point register to a controller.
- **debug lwapp errors enable -** Configures the debug of LWAPP errors.
- **debug dhcp message enable -** Configures the debug of DHCP messages that are exchanged to and from the DHCP server.
- **debug dhcp packet enable -** Configures the debug of DHCP packet details that are sent to and from the DHCP server.

In some cases, LWAPP APs in the same mobility group are seen as rogue APs by another WLC. This is because of Cisco bug ID CSCse87066 (registered customers only) . This can happen in one of two scenarios:

1. The AP sees more than 24 neighbors. The neighbor list size is 24, so any other neighbors are reported as rogues.
2. AP1 can hear a client that communicates to AP2, but AP2 cannot be heard and therefore cannot be validated as a neighbor.

The workaround is to manually set the APs to **known internal** on the WLC and/or WCS.

Complete these steps on the controller in order to manually set the APs to **known internal**.

1. Go to the WLC GUI, and choose **Wireless**.
2. Click on the **Rogue Aps** in the left side menu.
3. From the Rogue-AP list, choose **Edit**.

4. From the **Update Status** menu choose **Known internal**, and click **Apply**.

Related Information

- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Cisco Wireless LAN Controller Configuration Guide, Release 3.2**
- **Deploying Cisco 440X Series Wireless LAN Controllers**
- **Cisco Wireless LAN Controller Command Reference**
- **Wireless LAN Controller (WLC) Software Upgrade**
- **Wireless Support Page**
- **Technical Support & Documentation - Cisco Systems**