

Workgroup Bridges in a Cisco Unified Wireless Network Configuration Example

Document ID: 100254

Introduction

Prerequisites

Requirements

Components Used

Guidelines and Limitations for Using Workgroup Bridges in a Lightweight Environment

Conventions

Workgroup Bridge in a Cisco Unified Wireless Network

Passive Clients Behind a WGB

Configure

Network Diagram

How to Configure the Workgroup Bridge

How to Configure the Wireless LAN Controller (WLC)

Verify and Troubleshoot

Verify

Troubleshoot

Related Information

Introduction

This document provides an example for the configuration of Cisco Autonomous IOS[®] access points to operate in Workgroup Bridge (WGB) mode and connect to a Cisco Unified wireless network.

Prerequisites

Requirements

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

- Knowledge of Cisco Autonomous solution and Cisco IOS–based Access Points
- Knowledge of Lightweight Access Point Protocol (LWAPP)

Components Used

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

- Cisco 1231G AP that runs Cisco IOS Software Release 12.3 (8)JEC
- Cisco 4400 WLC that runs version 4.2
- Cisco 1130 series Light Weight AP

The WGB can be any Cisco Autonomous Access Point that supports the Workgroup Bridge mode and runs Cisco IOS Software Release 12.4(3g)JA or later (on 32–MB access points) or Cisco IOS Software Release 12.3(8)JEB or later (on 16–MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS software releases prior to Cisco IOS Software Releases 12.4(3g)JA and 12.3(8)JEB are not supported.

On the wireless LAN controller, you should have software version 4.1.185.0 or later. The Workgroup Bridge mode is not supported on the controller on any of the earlier versions.

Guidelines and Limitations for Using Workgroup Bridges in a Lightweight Environment

There are various guidelines that must be completed and limitations that need to be understood before you use workgroup bridges in a lightweight environment. Refer to Guidelines for Using Workgroup Bridges in a Lightweight Environment for more information.

Conventions

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

Workgroup Bridge in a Cisco Unified Wireless Network

You can configure an access point to operate as a workgroup bridge so that it can provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the workgroup bridge access point. When you configure the access point to operate as a workgroup bridge and connect to a Cisco Unified network, it can provide wireless connectivity to wired clients that are connected by Ethernet to the workgroup bridge access point. For example, if you need to provide wireless connectivity for a group of wired devices, you can connect the devices to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge.

A workgroup bridge connects to a wired network over a single wireless segment by learning the MAC address of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The workgroup bridge provides wireless access connectivity to wired clients by establishing a single connection to the lightweight access point. The lightweight access point treats the workgroup bridge as a wireless client.

If your access point has two radios, either the 2.4-GHz radio or the 5-GHz radio can function in workgroup bridge mode. When you configure one radio interface as a workgroup bridge, the other radio interface remains up.

Passive Clients Behind a WGB

The controller might not be able to see passive clients behind a WGB. Clients (such as cameras and programmable logic devices) do not initiate a traffic stream unless they are connected. Complete these steps in order avoid this issue:

1. Add a static MAC filter entry for the passive WGB device and MAC filter entry for the devices that are behind it.
2. Use this command in order to enable MAC filtering on the WLAN along with aaa override:

```
config macfilter add <STA MAC_addr> <WLAN id> [STA IP_address].
```

3. Add a static entry on the WGB IOS-based device: **bridge 1 addressxxxx.xxxx.xxxx forward FastEthernet0**

Note: In addition, increase the dot11 activity timer.

4. Add a static ARP entry on the L3 router:

```
hostname(config)#arp <ip addr> <mac addr>  
arpa
```

This feature allows the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the MAC address of the WGB wired client. When this message is received from the WGB, the controller checks the local MAC filter list or, if the WGB has roamed, the MAC filter list of the anchor controller for the MAC address of the client. If an entry is found and it contains an IP address for the client, the controller adds the client to the client table of the controller.

Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients. WGB wired clients that use MAC filtering do not need to obtain an IP address through DHCP to be added to the client table of the controller.

Configure

In this example, the 1231 Autonomous Access Point is configured as a workgroup bridge and connects to the LWAPP network. Use the SSID **WGB_LWAPP** for the connection to the WLAN and use the Open authentication with WEP for the authentication of the WGB to the LWAPP network.

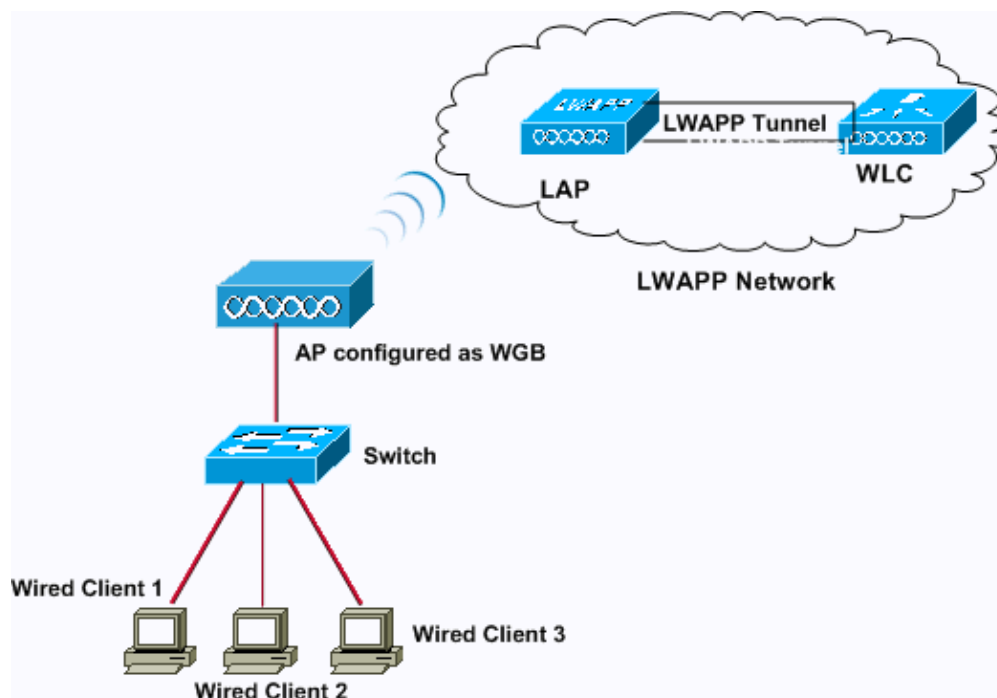
Note: Open authentication with WEP is NOT a secure method for authenticating devices. Cisco recommends that you use advanced authentication methods, such as WPA+TKIP, WPA2+AES, EAP-FAST, and EAP-TLS authentication, in order to secure the WLAN. WGB supports Open, WEP, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, Local EAP and EAP-TLS authentication modes. This document uses Open with WEP only for simplicity.

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

Network Diagram

This document uses this network setup:

Note: This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. Refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) for more information on how a new user can set up the WLC for basic operation with LAPs.



How to Configure the Workgroup Bridge

The workgroup bridge can be configured using either the CLI or the GUI.

Complete these steps in order to configure the workgroup bridge with the GUI:

1. Complete these steps in order to configure an SSID that the WGB can use to connect to the LWAPP network:

- a. Choose **Security > SSID Manager** from the left navigation pane.

The Global SSID Manager page appears.

The screenshot shows the Cisco Aironet 1200 Series Access Point GUI. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "WGB-1231". The page is titled "Security: Global SSID Manager". The left navigation pane shows "SSID Manager" selected. The main content area is divided into "SSID Properties" and "Client Authentication Settings". Under "SSID Properties", there is a "Current SSID List" table with one entry "admin". To the right, there are input fields for "SSID" (WGB_LWAPP), "VLAN" (2), "Interface" (Radio0-802.11G), and "Network ID" (0-4096). Under "Client Authentication Settings", there are three rows for "Methods Accepted": "Open Authentication" (checked), "Shared Authentication" (unchecked), and "Network EAP" (unchecked). Red circles highlight the SSID, VLAN, Interface, and Open Authentication fields.

- b. Enter the SSID name, VLAN ID, and the RADIO interface. This example uses *WGB_LWAPP* as the SSID.
- c. In the Client Authentication Settings area, check the **Open Authentication** check box.
- d. Leave all other parameters with their default values.
- e. Click **Apply**.
- f. In order to configure the WEP keys, choose **Security > Encryption Manager** from the left navigation pane.

The Encryption Manager page appears.

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page for Security: Encryption Manager. The page is titled "Cisco Aironet 1200 Series Access Point" and shows the hostname "WGB-1231" and uptime "WGB-1231 uptime is 4 days, 5 minutes". The left navigation pane includes sections like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, and SERVICES. The main content area is divided into sections: "Set Encryption Mode and Keys for VLAN:" (VLAN 2), "Encryption Modes", and "Encryption Keys".

Encryption Modes:

- None
- WEP Encryption** Mandatory
- Cipher WEP 128 bit

Encryption Keys:

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text" value="123456789123456789abc"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

At the bottom right, there are "Apply" and "Cancel" buttons.

g. In the Encryption Modes area, click the **WEP Encryption** radio button, and choose **Mandatory** from the drop-down list.

h. In the Encryption Keys area, enter the encryption key for WEP.

Note: The WEP encryption keys can be 40 bits or 128 bits in length. This example uses the 128-bit WEP encryption key 123456789123456789abc.

i. Click **Apply** in order to save the settings.

2. Complete these steps in order to configure the AP as a WGB:

- a. Click **Network Interfaces** in the left navigation pane in order to browse to the Network Interfaces Summary page.
- b. Choose the radio interface that you want to configure as a WGB. This example uses interface **Radio0-802.11G**. The action allows you to browse to the Network Interfaces: Radio Status page.
- c. Click the **Settings** tab in order to open the Settings page for the radio interface.
- d. Click the **Enable** radio button in order to enable the radio.
- e. For Role in Radio Network, click the **Workgroup Bridge** radio button. This option enables the radio to operate in Workgroup Bridge mode.
- f. Leave all the other settings on the page with the default values.

g. Click **Apply** in order to save the settings

Use these commands in order to configure the AP through the CLI:

```
AP_WGB#configure terminal
```

!--- Enter configuration commands, one on each line. End with CNTL/Z.

```
AP_WGB(config)#dot11 ssid WGB_LWAPP
```

```
AP_WGB(config-ssid)#authentication open
```

```
AP_WGB(config-ssid)#guest-mode
```

```
AP_WGB(config-ssid)#exit
```

```
AP_WGB(config)#interface dot11Radio 0
```

```
AP_WGB(config)#station-role workgroup-bridge
```

```
AP_WGB(config-if)#encryption vlan 2 mode wep mandatory
```

```
AP_WGB(config-if)#encryption vlan 2 key 1 size 128bit 12345678912345678912345
```

```
AP_WGB(config-if)#WGB_LWAPP
```

```
AP_WGB(config-if)#end
```

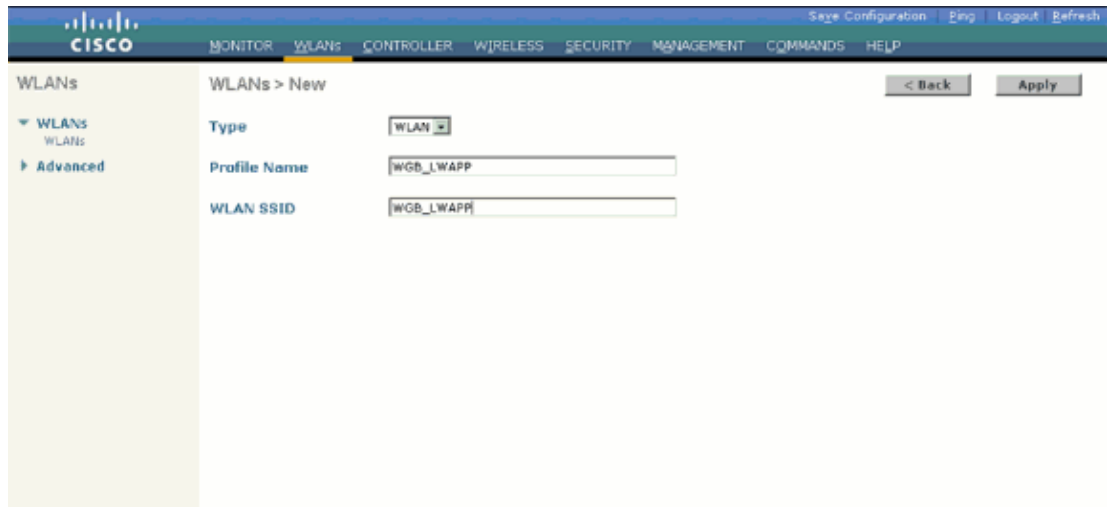
How to Configure the Wireless LAN Controller (WLC)

On the wireless LAN controller, create a WLAN that matches the SSID and security method that was configured on the workgroup bridge. This is the only configuration required on the controller for the WGB to associate with it.

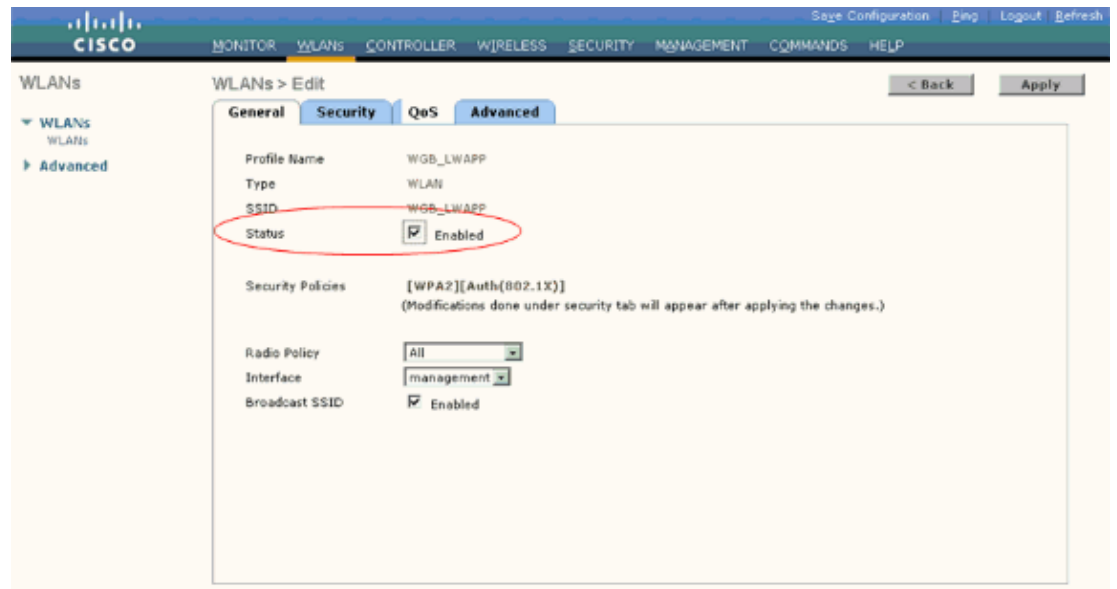
Note: Aironet IE also needs to be enabled. It is enabled by default with a new WLAN.

Complete these steps in order to configure a WLAN on the controller:

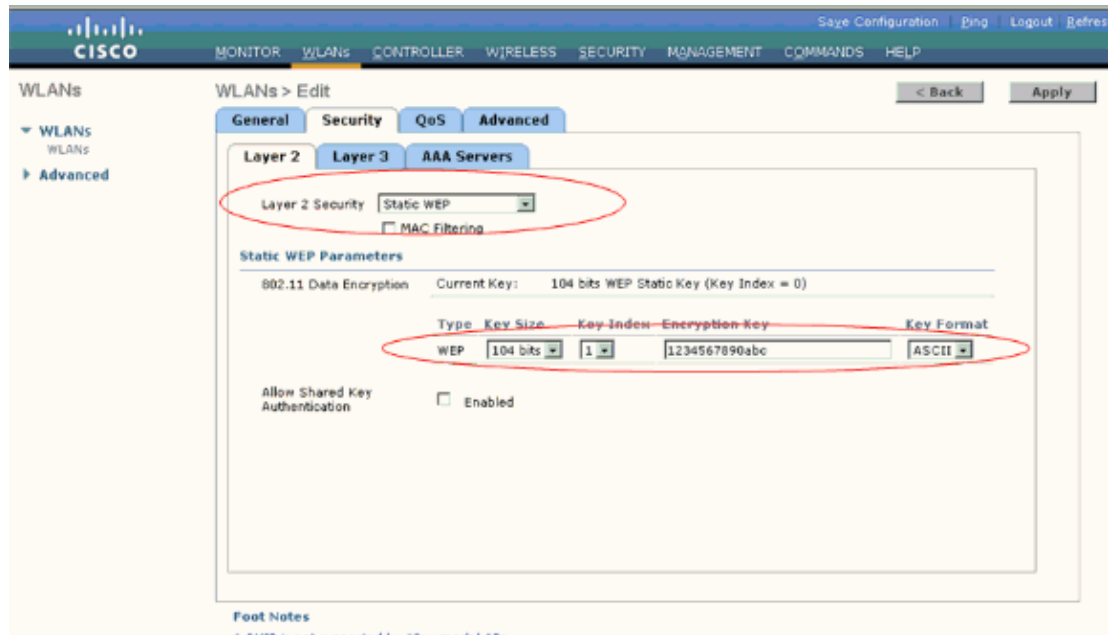
1. Click **WLANs** from the controller GUI in order to create a WLAN. The WLANs window appears. This window lists the WLANs configured on the controller.
2. Click **New** in order to configure a new WLAN. In this example, the WLAN is named *WGB_LWAPP*.



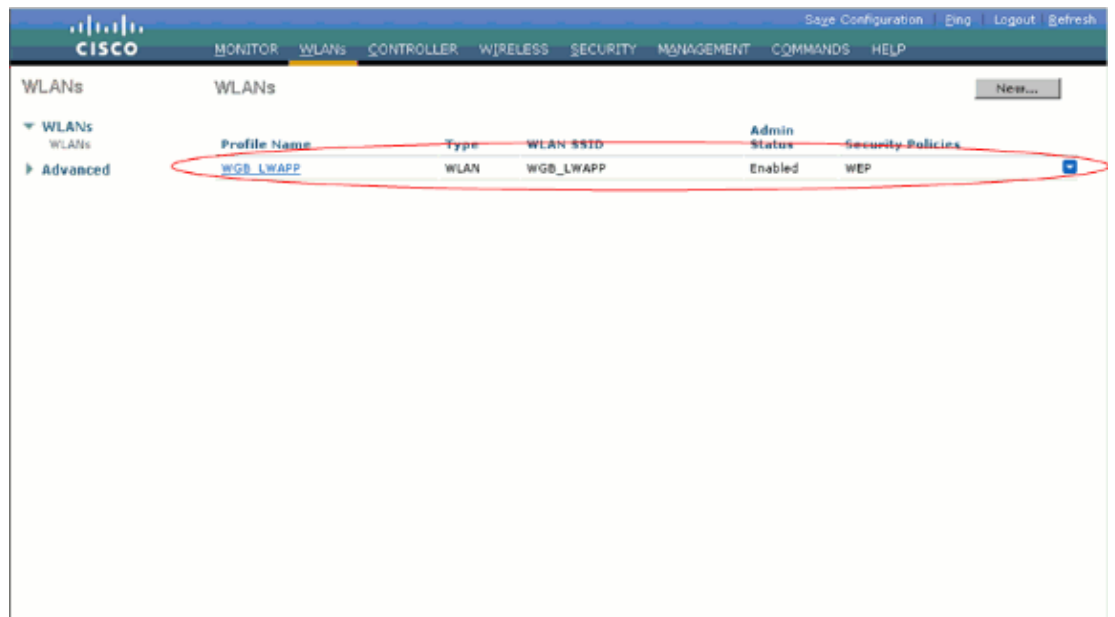
3. Click **Apply**.
4. In the WLANs > Edit window, define the parameters specific to the WLAN.
 - a. Under General Policies, check the **Status** check box in order to enable the WLAN.



- b. Under Security Policies, choose **Static WEP** from the Layer 2 Security drop-down list, and specify the WEP parameters within the Static WEP Parameters area.



c. Change other parameters depending on the design of the network, and click **Apply**.

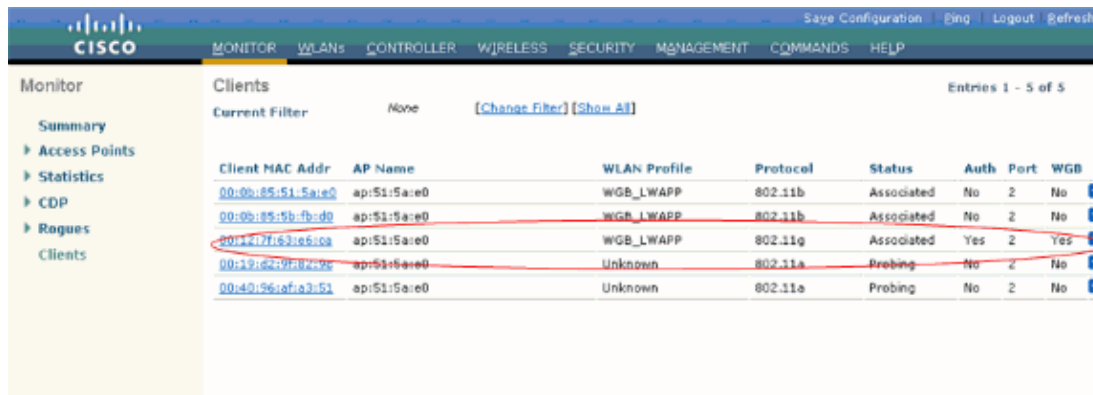


Verify and Troubleshoot

Verify

Once the WLC and the WGB AP are configured, the WGB associates to the LAP as a client. You can view the status of WGBs on your network with the controller GUI.

From the controller GUI, choose **Monitor > Clients** in order to open the Clients page. The WGB field on the right side of the page indicates whether any of the clients on your network are workgroup bridges.



The screenshot shows the Cisco WLC Monitor interface. The 'Clients' page is active, displaying a table of client information. The table has columns for Client MAC Addr, AP Name, WLAN Profile, Protocol, Status, Auth, Port, and WGB. Five entries are listed, with the third entry (MAC: 00:12:7f:63:e6:ca) circled in red.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:0b:85:51:5a:e0	ap:51:5a:e0	WGB_LWAPP	802.11b	Associated	No	2	No
00:0b:85:5b:fb:d0	ap:51:5a:e0	WGB_LWAPP	802.11b	Associated	No	2	No
00:12:7f:63:e6:ca	ap:51:5a:e0	WGB_LWAPP	802.11g	Associated	Yes	2	Yes
00:12:62:9f:04:26	ap:51:5a:e0	Unknown	802.11a	Probing	No	2	No
00:10:96:af:a3:51	ap:51:5a:e0	Unknown	802.11a	Probing	No	2	No


Click the MAC address of the desired client in order to view the details of the WGB. The Clients > Detail page appears.



The screenshot shows the 'Clients > Detail' page for the client with MAC address 00:12:7f:63:e6:ca. The 'Client Properties' section is highlighted, and the 'Client Type' is circled in red, showing it is 'WGB'.

Client Properties		AP Properties	
MAC Address	00:12:7f:63:e6:ca	AP Address	00:0b:85:51:5a:e0
IP Address	10.77.244.215	AP Name	ap:51:5a:e0
Client Type	WGB	AP Type	802.11g
Number of Wired Client(s)	2	WLAN Profile	WGB_LWAPP
User Name		Status	Associated
Port Number	2	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	0	Reason Code	0
CCX Version	CCXv1	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Management Frame Protection	No	Channel Agility	Not Implemented
		Timeout	0
		WEP State	WEP Enable
Security Policy Completed	Yes		
Policy Type	N/A		

In order to see the details of any wired clients that are connected to a particular WGB, go to the Clients page, hover your cursor over the blue drop-down arrow for the desired WGB, and choose **Show Wired Clients**. The WGB Wired Clients page appears.



The screenshot shows the 'Clients' page with a dropdown menu open for the third client (MAC: 00:12:7f:63:e6:ca). The menu options are 'Show Wired Clients', 'Link Test', 'Disable', and 'Remove'. The 'Show Wired Clients' option is highlighted.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:0b:85:51:5a:e0	ap:51:5a:e0	WGB_LWAPP	802.11b	Associated	No	2	No
00:0b:85:5b:fb:d0	ap:51:5a:e0	WGB_LWAPP	802.11b	Associated	No	2	No
00:12:7f:63:e6:ca	ap:51:5a:e0	WGB_LWAPP	802.11g	Associated			
00:12:62:9f:04:26	ap:51:5a:e0	Unknown	802.11a	Probing			
00:10:96:af:a3:51	ap:51:5a:e0	Unknown	802.11a	Probing			

From the controller CLI, you can use this command in order to view the list of WGBs connected to the network:

```
show wgb summary
```

Here is an example:

```
(Cisco Controller) >show wgb summary

Number of WGBs..... 1

MAC Address          IP Address          AP Name              Status   WLAN  Auth  Protocol  Client
-----
00:12:7f:63:e6:ca   10.77.244.215      ap:51:5a:e0         Assoc   2     Yes  802.11g   2
```

Enter this command in order to see the details of any wired clients that are connected to a particular WGB:

```
show wgb detail wgb_mac_address
```

Here is an example:

```
(Cisco Controller) >show wgb detail 00:12:7f:63:e6:ca

Number of wired client(s): 2

MAC Address          IP Address          AP Name              Mobility  WLAN  Auth
-----
00:0b:85:5b:fb:d0   Unknown            ap:51:5a:e0         Local    2     No
00:0b:85:51:5a:e0   Unknown            ap:51:5a:e0         Local    2     No
```

Troubleshoot

A common problem has been observed mainly with the Cisco IOS–Based workgroup bridge. When a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if the traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. In order to avoid the traffic loss and removal of the wired client from the bridge table, use this command in order to configure the aging–out timer on the WGB to a large value:

bridge <bridge–group–number> **aging–time** <seconds>, where *bridge–group–number* is a value between 1 and 255 and *seconds* is a value between 10 and 1,000,000 seconds. Cisco recommends that you configure the seconds parameter to a value greater than the idle period of the wired client.

Note: This can be particularly helpful if you have devices such as a printer that sits idle for a long period of time.

Related Information

- [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
- [Wireless LAN Controller \(WLC\) Configuration Best Practices](#)
- [Cisco Aironet Workgroup Bridge FAQ](#)
- [Access Point as a Workgroup Bridge Configuration Example](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

