

MOXA AirWorks AWK-1100

User's Manual

www.moxa.com/product

First Edition, July 2005



Moxa Networking Co., Ltd.

Tel: +886-2-2910-1230

Fax: +886-2-2910-1231

Web: www.moxa.com

MOXA Technical Support

Worldwide: support@moxanet.tw

The Americas: support@moxa.com

MOXA AirWorks AWK-1100 User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2005 Moxa Networking Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of the Moxa Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Table of Contents

Chapter 1	Introduction	1-1
	Overview	1-2
	Package Checklist.....	1-2
	Product Features	1-2
	Product Specifications	1-2
Chapter 2	Getting Started	2-1
	First-Time Installation and Configuration	2-2
	Deploying the Access Point (AP)	2-5
	Setting up Client Computers.....	2-5
	Configuring IEEE 802.11g-related Settings.....	2-5
	Configuring TCP/IP-related Settings	2-6
	Confirming the Settings of the AP and Client Computers	2-6
	Checking if the IEEE 802.11g-related Settings Work.....	2-6
	Checking if the TCP/IP-related Settings Work	2-7
Chapter 3	Web Console Configuration	3-1
	Overview	3-2
	Menu Structure.....	3-2
	Save, Save & Restart, and Cancel Buttons.....	3-3
	Home and Refresh Buttons.....	3-3
	Viewing Status.....	3-4
	Associated Wireless Clients	3-4
	Current DHCP Mappings	3-4
	System Log.....	3-4
	Link Monitor (AP Client mode only).....	3-5
	General Operations.....	3-5
	Specifying the Operational Mode.....	3-5
	Administrative Password.....	3-6
	Managing the Firmware	3-6
	Configuring TCP/IP-related Settings.....	3-10
	Addressing.....	3-10
	DHCP Server (AP/Bridge modes only).....	3-11
	Configuring IEEE 802.11g-related Settings	3-12
	Communication	3-12
	Security	3-15
	IEEE 802.1X/RADIUS (AP mode only).....	3-19
	Configuring Advanced Settings.....	3-21
	Packet Filters.....	3-21
	Management.....	3-22
Appendix A	Default Settings	A-1
Appendix B	Troubleshooting	B-1
	Wireless Settings Problems	B-1
	TCP/IP Settings Problems	B-2
	Unknown Problems	B-3

Appendix C	Regulatory Statement	C-1
Appendix D	Service Information.....	D-1
	MOXA Internet Services	D-2
	Problem Report Form.....	D-3
	Product Return Procedure.....	D-4

1

Introduction

MOXA AirWorks AWK-1100 enables wireless users to access network resources wirelessly. AWK-1100 can authenticate and authorize wireless users by IEEE 802.1X and RADIUS, and communicate with a back-end RADIUS (Remote Authentication User Dial-In Service) server to determine if a wireless user is allowed to access the wireless network..

The following topics are covered in this chapter:

- Overview**
- Package Checklist**
- Product Features**
- Product Specifications**

Overview

AWK-1100 is rated to operate at temperatures ranging from 0 to 60°C, and is rugged enough for any harsh industrial environment. It can be installed easily on DIN-Rail mounting as well as in distribution boxes. The DIN-Rail mounting capability, wide operating temperature range, and the IP30 case with LED indicators make AWK-1100 a ready, plug-and-play, yet reliable solution for your Industrial Wireless application.

Package Checklist

MOXA AWK-1100 is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 × AWK-1100 802.11g/b Wireless AP/Bridge/Client
- 2 × Swivel Type Antenna (2 dBi RP-SMA)
- Quick Installation Guide
- Documentation & Software CD; includes User's Manual and Windows Utility
- Warranty Booklet

Product Features

- IEEE 802.11b/g Compliant
- Redundant 24 VDC power inputs or Power-over-Ethernet
- Powerful security with WPA/802.1X/MAC address filtering
- DIN-Rail mounting capability
- Case design meets IP30 protection standard

Product Specifications

WLAN

Standards	IEEE802.11g/b for wireless LAN, IEEE802.3u 10/100BaseTX for Ethernet LAN, IEEE802.3af for Power over Ethernet
Frequency Range	2.4-2.4835 GHz, Direct Sequence Spread Spectrum (DSSS)
Data Rate & Modulation	OFDM@54Mbps, CCK@11/5.5Mbps, DQPSK@2Mbps and DBSK@1Mbps
Operating Channels	USA: 1-11 (FCC) / Europe: 1-13 (ETSI)
Security	64-bit and 128-bit WEP encryption, WPA (IEEE 802.1X/RADIUS and TKIP)
Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Transmit Power	<u>802.11b:</u> ≥17dBm <u>802.11g:</u> 6/9Mbps≥17dBm, 12/18Mbps≥15dBm, 24Mbps≥14dBm, 36Mbps≥14dBm, 48Mbps≥12dBm, 54Mbps≥12dBm
Receiver Sensitivity	<u>802.11b:</u> 8% FER@1Mbps≤-91dBm, 8% FER@2Mbps≤-88dBm 8% FER@5.5Mbps≤-85dBm, 8% FER@11Mbps≤-83dBm

802.11g:

10% PER@6Mbps≤-88dBm,
 10% PER@9Mbps≤-87dBm
 10% PER@12Mbps≤-84dBm,
 10% PER@18Mbps≤-82dBm
 10% PER@24Mbps≤-79dBm,
 10% PER@36Mbps≤-75dBm
 10% PER@48Mbps≤-69dBm,
 10% PER@54Mbps≤-68dBm

Software Features

Protocols	HTTP, DHCP, TCP/IP, RADIUS, DNS, NetBIOS, NetBEUI, AppleTalk, and IPX/SPX
Configuration	Web-based management
Client OS Support	Windows 95/98/2000/ME/NT/XP, Unix and Macintosh

Interface

Antenna	2dBi diversity antenna with an R-SMA connector
RJ45 port	10/100BaseT(X) auto negotiation speed
LED Indicators	PWR1, PWR2, WLAN (Link/ACT), LAN (Link/ACT)

Power

Input Voltage	12 to 45 VDC; Redundant dual DC power inputs or Power over Ethernet (PoE, power on RJ45 pins 4, 5 for power + and pins 7, 8 for power -)
Input Current (@24V)	0.3A
Connection	Removable Terminal Block
Overload Current Protection	1.6A
Reverse Polarity Protection	Present

Mechanical

Casing	IP30 protection, aluminum case
Installation	DIN-Rail or panel mounting

Environmental

Operating Temperature	0 to 60°C (32 to 140°F)
Storage Temperature	-20 to 70°C (-4 to 158°F)
Ambient Relative Humidity	5 to 95% (non-condensing)

Regulatory Approvals

Safety	UL, TÜV
Emissions	FCC, CE, SRRC
WARRANTY	5 years

2

Getting Started

This chapter explains how to install MOXA AirWorks AWK-1100 for the first time.

The following topics are covered:

- ❑ **First-Time Installation and Configuration**
- ❑ **Deploying the Access Point (AP)**
- ❑ **Setting up Client Computers**
 - Configuring IEEE 802.11g-related Settings
 - Configuring TCP/IP-related Settings
- ❑ **Confirming the Settings of the AP and Client Computers**
 - Checking if the IEEE 802.11g-related Settings Work
 - Checking if the TCP/IP-related Settings Work

First-Time Installation and Configuration

Before installing AWK-1100, check to make sure that all items in the Package Checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. AWK-1100 has a default IP address that you must use when connecting to AWK-1100 for the first time.

NOTE For testing requirements, if you only have one AWK-1100, we strongly suggest that you prepare a notebook computer or PC with a wireless LAN adapter installed. After finishing the installation and configuration, you should test AWK-1100 to make sure the wireless transmission is working normally.

Step 1: Select the Power Source

AWK-1100 can be powered by a DC power input, or by PoE (Power over Ethernet). AWK-1100 will use the power source that you choose.

NOTE The PoE capability of the bridge is PowerDsine-compatible. Please visit PowerDsine's website for more information (<http://www.powerdsine.com>).

Step 2: Connect AWK-1100 to a notebook or PC

Since AWK-1100 supports MID/MID-X auto-sensing, you can use either a straight-through cable or cross-over cable to connect AWK-1100 to the notebook, if the LAN LED on AWK-1100's front panel lights up, it means the connection is established.

Step 3: Set up the computer's IP address

In a Windows environment, the computer's IP address can be changed in the TCP/IP settings window. Select an IP address on the same subnet as the AWK-1100. Since AWK-1100's default IP address is 192.168.127.253, and the subnet mask is 255.255.255.0, you should set the IP address of the computer to 192.168.127.xxx.

Step 4: Use the web-based manager to configure AWK-1100

Open your computer's web browser and then type **http://192.168.127.253** in the address box to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on **OK**:

Default user name & password

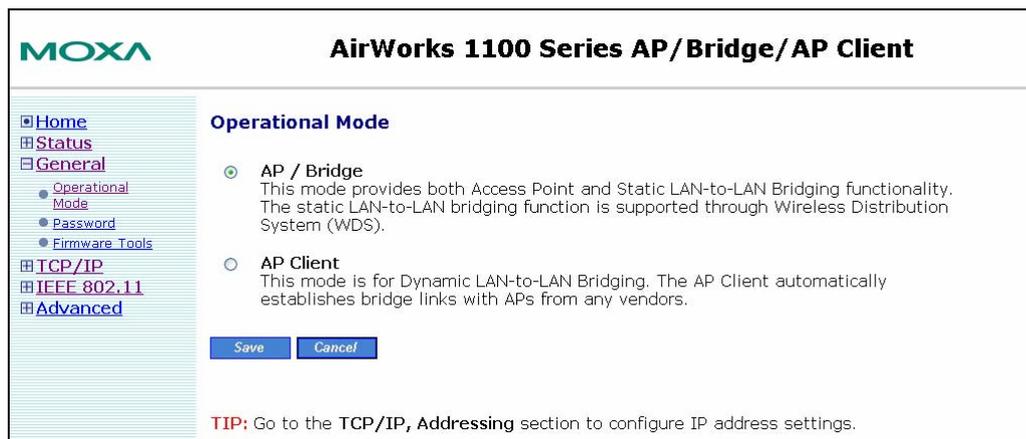
User name: **admin**
Password: **root**



NOTE For security reasons, we strongly recommended changing the password. To do so, open the Network Manager homepage, click on **General** → **Password**, and then follow the onscreen instructions.

Step 5: Select the Operational Mode for AWK-1100

By default, AWK-1100's operation mode is set to **AP/Bridge**. If you want to change the setting, click on **General** → **Operational Mode**, as shown in the following figure, select an operation mode, and then click on **Save** to activate the change.



Go to the **General, Operational Mode** section, select an operational mode and then click **Save** at the bottom of this page. This will take you back to the starting page.

The AP supports 2 operational modes:

- **AP/Bridge.**
This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through WDS (Wireless Distribution System).
- **AP Client.**
This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.
In either mode, the AWK-1100 forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

NOTE Detailed information about configuring AWK-1100's Operation Mode is given in Chapter 3.

Step 6: Configure AWK-1100's IEEE 802.11 settings

AP functionality:	Enabled ▾
RF type:	Mixed ▾
Regulatory domain:	FCC (U.S.)
Channel number:	11 ▾
Network name (SSID):	MOXA
Data rate:	Auto ▾
Transmit power:	100% ▾
Fragment threshold:	2346
RTS threshold:	3000
Preamble type:	Auto ▾

Go to the IEEE 802.11 Communication section to configure IEEE 802.11g-related communication settings, including Regulatory domain, Channel number, and Network name (SSID).

The number of available RF channels depends on local regulations; therefore, you will need to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the AWK-1100 must be identical for them to be able to communicate with each other.

When you are finished, click on **Save** at the bottom of the page. This will return you to the home page.

Step 7: Review and Apply Settings


AirWorks 1100 Series AP/Bridge/AP Client

- [Home](#)
- [Status](#)
- [General](#)
- [TCP/IP](#)
- [IEEE 802.11](#)
- [Advanced](#)

Restart
Cancel

The settings have been changed. Click **Restart** to restart the Bridge/AP for the settings to take effect.

Bridge/AP Settings and Info	
Model	AWK-1100
BIOS/Firmware Version	APXS-2510 v1.3/1.0.0.1
Operational Mode	Access Point
MAC Address	00-09-92-01-60-AE
System Up Time (hr:min:sec)	0:00:20
TCP/IP Settings	LAN Interface <ul style="list-style-type: none"> • IP address: 192.168.127.253 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	<ul style="list-style-type: none"> • RF type: Mixed • Regulatory domain: FCC (U.S.) • Channel number: 6 • Network name (SSID): moxa • Data rate: Auto • Transmit power: High • Security mode: Open System

On the home page, you can review all of the settings you have made. Changes are highlighted in red. If the changes are okay, click on **Restart** to restart the AWK-1100 for the new settings to take effect.

NOTE About 10 seconds are needed for the AP to complete its restart process.

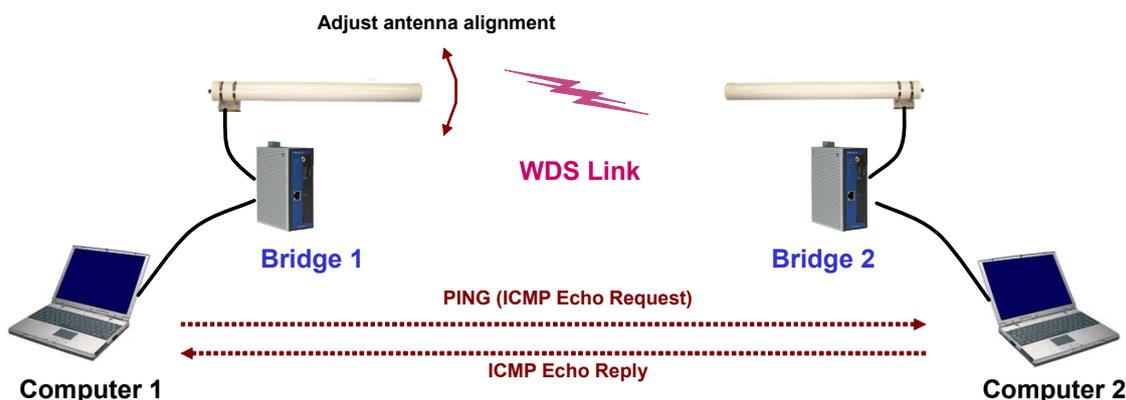
Deploying the Access Point (AP)

After the settings have been configured, deploy the AP to the field application environment. Connect the AP to an Ethernet LAN through an Ethernet switch or hub.

If you are configuring a pair of the AWK-1100s for AP mode for a dynamic or static bridging application and external high-gain directional antennas are used, it is difficult to adjust alignments of the antennas when the pair of devices are far away.

To adjust the alignments of a pair of bridges' directional antennas:

1. Connect each bridge to a computer via Ethernet
2. Configure the data rate of each bridge to the lowest value, 1 Mbps.
3. Fix the alignment of the antenna on one side.
4. Adjust the alignment of the antenna on the other side by using response time information obtained by pinging (i.e., running PING.exe) the "fixed-side" computer.
5. Fine-tune the alignment of the antenna until you get a best response time.
6. Increase the data rate of each bridge simultaneously until a maximum workable data rate is reached. You may not be able to use the highest data rate, 54 Mbps, because of the distance and the gain of the antennas.



Setting up Client Computers

The TCP/IP and IEEE 802.11g-related settings of wireless client computers must match those of the Access Point.

Configuring IEEE 802.11g-related Settings

Open Internet Explorer and type AWK-1100's IP address in the **Address** field. Press **Enter** to establish the connection.

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between this wireless computer and an Access Point.

To establish a wireless link to an Access Point:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.
2. Use the utility to make appropriate *Operating Mode*, *SSID*, and *WEP* settings.

NOTE A wireless client computer must be in *infrastructure* mode to associate with an AP.

NOTE The SSID of the wireless client computer and the SSID of the AP must be identical. Or, if the **SSID broadcast** capability of the AP is enabled (default setting), the SSID of the wireless client computer could be set to "any."

NOTE Both the wireless client computer and the Access Point must have the same WEP settings for them to communicate with each other.

NOTE For better wireless security, IEEE 802.1X capability of the Access Point must be enabled so that only authenticated wireless users can access the wireless network.

Configuring TCP/IP-related Settings

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the client computers so that the IP addresses of the client computers and the IP address of the Access Point are in the same IP subnetwork.

If a client computer is originally setup with a static IP address, you can either change its IP address to match the IP address of the Access Point, or select the option "automatically-obtain-an-IP-address" if there is a DHCP server on the network.

NOTE For some versions of Windows, the computer needs to be restarted for the new TCP/IP settings to take effect.

Confirming the Settings of the AP and Client Computers

After you have completed deploying the Access Point and setting up client computers, you must make sure the settings you have made are correct.

Checking if the IEEE 802.11g-related Settings Work

To check if a wireless client computer can associate with the AWK-1100:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.
2. Check if the client computer is associated to an AWK-1100. If the check fails, see Appendix B, "Wireless Settings Problems," to troubleshoot the problem.

Checking if the TCP/IP-related Settings Work

To check if a client computer can assess the Internet:

1. Open a **Windows Command Prompt** window on the client computer.
2. Type "**ping** *AP*", where *AP* is the IP address of the Access Point. Replace it with your real IP address—for example, 192.168.127.253, and then press **Enter**.
If the AP responds, go to the next step; otherwise see Appendix B, "TCP/IP Settings Problems" to troubleshoot the problem.
3. Type "**ping** *default_gateway*", where *default_gateway* is the IP address of the default gateway of the wireless client computer, and then press **Enter**. If the gateway responds, go to the next step; otherwise, see Appendix B, "TCP/IP Settings Problems," to troubleshoot the problem.
4. Type "**ping** *Ist_dns_server*", where *Ist_dns_server* is the IP address of the primary DNS server of the wireless client computer, and then press **Enter**. If this DNS server responds, go to the next step; otherwise, see Appendix B, "TCP/IP Settings Problems," to troubleshoot the problem.

Web Console Configuration

In this chapter, we will explain each Web management page of the Web-based Network Manager.

The following topics are covered in this chapter:

- ❑ **Overview**
 - Menu Structure
 - Save, Save & Restart, and Cancel Buttons
 - Home and Refresh Buttons
- ❑ **Viewing Status**
 - Associated Wireless Clients
 - Current DHCP Mappings
 - System Log
 - Link Monitor (AP Client mode only)
- ❑ **General Operations**
 - Specifying Operational Mode
 - Administrative Password
 - Managing the Firmware
- ❑ **Configuring TCP/IP-related Settings**
 - Addressing
 - DHCP Server (AP/Bridge modes only)
- ❑ **Configuring IEEE 802.11g-related Settings**
 - Communication
 - Security
 - IEEE 802.1X/RADIUS (AP mode only)
- ❑ **Configuring Advanced Settings**
 - Packet Filters
 - Management

Overview

MOXA AirWorks 1100 Series AP/Bridge/AP Client

[Home](#) [Status](#) [General](#) [TCP/IP](#) [IEEE 802.11](#) [Advanced](#)

[Restart](#) You can click **Restart** to restart the AP

Bridge/AP Settings and Info	
Model	AWK-1100
BIOS/Firmware Version	APXS-2510 v1.3/1.0.0.1
Operational Mode	Access Point
MAC Address	00-09-92-01-60-AE
System Up Time (hr:min:sec)	0:00:02
TCP/IP Settings	<p>LAN Interface</p> <ul style="list-style-type: none"> IP address: 192.168.127.253 Subnet mask: 255.255.255.0 Default gateway: 0.0.0.0
	<ul style="list-style-type: none"> RF type: Mixed Regulatory domain: FCC (U.S.) Channel number: 11 Network name (SSID): MOXA Data rate: Auto Transmit power: High Security mode: Open System

Menu Structure

The left side of the home page contains a menu that you can use to carry out commands. Here is a brief description of the hyperlinks in the menu:

- **Home.** For returning to the home page.
- **Status.** Status information.
 - **Wireless Clients.** The status of the wireless clients currently associated with the AP.
 - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.
 - **System Log.** System events log.
 - **Link Monitor.** When the AWK-1100 is in *AP Client* mode, this page shows the signal strength and link quality of the wireless link to its associated access point.
- **General.** Global operations.
 - **Operational Mode.** Operational mode of the AWK-1100—*AP/Bridge* or *AP Client*.
 - **Password.** For gaining rights to change the settings of the AWK-1100.
 - **Firmware Tools.** For upgrading the firmware of the AWK-1100, backing up and restoring the configuration, and resetting the AWK-1100's configuration to factory defaults.
- **TCP/IP.** TCP/IP-related settings.
 - **Addressing.** IP address settings for the AP to work with TCP/IP.
 - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the Access Point.
- **IEEE 802.11.** IEEE 802.11g-related settings.
 - **Communication.** Basic settings for the IEEE 802.11g interface of the AWK-1100 to work properly with wireless clients.
 - **Security.** Security settings for authenticating wireless users and encrypting wireless data.
 - **IEEE 802.1X/RADIUS.** IEEE 802.1X Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service) settings for better wireless security.

- **Advanced.** Advanced settings of the AWK-1100.
 - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
 - **Management.** UPnP, System Log, and SNMP settings.

Save, Save & Restart, and Cancel Buttons



There are three buttons at the bottom of each page that contains configurable settings—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores changes to the AWK-1100's memory and returns you to the home page. Clicking **Save & Restart** stores the changes to the AWK-1100's memory and restarts the AWK-1100 to activate the new settings. Clicking **Cancel** discards any changes already made and returns you to the home page.

Note that if you click on **Save**, the home page will reflect the fact that the configuration settings have been changed by displaying two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Restart** restarts the AP to activate the new settings. Clicking **Cancel** discards all of the changes.

 A screenshot of the MOXA web console configuration page for an AirWorks 1100 Series AP/Bridge/AP Client. The page has a sidebar menu on the left with options: Home (selected), Status, General, TCP/IP, IEEE 802.11, and Advanced. The main content area shows a 'Bridge/AP Settings and Info' table. Above the table are 'Restart' and 'Cancel' buttons. A red message states: 'The settings have been changed. Click Restart to restart the Bridge/AP for the settings to take effect.' The table contains the following data:

Bridge/AP Settings and Info	
Model	AWK-1100
BIOS/Firmware Version	APXS-2510 v1.3/1.0.0.1
Operational Mode	Access Point
MAC Address	00-09-92-01-60-AE
System Up Time (hr:min:sec)	0:00:20
TCP/IP Settings	LAN Interface • IP address: 192.168.127.253 • Subnet mask: 255.255.255.0 • Default gateway: 0.0.0.0
	• RF type: Mixed • Regulatory domain: FCC (U.S.) • Channel number: 6 • Network name (SSID): moxa • Data rate: Auto • Transmit power: High • Security mode: Open System

Home and Refresh Buttons



At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the home page. Clicking **Refresh** updates the status information showing on the page.

Viewing Status

Associated Wireless Clients

Wireless Clients Status						
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-90-4B-00-40-94	192.168.168.226		7521	1162	00h:01m:56s

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1X authenticated), number of bytes it has sent, number of bytes it has received, and the time of its last activity, is shown.

Current DHCP Mappings

DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

On this page, all the current *static* or *dynamic* DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page. A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool specified by the **First allocateable IP address** and **allocateable IP address count** settings on the **DHCP Server** configuration page.

System Log

Model:	AWK-1100
BIOS/Firmware version:	APXS-2510 v1.3/1.0.0.1
Operational mode:	Access Point
Current time:	2005/07/04
<hr/>	
2005/07/04 13:14:20 SYSTEM START UP!	
2005/07/04 13:14:20 Wireless LAN interface initializes success.	
2005/07/04 13:14:20 Mac address --> 00-09-92-01-60-99	
2005/07/04 13:14:20 LAN IP address --> 192.168.127.104.	
2005/07/04 13:14:20 Wireless client 00-12-F0-5B-86-43 is associated with.	
2005/07/04 13:14:20 Wireless client 00-12-F0-5B-86-43 is disassociated with.	
2005/07/04 13:14:20 DHCPD: 192.168.127.21 is assigned to client(00-0C-F1-1D-5A-E3).	
2005/07/04 13:14:20 DHCPD: 192.168.127.21 is released to IP pool.	
2005/07/04 13:14:20 DHCPD: 192.168.127.22 is assigned to client(00-0C-F1-1D-5A-E3).	

System events are recorded in the memory of the AWK-1100. The logged information is useful for troubleshooting purposes. The system events are divided into several categories, and you can select which categories of events to log.

Link Monitor (AP Client mode only)

Linking Quality :	10 %
Signal Strength :	25 %

When the AWK-1100 is in *AP Client* mode, you can use the Link Monitor status page to monitor the link quality and signal strength sensed by its RF module. Larger values means better wireless connectivity to its associated Access Point. This feature is especially useful when you are aligning a pair of directional antennas for bridging applications.

NOTE The values are updated every 20 seconds.

General Operations

Specifying the Operational Mode

- AP / Bridge**
This mode provides both Access Point and Static LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- AP Client**
This mode is for Dynamic LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendors.

Go to the **General, Operational Mode** section, select an operational mode and then click **Save** at the bottom of this page. This will take you back to the starting page.

The AP supports 2 operational modes:

- **AP/Bridge.**
This mode provides both Access Point and *Static* LAN-to-LAN Bridging functionality. The static LAN-to-LAN bridging function is supported through Wireless Distribution System (WDS).
- **AP Client.**
This mode is for *Dynamic* LAN-to-LAN Bridging. The AP Client automatically establishes bridge links with APs from any vendor.

In either mode, the AWK-1100 forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links as specified by the IEEE 802.11 standard.

- **STA-AP.**
This type of wireless link is established between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC). The AP Client mode is actually an STA.
- **WDS.**
This type of wireless link is established between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP/Bridge	AP Client
AP/Bridge	WDS	STA-AP
AP Client	STA-AP	

To establish a *static* bridge link based on WDS, the AP/bridges at both end of the WDS link must be configured *manually* with each other's MAC addresses. To establish a *dynamic* bridge link between an AP and an AP Client, both devices must be configured with the same SSID and WEP settings. The AP Client automatically scans for any AP that is using the matched SSID and establishes a bridge link with the scanned AP.

NOTE Although it's more convenient to use dynamic bridging, it has a limitation—the AP Client can only transmit TCP/IP packets between its wireless interface and Ethernet interface; other types of traffic (such as IPX and AppleTalk) are not forwarded.

TIP When the AP is configured to be in AP Client, it can be used as an Ethernet-to-wireless network adapter. For example, a notebook computer equipped with an Ethernet adapter, but no wireless card, can be connected to this device with an Ethernet cable for wireless connectivity to another access point.

Administrative Password

Old password:	<input type="password" value="****"/>
New user name:	<input type="text" value="admin"/>
New password:	<input type="password" value="*****"/>
New password again:	<input type="password" value="*****"/>

On this page, you can change the user name and password. The new password must be typed twice to confirm (note that the default user Name and Password or “admin” and “root,” respectively).

Managing the Firmware

Firmware management protocol:	<input type="text" value="HTTP"/>
-------------------------------	-----------------------------------

Firmware management operations for AWK-1100 include “Firmware Upgrade,” “Configuration Backup,” “Configuration Restore,” and “Configuration Reset (Factory Defaults). Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based method is suggested because it is more user friendly. However, due to the fact that different Web browsers and versions behave differently, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based method.

Upgrading Firmware by HTTP

Firmware Upgrade	
Firmware file name:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	

To upgrade the firmware of AWK-1100 by HTTP:

1. Click **Browse** and then select a correct firmware **.bin** file. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Upgrade** to begin the upgrade process.

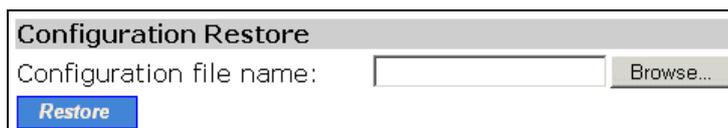
Backing up and Restoring Configuration Settings by HTTP



To back up the configuration of AWK-1100 by HTTP (i.e., export the configuration to a file):

1. Click on **Back Up**
2. You will be prompted to open or save the configuration file. Click on **Save**.
3. The configuration file is named with the AWK-1100's MAC address. For example, if the AWK-1100's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex". Don't change the configuration file name in the **Save As** dialog box. Select the folder in which the configuration file is to be stored, and then click on **Save**.

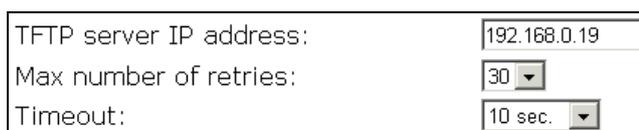
NOTE The procedure may be different for different Web browsers (IE, Netscape, etc.).



To restore the configuration of the AWK-1100 by HTTP (i.e., import the configuration from a file):

1. Click **Browse** and then select the correct configuration **.hex** file. You must make sure the file name is the AWK-1100's MAC address. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Restore** to upload the configuration file to the AWK-1100.

Upgrading Firmware by TFTP



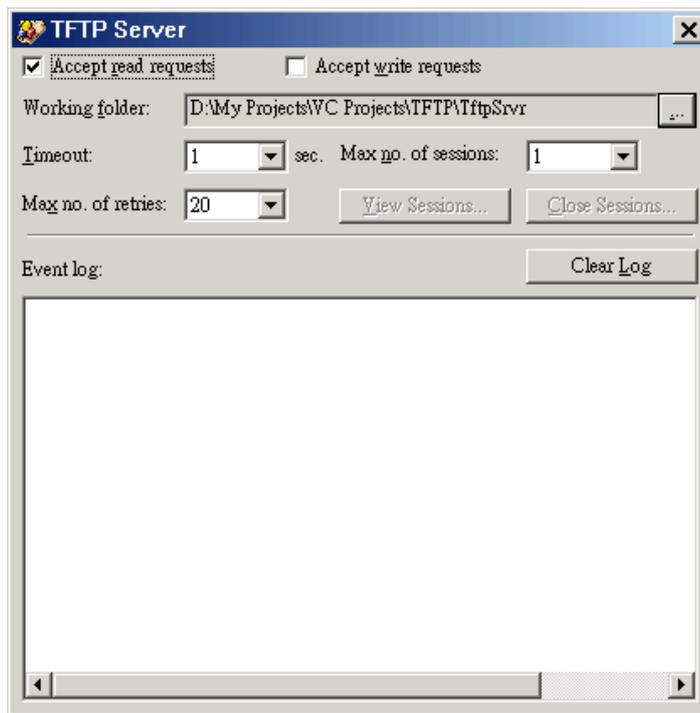
When using TFTP as the firmware management protocol, you can configure settings for the AP's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. The **Max number of retries** setting specifies the maximum number of resends before the TFTP client stops communicating with the TFTP server.



To upgrade AWK-1100's firmware by TFTP:

1. Prepare a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.

- Configure the IP address of the computer so that the AWK-1100 and the computer are on the same IP subnet.
- On the computer, run the TFTP Server utility, and specify the folder in which the firmware files will be placed.
- On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
- Choose **TFTP** as the **Firmware management protocol**.
- Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type **ipconfig**, then press the **Enter** key.
- Trigger the firmware upgrade process by clicking **Upgrade**.



NOTE After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

Make sure the **Accept read requests** check box of the TFTP Server is selected.

The LAN IP address of the AP and the IP address of the TFTP server must be on the same IP subnet for TFTP to work.

Due to the unreliable nature of wireless media, it is highly recommended that the TFTP server and the wireless AP that is being upgraded are connected by Ethernet on the same LAN. Doing so will help ensure a much smoother upgrade process.

After the firmware is upgraded, be sure to delete the contents of the Web browser cache so that the Web management pages can be shown correctly.

A failed upgrade may corrupt the firmware and cause the AWK-1100 to fail. When this occurs, contact MOXA technical support for assistance.

TIP If you want to upgrade the firmware of a deployed AP from a remote location over the Internet, adjust the **Timeout** and **Max no. of retries** settings of the TFTP Server for remote TFTP upgrade to succeed.

Backing up and Restoring Configuration Settings by TFTP



To back up the configuration of the AWK-1100 by TFTP:

1. Prepare a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.
2. Connect the computer and one of the LAN Ethernet switch ports with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the AWK-1100 are on the same IP sub-net.
4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the AP will be saved.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer that acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type **ipconfig**, then press the **Enter** key.
8. Trigger the backup process by clicking **Back Up**. The AWK-1100's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "**AaBbCcDdEeFf**" is the AWK-1100's MAC address. For example, if the AWK-1100's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE Remember to select the **Accept write requests** check box of TFTP Server.

To restore the configuration of the AWK-1100 by TFTP:

1. Prepare a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.
2. Connect the computer and one of the LAN Ethernet switch ports with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the AWK-1100 are on the same IP subnet.
4. On the computer, run the TFTP Server utility, and specify the folder in which the configuration backup file resides. A configuration backup file is named with the AWK-1100's MAC address. For example, if the AWK-1100's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".
5. On the computer, open the web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. In the **Configuration Backup/Restore** section, specify the IP address of the computer that acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, type **ipconfig**, and then press the **Enter** key.
8. Trigger the restoring process by clicking **Restore**. The AWK-1100 will then download the configuration backup file from the TFTP server.

NOTE Make sure the file is a valid configuration backup file for AWK-1100.

TIP If you want to back up or restore the configuration from a remote location over the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

Resetting the Configuration to Factory Defaults

Configuration Reset (Factory Defaults)
<input type="button" value="Reset"/>

Clicking the **Reset** button resets the device configuration to factory defaults.



WARNING

Think twice before clicking the **Reset** button. Doing so will cause you to lose all of your current configuration settings.

Configuring TCP/IP-related Settings

Addressing

Method of obtaining an IP address:	<input type="text" value="Set Manually"/>
IP address:	<input type="text" value="192.168.168.214"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Default gateway:	<input type="text" value="0.0.0.0"/>
Host name:	<input type="text" value="AP1"/>
Domain (DNS suffix):	<input type="text"/>

The IP address of the AP can be set manually (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server**). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the AWK-1100.

DHCP Server (AP/Bridge modes only)

Basic

Functionality:	Disabled ▾
Default gateway:	192.168.0.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.0.1
Secondary DNS server:	
First allocatable IP address:	192.168.0.2
Allocatable IP address count:	20

AWK-1100 can assign IP addresses to client computers automatically by DHCP. In this section of the management page, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocatable IP addresses.

NOTE There should only be *one* DHCP server on the LAN; otherwise, DHCP will not work properly. If there already is a DHCP server on the LAN, disable the DHCP server functionality of the AWK-1100.

By default the DHCP server function is disabled.

Static DHCP Mappings

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	Bill	00-22-32-5D-80-02	192.168.0.203
<input type="checkbox"/>			

IP addresses of servers are often static so that clients can always locate the servers by the static IP addresses. By using **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP so that it is always assigned the same IP address.

To assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.
2. Select the corresponding **Enabled** check box.

Configuring IEEE 802.11g-related Settings

Communication

Basic

Basic IEEE 802.11g-related communication settings include **AP functionality**, **RF type**, **Regulatory domain**, **Channel number**, **Network name (SSID)**, **Data rate**, and **Transmit power**.

AP functionality:	Enabled ▾
RF type:	Mixed ▾
Regulatory domain:	FCC (U.S.)
Channel number:	11 ▾
Network name (SSID):	MOXA
Data rate:	Auto ▾
Transmit power:	100% ▾
Fragment threshold:	2346
RTS threshold:	3000
Preamble type:	Auto ▾

For specific needs such as configuring the AWK-1100 as a wireless LAN-to-LAN bridge, the AP functionality can be disabled so that no wireless client can associate with the AP.

The RF type of the WLAN interface can be configured to work with IEEE 802.11b only (B Only), IEEE 802.11g only (G Only), B WIFI mode (for internal usage), or mixed mode (Mixed—802.11g and 802.11b simultaneously).

The number of available RF channels depends on local regulations; therefore, you must choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the AP must be identical for them to communicate with each other.

If you experience RF interference, you may want to reduce the Data rate to ensure a more reliable wireless transmission. In most cases, leave the setting to Auto.

The transmit power of the RF module of the AWK-1100 can be adjusted so that the RF coverage of the AWK-1100 can be changed.

Link Integrity

Functionality:	Disabled ▾
Reference host:	0.0.0.0

When the Ethernet LAN interface has been detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the AP and no wireless client can associate with the AP. The detection mechanism is based on pinging the IP address specified in the **Reference host**.

Association Control

Max number of clients (1~64):	<input type="text" value="64"/>
Block clients if traffic load exceeds:	<input type="button" value="Disabled"/>

If the number of currently associated wireless clients exceeds the value specified in the **Max number of clients** setting, no more wireless clients can associate with the AWK-1100. If the traffic load of the AWK-1100 exceeds the load specified in the **Block clients if traffic load exceeds** setting, no more wireless clients can associate with the AWK-1100.

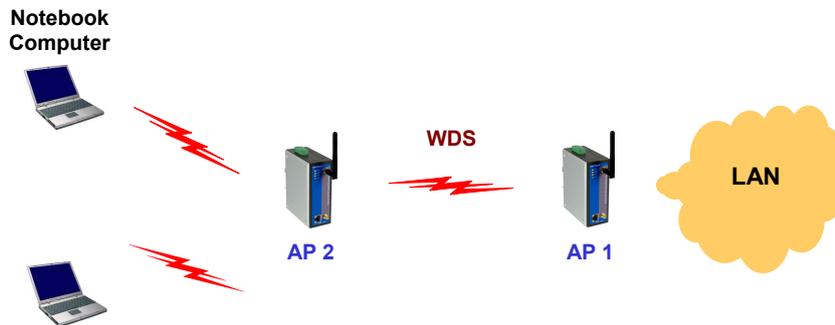
AP Load Balancing

Functionality:	<input type="button" value="Enabled"/>
Group ID:	<input type="text" value="APLB_Group"/>
Policy by:	<input type="button" value="Number of Users"/>

Several APs can form a load-balancing group if they are set with the same Group ID. The load-balancing policy can be by **Number of Users** or by **Traffic Load**.

If the *by-number-of-users* policy is selected, a new wireless user can only associate with an AP that has the smallest number of associated wireless users in the group. On the other hand, if the *by-traffic-load policy* is selected, a new wireless user can only associate with an AP that has the least traffic load in the group.

Wireless Distribution System



Traditionally, access points are connected by Ethernet. By using a Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 plays a role of “AP repeater.”



By WDS, two or more LAN segments can be connected wirelessly. As illustrated in the above figure, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled, it can be used as a wireless bridge.

NOTE An AWK-1100 can have up to 6 WDS links to other APs or wireless bridges.

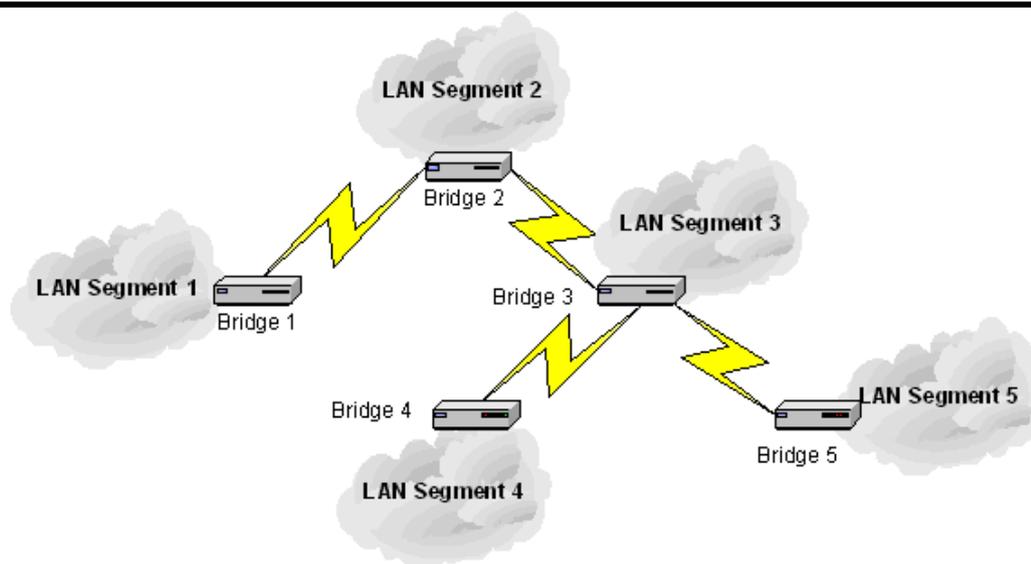
Port	Enabled	Peer MAC Address
1	<input type="checkbox"/>	00-02-6F-01-62-C5
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	

To enable a WDS link:

1. Specify the MAC address of the AWK-1100 at the other end of the WDS link.
2. Select the corresponding **Enabled** check box.

For example, assume that you want two AWK-1100s with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link. On the AWK-1100 with MAC address 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AWK-1100 with MAC address 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP Plan your wireless network and draw a diagram so that you know how each AWK-1100 is connected to other peer APs or wireless bridges by WDS, and how bridges are connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

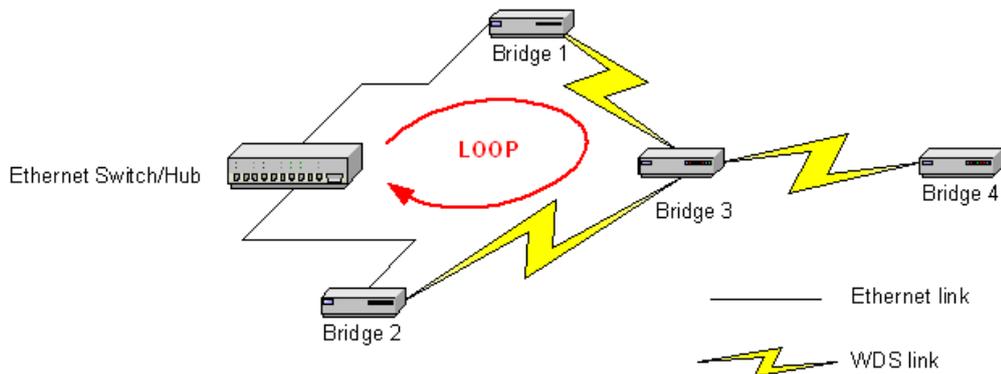


Sample wireless bridge network topology.



WARNING

Be sure to eliminate loops from networks that consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.



Network topology containing a loop

Security

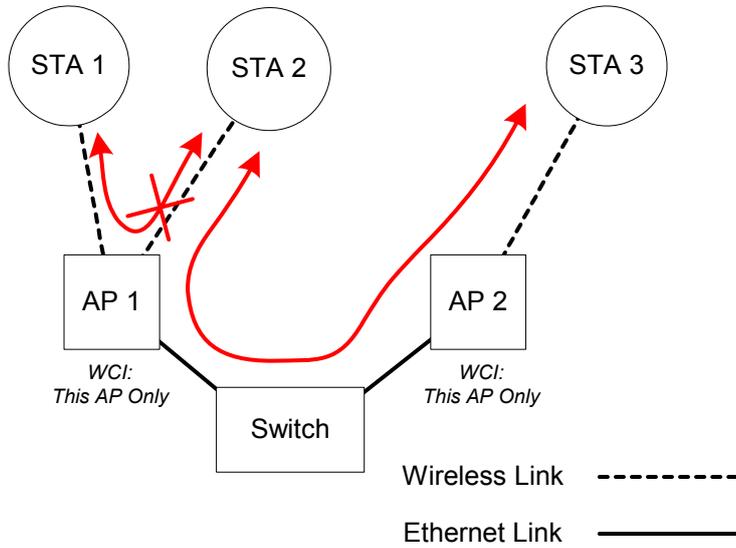
IEEE 802.11g security settings include **SSID broadcasts**, **Wireless client isolation**, **Security mode**, **IEEE 802.11 Authentication algorithm**, **WEP keys**, **MAC-Address-Based Access Control**.

Basic

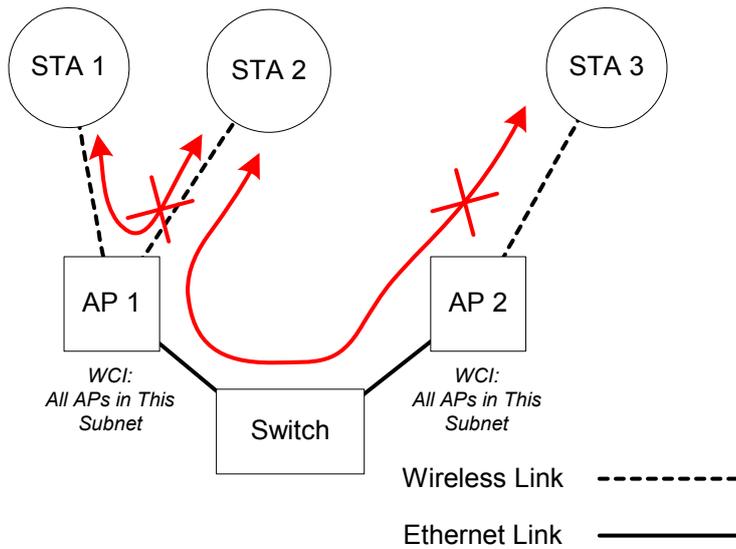
SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	Static WEP
Authentication algorithm:	Auto
Key length:	64 Bits
Selected key:	Key 1
Key 1:	*****
Key 2:	*****
Key 3:	*****
Key 4:	*****

For security reasons, it is highly recommended that the security mode be set to options other than **Open System**. When the security mode is set to Open System, no authentication or data encryption will be performed. In addition, you can disable the SSID broadcast functionality so that a wireless client computer with an SSID set to “any” cannot associate with the AWK-1100.

When the Wireless client isolation setting is set to **This AP Only**, wireless clients of this AP cannot see each other, and wireless-to-wireless traffic is blocked. When the setting is set to **All APs in this Subnet**, traffic among wireless users from different APs in the same IP subnet is blocked. This feature is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a hotspot. The behaviors are illustrated in the following figures.



Behavior of the “This AP Only” wireless client isolation option



Behavior of the “All APs on This Subnet” wireless client isolation option

When AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, whereas wireless traffic between STA 2 and STA 3 (which are associated with different APs) is still allowed. If the “All APs in This Subnet” option is used as shown in above figure, AP 1 and AP 2 communicate with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

A total of 7 security modes are available with the different AWK-1100 models:

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.
- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you need to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

NOTE The number of characters of the **Pre-shared key** setting must be at least 8 and can be up to 63.

- **IEEE 802.1X EAP without Encryption (EAP-MD5).** The IEEE 802.1X functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- **IEEE 802.1X EAP with Static WEP (EAP-MD5).** The IEEE 802.1X functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- **IEEE 802.1X EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1X functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- **IEEE 802.1X EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1X dynamic key exchange mechanisms are enabled. The AP is highly secure in this mode.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled. See Section 0 for more information about IEEE 802.1X and RADIUS.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless clients with various WLAN network adapters. There are three options available, including *Open System*, *Shared Key*, and *Auto*.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

NOTE Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

MAC-Address-Based Access Control

Functionality:	<input type="text" value="Enabled"/>
Access control type:	<input checked="" type="radio"/> inclusive <input type="radio"/> exclusive
<input type="text"/>	<input type="button" value="Add"/>
MAC address format: 00-02-DD-30-03-1E	
MAC Address	Delete
00-50-C2-01-96-4D	<input type="button" value="Delete"/>
00-09-92-01-02-55	<input type="button" value="Delete"/>

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to associate with the AWK-1100. When the table type is set to *inclusive*, entries in the table are permitted to associate with the AWK-1100. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the AWK-1100.

To *deny* access for wireless clients to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *exclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To *grant* access for wireless clients to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *inclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

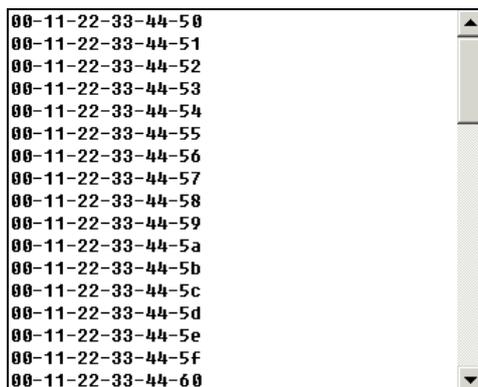
To delete an entry in the access control table:

- Click **Delete** next to the entry.

NOTE The size of the access control table is 64.

TFTP server IP address:	<input type="text" value="192.168.0.125"/>
MAC ACL file name:	<input type="text" value="MacAcl.txt"/>
<input type="button" value="Download"/>	

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the AWK-1100 to download the MAC ACL (Access Control List) file from the TFTP server. The following figure shows the contents of a sample ACL file.



```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60
```

Sample MAC ACL file

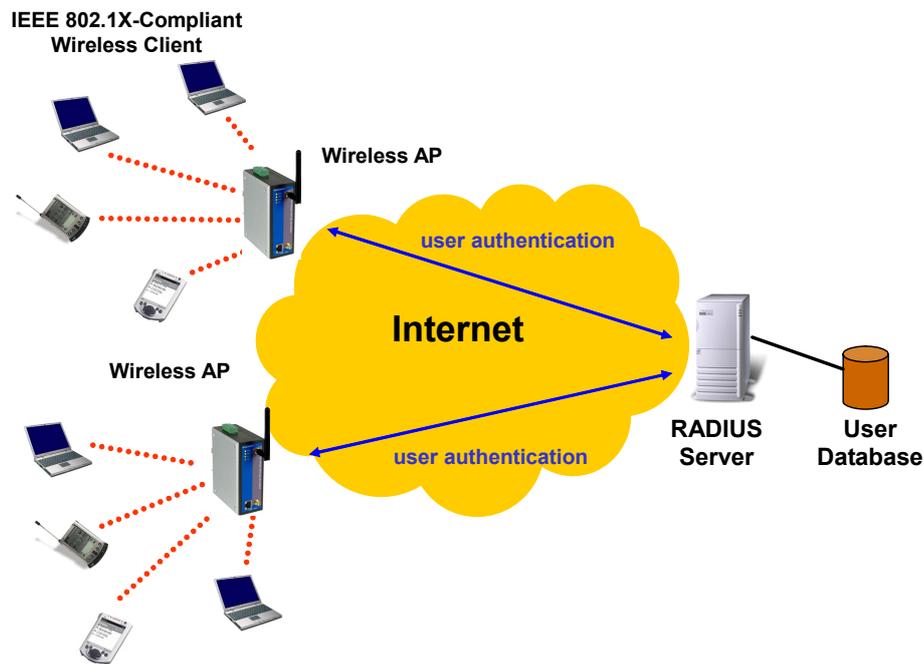
To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.
2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.
3. Click **Download**.

IEEE 802.1X/RADIUS (AP mode only)

IEEE 802.1X *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1X and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before being granted access to a wireless LAN supporting IEEE 802.1X, a user needs to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information, such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1X functionality of the access point is controlled by the *security mode*. So far, the wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5), EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user must give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is generated automatically for encrypting wireless packets sent between the wireless client computer and the associated wireless access point. In short, EAP-MD5 only supports user authentication, whereas EAP-TLS supports both user authentication and dynamic encryption key distribution.



IEEE 802.1X and RADIUS

An access point supporting IEEE 802.1X can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the *secondary* RADIUS server after failing to communicate with the primary RADIUS server.

An IEEE 802.1X-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1X-capable wireless access point must have a *unique* NAS identifier.

Primary RADIUS server:	<input type="text" value="192.168.168.220"/>
Secondary RADIUS server:	<input type="text"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Timeout (sec.):	<input type="text" value="5"/>
Max number of retries:	<input type="text" value="3"/>
Shared key:	<input type="password" value="*****"/>
Identifier of this NAS:	<input type="text" value="AP1"/>

Configuring Advanced Settings

Packet Filters

The AWK-1100 provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

- **Functionality:** whether this filtering capability is *enabled* or *disabled*.
- **Policy for matched packets:** how a matched packet is processed—*discard* or *pass*.
- **To enable a filtering rule:** select the check box to the left of the rule.

Ethernet Type Filters

Functionality:	Disabled
Policy for matched packets:	Discard
Name	Number
<input checked="" type="checkbox"/> RARP	0x8035
<input type="checkbox"/> ARP	0x0806
<input type="checkbox"/> NetBUI	0xF0F0
<input type="checkbox"/> Novell IPX	0x8138
<input type="checkbox"/> IPX 802.3	0x00FF

The filed *Ethernet type* of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. As a rule, specify the hex-decimal Ethernet type number and give the rule a name.

IP Protocol Filters

Functionality:	Disabled			
Policy for matched packets:	Discard			
Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask
<input checked="" type="checkbox"/> 0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255
<input type="checkbox"/> 0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
<input type="checkbox"/> 0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. As a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

A source/destination IP address range is determined by performing an AND operation on the source/destination IP address field and the source/destination subnet mask field. For example, if the source IP address field is 192.168.127.253 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.127.0 to 192.168.127.255.

TCP/UDP Port Filters

Functionality:	Disabled ▾	
Policy for matched packets:	Discard ▾	
	Destination Port	Protocol
<input checked="" type="checkbox"/>	80	TCP ▾
<input type="checkbox"/>	0	TCP ▾
<input type="checkbox"/>	0	TCP ▾
<input type="checkbox"/>	0	TCP ▾
<input type="checkbox"/>	0	TCP ▾
	Application Name	
	HTTP	

The *destination port* field of the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. As a rule, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

Management

UPnP

Functionality:	Enabled ▾
Device friendly name:	Wireless AP

UPnP (Universal Plug and Play) enables a Windows XP user to discover peripheral devices automatically by HTTP. When the UPnP functionality is enabled, you can see the AP in My Network Places of Windows XP. The AWK-1100 can be given a *friend name* that will be shown in My Network Places. *Double-clicking* the icon in My Network Places that stands for the AP will launch the default Web browser for you to configure the AWK-1100.

System Log

<input checked="" type="checkbox"/> Local log
<input type="checkbox"/> Remote log by SNMP trap
Event Types
<input checked="" type="checkbox"/> General
<input checked="" type="checkbox"/> Build-in AP
<input checked="" type="checkbox"/> MIB II traps
<input checked="" type="checkbox"/> RADIUS user authentication

System events can be logged to the on-board RAM of the AWK-1100 (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

The system events are divided into the following categories:

- **General:** system and network connectivity status changes.
- **Built-in AP:** wireless client association and WEP authentication status changes.
- **MIB II traps:** *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication:** RADIUS user authentication status changes.

NOTE The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the AP via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

SNMP

Functionality:	Enabled ▾
Read-only community:	*****
Read-write community:	*****
SNMP Trap Table	
IP Address	Community
<input checked="" type="checkbox"/> 192.168.0.2	*****
<input type="checkbox"/> 0.0.0.0	

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

To specify a trap target :

1. Type the IP address of the target host.
2. Type the **Community** for the host.

Select the corresponding check box next to the IP address text box.



Default Settings

TIP Press the **Reset (SF-Reset, or Soft-Reset)** switch on the housing of a *powered-on* AP to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	admin
Password	root
IEEE 802.11g	
Regulatory Domain	FCC (U.S.) or ETSI (Europe)
Channel Number	11 for FCC or 13 for ETSI
SSID	MOXA
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	100%
MAC Address	See the label on the accompanying PCMCIA card or the label on the housing of the AWK-1100.
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
Link Integrity	Disabled
Association Control	
Max Number of Clients	64
Block Clients if Traffic Load Exceeds	Disabled

LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.127.253
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private
TELNET	Enabled

B

Troubleshooting

Check the following first:

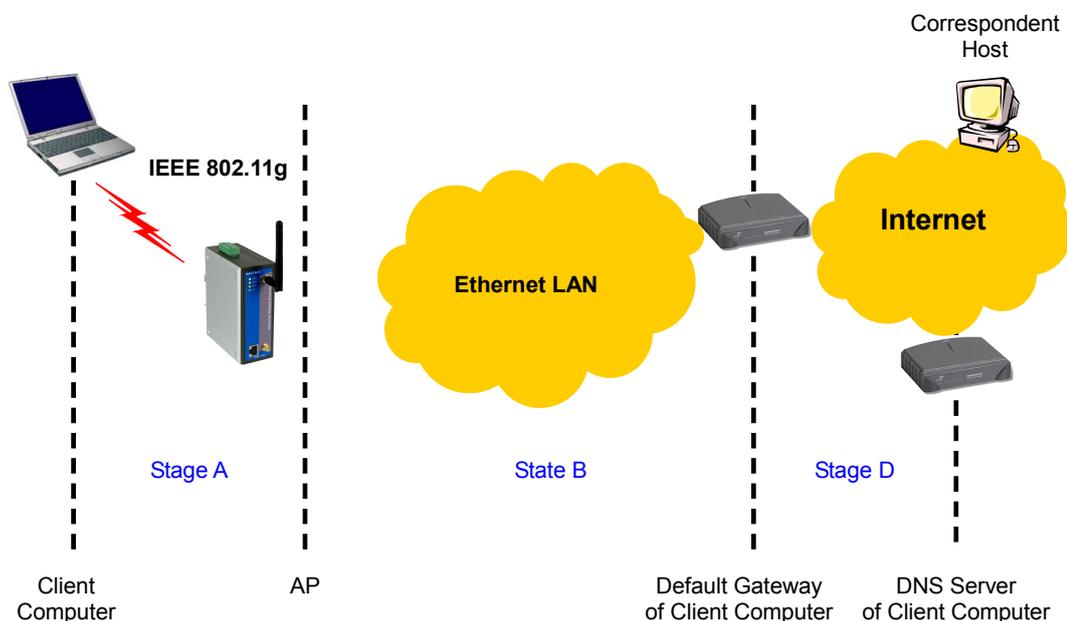
- Make sure that the AWK-1100's power is on and the Ethernet cables are connected firmly to the RJ45 jacks of the AWK-1100.
- Make sure the LED WLAN of the AP is blinking to indicate that the RF is working.
- Make sure you are using the correct types of Ethernet cables. Keep in mind that there are two kind of Ethernet cable—*normal* and *crossover*.

Wireless Settings Problems

The wireless client computer cannot associate with an AWK-1100.

- Is the wireless client set in *infrastructure* mode?
 - Check the *operating mode* of the WLAN NIC.
- Is the SSID of the WLAN NIC identical to that of the prospective AWK-1100?
 - Check the SSID setting of the WLAN NIC and of the AWK-1100.
- Is the WEP functionality of the prospective AWK-1100 enabled?
 - Make appropriate WEP settings of the client computer to match those of the AWK-1100.
- Is the prospective AWK-1100 within range of wireless communication?
 - Check the *signal strength* and *link quality* sensed by the WLAN NIC.

TCP/IP Settings Problems



Communication stages for a client to reach its correspondent host

For a wireless client computer to communicate with a host on the Internet by the host's domain name (e.g., <http://www.wi-fi.com>), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, and then the AP relays this request to the default gateway of the client computer. Finally, this request is forwarded by the gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends additional packets to this IP address.

As illustrated in the above figure, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to determine TCP/IP-related communication problems.

NOTE If *two or more* NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **route.exe**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

The AP does not respond to *ping* from the client computer.

- Are two or more NICs installed on the client computer?
 - Use the OS-provided command-line network tool, **route.exe**, to modify the contents of the routing table.
 - Use Windows-provided **Device Manager** to disable unnecessary NICs.
- Is the underlying link (Ethernet or IEEE 802.11g) established?
 - Make sure the Ethernet link is OK.
 - Make sure the wireless settings of the wireless client computer and of the AP match.

- Are the IP address of the *client computer* and the IP address of the *AP* on the same IP subnet?
 - Use **WinIPCfg.exe** or **IPConfig.exe** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the AP are on the same IP subnet.

TIP

If you forget the current IP address of the AP, use a Wireless Router/AP Browser combination to get the information (see Appendix B-3).

The default gateway of the client computer does not respond to *ping* from the client computer.

- Solve the preceding problem first.
- Are the IP address of the *AP* and the IP address of the *client computer* on the same IP subnet?
- If you cannot locate any incorrect AP settings, the default gateway may be down, or there are other communication problems on the network backbone.

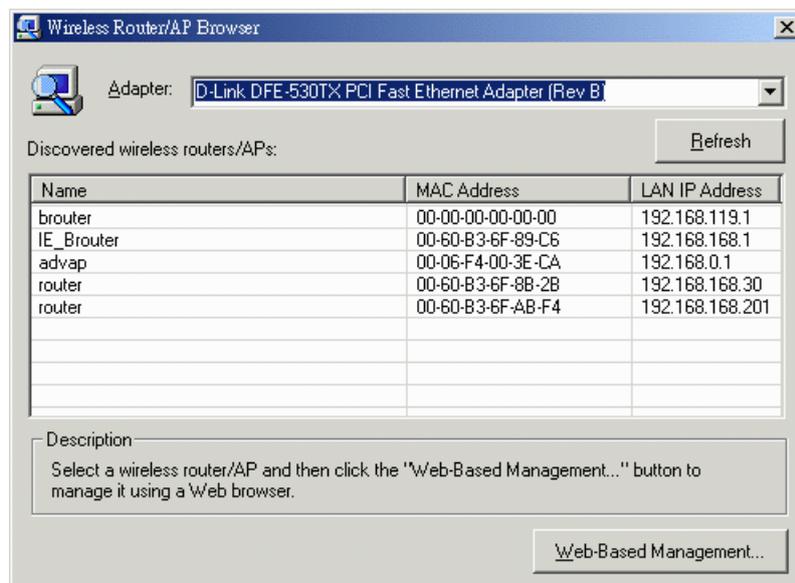
The DNS server(s) of the client computer do not respond to *ping* from the client computer.

- Solve the preceding problems first.
- If you cannot locate any incorrect AP settings, the default gateway of the AP may be down, or there are other communication problems on the network backbone.

Unknown Problems

The AP has been set to obtain an IP address automatically by DHCP. How can I determine the acquired IP address so that I can manage it using a Web browser?

- Use the utility, Wireless Router/AP Browser (**WLBwrsr.exe**), in the “Utilities” folder on the companion CD-ROM disc. This utility can discover nearby APs and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.



Wireless Router/AP Browser

The AWK-1100 stops working and does not respond to Web management requests.

- The firmware of the AP may be stuck in an incorrect state.
 - Unplug the power connector from the power jack, and then re-plug the connector to restart the AP.
 - Report this problem to our technical support staff.
- If the AP still does not work after being restarted, some hardware components of the AP may have failed.
 - Contact our technical support staff.



Regulatory Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.

D

Service Information

This appendix shows you how to contact Moxa for information about this and other products, and how to report problems.

In this appendix, we cover the following topics.

- MOXA Internet Services**
- Problem Report Form**
- Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....support@moxanet.com

World Wide Web (WWW) Site for product information:

.....<http://www.moxa.com>

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- ◆ Provide evidence of original purchase.
- ◆ Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- ◆ Fill out the Problem Report Form (PRF). Include as much detail as possible for a shorter product repair time.
- ◆ Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.