

IWE3200 HotSpot Gateway

User's Guide

Version: 1.0

Last Updated: 08/22/2006



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 radiate 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.

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, 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.

Table of Contents

1. Introduction	1
1.1. Overview	1
1.2. Features.....	2
1.3. LED Definition	7
1.4. Feature Comparison	7
2. First-Time Installation and Configuration	8
2.1. Selecting a Power Supply Method	8
2.2. Mounting the IWE3200 on a Wall	9
2.3. Preparing for Configuration.....	10
2.3.1. Connecting the Managing Computer and the IWE3200	10
2.3.2. Changing the TCP/IP Settings of the Managing Computer	11
2.4. Configuring the IWE3200.....	11
2.4.1. Entering the User Name and Password	11
2.4.2. SETUP WIZARD Step 1: Selecting an Operational Mode	12
2.4.3. SETUP WIZARD Step 2: Configuring TCP/IP Settings	13
2.4.4. SETUP WIZARD Step 3: DHCP Server Settings	15
2.4.5. SETUP WIZARD Step 4: Configure IEEE 802.11 Settings	15
2.4.6. Configuring User Authentication Settings	16
2.4.7. Configuring RADIUS Settings.....	20
2.5. Deploying the IWE3200	21
2.6. Setting up Client Computers.....	22
2.6.1. Configuring IEEE 802.11-Related Settings	22
2.6.2. Configuring TCP/IP-Related Settings	23
2.7. Confirming the Settings of the IWE3200 and Client Computers	23
2.8. Using Web-Based Network Management.....	25
2.8.1. Menu Structure	25
2.8.2. Save, Save & Restart, and Cancel Commands.....	27
2.8.3. Home and Refresh Commands	27
2.9. Seeing Status	28
2.9.1. Associated Wireless Clients	28
2.9.2. Authenticated Users	28
2.9.3. Account Table.....	29
2.9.4. Session List	29
2.9.5. Managed LAN Devices.....	30
2.10. System.....	30
2.10.1. Specifying Operational Mode	30
2.10.2. Changing Password	32
2.10.3. Managing Firmware.....	32
2.10.4. Setting Time Zone	36
2.11. Configuring TCP/IP Related Settings	36
2.11.1. Address	36
2.11.2. DNS	39
2.11.3. NAT	40
2.11.4. DHCP Server.....	41
2.11.5. Load Balancing.....	43
2.11.6. Zero Client Reconfiguration	44
2.12. Configuring Wireless Settings.....	44
2.12.1. Communication.....	44
2.12.2. Security.....	47
2.13. Configuring AAA (Authentication, Authorization, Accounting) Settings	51
2.13.1. Web Redirection	51

2.13.2. RADIUS	55
2.13.3. Authentication Session Control	57
2.13.4. Authentication Page Customization.....	57
2.14. DDNS.....	59
2.15. Configuring Advanced Settings	60
2.15.1. Filters and Firewall	60
2.15.2. Management.....	62
2.15.3. LAN Device Management.....	64
Appendix A.....	66
A-1: Default Settings	66
A-2: LED Definitions	67
A-3: Rear Panel	67
Appendix B: Troubleshooting.....	68
B-1: TCP/IP Settings Problems	68
B-2: Wireless Settings Problems	70
B-3: Other Problems	71
Appendix C: Technical Specifications.....	72
C-1: IWE3200	72
C-2: IWE500-INJ Power Injector.....	74
C-3: IWE810-POS mini-POS Ticket Printer	75

1. Introduction

1.1. Overview

The **IWE3200** Wireless HotSpot Gateway enables Telco operators, wireless ISPs, enterprises, government institutes, or school campuses to deploy WLANs with secured user authentication support. It generates the user log on/off information for back-end billing systems, and user access log status for tracking purpose, which is very useful and demanded function for the environment requires highly security deployment, such as government institute, bank, or military campus.

The **IWE3200** supports multiple xDSL/Cable connections, which balances the in-bond/out-bond load (Multi-homing) and the bandwidth aggregation. The multiple WAN connections provide the failed-over and connection back-up capability to guarantee the ‘always-on-line’ connections. Moreover, with 802.11b/g wireless access point function, it provides wireless bridge mode – WDS. WDS (Wireless Distribution System) provides standard ‘static’ bridges function to joint the LAN segments that may be far separated (e.g., in two buildings, or in campus) to a complete network. Up to 6 WDS bridge links are supported to work with AP function simultaneously.

For hotspot service, **IWE3200** provides 2 kinds of user authentication method: 802.1x/RADIUS and Access Log-on Control. 802.1x/RADIUS is the standard authentication procedure where the *standard 802.1x/RADIUS client and server* devices are both required, while Access Log-on Control provides more flexible authentication procedure that allows the *non-802.1x* wireless users can still be authenticated and managed by the remote RADIUS server. **IWE3200** also provides the capability to allow the operators or the venues owner display their web or advertisement contents during the user login period. With Walled-Garden function, some of the unauthorized wireless users who want to access the internet, the venue owners can limit such users to access certain level of internet resources.

Furthermore, considering the wireless users who may not configure their own network settings on their own Notebook or Handheld device for any reasons, **IWE3200** provides the ‘Zero IP Configuration’ features, so that the wireless users can associate to the hotspot environment without any network configuration on their own Notebook or Handheld device.

IWE3200 also supports the external ticket printer. With optional *IWE810-POS HotSpot mini-POS* for ticket printing and device control, **IWE3200** enables the HotSpot venues to print a ticket for temporary user who will only need the fractal time for internet access in HotSpot Venues.

For the environment or location where the power is difficult to get, **IWE3200** Wireless HotSpot Gateway series provides the optional POE function that compliant with the IEEE802.3af standard with flexible power input via Ethernet cable in some particular environment. It is associated with the *IWE500-INJ POE Injector* for POE application.

The flexible R-SMA detachable antennas can be replaced with high-gain directional/omni-directional antennas for different purposes. All in all, the **IWE3200** Wireless HotSpot Gateway series is the best solution for flexible and security wireless application of SOHO, SME, Enterprise, HotSpots, ISP, Telco operators.

1.2. Features

- **User Authentication, Authorization, and Accounting**

- **Web redirection.** When an unauthenticated wireless user is trying to access a Web page, he/she is redirected to a logon page for entering the user name and password. Then, the user credential information is sent to a back-end RADIUS server for authentication.
- ◆ **Local pages or external pages.** The **IWE3200** can be configured to use *log-on*, *log-off*, *authentication success*, and *authentication failure* pages, which are stored in itself or stored in an external Web server maintained by the WISP. The contents of local authentication pages can be customized.
- ◆ **Advertisement links.** The *log-off* authentication page can be configured to show a sequence of advertisement banners.
- ◆ **Unrestricted clients.** Client computers with specific IP addresses or MAC addresses can bypass the Web redirection-based access control.
- ◆ **Walled garden.** Some specific URLs can be accessed without authentication. These URLs can be exploited by WISPs for advertisement purposes.
- **IEEE 802.1x.** If a wireless client computer supports IEEE 802.1x Port-Based Network Access Control, the user of the computer can be authenticated by the access Router and wireless data can be encrypted by 802.1x EAP authentication method combined with WEP encryption.
- **RADIUS client.** The **IWE3200** communicates with a back-end RADIUS server for wireless user authentication, authorization, and accounting. Authentication methods including EAP-MD5, EAP-TLS/EAP-TTLS, PAP, and CHAP are supported.
- ◆ **Robustness.** To enhance authentication integrity, the access Router can be configured to notify the RADIUS server after it reboots.
- ◆ **Showing authenticated users.** Showing the status and statistics of every RADIUS-authenticated user. And an authenticated user can be terminated at any time for management purposes.
- **Authentication session control.** Several mechanisms are provided for the network administrator to control user authentication session lifetimes.

- **IEEE 802.11b/g Compliant**

- **Wireless Operation**

- ◆ **Access Point.** The AP enables IEEE 802.11 *Stations* (STAs) to *automatically* associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to *manually* establish wireless links between two APs.
- ◆ **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For authentication and data encryption.

- ◆ **Enabling/disabling SSID broadcasts.** The user can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcasts functionality is disabled, a client computer cannot associate the wireless AP with an “any” network name (SSID, Service Set ID); the correct SSID has to be specified on client computers.
 - ◆ **MAC-address-based access control.** Blocking unauthorized wireless client computers based on MAC (Media Access Control) addresses.
 - ◆ **Repeater.** A wireless AP can communicate with other wireless APs via WDS (Wireless Distribution System). Therefore, the wireless AP can wirelessly forward packets from wireless clients to another wireless AP, and then the later wireless AP forwards the packets to the Ethernet network.
 - ◆ **Wireless client isolation.** Wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users’ computers.
 - ◆ **AP load balancing.** Several wireless APs can form a load-balancing group. Within a group, wireless client associations and traffic load can be shared among the wireless APs.
 - ◆ **Transmit power control.** Transmit power of the wireless AP’s RF module can be adjusted to change RF coverage of the wireless AP.
 - ◆ **Showing associated wireless clients.** Showing the status of every wireless client that is associated with the wireless AP.
 - ◆ **Replaceable antennas.** The factory-mounted antennas can be replaced with high-gain antennas for different purposes.
- **Internet Connection Sharing**
 - **DNS proxy.** The **IWE3200** can forward DNS (Domain Name System) requests from client computers to DNS servers on the Internet. And DNS responses from the DNS servers can be forwarded back to the client computers.
 - ◆ **Static DNS mappings.** The network administrator can specify static FQDN (Fully Qualified Domain Name) to IP address mappings. Therefore, a host on the internal network can access a server also on the intranet by a registered FQDN.
 - **DHCP server.** The **IWE3200** can automatically assign IP addresses to client computers by DHCP (Dynamic Host Configuration Protocol).
 - ◆ **Static DHCP mappings.** The network administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.
 - ◆ **Showing current DHCP mappings.** Showing which IP address is assigned to which host identified by an MAC address.

- **NAT server.** Client computers can share a public IP address provided by an ISP (Internet Service Provider) by NAT (Network Address Translation). And our NAT server functionality supports the following:
 - ◆ **Virtual server.** Exposing servers on the intranet to the Internet.
 - ◆ **PPTP, IPsec, and L2TP passthrough.** Passing VPN (Virtual Private Network) packets through the intranet-Internet boundary. PPTP means Point-to-Point Tunneling Protocol, IPsec means IP Security, and L2TP means Layer 2 Tunneling Protocol.
 - ◆ **DMZ (DeMilitarized Zone).** All unrecognized IP packets from the Internet can be forwarded to a specific computer on the intranet.
 - ◆ **Multiple public IP addresses support.** An ISP may provide several public IP addresses to a customer. The **IWE3200** can map each of the public IP addresses to a host with a private IP address on the intranet.
 - ◆ **H.323 passthrough.** Passing H.323 packets through the intranet-Internet boundary so that users on the intranet can use VoIP (Voice over IP) applications.
 - ◆ **MSN Messenger support.** Supporting Microsoft MSN Messenger for chat, file transfer, and real-time communication applications.
 - ◆ **Session monitoring.** Latest 50 incoming sessions and 50 outgoing sessions are shown for monitoring user traffic.
- **DSL/Cable Modem Support.** Supporting dynamic IP address assignment by PPPoE (Point-to-Point Protocol over Ethernet) or DHCP and static IP address assignment.
- **Multiple DSL/Cable connections support.** Supporting up to 4 DSL/cable-based Internet connections. All outgoing traffic load from the internal network is shared among the multiple Internet connections, so that total outgoing throughput is increased.
- **Network Security**
 - **Packet address and port filtering.** Filtering outgoing packets based on IP address and port number. (Incoming packet filtering is performed by NAT.)
 - **URL filtering.** Preventing client users from accessing unwelcome Web sites. The HTTP (HyperText Transfer Protocol) traffic to the specified Web sites identified by URLs (Universal Resource Locators) is blocked.
 - **WAN ICMP requests blocking.** Some DoS (Denial of Service) attacks are based on ICMP requests with large payloads. Such kind of attacks can be blocked.
 - **Stateful Packet Inspection (SPI).** Analyzing incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile.

- **Wireless-to-Ethernet-LAN traffic blocking.** Traffic between the wireless interface and the Ethernet LAN interface can be blocked.
- **Changeable MAC Address of the Ethernet WAN Interface.** Some ADSL modems work only with Ethernet cards provided by the ISP. If **IWE3200** is used in such an environment, the MAC address of the WAN interface of the Router has to be changed to the MAC address of the ISP-provided Ethernet network card.
- **SNTP.** Support for absolute system time by SNTP (Simple Network Time Protocol).
- **Dynamic DNS.** Support for dynamic DNS services provided by *dyndns.org* and *no-ip.com*, so that the access Router can be associated with a domain name even if it obtains an IP address dynamically by PPP, PPPoE or DHCP.
- **LAN Device Management.** The access Router can pass management requests from the Internet through its built-in NAT server to devices on the private network. As a result, network devices (such as access points) behind the NAT server can be managed from the Internet. In this way, the access Router acts as a management proxy for the LAN devices.
- **Firmware Tools**
 - **Firmware upgrade.** The firmware of the IWE3200 can be upgraded, so that more features can be added in the future.
 - ◆ **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).
 - ◆ **HTTP-based.** Upgrading firmware by HTTP (Hepertext Transfer Protocol).
 - **Configuration backup.** The configuration settings of the **IWE3200** can be backed up to a file via TFTP for later restoring.
- **Management**
 - **Web-based Network Manager** for configuring and monitoring the **IWE3200**. The management protocol is HTTP (Hepertext Transfer Protocol)-based. The management protocol is HTTP-based. The access Router can be configured to be managed
 - ◆ Only from the LAN side.
 - ◆ Both from the LAN side and WAN side.
 - ◆ Only from the WAN side.

In addition, it can also be configured to accept management commands only from specific hosts.

- **UPnP.** The access Router responds to UPnP discovery messages so that a Windows XP user can locate the access Router in My Network Places and use a Web browser to configure it.
- **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, Private Enterprise MIB are supported.
- **System log.** For system operational status monitoring.
 - ◆ **Local log.** System events are logged to the on-board RAM of the access Router and can be viewed using a Web browser.
 - ◆ **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.
- **LAN/WAN Configurable Ethernet Switch Ports.** The **IWE3200** provides a 4-port Ethernet switch so that a stand-alone Ethernet hub/switch is not necessary for connecting Ethernet client computers to the Router. These Ethernet ports can be configured as WAN ports for multiple DSL/cable-based Internet connections support.
- **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the **IWE3200**. Accordingly, the **IWE3200** can provide continuous services.
- **Configuration Reset.** Resetting the configuration settings to factory-set values.

1.3. LED Definition

- **PWR** : Power
- **ALV** : Alive. Blinks when the **IWE3200** is working normally.
- **RF** : IEEE 802.11b/g interface activity
- **WAN/LAN** : Ethernet WAN/LAN interface activity

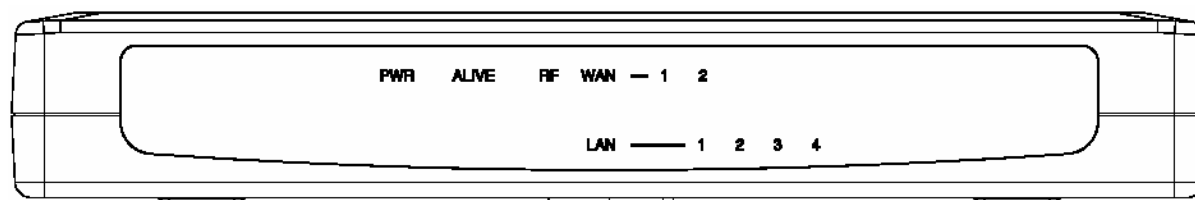


Fig. 1. LED Indicator.

1.4. Feature Comparison

	<i>IWE32000S36X</i> <i>Wired Advanced</i>	<i>IWE32009S36X</i> <i>Wireless Advanced</i>
IEEE 802.11 AP functionality		■
IEEE 802.1x		■
SNMP IEEE 802.1x MIB		■
Wireless client isolation		■
AP load balancing		■

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

The **IWE3200** can be powered by either the supplied AC power adapter or the optional **IWE500-INJ** POE Power Injector. The **IWE3200** automatically selects the suitable power depending on your decision.

To power the IWE3200 by the supplied power adapter:

1. Plug the power adapter to an AC socket.
2. Plug the connector of the power adapter to the power jack of the **IWE3200**.

NOTE:	This product is intended to be power-supplied by a Listed Power Unit, marked “Class 2” or “LPS” and output rated “12V DC, 1.25 A minimum” or equivalent statement.
--------------	--

To power the IWE3200 by IWE500-INJ Power Injector:

1. Connect the power cord cable from power outlet to the **IWE500-INJ** power connector.

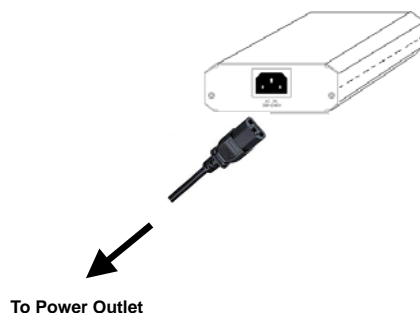


Fig. 2. Connecting the power cord cable to IWE500-INJ.

2. Check the “POWER” LED: if system is normal, the LED will be on (Green light); otherwise, the “POWER” LED will be off.
3. Connect the Ethernet cable (RJ-45 Category 5) from Ethernet Hub/Switch to the “DATA IN” port of **IWE500-INJ** Power Injector.
4. Connect another Ethernet cable (RJ-45 Category 5) from “POWER & DATA OUT” port of the **IWE500-INJ** Power Injector to the **IWE3200**. Please note the indication on the panel of POE-enabled RJ45 port of **IWE3200** (LAN interface #4).

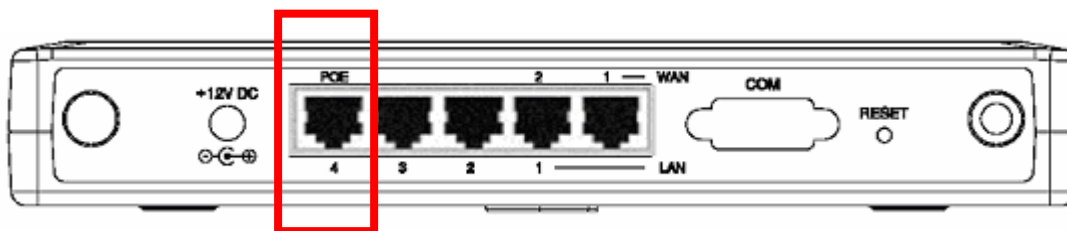


Fig. 3. POE enabled LAN Port Position.

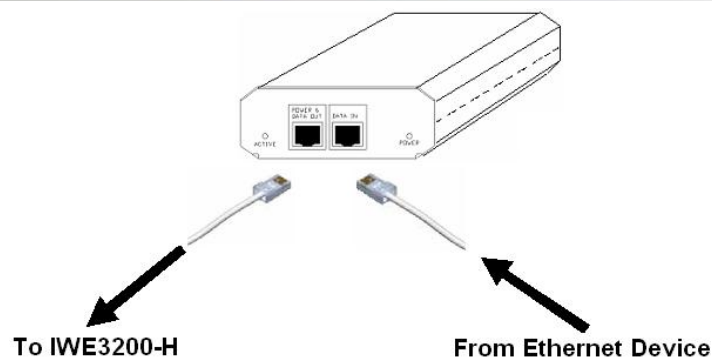


Fig. 4. Connecting Ethernet cables to IWE500-INJ.

5. Check the “ACTIVE” LED: if power is successfully fed into the **IWE3200**, the “ACTIVE” LED will be on (Red light); otherwise, the “ACTIVE” LED will be off.
6. If the electricity current is over the normal condition ($I_o > 1.0\text{ A}$), the “ACTIVE” LED will flash (Red light).

NOTE:

IWE500-INJ is specially designed for **IWE3200**. The use of **IWE500-INJ** with other Ethernet-ready devices that are not compliant to IEEE 802.3af may cause damage to the devices.

2.2. Mounting the IWE3200 on a Wall

The **IWE3200** is wall-mountable.

1. Stick the supplied sticker for wall-mounting.
2. Use a $\phi 6.5\text{mm}$ drill to drill a 25mm-deep hole at each of the cross marks.
3. Plug in a supplied plastic conical anchor in each hole.
4. Screw a supplied screw in each plastic conical anchor for a proper depth so that the **IWE3200** can be hung on the screws.
5. Hang the **IWE3200** on the screws.

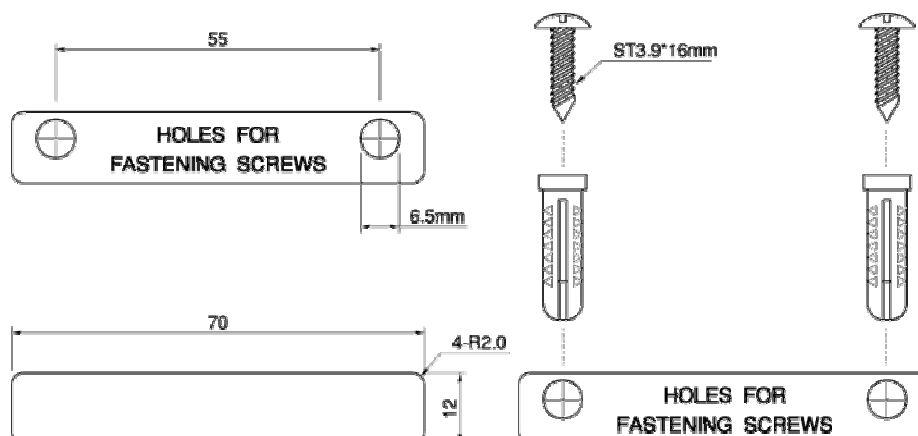


Fig. 5. Mounting the IWE3200 on a wall.

2.3. Preparing for Configuration

To configure a **IWE3200**, a *managing computer* with a Web browser is needed. For first-time configuration of a **IWE3200**, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed **IWE3200**, either a wireless computer or a wired computer can be employed as the managing computer.

NOTE:

If “Opera” browser is used to configure an **IWE3200**, click the menu item **File**, click **Preferences...** click **File types**, and edit the MIME type, **text/html**, to add a file extension “.sht” so that Opera can work properly with the Web management pages of the **IWE3200**.

Since the configuration/management protocol is HTTP-based, you have to make sure that the IP address of the managing computer and the IP address of the *managed IWE3200* are in the same IP subnet (the default IP address of an AP is **192.168.0.1** and the default subnet mask is **255.255.255.0**.)

2.3.1. Connecting the Managing Computer and the IWE3200

To connect the managing computer and the **IWE3200** for first-time configuration, you have two choices as illustrated in Fig. 6.

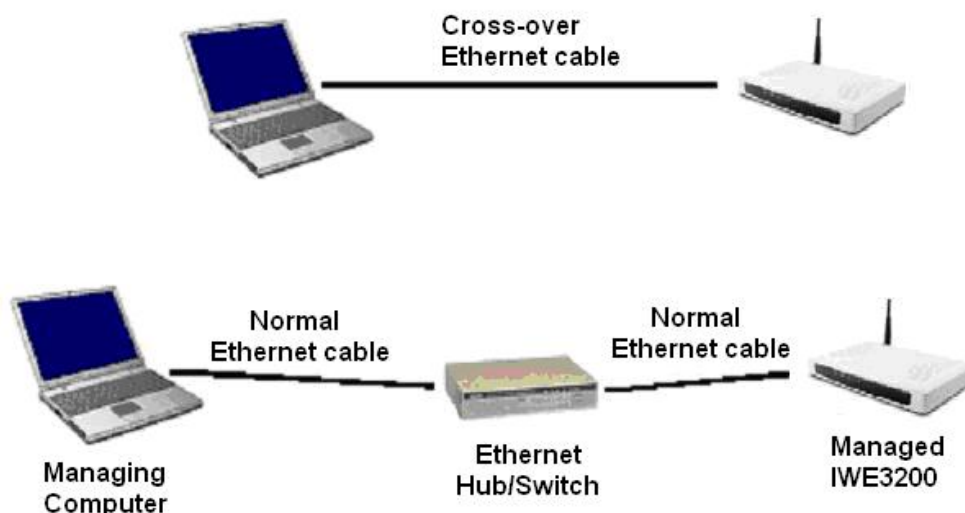


Fig. 6. Connecting a managing computer and an IWE3200 via Ethernet.

You can use either a *cross-over* Ethernet cable (included in the package) or a switch/hub with 2 straight-through Ethernet cables.

NOTE:

One connector of the Ethernet cable must be plugged into the **LAN** Ethernet port of the **IWE3200** for configuration.

2.3.2. Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the **IWE3200** are in the same IP subnet. Set the IP address of the computer to **192.168.0.xxx**.

NOTE:

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

2.4. Configuring the IWE3200

The **IWE3200** is DHCP server enabled by default. After the IP addressing is configured, launch a Web browser on the managing computer. Then, go to “**http://192.168.0.1**” to log on to the **IWE3200** for Web-based management.

TIP:

For maintenance configuration, the **IWE3200** can be reached by its *host name* using a Web browser. For example, if the **IWE3200** is named “AP”, you can use the URL “http://AP” to access the Web-based management interface of the **IWE3200**.

2.4.1. Entering the User Name and Password

Before the Home page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based Network Manager. For first-time configuration, use the default user name “**root**” and default password “**root**”, respectively.



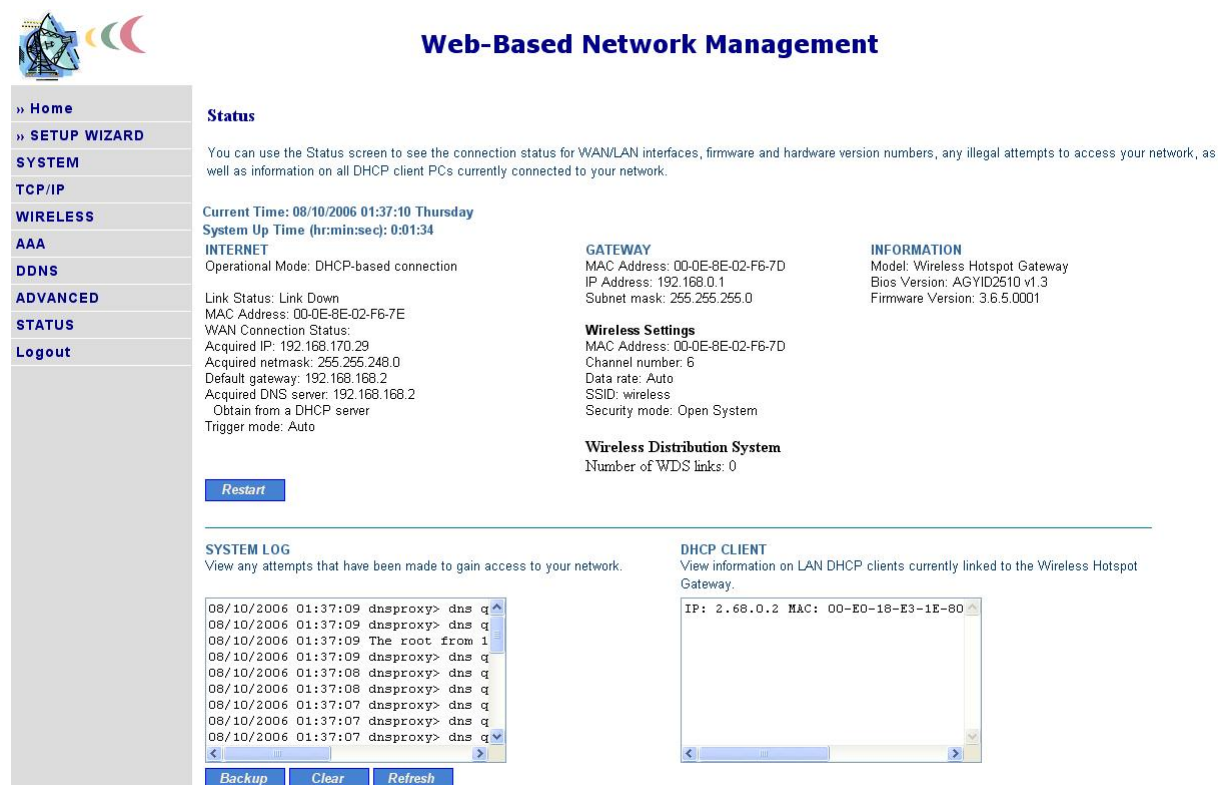
The image shows a web-based login screen for a 'Wireless Hotspot Gateway'. The title bar at the top says 'Wireless Hotspot Gateway'. Below it, the main heading is 'Login Screen'. There are two input fields: 'User name:' and 'Password:'. Below these fields are two buttons: 'LOGIN' and 'CANCEL'.

Fig. 7. Entering the user name and password.

NOTE:

It is strongly recommended that the password be changed to other value for security reasons. (See Section 2.10.2 for more information).

On the Home page, click the **SETUP WIZARD** to quickly change the configuration of the gateway.



Web-Based Network Management

Status

You can use the Status screen to see the connection status for WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 08/10/2006 01:37:10 Thursday
 System Up Time (hr:min:sec): 0:01:34

INTERNET
 Operational Mode: DHCP-based connection

Link Status: Link Down
 MAC Address: 00-0E-8E-02-F6-7E
 WAN Connection Status:
 Acquired IP: 192.168.170.29
 Acquired netmask: 255.255.248.0
 Default gateway: 192.168.168.2
 Acquired DNS server: 192.168.168.2
 Obtain from a DHCP server
 Trigger mode: Auto

GATEWAY
 MAC Address: 00-0E-8E-02-F6-7D
 IP Address: 192.168.0.1
 Subnet mask: 255.255.255.0

INFORMATION
 Model: Wireless Hotspot Gateway
 Bios Version: AGYID2510 v1.3
 Firmware Version: 3.6.5.0001

Wireless Settings
 MAC Address: 00-0E-8E-02-F6-7D
 Channel number: 6
 Data rate: Auto
 SSID: wireless
 Security mode: Open System

Wireless Distribution System
 Number of WDS links: 0

SYSTEM LOG
 View any attempts that have been made to gain access to your network.

DHCP CLIENT
 View information on LAN DHCP clients currently linked to the Wireless Hotspot Gateway.

08/10/2006 01:37:09 dnsproxy> dns q
 08/10/2006 01:37:09 dnsproxy> dns q
 08/10/2006 01:37:09 The root from 1
 08/10/2006 01:37:09 dnsproxy> dns q
 08/10/2006 01:37:08 dnsproxy> dns q
 08/10/2006 01:37:08 dnsproxy> dns q
 08/10/2006 01:37:07 dnsproxy> dns q
 08/10/2006 01:37:07 dnsproxy> dns q
 08/10/2006 01:37:07 dnsproxy> dns q
 08/10/2006 01:37:07 dnsproxy> dns q

IP: 2.68.0.2 MAC: 00-E0-18-E3-1E-80

Buttons: Restart, Backup, Clear, Refresh

Fig. 8. The Home Page.

2.4.2. SETUP WIZARD Step 1: Selecting an Operational Mode

☐ Gateway with a PPPoE-Based DSL/Cable Connection
☐ Gateway with a DHCP-Based DSL/Cable Connection
☐ Gateway with a Static-IP DSL/Cable Connection
☒ Gateway with DSL/Cable Connections

WAN Connection Types

WAN 1: with Downlink: Uplink:
 WAN 2: with Downlink: Uplink:

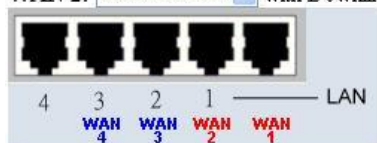


Fig. 9. Operational modes.

2.4.3. SETUP WIZARD Step 2: Configuring TCP/IP Settings

2.4.3.1. Router with a PPPoE-Based DSL/Cable Connection

Ethernet WAN Interface	
Trigger mode:	Auto
Maximum transmission unit:	1492
User name:	username
Password:	
Confirm password:	
Service name:	
Idle disconnect time (min.):	10
Host name:	gateway
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 10. TCP/IP settings for **Router with a PPPoE-Based DSL/Cable Connection** mode.

In this mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct **User name**, **Password**, and **Service name** settings.

The **Trigger mode** setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and torn down *manually* (**Manual**) by clicking the **Connect** and **Disconnect** buttons on the Start page, respectively. Or you can choose to let the device *automatically* (**Auto**) establish a PPPoE connection at boot-up time. In **Auto** mode, if the connection is disrupted, the device will try to re-establish the broken connection automatically.

2.4.3.2. Router with a DHCP-Based DSL/Cable Connection

Ethernet WAN Interface	
Trigger mode:	Auto
Host name:	gateway
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 11. TCP/IP settings for **Router with a DHCP-Based DSL/Cable Connection** mode.

In this mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**.

The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained by DHCP from the ISP. The **Trigger mode** setting affects the behavior of the DHCP client of the Router. In **Auto** mode, you don't have to worry about the DHCP process; the device takes care of everything. In **Manual** mode, there are two buttons on the Start page for you to manually release an obtained IP address (**Release**) and re-obtain a new one from a DHCP server (**Renew**).

2.4.3.3. Router with a Static-IP DSL/Cable Connection

Ethernet WAN Interface	
IP address:	<input type="text"/>
Subnet mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Ethernet/Wireless LAN Interfaces	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Host name:	<input type="text" value="gateway"/>

Fig. 12. TCP/IP settings for **Router with a Static-IP DSL/Cable Connection** mode.

In this mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct **IP address**, **Default Router**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

2.4.3.4. Router with a Multiple DSL/Cable Connections

WAN 1: Static-IP DSL/Cable Connection	
IP Address:	<input type="text"/>
Subnet mask:	<input type="text"/>
Default gateway:	<input type="text"/>
WAN 2: PPPoE-based DSL/Cable Connection	
Trigger mode:	<input type="text" value="Auto"/>
Maximum transmission unit:	<input type="text" value="1492"/>
User name:	<input type="text" value="username"/>
Password:	<input type="text"/>
Confirm password:	<input type="text"/>
Service name:	<input type="text"/>
LAN Interface	
IP address:	<input type="text" value="192.168.0.1"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Host name:	<input type="text" value="gateway"/>

Fig. 13. TCP/IP settings for **Router with Multiple DSL/Cable Connections** mode.

Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of **Router with a PPPoE-Based DSL/Cable Connection**, **DHCP-Based DSL/Cable Connection**, or **Router with a Static-IP DSL/Cable Connection**, respectively. As a result, refer to Sections 2.4.3.1, 2.4.3.2, and 2.4.3.3 for more information.

2.4.4. SETUP WIZARD Step 3: DHCP Server Settings

Functionality:

Basic

Default gateway:

Subnet mask:

Primary DNS server:

Secondary DNS server:

First allocatable IP address:

Allocatable IP address count:

Fig. 14. DHCP Server Setting

The **IWE3200** can automatically assign IP addresses to client computers by DHCP. You can specify the first IP address that will be assigned to the clients and the number of allocatable IP addresses. In most cases **Default gateway** and **Primary DNS server** should be set to the IP address of the Router's LAN interface (e.g., the default LAN IP address is **192.168.0.1** and the **Subnet mask** is set to **255.255.255.0**.)

Functionality:

DHCP Relay Setting

DHCP Server IP address:

Fig. 15. DHCP Relay Setting

When functionality is set to **DHCP Relay**, the **IWE3200** would not assign any IP address to the clients. It forwards the received DHCP requests from the clients to the designate DHCP server.

2.4.5. SETUP WIZARD Step 4: Configure IEEE 802.11 Settings

Regulatory domain:

Channel number:

Network name (SSID):

Fig. 16. IEEE 802.11b communication settings.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client com-

puter and the SSID of the wireless access Router must be identical for them to communicate with each other.

2.4.6. Configuring User Authentication Settings

The **IWE3200** supports both *Web redirection-based and non-802.1x-based user* and *IEEE 802.1x-based user* authentication.

After the IP addressing settings have been set using SETUP WIZARD, you have to configure Web redirection settings and/or IEEE 802.1x settings for wireless user authentication.

When both Web redirection and IEEE 802.1x are enabled, the authentication process will first tried *IEEE 802.1x* and then *Web Redirection*. In this way, the wireless access router can serve both IEEE 802.1x-enabled and IEEE 802.1x-disabled wireless users.

2.4.6.1. Web Redirection

To setup Web redirection-based user authentication, go to the **AAA→Web Redirection.** section for configuration. There are three combinations for Web Redirection and Authentication method:

1. Enable with Authentication – Enable both Web-Redirection and user Authentication mechanism.

Functionality:	Enabled with Authentication ▼
Encryption method:	401 Authorization ▼
Authentication protocol:	RADIUS ▼
RADIUS authentication method:	EAP-MD5 ▼
RADIUS link integrity:	Disabled ▼

Fig. 17. Web redirection settings – Enable with Authentication

1.1. Encryption Method:

- 1.1.1. 401 Authorization: Logon page on Pop-up window.
- 1.1.2. CGI with Plain Code: Logon page on web browser, username/password without encryption (plain text).
- 1.1.3. CGI with Base64: Logon page on web browser, username/password with Base64 encryption.
- 1.1.4. CGI with SSL: Logon page on web browser, username/password with SSL encryption.

1.2. Authentication protocol:

- 1.2.1. RADIUS: Authentication by external RADIUS server.
- 1.2.2. Local Accounts: Authentication by local database, associated with ticket printing.

1.3. RADIUS authentication method:

- 1.3.1. EAP-MD5

- 1.3.2. PAP
- 1.3.3. CHAP

2. Enable without Authentication – Enable only the Web-Redirection, but disable the user Authentication mechanism. User will automatically redirect to the destination web page if the URL indicated.

Functionality:	Enabled without Authentication ▼
User redirect page http://	<input type="text"/>

Fig. 18. Web redirection settings – Enable without Authentication

3. Disable – Disable all Web-Redirection mechanisms.

2.4.6.2. Local Authentication Sever

The **IWE3200** supports the local Authentication Sever for some hotspot venues where standard RADIUS or Billing server(s) is difficult to be implemented. The local Authentication Server contains the built-in database for **2,000** user entries.

To setup the Local Authentication method:

1. Go to the section **AAA→Web Redirection**, in ‘**Functionality**’ of ‘**Basic**’ column, select ‘**Enable with Authentication**’.
2. In ‘**Authentication protocol**’, select ‘**Local Accounts**’.

Functionality:	Enabled with Authentication ▼
Encryption method:	401 Authorization ▼
Authentication protocol:	Local Accounts ▼

Fig. 19. Local Authentication Server Settings

3. Go to the **AAA→Ticket Setting** to setup the billing information. In the Ticket Setting page, the information reflects the billing information is the ‘**Monetary Unit**’ and the ‘**Amount of Money Per Unit**’, while the information reflects the user permitted access time frame is ‘**Unit of Session Time (min)**’ and ‘**Valid period (hour)**’. The reset of the settings is for ticket format customization, you can specify the appropriate content which reflected the information of hotspot venues to be shown on the ticket content. Detail billing setting is described as below:

- **Monetary Unit:** to define the unit of currency, e.g., input ‘USD’ for US Dollars or ‘EURO’ for Euro Dollars. The currency unit will also shown on the billing ticket.
- **Amount of Money Per Unit:** to define the money to be charged per unit, which is used with the input unit by the control keypad. For example, if the per unit charged money is 50 and the control keypad is input to be 5 (units), then the total money to be charged to the user is $50 \times 5 = 250$. Default is ‘10’ per unit.
- **Unit of Session time (min):** to define the time frame (by min) of the user to access the

Internet , which is used with the input unit by the control keypad. For example, if the per unit time is 50 (min) and the control keypad is input to be 5 (units), then the total available access time frame of the user is $50 \times 5 = 250$ (min). Default is '1' min.

- **Valid period (hour):** to define the valid period (by hour) while the user account generated. If the user account generated but not activated during the valid period, the gateway will automatically disable the user after the valid period expired. Default is '1' hour.

Title of List:	Hotspots Logo
Store Code	1111200137
Terminal Code	1236210
Name of Supplier:	Company Name
Web of Supplier:	www.company.com
Phone Number:	0800-012345
Monetary Unit:	Unit
Amount of Money Per Unit:	10
Unit of Session Time (min.):	1
Valid period (hour):	1
Serial Number of Product:	10000012

Fig. 20. Ticket Setting

4. Go to the section **STATUS→Account Table**, there are four buttons for management the account table. Input the user name and password then press '**Add**' button to generate the new local user. Input the user name then press '**Delete**' button to remove the user from the account table. "**Clean Table**" button uses to remove all user accounts. "Table Defragment" button provides to remove accounts with inactive state. The local user account can be also generated by the control keypad, see Sec. 2.4.7.3 for more details.

Account Table

Remove all accounts from table

Remove accounts with inactive state

Select : Page 1
User name:
Password:

(The maximum length for user name and password is 9 characters.)

Fig. 21. Local User Database Management

5. All the status of generated local users will show in the 'Account Table List'. The account table list also includes the accounts which are randomly generated by the gateway as using the control keypad. The user must use the generated username and password for access logon process. There are 4 type status of each user account:

- **Register:** to show the generated user who has not yet logon and been activated.
- **Active:** the generated user who has successfully logon and access the Internet. The MAC address and Login Time of the activated user will be also shown while user has been activated.

- **Inactive:** to show the user account that access time frame expired, or 'Valid Period' expired.
- **Permanent:** to show the user account that would never expire. The state for the user accounts which created by manual would be permanent. This kind of account would not have any information for the session time and cost

Account Table List						
No.	User Name	Pass word	Mac Address	Session(min.)	Cost	States
1	O440jm0vg	K4g292992	-	50	500	Register
2	KcP2AC0aV	cvsFKqrr3	-	100	1000	Register
3	5Dg3570wa	332ha9mCg	-	60	600	Register
4	Yu84Vr0hr	20eG2C46v	-	30	300	Register
5	jason	jason	-	-	-	Permanent
6	rK96fk0io	9950oaqTn	00A0D1D65B84	80	800	Active
7	by97BH02n	636a8crha	-	120	1200	Register

Fig. 22. Account Table List

2.4.6.3. How to Setup the mini-POS Ticket Printer

The **IWE3200** supports the built-in user database for local authentication, this function also associates the optional external mini-POS Ticket Printer for billing printing purpose. The benefit of the built-in user database is to provide the flexibility that there may some hotspot venues without the capability to setup the complete RADIUS environment for user authentication. More over, the external control keypad also can play the role to control the ticket printing and gateway control without addition control PC required, hence reduce the cost of hotspot venue deployment.

To setup the mini-POS Ticket Printer:

1. Find the 'Y-cable' in the package of **IWE810-POS mini-POS Ticket Printer**.
2. Use the 'Y-cable' to connect the **IWE3200**, **IWE810-POS**, and the **control keypad**. Make sure the Y-cable is well connected to the interface correctly.
3. Power on the **IWE810-POS**. To make sure the **IWE810-POS** is in good condition, you can print out the testing ticket by holding the 'FEED' button on the **IWE810-POS** then power on. The test ticket will be automatically printed.

The usage of control keypad:

1. Press the digit key on the control keypad to input the access 'unit'.
2. The input 'unit' value will be only effected after user press the 'Enter' button on the keypad. For example, if a new user need to be generated 30 units of access time frame, the key input must be

3

 +

0

 +

Enter
3. If there's the type error, just leave the control keypad for 4sec before pressing the 'Enter' button, then the keypad will automatically clear and renew the previous input value.
4. After pressing the 'Enter' button on the control keypad, the new local account will be automatically generated, and the billing ticket will be printed simultaneously. The content of the ticket is

defined Fig 24 of Sec.2.4.7.2.

2.4.6.4. IEEE 802.1x

SSID broadcasts:	Enabled
Wireless client isolation:	This AP Only
Security mode:	802.1x EAP-MD5

Fig. 23. Changing security mode to an IEEE 802.1x option.

To setup IEEE 802.1x-based user authentication, go to **WIRELESS→Communication→Security** section, and then change the **Security mode** setting to an IEEE 802.1x-related option according to your needs. The advanced wireless access Router supports IEEE 802.1x EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, and WAP authentication methods. Click **Save** when finished.

2.4.7. Configuring RADIUS Settings

The RADIUS client on the **IWE3200** works in conjunction with the Web redirection component and IEEE 802.1x component for wireless user authentication. The Web redirection and IEEE 802.1x components are responsible for acquiring user credential information, and the RADIUS client communicates with a back end RADIUS server using the user credential information.

Go to the **AAA→RADIUS** section, and then configure the RADIUS settings. You have to configure at least **Authentication method**, **Primary RADIUS server**, **Shared key**, and **Identifier of this NAS** settings. And leave other settings to their default values. Click **Save & Restart** when finished.

Primary RADIUS server:	
RADIUS server:	192.168.0.2
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	*****
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 24. RADIUS settings.

NOTE:

The RADIUS server do not support all combinations of authentication methods if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes.

	IEEE 802.1x Disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
--	----------------------	---------------------	---------------------

		Web Redirection Disabled	■	■	■
--	--	-----------------------------	---	---	---

Table 1. Allowable authentication modes.

2.5. Deploying the IWE3200

After the settings have been configured, deploy the Router to the field application environment. You have to connect AP(s), modem(s), and RADIUS server(s) to the **IWE3200**. The system configuration in Fig. illustrates how to deploy the **IWE3200**.

In this configuration, one DSL/cable modem is connected to the WAN port (as WAN 1) of the **IWE3200** and another modem is connected to the LAN 1 port (as WAN 2) of the **IWE3200**. Two APs are connected to the LAN 2 port and LAN 3 port, respectively. Finally, a RADIUS server is connected to the LAN 4 port of the **IWE3200**. The **IWE3200** works together with the RADIUS server to decide whether a wireless client (the notebook computer or the PDA) is allowed to access the Internet through the broadband modems.

NOTE: Although the RADIUS server in this sample configuration is on the “LAN” side, in a real application, it can be on the “WAN” side, that is, on the Internet.

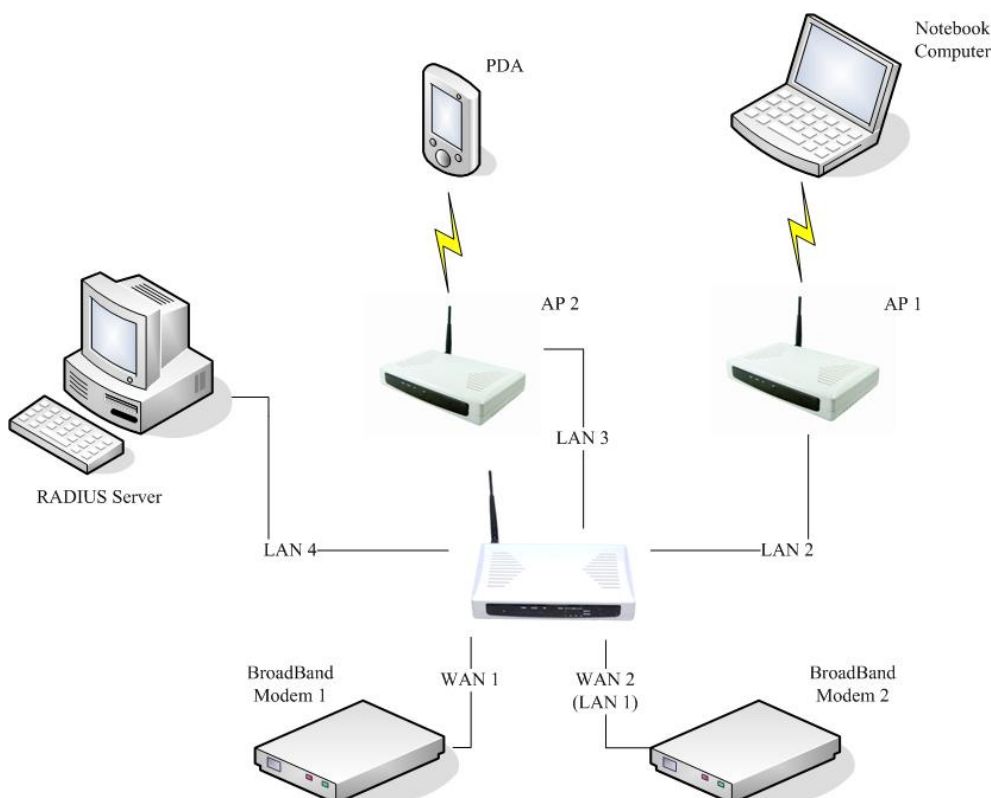


Fig. 25. Example IWE3200 deployment.

The **IWE3200** has a built-in access point. If the RF coverage of the built-in access point is enough for your venue, no additional stand-alone access point is necessary.

Since **IWE3200** also provides the WDS static wireless bridge function, it can also connect the other wireless AP with WDS method (See 3.5.1.3 Wireless Distribution System for more detail informa-

tion).

The **IWE3200** supports the built-in user database for local authentication, this function also associates the optional external mini-POS Ticket Printer for billing printing purpose. The setup scenario is shown in Fig 28. Please also refer to Sec. 2.4.7.3 for detail operation instruction of mini-POS, keypad, and ticket printing.



Fig. 26. mini-POS Ticket Printer & Control Keypad Deployment.

2.6. Setting up Client Computers

Before a wireless user can access the Internet through the **IWE3200**, the wireless and TCP/IP settings of his/her computer or PDA must be configured adequately to match the environment of **IWE3200**. In addition, if Web redirection or IEEE 802.1x EAP-MD5 authentication methods are used, *user name* and *password* information must be set up on the RADIUS server. On the other hand, if IEEE 802.1x EAP-TLS authentication method is used, a *digital certificate* must be installed on the computer or PDA and on the back end RADIUS server.

2.6.1. Configuring IEEE 802.11-Related Settings

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 a deployed AP or the wireless access Router's built-in AP.

To establish a wireless link to an AP:

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.

A wireless client computer must be in *infrastructure* mode, so that it can associate with a wireless access point. Also, the SSID of the wireless client computer and the SSID of the deployed APs must be identical. Or, in case the **SSID broadcasts** capability of the deployed APs is enabled (by default), the SSID of the wireless client computer could be set to "any".

Both the wireless client computer and the deployed APs must have the same WEP settings for them to communicate with each other. Therefore, unless IEEE 802.1x EAP-TLS, which supports dynamic WEP key distribution, is used, it's strongly suggested not to enable WEP functionality of the deployed APs for *hotspot* applications.

2.6.2. Configuring TCP/IP-Related Settings

Windows based user can use **Windows Network Control Panel Applet** to change the TCP/IP settings of his/her computers, so that the IP addresses of the client computers and the IP address of the Router are in the same IP subnet. Also, the client computers must be set to obtain IP addresses automatically by DHCP.

NOTE:

Configure the client computers so that Web browsing is not through any Web Proxy servers; otherwise the Web redirection-based authentication will not work properly.

If a client computer is already set to obtain an IP address automatically, you can use the Windows-provided tool, **WinIPCfg.exe** (on Windows 9x) or **IPConfig.exe** (on Windows 2000), to re-obtain an IP address from the Router. **WinIPCfg.exe** is a GUI program, and has command buttons for releasing the current IP address and re-obtaining an IP address. **IPConfig.exe** is a command-line program, and the **/release** option releases the current IP address and the **/renew** option triggers the Windows DHCP client subsystem to re-obtain an IP address.

2.7. Confirming the Settings of the IWE3200 and Client Computers

To make sure whether you have correctly set up the **IWE3200** for Web redirection-based authentication or not, follow the procedure below:

1. Establish a wireless link from the wireless client computer or PDA to an AP that is controlled by the **IWE3200**.
2. On the wireless client computer or PDA, run a Web browser, and then go to a Web site on the Internet, e.g., <http://www.wi-fi.com>.
3. Instead of showing the requested page, a log-on page is shown. Click **Log On** for authentication.

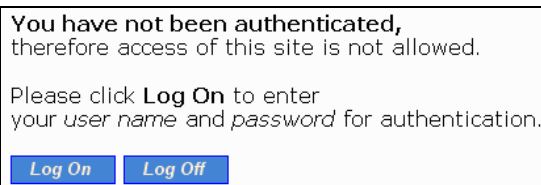


Fig. 27. Log-on page.

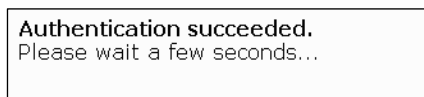
4. Type a correct user name and password that has been registered on the RADIUS server.



The image shows a web browser window titled "Wireless Hotspot Gateway". Inside, there is a "Login Screen" with two input fields: "User name:" and "Password:". Below these fields are two buttons: "LOGIN" and "CANCEL".

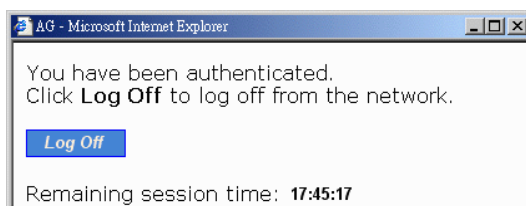
Fig. 28. User name and password for authentication.

5. If the user name and password are correct. Now you'll be brought to the original page you have requested after waiting for a few seconds. Meanwhile, a window for log-off and session status appears.



The image shows a small rectangular message box with a black border. It contains the text: "Authentication succeeded. Please wait a few seconds..."

Fig. 29. Authentication success.



The image shows a Microsoft Internet Explorer window titled "AG - Microsoft Internet Explorer". The main content area displays the message: "You have been authenticated. Click **Log Off** to log off from the network." Below this message is a blue button labeled "Log Off". At the bottom of the window, it says "Remaining session time: 17:45:17".

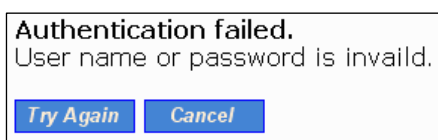
Fig. 30. Log-off window.

6. Click **Log Off** within the log-off window to end the session.

NOTE:

On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the Log-on page, and then click **Log Off** to end the session.

7. If the user name or password is invalid, you will be prompted to try again or cancel the authentication process.



The image shows a small rectangular message box with a black border. It contains the text: "Authentication failed. User name or password is invalid." Below this text are two buttons: "Try Again" and "Cancel".

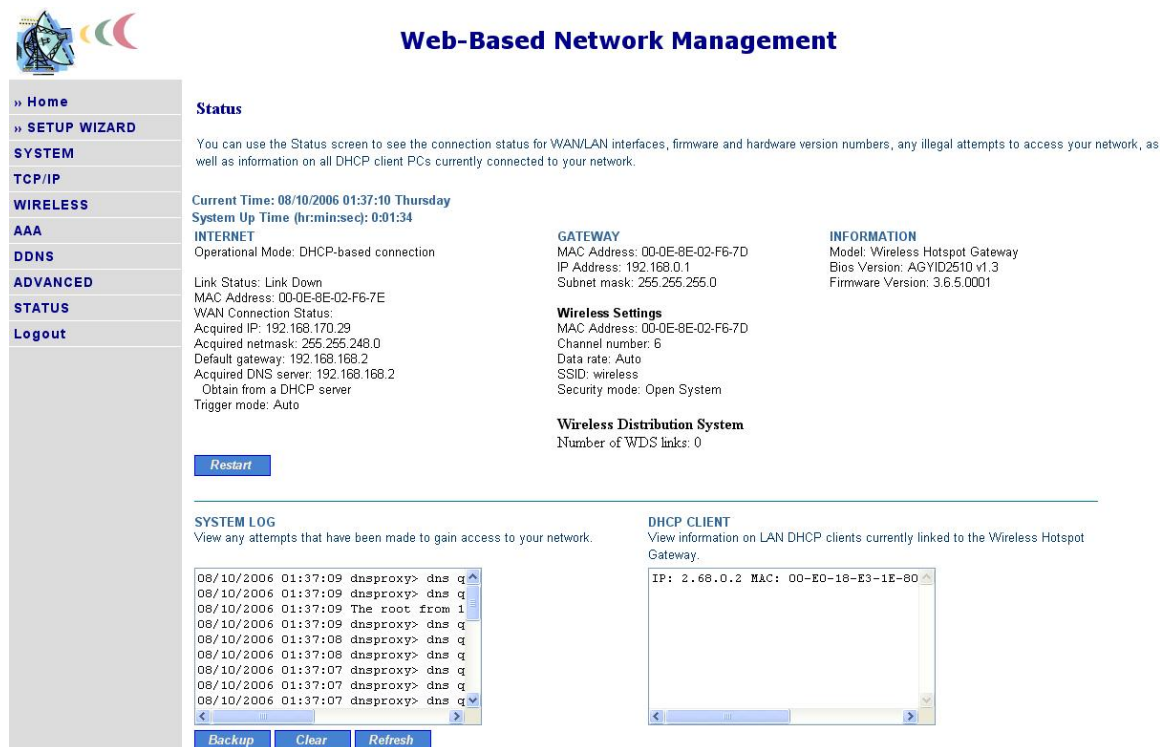
Fig. 31. Authentication failure.

NOTE:

If IEEE 802.1x capability of the *Wireless Advanced* edition of access Router is enabled, the user of an IEEE 802.1x-compliant wireless client computer is authenticated by IEEE 802.1x rather than by Web redirection.

If you complete the above procedure without error, the Router together with the RADIUS server has been correctly set up for Web redirection-based authentication.

2.8. Using Web-Based Network Management



Web-Based Network Management

Status

You can use the Status screen to see the connection status for WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 08/10/2006 01:37:10 Thursday
 System Up Time (hr:min:sec): 0:01:34

INTERNET
 Operational Mode: DHCP-based connection

Link Status: Link Down
 MAC Address: 00-0E-8E-02-F6-7E
 WAN Connection Status:
 Acquired IP: 192.168.170.29
 Acquired netmask: 255.255.248.0
 Default gateway: 192.168.168.2
 Acquired DNS server: 192.168.168.2
 Obtain from a DHCP server
 Trigger mode: Auto

GATEWAY
 MAC Address: 00-0E-8E-02-F6-7D
 IP Address: 192.168.0.1
 Subnet mask: 255.255.255.0

INFORMATION
 Model: Wireless Hotspot Gateway
 Bios Version: AGYID2510 v1.3
 Firmware Version: 3.6.5.0001

Wireless Settings
 MAC Address: 00-0E-8E-02-F6-7D
 Channel number: 6
 Data rate: Auto
 SSID: wireless
 Security mode: Open System

Wireless Distribution System
 Number of WDS links: 0

SYSTEM LOG
 View any attempts that have been made to gain access to your network.

DHCP CLIENT
 View information on LAN DHCP clients currently linked to the Wireless Hotspot Gateway.

IP: 2.68.0.2 MAC: 00-E0-18-E3-1E-80

Restart

Backup **Clear** **Refresh**

Fig. 32. The Home page.

2.8.1. Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

- **Home.** For configuration setting summary.
- **SETUP WIZARD.** For you to quickly set up the Router.
- **SYSTEM.** System monitoring information.
 - **Operational Mode.** Operational mode of the **IWE3200** based on the type of the Internet connection provided by the ISP.
 - **Password Settings.** For gaining right to change or view the settings and status of the Router.
 - **Firmware Tools.** For upgrading the firmware of the Router and backing up and restoring configuration settings of the Router.
 - **Time Zone.** Time zone and SNTP (Simple Network Time Protocol) server settings.

- **TCP/IP.** TCP/IP-related settings.
 - **Address.** IP addressing settings for the Router to work in the TCP/IP networking world, or user name and password provided by the ISP.
 - **DNS.** DNS (Domain Name System) proxy settings.
 - **NAT.** Settings for the NAT (Network Address Translation) server on the Router.
 - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the Router.
 - **Load Balancing.** Settings for the WAN ports load-balancing policy by Port or IP address range.
 - **Zero Client Reconfiguration.** Settings for wireless clients to associate to **IWE3200** without any network setting modification.
 - **PPTP Client.** Settings for VPN (Virtual Private Network) packets to pass through inter-net-internet boundary.
- **WIRELESS.** IEEE 802.11-related settings.
 - **Communication.** Communication settings for the IEEE 802.11b/g interface of the wireless access Router to work properly with wireless clients.
 - **Security.** Security settings for authenticating wireless users by IEEE 802.1x and encrypting wireless data.
- **AAA.** Authentication, Authorization, and Accounting settings.
 - **Web Redirection.** Web redirection settings for how a wireless user's HTTP request is "redirected" for authentication.
 - **RADIUS.** RADIUS settings for communication with the primary and secondary RADIUS servers.
 - **Session Control.** Settings for controlling lifetimes of user authentication sessions.
 - **Auth Page Customization.** Settings for customizing the contents of *log-on*, *log-off*, *authentication success*, and *authentication failure* authentication pages.
 - **Ticket Settings.** Settings for the billing ticket format.
- **DDNS.** Settings for Dynamic DNS.
- **ADVANCED.** Advanced settings of the Router.
 - **Filters & Firewall.** Packet filtering and firewall settings for user access control and protection from hacker attacks from the Internet, respectively.
 - **Management.** Web-based management types, UPnP, and SNMP settings.

- **Access Rules.** Settings for the time frame policy to Permit/Deny administrator to access the **IWE3200**.
- **LAN Device Management.** Settings for the Router to know what LAN devices it has to manage.
- **Status.** System monitoring information.
 - **Associated Wireless Clients.** Display the status of all wireless clients who associated to **IWE3200**.
 - **Authenticated Users.** Display the status of the users who have been authenticated by **IWE3200**. Authenticated users can be also forced terminated in this table.
 - **Account Table.** Generate the new users in the authentication mode by Local Accounts. Billing ticket will be also generated and printed by pressing 'Generator' button on this page.
 - **Account Statistics.** Display the statistics for the account table.
 - **Session list.** Display the status of session traffic of **IWE3200**.
 - **Managed LAN Devices.** Display the status of local LAN devices which connected to **IWE3200**.

2.8.2. Save, Save & Restart, and Cancel Commands



Fig. 33. Save, Save & Restart, and Cancel.

At the bottom of each page, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the Router and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the Router and restarts the Router immediately for the settings changes to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in **red**. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the Router for the settings changes to take effect.

2.8.3. Home and Refresh Commands



Fig. 34. Home and Refresh.

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 start page. Clicking **Refresh** updates the shown status information.

2.9. Seeing Status

2.9.1. Associated Wireless Clients

Wireless Clients Status						
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-02-6F-01-31-5C	192.168.0.3		577563	1294922	01h:52m:32s

Fig. 35. Status of associated wireless clients.

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.

2.9.2. Authenticated Users

Authenticated Users Table							
No.	Idle Time (sec.)	User Name	IP Address	MAC Address	Status	Statistics	Terminate
1	6	test	192.168.168.142	00-00-1C-DE-4D-59	Connected	Detail	Terminate
2	8	test	192.168.168.132	00-50-C2-0C-66-77	Connected	Detail	Terminate
3	3	test	192.168.168.154	00-00-1C-DE-59-99	Connected	Detail	Terminate
4	0	test	192.168.168.128	00-50-BA-1F-7F-90	Connected	Detail	Terminate
5	20	test	192.168.168.64	00-50-BA-22-D6-04	Connected	Detail	Terminate
6	62	test	192.168.168.122	00-D0-59-0E-4A-DD	Connected	Detail	Terminate
7	10	test	192.168.168.162	00-40-95-30-23-02	Connected	Detail	Terminate
8	3	test	192.168.168.69	00-10-DC-07-D8-6F	Connected	Detail	Terminate
9	42	test	192.168.168.123	00-E0-18-E3-1E-82	Connected	Detail	Terminate
10	171	test	192.168.168.131	00-00-1C-D0-DC-78	Connected	Detail	Terminate
11	2	test	192.168.168.110	00-40-95-30-23-6F	Connected	Detail	Terminate
12	0	test	192.168.168.63	00-40-95-30-23-39	Connected	Detail	Terminate
13	493	test	192.168.168.161	00-50-22-91-01-0C	Connected	Detail	Terminate

Fig. 36. Authenticated users.

On this page, the status information of each RADIUS-authenticated user, including its current idle time, user name, IP address, MAC address, and status, is shown. In addition, you can click the **Detail** link in the **Statistics** column to see more detailed statistics information, such as **Input packets**, **Output packets**, **Input bytes**, and **Output bytes**.

Basic	
User name	test
IP address	192.168.0.4
MAC address	00-E0-18-7D-D1-6A
Time	
Current idle time/idle timeout (sec.)	35/300
Connection time (sec.)	127
Flow	
Input packets	621
Output packets	673
Input bytes	134497
Output bytes	85265

Fig. 37. Authenticated RADIUS user detailed information.

Any authenticated user can be terminated by clicking the corresponding **Terminate** link so that this user is blocked from using networking services provided by the Router. A terminated user is moved to the **Terminated Users Table**. Clicking the corresponding **Release** link puts a terminated user back into authenticated state.

Terminated Users Table		
No.	MAC Address	Release
1	00-00-1C-DE-4D-3C	Release
2	00-40-95-30-23-39	Release

Fig. 38. Terminated users.

2.9.3. Account Table

Account Table List							
No.	User Name	Pass word	Mac Address	Login Time	Session(min.)	Remaining(min.)	Cost States
1	PSW0WF0qy	5Qg0v3d30	-	-	30	30	10 Register
2	XAQ2yT0LT	yM94Nz309	-	-	30	30	10 Register
3	3zd3Zs06n	06s859f9k	-	-	30	30	10 Register
4	BPh43j0Eh	r90jeeN00	-	-	30	30	10 Register
5	Mij5Cb00p	5iedo38e0	-	-	60	60	20 Register
6	snm6N40z4	jgtI3nE4b	-	-	30	30	10 Register
7	iJA7cQ0T9	2a3H92eIC	-	-	30	30	10 Register
8	Or98mL0QQ	H0jv096m7	-	-	30	30	10 Register
9	ZTi9UK0dx	TbUCM28m5	-	-	30	30	10 Register
10	bnsauC0A5	83534Dyia	00E0187DD16A	245190	30	30	10 Active

Fig. 39. Account Table List

On this page, all the local under registered in local user database are shown. A activated user is identified by its MAC address, login time and the 'Active' under the 'Status' column.

2.9.4. Session List

Latest 50 Outgoing Session List					
No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	192.168.168.10	14484	210.62.128.1	53	UDP
2	192.168.168.10	14485	192.175.48.1	53	UDP
3	192.168.168.128	2619	210.59.144.141	80	HTTP
4	192.168.168.146	1185	216.87.176.15	80	HTTP
5	192.168.168.10	14488	192.175.48.1	53	TCP
6	192.168.168.146	1186	216.87.176.15	80	HTTP
7	192.168.168.146	1187	216.87.176.15	80	HTTP
8	192.168.168.109	1227	202.1.237.21	80	HTTP
9	192.168.168.10	14477	210.62.128.1	53	UDP

Fig. 40. Latest outgoing user traffic sessions.

Latest 50 Incoming Session List					
No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	0.0.0.0	0	192.168.168.122	512	ICMP
2	0.0.0.0	80	192.168.168.122	1476	HTTP
3	192.175.48.1	53	192.168.168.10	14488	TCP
4	216.87.176.15	80	192.168.168.146	1186	HTTP
5	216.87.176.15	80	192.168.168.146	1187	HTTP
6	202.1.237.21	80	192.168.168.109	1227	HTTP
7	0.0.0.0	0	192.168.168.123	512	ICMP
8	0.0.0.0	53	192.168.168.10	14477	UDP

Fig. 41. Latest incoming user traffic sessions.

On this page, latest 50 outgoing and 50 incoming user traffic sessions are shown for monitoring network activity.

2.9.5. Managed LAN Devices

LAN Devices Status								
Check devices if alive every 10 minutes								
No.	Device Name	Status	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface
1	AP1	Offline	60001	192.168.168.201	80	00-01-02-11-22-33	TCP	Wired
2	AP2	Offline	60002	192.168.168.202	80	00-01-02-11-22-44	TCP	Wired
3	AP3	Offline	60003	192.168.168.203	80	00-01-02-11-22-55	TCP	Wired

Fig. 42. Managed LAN devices.

On this page, the status of every managed LAN device is shown. The *Offline* status indicates a non-working device while the *Online* status indicates a working device. The **Add Device** button serves as a shortcut to the **Advanced, LAN Device Management** configuration page, on which you can specify which devices to manage. See Section 2.15.3 for more information.

2.10. System

2.10.1. Specifying Operational Mode

- ☐ Gateway with a PPPoE-Based DSL/Cable Connection
- ☐ Gateway with a DHCP-Based DSL/Cable Connection
- ☐ Gateway with a Static-IP DSL/Cable Connection
- ☒ Gateway with DSL/Cable Connections

WAN Connection Types

WAN 1: with Downlink: Uplink:

WAN 2: with Downlink: Uplink:

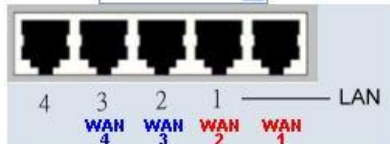


Fig. 43. Operational modes.

On this page, you can specify the operational mode for the Router. Currently, 5 modes are available:

- **Router with a PPPoE-based DSL/Cable Connection.** In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by PPPoE from the ISP.
- **Router with a DHCP-based DSL/Cable Connection.** In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by DHCP from the ISP.
- **Router with a Static-IP DSL/Cable Connection.** In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface must be manually set.
- **Router with n DSL/Cable Connections.** In this mode, the Router can support up to 4 ($n = 2$ to 4) DSL/cable-based Internet connections. The client computers can share the bandwidth of these Internet connections by the NAT server functionality. Since there are multiple Internet connections, total throughput is increased. The specified downlink and uplink data rates affect the load-balancing engine of the Router.

In this mode, connect your *first* DSL/Cable connection to WAN, the *second* to LAN 1, the *third* to LAN 2, and the *fourth* to LAN 3. Then, WAN becomes WAN 1, LAN 1 becomes WAN 2 when referred to on the Web management pages.

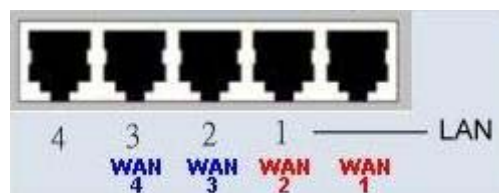
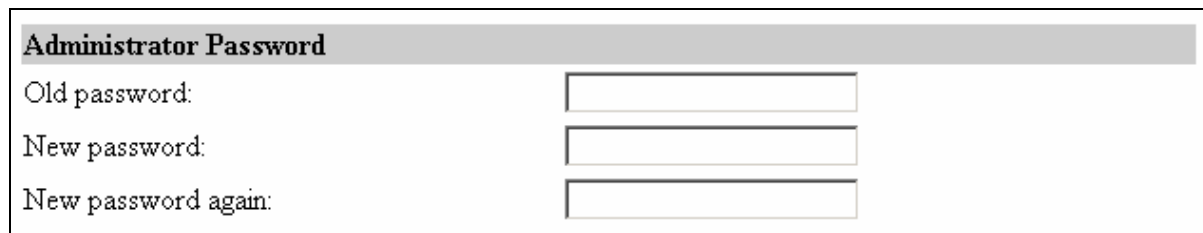


Fig. 44. WAN port IDs.

After the operational mode of the Router has been selected, go to the **TCP/IP→Addressing** section of the management UI (see Section 2.11.1) to configure the addressing settings of the WAN and LAN interfaces.

Since the WAN load-balancing algorithm is based on the “TCP session” rather than on the “packet,” a TCP session is allocated to a WAN connection at session initialization time. As a result, if there is only one client, no throughput improvement will be perceived even if there are several WAN connections. WAN load balancing is for multiple clients to share the multiple WAN connections. All the TCP sessions from the clients are intelligently distributed to the WAN connections by the built-in NAT server.

2.10.2. Changing Password

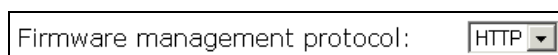


A screenshot of the 'Administrator Password' form. It has a title bar 'Administrator Password' and three input fields labeled 'Old password:', 'New password:', and 'New password again:'.

Fig. 45. Password.

On this page, you could change the user name and password of the administrator. The administrator can view and modify the configuration of the **IWE3200**. The new password must be typed twice for confirmation.

2.10.3. Managing Firmware

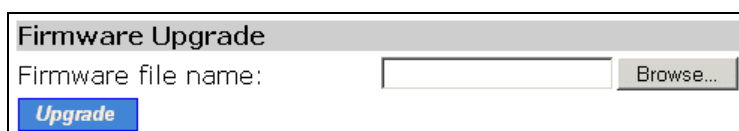


A screenshot of the 'Firmware management protocol' setting. It shows a text label 'Firmware management protocol:' followed by a dropdown menu currently set to 'HTTP'.

Fig. 46. Firmware management protocol setting.

Firmware management operations for the access Router include *Firmware Upgrade*, *Configuration Restore*, *Configuration Backup*, *Configuration Reset*, and *Access Server Certificate And Private-Key Upload*. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it's more user-friendly. However, due to different behavior of different Web browser versions, 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 way.

2.10.3.1. Upgrading Firmware by HTTP



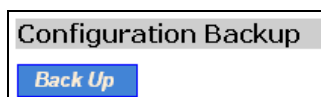
A screenshot of the 'Firmware Upgrade' form. It has a title bar 'Firmware Upgrade', a text label 'Firmware file name:' followed by an input field and a 'Browse...' button, and a blue 'Upgrade' button.

Fig. 47. Firmware upgrade by HTTP.

To upgrade firmware of the access Router 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.

2.10.3.2. Backing up and Restoring Configuration Settings by HTTP



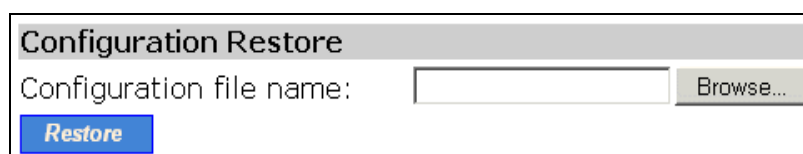
A screenshot of the 'Configuration Backup' form. It has a title bar 'Configuration Backup' and a blue 'Back Up' button.

Fig. 48. Configuration backup by HTTP.

To back up configuration of the access Router by HTTP:

1. Click **Back Up**.
2. You'll be prompted to open or save the configuration file. Click **Save**.
3. The configuration file is named by the **IWE3200**'s MAC address. For example, if the **IWE3200**'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 a folder in which the configuration file is to be stored. And then, click **Save**.

NOTE: The procedure may be a little different with different Web browsers.



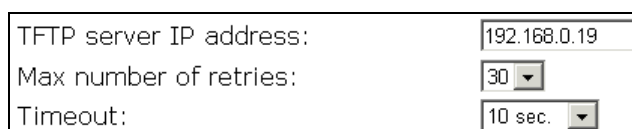
The image shows a web browser window titled "Configuration Restore". It contains a text input field labeled "Configuration file name:" followed by a "Browse..." button. Below the input field is a blue button labeled "Restore".

Fig. 49. Configuration restore by HTTP.

To restore configuration of the access Router by HTTP:

1. Click **Browse** and then select a correct configuration .hex file. You have to make sure the file name is the access Router'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 access Router.

2.10.3.3. Upgrading Firmware by TFTP

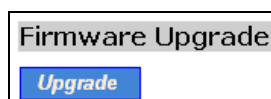


The image shows a form titled "TFTP server settings". It contains three rows: "TFTP server IP address:" with a text input field containing "192.168.0.19"; "Max number of retries:" with a dropdown menu showing "30"; and "Timeout:" with a dropdown menu showing "10 sec.".

Fig. 50. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the access Router'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 maximal number of resend before the TFTP client stops communicating with the TFTP server.

Within the folder "**Utilities**" on the companion CD-ROM disk, we offered a TFTP server program (**TftpSrvr.exe**) for firmware upgrade. Run this program on the computer that is to serve as a TFTP server.



The image shows a web browser window titled "Firmware Upgrade". It contains a blue button labeled "Upgrade".

Fig. 51. Firmware upgrade by TFTP.

To upgrade firmware of the access Router by TFTP:

1. Get 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.
3. Configure IP address of the computer so that the Router and the computer are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.
5. On the computer, run a Web browser and click the **General, Firmware Upgrade** hyperlink.
6. 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.
7. Trigger the firmware upgrade process by clicking **Upgrade**.

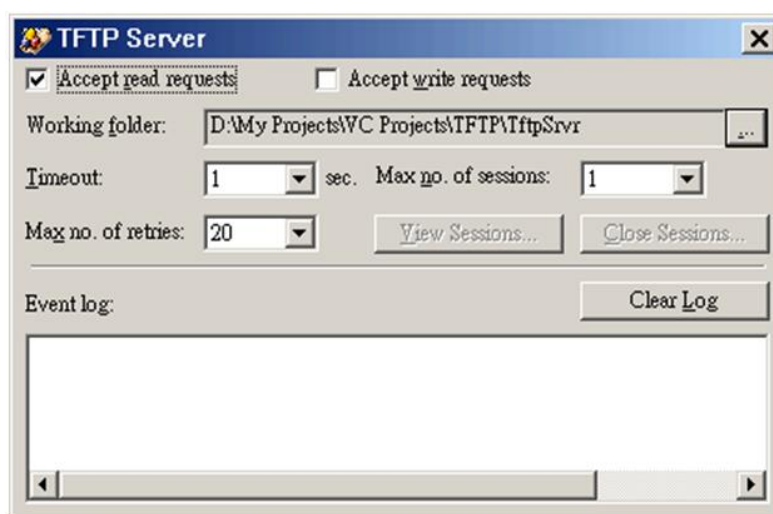


Fig. 52. TFTP Server.

After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside and the **Accept read requests** check box of TFTP Server is selected. Also, the LAN IP address of the Router and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless access Router be connected by Ethernet, and on the same LAN, so that the upgrade process would be smooth. A failed upgrade may corrupt the firmware and make the Router unstartable. When this occurs, call for technical support.

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.

TIP:	The firmware of a <i>deployed</i> access Router can also be upgraded remotely from the Inter-
-------------	---

net. In this case, you must have configured the Router to be remotely manageable (see Section 2.13.1.1) and adjust the Timeout and Max no. of retries settings of TFTP Server for remote TFTP upgrade to succeed.

2.10.3.4. Backing up and Restoring Configuration Settings by TFTP



Fig. 53. Configuration backup/restore.

To back up configuration of the access Router by TFTP:

1. Get 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 port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the Router are in the same IP subnet.
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 Router will be saved.
5. On the computer, run a Web browser and click the **SYSTEM\Firmware Tools** hyperlink.
6. Within the **Configuration Backup/Restore** section, 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.
7. Trigger the backup process by clicking **Back Up**. The Router's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the Router's MAC address. For example, if the Router'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 configuration of the IWE3200 by TFTP:

1. Get 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 port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the Router are in 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 by the Router's MAC address. For

example, if the Router's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Within the **Configuration Backup/Restore** section, 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.
7. Trigger the restoring process by clicking **Restore**. The Router will then download the configuration backup file from the TFTP server.

NOTE:	Make sure the file is a valid configuration backup file for the access Router.
--------------	--

2.10.3.5. Resetting Configuration to Factory Defaults

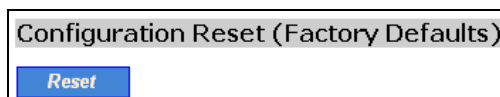


Fig. 54. Configuration reset.

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

WARNING:	Clicking the Reset button will lose all your current configuration settings.
-----------------	---

2.10.4. Setting Time Zone

Set the time zone of the SMCWHS44-G.	
Set Time Zone:	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Configure Time Server (NTP): You can automatically maintain the system time on your SMCWHS44-G by synchronizing with a public time server over the Internet.	
Time server:	clock.hinet.net
Daylight:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Fig. 55. Time zone and time server settings.

The **IWE3200** supports absolute system time by querying the SNTP (Simple Network Time Protocol) time server specified by the **Time server** setting. And you should specify the **Time zone** according to where you are.

2.11. Configuring TCP/IP Related Settings

2.11.1. Address

The addressing settings depend on the operational mode of the **IWE3200**. Each operational mode requires different addressing settings.

2.11.1.1. Router with a PPPoE-Based DSL/Cable Connection

Ethernet WAN Interface	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-09-92-00-19-F1
Trigger mode:	Auto
User name:	john
Password:	*****
Password again:	*****
Service name:	servicename
Host name:	gateway
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 56. TCP/IP settings for **Router with a PPPoE-Based DSL/Cable Connection** mode.

If the **IWE3200** was set to be in **Router with a PPPoE-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct **User name**, **Password**, and **Service name** settings.

The **Trigger mode** setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and torn down *manually (Manual)* by clicking the **Connect** and **Disconnect** buttons on the Start page, respectively. Or you can choose to let the device *automatically (Auto)* establish a PPPoE connection at bootup time. In **Auto** mode, if the connection is disrupted, the device will try to re-establish the broken connection automatically.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.11.1.2. Router with a DHCP-Based DSL/Cable Connection

Ethernet WAN Interface	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-09-92-00-19-F1
Trigger mode:	Auto
Host name:	gateway
Domain (DNS suffix):	
Release/Renew:	Release Renew
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 57. TCP/IP settings for **Router with a DHCP-Based DSL/Cable Connection** mode.

If the **IWE3200** was set to be in **Router with a DHCP-Based DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained by DHCP from the ISP. The **Trigger mode** setting affects the behavior of the DHCP client of the Router. In **Auto** mode, you don't have to worry about the DHCP process; the device takes care of everything. In **Manual** mode, there are two buttons on the Start page for you to manually release an obtained IP address (**Release**) and re-obtain a new one from a DHCP server (**Renew**).

'Heartbeat for BigPond Cable' is the settings for service of Telstra, Australia. Please consult the Telstra ISP for detail information.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.11.1.3. Router with a Static-IP DSL/Cable Connection

Ethernet WAN Interface	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-09-92-00-19-F1
Address Settings	
IP address:	192.168.168.221
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1
Host name:	gateway
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0

Fig. 58. TCP/IP settings for **Router with a Static-IP DSL/Cable Connection** mode.

If the Router was set to be in **Router with a Static-IP DSL/Cable Connection** mode, two IP addresses are needed—one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a *private IP address*, say **192.168.0.xxx**. The default LAN IP address is **192.168.0.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct **IP address**, **Default Router**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS server** settings.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.11.1.4. Router with Multiple DSL/Cable Connections

WAN 1: Static-IP DSL/Cable Connection	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-09-92-00-19-F1
IP Address:	192.168.168.221
Subnet mask:	255.255.255.0
Default gateway:	192.168.168.1
WAN 2: PPPoE-based DSL/Cable Connection	
<input type="checkbox"/> Custom MAC address of WAN interface:	00-09-92-00-19-E1
Trigger mode:	Auto
User name:	john
Password:	*****
Password again:	*****
Service name:	servicename
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.0.1
Subnet mask:	255.255.255.0
Host name:	gateway
Domain (DNS suffix):	

Fig. 59. TCP/IP settings for **Router with Multiple DSL/Cable Connections** mode.

Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of **Router with a PPPoE-Based DSL/Cable Connection**, **DHCP-Based DSL/Cable Connection**, or **Router with a Static-IP DSL/Cable Connection**, respectively. As a result, refer to Sections 2.11.1.1, 2.11.1.2, and 2.11.1.3 for more information.

2.11.2. DNS

2.11.2.1. DNS Proxy

IWE3200 provides the DNS Proxy function to enhance the network flexibility. Once the DNS Proxy function enabled, **IWE3200** will forward the DNS request from client to remote DNS server, the destination IP address response will also be forwarded by the DNS Proxy. The benefit is to allow the wireless clients only need to point the DNS to the IP address of default gateway of **IWE3200**, no remote DNS IP address required to be set on wireless clients.

The setting of DNS Proxy corresponds with the 'Router with a Static-IP DSL/Cable Connection' of WAN port. If multiple WAN ports enabled, all the DNS Proxy settings of the bound WAN ports under 'Router with a Static-IP DSL/Cable Connection' settings will be shown. For example, if WAN1 and WAN2 are both enabled and WAN1 is using 'Router with a Static-IP DSL/Cable Connection' mode, the DNS Proxy settings will be shown as below:

Proxy	
WAN 1 Primary DNS server:	0.0.0.0
WAN 1 Secondary DNS server:	0.0.0.0

Fig. 60. DNS Proxy under MultiWAN port enable.

2.11.2.2. Static DNS Mappings

Enabled	Domain Name	IP Address
<input type="checkbox"/>	www.company-name.com	192.168.0.201
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Fig. 61. Static DNS mappings.

By **Static DNS Mappings**, an internal server can be given a domain name, so that other hosts on the intranet can access the server by its domain name instead of by its IP address. For example, an internal Web server for the intranet, say 192.168.0.2, may be associated with the domain name, www.company-name.com.

To give an internal server a domain name:

1. Specify the domain name and the private IP address of the internal server.
2. Select the corresponding **Enabled** check box for the internal server.

2.11.3. NAT

2.11.3.1. Basic

Max number of sessions per user:	60
<input type="checkbox"/> DMZ host:	

Fig. 62. Basic NAT server settings.

When the Router is in **Router with a Static-IP DSL/Cable Connection** mode, the NAT server functionality can be enabled or disabled.

You can restrict the maximum number of user traffic sessions by specifying the **Max number of sessions per user** setting. In this way, you can prevent a single user from consuming too many network resources by initiating a large number of network sessions.

A DMZ (*DeMilitarized Zone*) host receives all unrecognized TCP/IP packets from the NAT server on the Router; therefore TCP/IP networking applications running on the DMZ host would have better compatibility with NAT.

To specify the DMZ host:

- Enter the private IP address of the computer to be used as a DMZ host, and select the corresponding check box.

2.11.3.2. Virtual Server Mappings

Enabled	Service Name	Private IP Address	Port	Protocol
<input type="checkbox"/>	FTP	192.168.0.201	21	TCP
<input type="checkbox"/>	IMAP4		143	TCP
<input type="checkbox"/>	SMTP		25	TCP
<input type="checkbox"/>	POP3		110	TCP
<input type="checkbox"/>	TELNET		23	TCP
<input type="checkbox"/>	HTTP		80	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP
<input type="checkbox"/>			0	TCP

Fig. 63. Virtual server mappings.

The gateway enables you to expose internal servers on the intranet through NAT to the Internet for public use. The exposed internal servers are called *virtual servers* because from perspective of hosts on the Internet, these servers are invisible in terms of TCP/IP.

To expose “preset” internal servers:

1. Select the corresponding **Enabled** check boxes for the kinds of servers (FTP, IMAP4, SMTP, POP3, TELNET, and HTTP) you want to expose.
2. Specify the private IP addresses of the internal servers.

To expose other internal servers:

1. Specify the **Service Name**, **Private IP Address**, **Port Number**, and whether the service is *TCP-based* or *UDP-based* for a non-preset internal server you want to expose.
2. Select the corresponding **Enabled** check box for the internal server.
3. Repeat Steps 1 to 2 for other non-preset internal servers.

2.11.4. DHCP Server

2.11.4.1. Functionality

There are three mode of DHCP Server to be defined in ‘Functionality’: Disable, DHCP Server , and DHCP Relay.

2.11.4.2. Basic

Functionality:	Enabled ▾
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

Fig. 64. Basic DHCP server settings.

The Router can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the **Default Router**, **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 allocateable IP addresses.

In most cases, **Default Router** and **Primary DNS server** should be set to the IP address of the Router's LAN interface (e.g., the default LAN IP address is **192.168.0.1**), and **Subnet mask** is set to **255.255.255.0**. There should be only *one* DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the Router.

2.11.4.3. 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"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Fig. 65. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **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 and it is always assigned the same IP address.

To always 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.

2.11.5. Load Balancing

The **IWE3200** provides the multiple WAN port Load Balancing mechanism. Without any policy specified in default settings, the incoming traffic (from WAN to LAN, also known as ‘*Out-bound Load-balancing*’) will be automatically balanced between every enabled WAN port, hence the incoming traffic will be equally balanced under the same throughput level of every WAN interface.

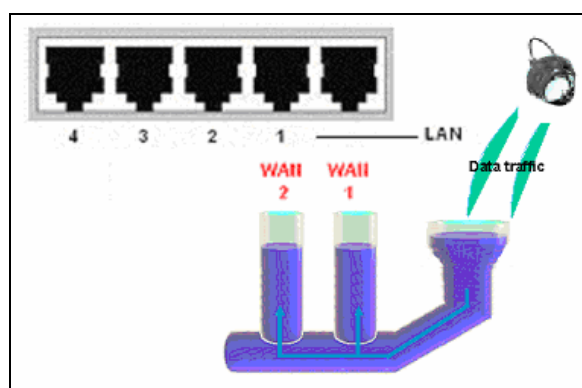


Fig. 66. Load Balancing mechanism.

In addition, the **IWE3200** can also set the load balancing policy by Port or IP range, so that the traffic of specified Port or IP range will be assigned the appointed WAN interface.

Load Balancing				
Policy by Port Range				
Starting Port	End Port	Interface		
<input type="text"/>	<input type="text"/>	WAN 1	<input type="button" value="Add"/>	
Port Range Policy				
No.	Starting Port	End Port	Interface	Delete
Policy by IP Address Range				
Starting IP	End IP	Interface		
<input type="text"/>	<input type="text"/>	WAN 1	<input type="button" value="Add"/>	
IP Address Range Policy				
No.	Starting IP Address	End IP Address	Interface	Delete
1	192.168.168.10	192.168.168.10	WAN 1	<input type="button" value="Delete"/>

Fig. 67. Load Balancing Policy Settings.

2.11.6. Zero Client Reconfiguration

☐ Client IP/ARP handling

☐ Transparent SMTP proxy

SMTP server:

SMTP port:

Account:
 ('Account' should be something like UserName@company.com)

Password:

Fig. 68. Zero Client Reconfiguration Settings.

The **IWE3200** provides the 'Zero Client Reconfiguration' function to allow the wireless clients associate to the **IWE3200** without any network setting modification required. It is convenient function for the wireless users who can associate the **IWE3200** automatically and no need to learn the network environment detail where the **IWE3200** deployed. The 'Zero Client Reconfiguration' function is enabled by checking the box of 'Client IP/ARP handling'.

The 'Transparent SMTP proxy' function provides the capability that the outgoing email of all wireless clients who associated to the **IWE3200** will use ONLY the specified SMTP email account, the original email account will be replaced by the specified email account. For example, if the email account of SMTP proxy of **IWE3200** is 'xxx@yyy.com' and the original email of wireless users is 'abc@xyz.com', if the SMTP proxy enable, the outgoing email of original 'abc@xyz.com' will be replaced by 'xxx@yyy.com' which specified in the SMTP proxy setting.

NOTE:

The SMTP proxy function can only replace the outgoing email to be the specified email account. Only the user(s) who has the SMTP settings (SMTP address, username, and password) of specified email account can receive the email(s) from the specified SMTP proxy account.

2.12. Configuring Wireless Settings

2.12.1. Communication

2.12.1.1. Basic

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

AP functionality:

Regulatory domain:

Channel number:

Network name (SSID):

Data rate:

Transmit power:

Fig. 69. Basic IEEE 802.11b/g communication settings.

For specific needs such as configuring the **IWE3200** as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the **IWE3200**.

Since the IEEE 802.11g-based **IWE3200** is also IEEE 802.11b compatible, you can configure the **Date rate** setting to meet your backwards compatibility needs. If there is RF interference, you may want to reduce the **Data rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the **IWE3200** must be identical for them to communicate with each other.

NOTE:

The **Regulatory domain** setting of the **IWE3200** sold in the U.S. and Canada is not configurable. It's set to FCC by default. As a result, only channels from 1 to 11 are available.

The transmit power of the RF module of the **IWE3200** can be adjusted so that the RF coverage of the **IWE3200** can be changed.

2.12.1.2. Wireless Distribution System

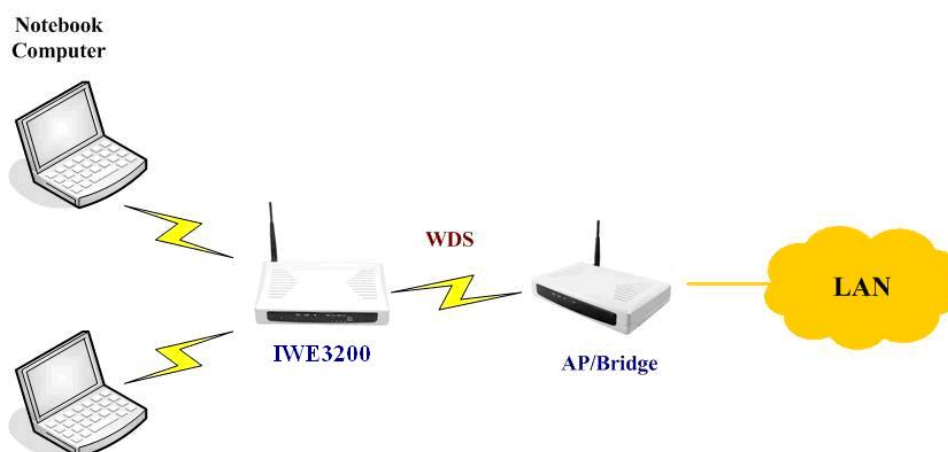


Fig. 70. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. , the wireless access Router acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to the AP/bridge through WDS. Then, the AP/bridge forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the **IWE3200** to the notebook computers. In this way, the **IWE3200** plays a role of “AP repeater.”

NOTE:

The **IWE3200** can have up to 6 WDS links to other wireless AP/bridge.

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"/>	

Fig. 71. Wireless Distribution System settings.

To enable a WDS link:

1. Specify the MAC address of the AP or wireless bridge at the other end of the WDS link.
2. Select the corresponding **Enabled** check box.

For example, assume you want a wireless access Router and an AP with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6, respectively, to establish a WDS link between them. On Router 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP 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 the **IWE3200** is connected to other peer APs or wireless bridges by WDS.

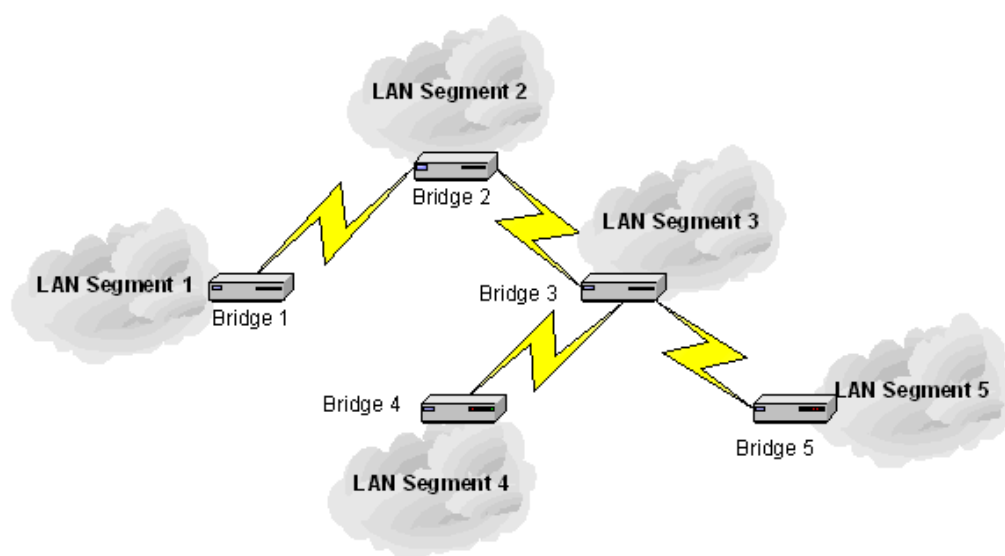


Fig. 72. Sample wireless bridge network topology.

WARNING:

Do not let your network topology consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links that form a *loop*. If there are any loops that exist, packets will circle around the loops and network performance will be seriously degraded.

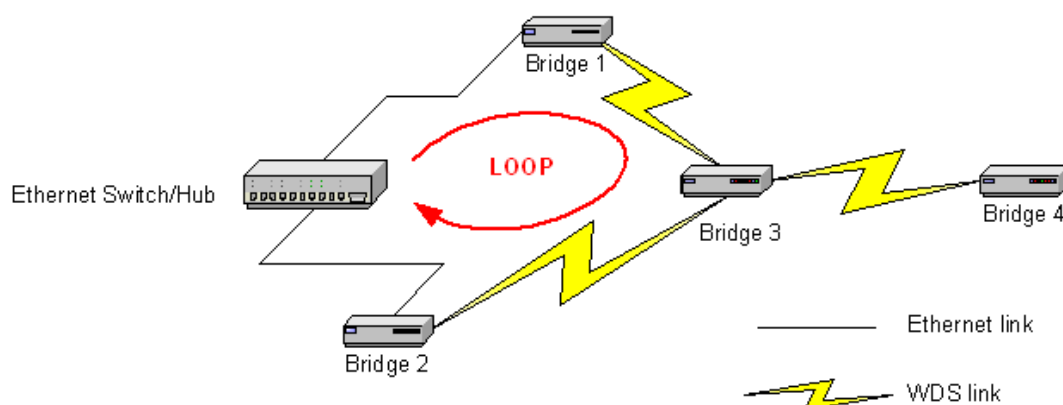


Fig. 73. Network topology containing a loop.

2.12.2. Security

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

2.12.2.1. 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:	*****

Fig. 74. Basic IEEE 802.11g security settings.

For security reasons, it's 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 and data encryption will be performed. Additionally, you can *disable* the SSID broadcasts functionality so that a wireless client (STA or Bridge Slave) with an "ANY" SSID cannot associate with the **IWE3200**.

Wireless Client Isolation is a feature for the **IWE3200** to block wireless-to-wireless traffic between STAs so that the STAs cannot see each other. This feature is useful for WLANs deployed in public places. This way, hackers have no chance to attack other wireless users in a *hotspot*.

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients (STAs) associated to this **IWE3200**, which acts as an AP, cannot see each other, and wireless-to-wireless traffic between the STAs is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different **IWE3200s** in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

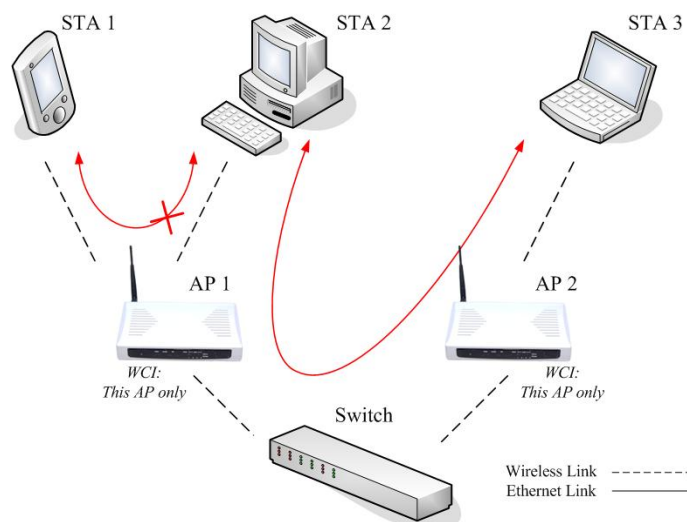


Fig. 75. Behavior of the "This AP Only" wireless client isolation option.

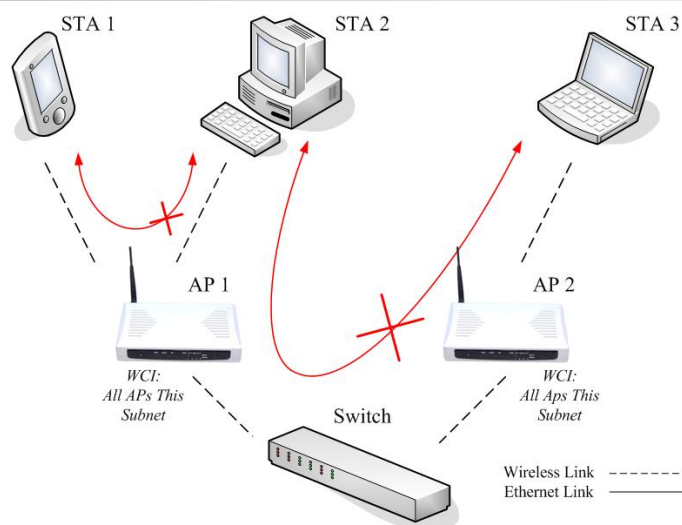


Fig. 76. Behavior of the “All APs on This Subnet” wireless client isolation option.

As illustrated in Fig. 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, while 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 Fig. , AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 7 security modes:

- **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 have 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 **IWE3200** is highly secured 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 2.13.2 for more information about IEEE 802.1x and RADIUS.

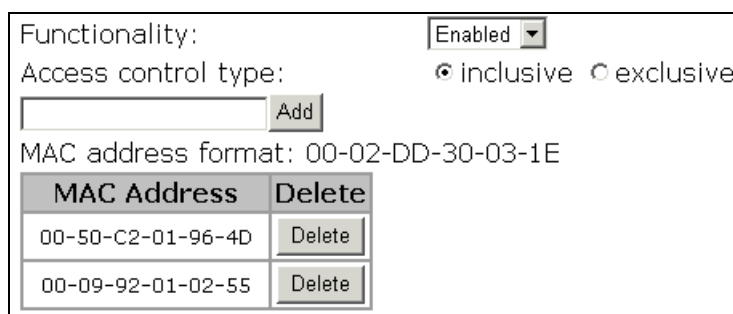
According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, *Shared Key* authentication is used if WEP data encryption is enabled. In rare cases, *Open System* authentication may be used when WEP data encryption is enabled. The **Authentication algorithm** setting is provided for better compatibility with wireless client computers 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 local device side to the remote device side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the remote device side to the local device side.

NOTE:

Each field of a WEP key setting is a *hex-decimal* number from 0-9, A-F. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

2.12.2.2. MAC-Address-Based Access Control



Functionality: 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"/>

Fig. 77. MAC-address-based access control settings.

With **MAC-Address-Based Access Control**, you can specify the wireless clients (STAs or Bridge Slaves) that are permitted or not permitted to associate with the **IWE3200**. When the table type is set to *inclusive*, entries in the table are permitted to associate with the **IWE3200**. When the table type is set to *exclusive*, entries in the table are not permitted to associate with the **IWE3200**.

To deny wireless clients' access 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 Step 3 for each other wireless client.

To grant wireless clients' access 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 allow access, and then click **Add**.
4. Repeat Step 3 for each other wireless client.

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"/>	

Fig. 78. MAC ACL download settings.

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 download the MAC ACL (Access Control List) file from the TFTP server to the **IWE3200**. Fig. 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

Fig. 79. 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**.

2.13. Configuring AAA (Authentication, Authorization, Accounting) Settings

2.13.1. Web Redirection

The **IWE3200** supports both IEEE 802.1x-based and Web redirection-based user authentication.

Here is a brief description of how Web redirection works: When an unauthenticated wireless user is trying to access a Web page, a logon page is shown instead of the requested page, so that the user can type his/her user name and password for authentication. Then, the user credential information is sent to a back-end RADIUS (Remote Authentication User Dial-In Service) server to see if the wireless user is allowed to access the Internet. The authentication mechanism employed for RADIUS is EAP-MD5, PAP, or CHAP.

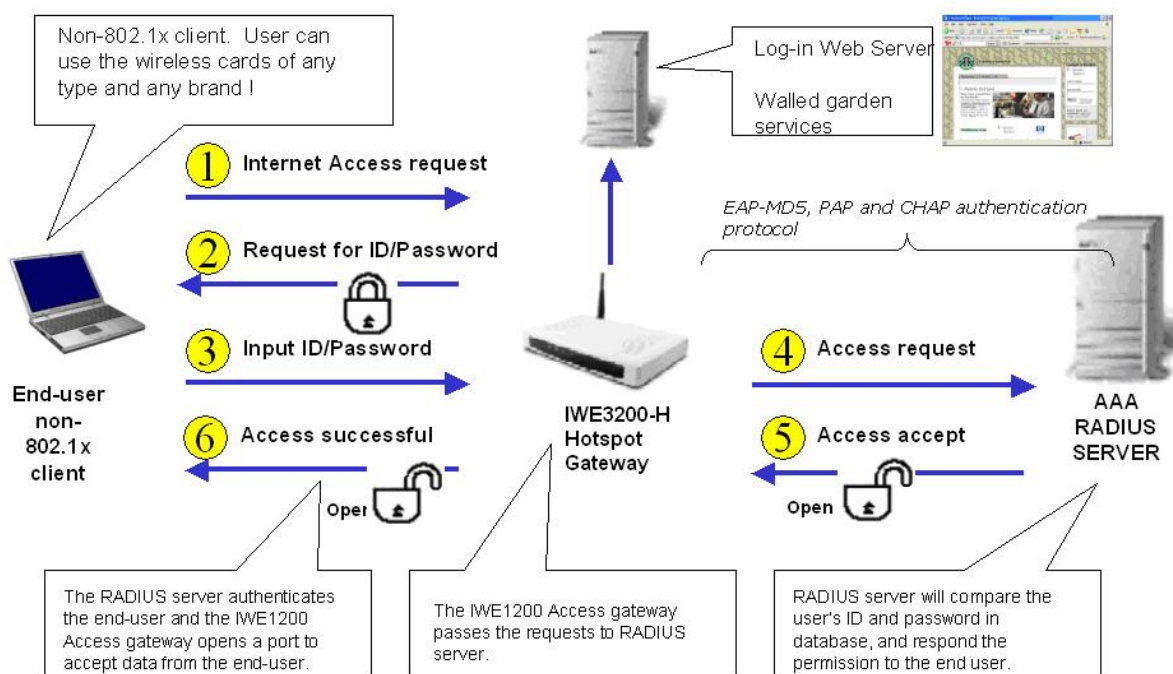


Fig. 80. Web-redirection mechanism.

TIP:

For IEEE 802.1x-based user authentication, see Section 3.5.3

2.13.1.1. Basic

Basic

Functionality: Enabled with Authentication

Encryption method: 401 Authorization

Authentication protocol: RADIUS

RADIUS authentication method: PAP

RADIUS link integrity: Disabled

Authentication login page:

☒ Default login page

☐ User-defined login page (Ex: <http://www.abc.com/index.htm> or <https://www.xyz.com/index.htm>):
 (HTTPS must use with "CGI with SSL" encryption)

Log-off and status page:

☒ Default log-off page

☐ The following URL:

☐ NONE

Web page shown after successful authentication:

☒ Original URL requested by the user

☐ The following URL:

Web page shown after failed authentication:

☒ Default URL

☐ The following URL:
 http://

Fig. 81. Web redirection enabled with authentication.

There are three modes for Web redirection—**Enabled with Authentication**, **Enabled without Authentication**, and **Disabled**.

In **Enabled with Authentication** mode, you specify the **RADIUS authentication method** that corresponds to your RADIUS server settings. Currently EAP-MD5, PAP, and CHAP are supported.

When a wireless user tries to access the Internet, he/she is redirected to a **Default log-on page** or a page stored on an external Web server (**The following URL**), depending on the network administrator's choice.

You have not been authenticated,
 therefore access of this site is not allowed.

Please click **Log On** to enter
 your user name and password for authentication.

Log On Log Off

Fig. 82. Default log-on page.

After the wireless user passes authentication, the wireless user can be brought to the originally requested Web page (**Original URL requested by the user**) or to a default page for advertisement purposes (**The following URL**). For example, if "<http://www.wi-fi.com>" is set for **The following URL**, the user will be brought to the home page of Wi-Fi Alliance.

In addition, the **Log-Off** window is also shown after the wireless passes authentication. The **Log-Off** window can be configured to contain the **Default log-off page** or a page stored on an external Web server (**The following URL**).

You have been authenticated.
Click **Log Off** to log off from the network.

Log Off

Remaining session time: 17:45:17

Fig. 83. Default log-off page.

NOTE:

On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the log-on page, and then click **Log Off** to end the session.

If the user fails the authentication, the user can be brought to a default warning page (**Default page**) or a page for the user to subscribe a wireless Internet access service (**The following URL**).

Authentication failed.
User name or password is invalid.

Try Again **Cancel**

Fig. 84. Default authentication failure warning page.

If you choose **The following URL for Log-on page for authentication, Log-off and status page, or Web page shown after failed authentication**, the pages stored on an external server have to contain specific HTML/JavaScript code so that Web redirection can work without error. Use the source of the default pages as templates for design your own authentication pages.

Because your customized versions of authentication pages have to contain references to the access Router's LAN IP address (**192.168.0.1** by default). If the LAN IP address of the access Router is changed, you must remember to change the IP address references in you customized pages.

Functionality: Enabled without Authentication

User redirect page http://

Fig. 85. Web redirection enabled without authentication.

In **Enabled without Authentication** mode, a user can access the Internet through the access Router without being authenticated first. However, instead of accessing his/her requested page, he/she is first redirected to a URL for advertisement purposes (**User redirect page**).

2.13.1.2. Unrestricted Clients

By IP Address:
Starting IP: End IP: **Add**

IP Pass-Through Table			
No.	Starting IP Address	End IP Address	Delete
1	210.12.11.10	210.12.11.20	Delete

By MAC Address:
MAC address: **Add**

MAC Pass-Through Table		
No.	MAC Address	Delete
1	00-09-92-01-02-05	Delete
2	00-09-92-01-02-08	Delete

Fig. 86. Unrestricted clients settings.

There are occasions on which you want some computers to be able to freely access the Internet without being authenticated first. For example, you may want your wired desktop computers connected with the Router to be uncontrolled by the Router while providing wireless Internet access service for your customers with wireless laptop computers. The **Unrestricted Clients** feature is for this purpose.

You can specify the computers to be uncontrolled by IP address or MAC address.

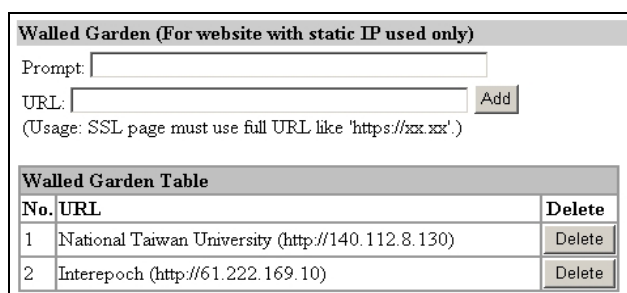
To specify uncontrolled computers within an IP address range:

1. Specify the **Stating IP** and **End IP** addresses of the IP address range.
2. Click **Add**. Then you'll see the newly entered IP address range appear in the **IP Pass-Through Table**.

To specify a uncontrolled computer by MAC address:

1. Specify its **MAC address**.
2. Click **Add**. Then you'll see the newly entered MAC address appear in the **MAC Pass-Through Table**.

2.13.1.3. Walled Garden



Walled Garden (For website with static IP used only)		
Prompt:	<input type="text"/>	
URL:	<input type="text"/>	<input type="button" value="Add"/>
(Usage: SSL page must use full URL like 'https://xxx.xxx'.)		
Walled Garden Table		
No.	URL	Delete
1	National Taiwan University (http://140.112.8.130)	<input type="button" value="Delete"/>
2	Interepoch (http://61.222.169.10)	<input type="button" value="Delete"/>

Fig. 87. Walled garden settings.

IP addresses or URLs in the *walled garden* can be accessed without authentication. This feature is useful for WISPs to do advertisement. For example, a WISP can set up a Web server to contain advertisement information for users who have not subscribed to its wireless Internet access service. The walled garden links are shown on the *log-on* authentication page.

To add a link to the walled garden:

1. Describe this link in the **Prompt** text box.
2. Specify the URL of this link in the **URL** text box.
3. Click **Add**. Then you'll see the newly entered hyperlink appear in the **Walled Garden Table**.

NOTE:

You cannot specify a Web site that supports *Web redirection*, which redirects HTTP requests to another URL, as a walled garden site. If such a Web-redirection-enabled site is specified in the walled garden, an HTTP access request to this site is redirected to another site that is “out of” the walled garden. And the user is therefore needs to be authenticated to access this out-of-walled-garden site. Always specify a Web site that actually hosts Web content as a walled garden site.

2.13.2. RADIUS

IEEE 802.1x *Port-Based Network Access Control* is a 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, 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 granting access to a wireless LAN supporting IEEE 802.1x, a user has 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* (see Section 2.12.2.1). 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 has to 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 automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

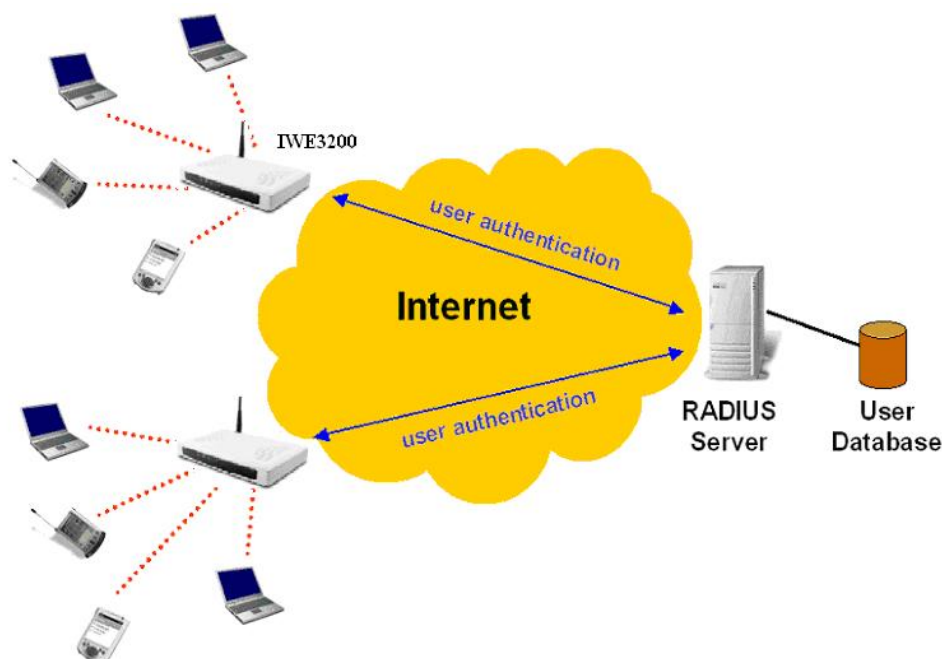


Fig. 88. IEEE 802.1x and RADIUS.

The **IWE3200** supports IEEE 802.1x and can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the **IWE3200** 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.

2.13.2.1. Basic

Primary RADIUS server:	
RADIUS server:	192.168.0.2
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	*****
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 89. RADIUS basic settings.

For the **IWE3200**, the RADIUS client component of the Router is shared by the IEEE 802.1x and Web redirection components. The RADIUS settings are for the RADIUS client to communicate with backend RADIUS servers.

NOTE:	The RADIUS server do not support all combinations of authentication methods if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes.			
		IEEE 802.1x Disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
	Web Redirection Disabled	■	■	■

Table 2. Allowable authentication modes.

The **IWE3200** can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the **IWE3200** 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.

The **IWE3200** and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, the **IWE3200** can identify itself by an NAS (Network Access Server) identifier. Each **IWE3200** must have a *unique* NAS identifier.

2.13.2.2. Robustness

<input checked="" type="checkbox"/> Notify RADIUS server after reboot
Reboot user name: <input type="text" value="reboot"/>

Fig. 90. RADIUS robustness settings.

The Router can be configured to notify the RADIUS server after it reboots. The RADIUS server can make use of the notification to clean up user authentication session records in the event that the Router reboots unexpectedly due to abnormal operation.

Select the **Notify RADIUS server after reboot** check box to enable this capability, and then specify the name of the *pseudo user* (default to “reboot”) for this operation in the **Reboot user name** text box.

2.13.3. Authentication Session Control

Idle timeout (min.):	<input type="text" value="10"/>
Session timeout (min.):	<input type="text" value="0"/>
Keep alive functionality:	<input type="button" value="Disabled"/>
Keep alive interval (min.):	<input type="text" value="0"/>
Periodical re-authentication functionality:	<input type="button" value="Disabled"/>
Periodical re-authentication interval (min.):	<input type="text" value="0"/>

Fig. 91. Authentication session control settings.

Authentication session control settings are for controlling the lifetimes of user authentication sessions. The **Idle timeout** setting specifies how long a user can be idle without generating any traffic before being terminated. The **Session timeout** setting specifies the maximum session lifetime. A zero value in the **Idle timeout**, **Session timeout**, or **Keep alive interval** setting disables the corresponding functionality effectively.

In addition, the Router provides a mechanism for detecting whether a user has left unexpectedly by handshaking between JavaScript code in the *log-off* authentication page and the Router. The *log-off* page notifies the Router periodically to announce user existence. When this mechanism for user existence detection is enabled (**Keep alive functionality**), the Router will terminate a user if no notification is received from the *log-off* page on the user's computer within the number of minutes specified by the **Keep alive interval** setting.

NOTE:

The **Log-Off** window cannot not be shown on a Windows CE-based Pocket PC, it is due to different JavaScript behavior of Pocket Explorer. To support Windows CE-based clients, you have to *disable* the keep-alive mechanism; otherwise the clients will be terminated unexpectedly.

2.13.4. Authentication Page Customization

2.13.4.1. Log-On, Log-Off, Authentication Success, and Authentication Failure Pages

Log-on, *log-off*, *authentication success*, and *authentication failure* authentication pages can be customized in a similar way. You can specify the **Text alignment** style, page title (**HTML title**) and the **Contents**. The **Contents** setting accepts HTML tagging. Clicking the **Preview** link shows a test page for you to see the results.

Text alignment:	<input type="button" value="Left"/>
HTML title:	<input type="text" value="Log-On"/>
Contents:	<pre>You have not been authenticated,
therefore access of this site is not allowed.

Please click Log On to enter
your <I>user name</I> and <I>password</I> for authentication.
Username:test</pre>
	Preview

Fig. 92. Log-on page customization settings.

Text alignment:	Left
HTML title:	Authentication Success
Contents:	<code>Authentication succeeded.
Please wait a few seconds...</code>
Preview	

Fig. 93. Authentication success page customization settings.

Text alignment:	Left
HTML title:	Authentication Failure
Contents:	<code>Authentication failed.
User name or password is invalid.</code>
Preview	

Fig. 94. Authentication failure page customization settings.

In addition to the **Text alignment**, **HTML title**, and **Contents** setting, two more settings are provided for specifying the size of the **Log-Off** window (**Windows width** and **Window height**).

Text alignment:	Left
Window width (pixel):	500
Window height (pixel):	400
HTML title:	Log-Off
Contents:	<code>You have been authenticated.

Click Log Off to log off from the network.</code>
Preview	

Fig. 95. Log-off page customization settings.

Furthermore, **Banner images** and **Hyperlinks** can be added to the **Log-Off** window for advertisement purposes. The banner images are shown in sequence at an interval specified by the **Update interval** setting. You can also specify the size of the banner image (**Image width** and **Image height**).

To specify an advertisement link:

1. Type the **Banner image** URL.
2. Type the **Hyperlink** URL.
3. Click the **Add** button, and then this advertisement link appears in the **Advertisement Links Table**.

Functionality:	Enabled ▾		
Update interval (sec.):	10		
Image width (pixel):	450		
Image height (pixel):	70		
Banner image:	http://		
Hyperlink:	http://		Add

Advertisement Links Table			
No.	Banner Image	Hyperlink	Delete
1	www.cis.nctu.edu.tw/~gis88586/80211.gif	www.80211-planet.com	Delete

Fig. 96. Advertisement links settings.



Fig. 97. Advertisement links in action.

2.14. DDNS

Functionality:	Disabled ▾
Account type:	dyndns.org (Dynamic) ▾
WAN interface:	WAN1 ▾
DDNS domain name:	johnsrv.dyndns.info
User name:	john
Password:	*****
Password again:	*****
Update interval (min):	5

Fig. 98. Dynamic DNS settings.

With the help of dynamic DNS (DDNS) services provided by *dyndns.org* or *no-ip.com*, you can make your device automatically register the IP address it obtains dynamically by PPPoE or DHCP with the DDNS servers. DDNS is useful if you want to set up a Web server whose IP address is dynamically obtained rather than statically configured.

Choose your DDNS service provider from the **Account type** drop-down list, choose the **WAN interface** on which the DDNS client operates, and specify the **DDNS domain name**, **User name**, and **Password** you have registered with your service provider. The DDNS client of the Router periodically communicates with its DDNS server at an interval specified by the **Update interval** setting.

2.15. Configuring Advanced Settings

2.15.1. Filters and Firewall

2.15.1.1. Packet Filters

Functionality:		Disabled					
Policy for unmatched packets:		Pass					
Rules:							
	Action	Protocol	Source IP Address	Subnet Mask	Destination IP Address	Subnet Mask	Destination Port
<input checked="" type="checkbox"/>	Block	ALL	192.168.0.1	255.255.255.0	140.113.23.1	255.255.255.255	100-200,80,25,1
<input type="checkbox"/>	Block	ALL					
<input type="checkbox"/>	Block	ALL					
<input type="checkbox"/>	Block	ALL					
<input type="checkbox"/>	Block	ALL					

Fig. 99. Packet filters settings.

You can specify rules for the firewall component of the Router to check outgoing packets. Packets that meet the rules can be permitted or denied. The *protocol* field, *source IP address* field, *destination IP address* field, and *destination port* field of a packet's IP header are inspected to see if it meets a rule. A packet that *meets* a rule can be dropped (*Block*) or accepted (*Accept*) as specified in the **Action** setting of the rule. Packets that *do not meet* any rules can be dropped (*Discard*) or accepted (*Pass*) as specified in the **Policy** setting.

A rule is composed of 5 parts:

- What to do if a packet meets this rule (**Action**)
- Protocol type
 - ◆ All
 - ◆ ICMP
 - ◆ TCP
 - ◆ UDP
- Source IP address range (**Source IP Address AND Source Subnet Mask**)
- Destination IP address range (**Destination IP Address AND Destination Subnet Mask**)
- Port ranges

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 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

Up to 5 port ranges can be specified in a rule, and these ranges must be separated by commas. For example, "21,80,85-89,140,200-230" in the destination port field signifies 5 port ranges.

To set a rule for packet filtering:

1. Specify the **protocol** type, **source IP address**, **source IP mask**, **destination IP address**, **destination IP mask**, and **destination port** for the rule. Then specify in the **Action** setting how to deal with a packet that meets the rule.
2. Select the corresponding **Enabled** check box.

NOTE:

Set the rules with great care since incorrect rules would make the Router inaccessible. The last resort to restore the Router to service may be resetting its configuration to factory-set values by pressing the **Default** switch on the housing of the Router.

2.15.1.2. VLAN

☐ Block wireless-to-Ethernet-LAN traffic

Fig. 100. VALN settings.

VLAN (Virtual Local Area Network) settings are for traffic isolation. When the **Block wireless-to-Ethernet-LAN traffic** check box is selected, the Router does not forward packets between the wireless network interface and the Ethernet LAN interface—traffic is allowed only between the Ethernet WAN interface and the wireless network interface.

2.15.1.3. Firewall

☐ Enable SPI (Stateful Packet Inspection)
☐ Block ICMP PING from Internet

Fig. 101. Packet filters and firewall settings.

SPI analyzes incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile. To enable SPI, select the **Enable Stateful Packet Inspection (SPI)** check box.

Some DoS (Denial of Service) attacks are based on sending invalid ICMP request packets to hosts. The Router can be set to not accept any ICMP requests on the Ethernet WAN interface to defense against attacks of this kind. Enable this capability by selecting the **Block ICMP PING from Internet** check box.

SPI can detect hacker attacks, including *IP-Spoofing*, *Zero IP Length*, *Land*, *Smurf*, *Fraggle*, *Tear-drop*, *Ping of Death*, *Syn-Flood*, and *X-Tree*. Because some of the Router's CPU resources are spent in checking packets for these security features, you may feel networking performance degradation if the security functions are enabled.

2.15.1.4. URL Filters

URL Filters

Functionality: Disabled ▼

Enabled	Keyword	Enabled	Keyword
<input type="checkbox"/>	www.nba.com	<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	

Fig. 102. URL filters settings.

The **IWE3200** is capable of blocking HTTP traffic from the intranet to specified unwelcome Web sites.

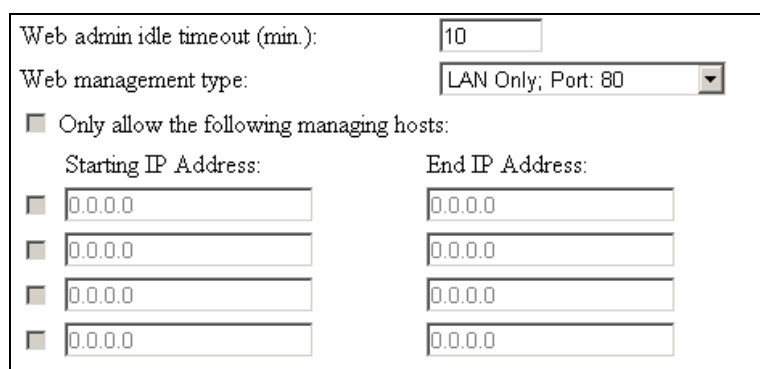
To block HTTP traffic to an unwelcome Web site:

1. Specify the URL (ex. www.xxx.com) of the unwelcome Web site.
2. Select the corresponding **Enabled** check box.

NOTE: Do not type “http://” when specifying a URL. Just type the domain name.

2.15.2. Management

2.15.2.1. Basic



Web admin idle timeout (min.):

Web management type:

☐ Only allow the following managing hosts:

Starting IP Address:	End IP Address:
<input type="checkbox"/> <input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> <input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> <input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> <input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

Fig. 103. Web-based management type setting.

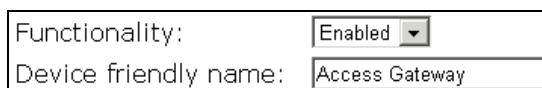
The **IWE3200** can be managed locally from the LAN side, remotely from the WAN side, or from both sides. Web admin idle timeout (min) means the idle timeout period for administrator. If the management type is **WAN Only** or **WAN and LAN**, be sure to specify the port **8080** when typing a URL for managing a Router within a Web browser. For example, if the WAN interface of a Router is configured to be 61.16.33.113, the URL for managing this Router is “http://61.16.33.113:8080”.

In addition, if the management type is set to **WAN Only**, the Router can be configured to be manageable only from specific hosts. In this way, security of remote management is enhanced.

To make the Router remotely manageable from specific hosts within an IP address range:

1. Select the **Only allow the following managing hosts** check box.
2. Type the **Starting IP address** and the **End IP Address** of the host IP address range.
3. Select the corresponding check box next to the IP address range.

2.15.2.2. UPnP



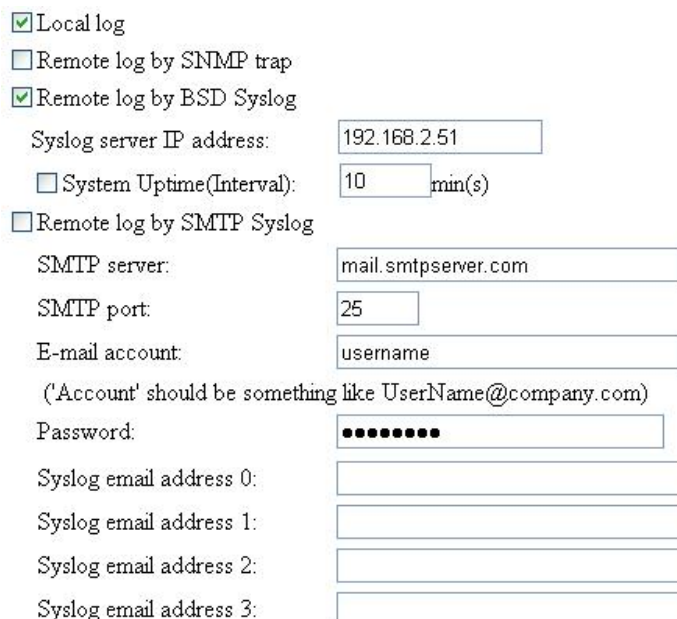
Functionality:

Device friendly name:

Fig. 104. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the Router in My Network Places of Windows XP. The Router 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 Router will launch the default Web browser for you to configure the Router.

2.15.2.3. System Log



☒ Local log
☐ Remote log by SNMP trap
☒ Remote log by BSD Syslog
Syslog server IP address: 192.168.2.51
☐ System Uptime(Interval): 10 min(s)
☐ Remote log by SMTP Syslog
SMTP server: mail.smtpserver.com
SMTP port: 25
E-mail account: username
(‘Account’ should be something like UserName@company.com)
Password: ••••••••
Syslog email address 0:
Syslog email address 1:
Syslog email address 2:
Syslog email address 3:

Fig. 105. System log settings.

System events can be logged to the on-board RAM of the **IWE3200 (Local log)** or sent in the form of SNMP trap (**Remote log by SNMP trap**) or [BSD Syslog](#) (**Remote log by BSD Syslog**) to a remote SNMP trap monitoring server or remote Syslog server, respectively. See the next subsection for more information about SNMP trap settings. Set the IP address of the Syslog server in the **Syslog server IP address** text box.

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:** user authentication status changes.
- **Managed LAN device:** Land device status changes

NOTE:

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

2.15.2.4. SNMP

Functionality:	Enabled <input type="button" value="v"/>
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	
<input type="checkbox"/> 0.0.0.0	
<input type="checkbox"/> 0.0.0.0	
<input type="checkbox"/> 0.0.0.0	

Fig. 106. SNMP settings.

The **IWE3200** can be managed by SNMP (Simple Network Management Protocol), and the SNMP management functionality can be disabled. 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.
3. Select the corresponding check box next to the **IP address** text box.

2.15.3. LAN Device Management

Check devices if alive every <input type="text" value="10"/> minutes							
Device Name	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface	Add/Delete
	<input type="text" value="0"/>		<input type="text" value="0"/>		TCP <input type="button" value="v"/>	Wired <input type="button" value="v"/>	<input type="button" value="Add"/>
AP1	60001	192.168.2.201	80	00-01-02-11-22-33	TCP	Wired	<input type="button" value="Delete"/>
AP2	60002	192.168.2.202	80	00-01-02-11-22-34	TCP	Wired	<input type="button" value="Delete"/>
AP3	60003	192.168.2.203	161	00-01-02-11-22-35	TCP	Wired	<input type="button" value="Delete"/>

Fig. 107. LAN device management settings.

LAN device management is for the **IWE3200** to pass management requests from the Internet through its built-in NAT server to devices on the private network. As a result, network devices (such as access points) behind the NAT server can be managed from the Internet. In this way, the access Router acts as a management proxy for the LAN devices. In addition, the **IWE3200** can periodically check whether the managed devices are working by PINGing them (**Check devices if alive every *n* minutes**). If it detects a device not working, it can send an SNMP trap (*remote system logging*) to a back-end server to report such a situation (see Section 2.15.2.3 for more information). The LAN device management functionality is especially useful for a WISP to remotely manage deployed APs that are usually invisible from the Internet due to the employment of NAT for IP address space conservation.

A management server from the Internet sees a managed LAN device as a combination of the access Router's WAN IP address and a **Virtual Port** reserved for this device. When a TCP or UDP-based management request (specified by the **Protocol** field) is received by the access Router from the Internet, the **IWE3200** translates the destination IP address and destination port of the request to the corresponding **Device IP Address** and **Device Port**. In other words, this request is passed through the built-in NAT server of the Router and routed to the corresponding managed LAN device.

For example, Fig. illustrates a LAN device management scenario based on the settings values in Fig. . AP1 can be managed from the management server by using a Web browser and a URL "<http://61.16.31.110:60001>". AP2 can be managed by using a Web browser and a URL "<http://61.16.31.110:60002>". AP3 can be managed from the management server by using an SNMP manager program via IP address 61.16.31.110 and port 60003. Destination IP addresses and destination ports of management packets for AP1, AP2, and AP3 are translated to 192.168.168.201:80, 192.168.168.202:80, and 192.168.168.201:161, respectively. (161 is a well known port for SNMP management.)

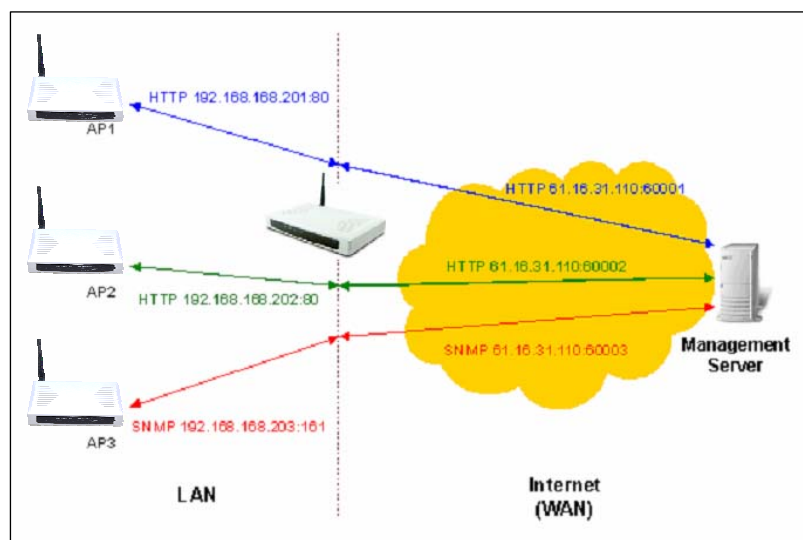


Fig. 108. Example for LAN device management.

To specify a LAN device to manage:

1. Give a name for this device in the **Device Name** text box.
2. Type the **Virtual Port**, **Device IP Address**, **Device Port**, and **Device MAC Address** for this device.
3. Choose the type of the management protocol (*TCP* or *UDP*) from the **Protocol** drop-down list.
4. Choose whether the Router communicates with the device *wirelessly* by WDS (**Wireless**) or by *Ethernet* (**Wired**) from the **Interface** drop-down list.
5. Select the corresponding check box next to the **Device Name** text box.

NOTE:	A valid input for the Virtual Port field must be between 60001 and 60100 inclusive.
NOTE:	The IP address in a Device IP Address text box and the Router's LAN IP address must be in the same IP subnet.
NOTE:	The Device Name , Device MAC Address , and the Interface fields are informational. They do not affect the inner workings of LAN device management.

Appendix A

A-1: Default Settings

TIP:

Press the **Default** switch on the housing of a *powered-on* Router to reset the configuration settings to factory-set values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	Gateway with a Static-IP DSL/Cable Connection
WAN Interface	
Type	DHCP
Changeable MAC Address	Default MAC address of WAN interface
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Host Name	gateway
Domain (DNS suffix)	Not set
PPP	
User Name	username
Password	Not set
Telephone Number	Not set
PPPoE	
User Name	username
Password	Not set
Service Name	Service name
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	
Functionality	Enabled
Default Gateway	192.168.0.1
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.0.1
Secondary DNS Server	0.0.0.0
First Allocataeble IP Address	192.168.0.2
Allocateable IP Address Count	20
NAT Server	
Functionality	Enabled
Virtual Server Mappings	Disabled
DMZ Host	Not set
Static NAT Mappings	Not set

DNS Proxy	
Static DNS Mappings	Not set
Filters/Firewall	
Packet Filters	Not set
URL Filters	Not set
VLAN	Disabled
WAN ICMP Request Blocking	Disabled
State Packet Inspection (SPI)	Disabled
Authentication	
Web Redirection	Disabled
RADIUS	Not set
RADIUS Robustness Reboot User Name	reboot
Session Control	Disabled
Management	
Web-Based Management Type	LAN only
SNMP	Enabled
SNMP Read-Only Community	public
SNMP Read-Write Community	private

A-2: LED Definitions

There are several LED indicators on the housing of a Router. They are defined as follows:

- **PWR** : Power
- **ALV** : *Alive*. Blinks when the **IWE3200** is working normally.
- **RF** : IEEE 802.11b/g interface activity
- **WAN/LAN** : Ethernet WAN/LAN interface activity

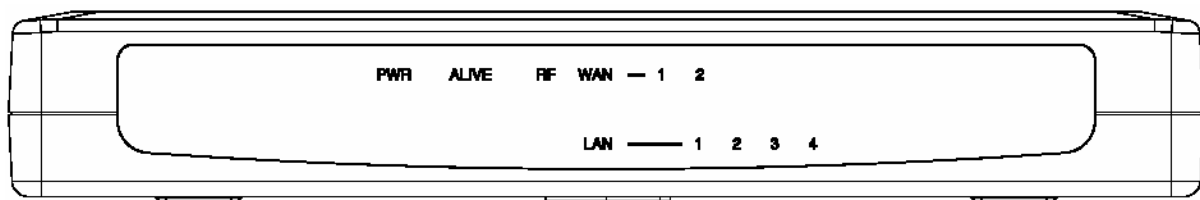


Fig. 109. LED Indicator.

A-3: Rear Panel

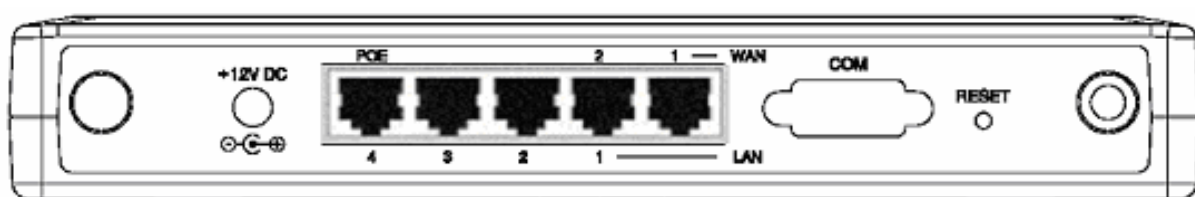


Fig. 120. Rear Panel.

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the Router is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the Router.
- Make sure that the LED ALV of the Router is blinking to indicate the Router is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.
- Make sure that the DSL, cable, V.90, or ISDN modem connected with the Router is powered on.

B-1: TCP/IP Settings Problems

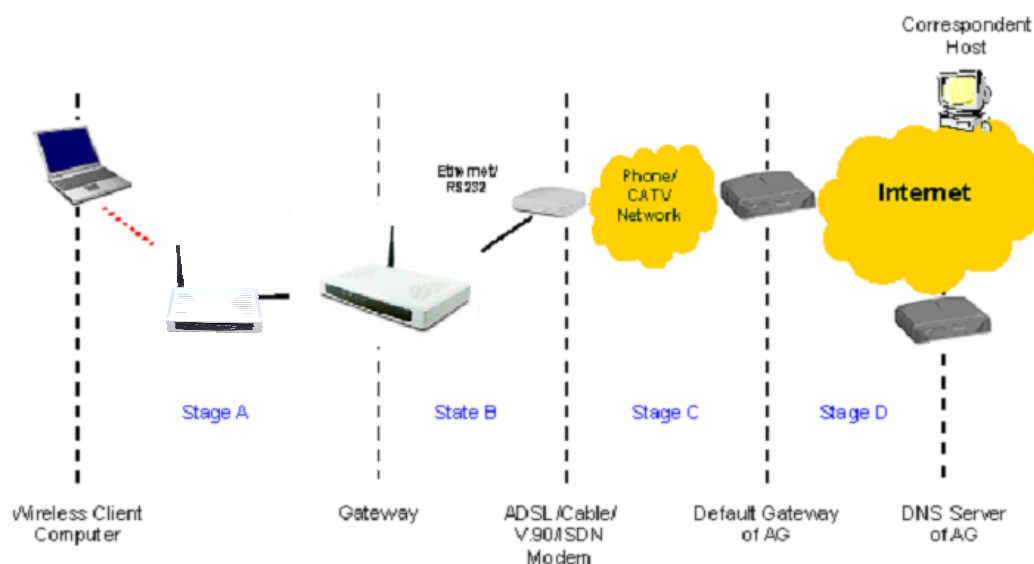


Fig. 121. Communication stages for a client to reach its correspondent host.

For a client computer to communicate with a correspondent 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 IWE3200, then the IWE3200 relays this request to the default Router of the IWE3200 through a modem. Finally, this request is forwarded by the default Router 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 further packets to this IP address.

As illustrated in Fig. , the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, **ping.exe**, can be employed to find out 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 wireless client cannot pass Web redirection-based authentication.**

- Are user name and password are correct?
 - ◆ Check the user credential information stored on the RADIUS server.
- Is the RADIUS server correctly set up?
 - ◆ Check whether the password for the wireless client is stored using *reversible encryption* on the RADIUS server.
 - ◆ Check if the RADIUS server is set to use EAP-MD5, PAP, and CHAP authentication.

- **The IWE3200 does not respond to *ping* from the client computer.**

- Are two or more NICs (wireless or wired) 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 communication link established?
 - ◆ Make sure the wireless link is OK.
 - ◆ Make sure the Ethernet link between the AP and the IWE3200 is OK.
 - ◆ Make sure the settings of the client computer and of the IWE3200 match.
- Are the IP address of the *client computer* and the IP address of the *IWE3200* in 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 IWE3200 are in the same IP subnet.

◆ **TIP:** If you forget the current IP address of the Router, use Router/AP Browser to get the information (see Appendix B-2).

- **The default Router of the IWE3200 does not respond to *ping* from the client computer.**

- Solve the preceding problem first.
- Is the modem working?
 - ◆ You may find out the answer by directly connecting the modem to a computer. Referring to the manual of the modem if necessary.
- Are the IP address of the IWE3200 and the IP address of its default Router in the same IP subnet?

- ◆ Find out the answer on the start page of the Web-Based Network Manager.
- Is the NAT server functionality of the IWE3200 enabled?
 - ◆ Find out the answer on the start page of the Web-Based Network Manager.
- If you cannot find any incorrect settings of the IWE3200, the default Router of the IWE3200 may be really down or there are other communication problems on the network backbone.
- **The DNS server(s) of the IWE3200 do not respond to *ping* from the client computer.**
 - Solve the preceding problems first.
 - If you cannot find any incorrect settings of the IWE3200, the default Router of the IWE3200 may be really down or there are other communication problems on the network backbone.
- **Cannot access the Internet.**
 - Solve the preceding problems first.
 - Make sure there are no incorrect packet filter settings that would block the traffic from the local computer to the Internet. In case you are not sure, the last resort may be resetting the configuration settings of the IWE3200 to default values by press the **Default** or **Soft-Reset** switch.

B-2: Wireless Settings Problems

- **The wireless client computer cannot associate with an IWE3200.**
 - 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 **IWE3200**?
 - ◆ Check the SSID setting of the WLAN NIC and of the **IWE3200**.
 - Is the WEP functionality of the prospective **IWE3200** enabled?
 - ◆ Make appropriate WEP settings of the client computer to match those of the **IWE3200**.
 - Is the prospective **IWE3200** within range of wireless communication?
 - ◆ Check the *signal strength* and *link quality* sensed by the WLAN NIC.

B-3: Other Problems

- I forget the IP address of the LAN interface of the IWE3200. What can I do to connect to it using a Web browser?
- My IWE3200 has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?
- Wireless Gateway/AP Browser (**WLBwrsr.exe**) in the “Utilities” folder on the companion CD-ROM disc. This utility can discover nearby WLAN APs, wireless routers, or IWE3200s and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.

NOTE: On Windows 2000/XP, Wireless Gateway/AP Browse can only be run by a user with administrator privilege.

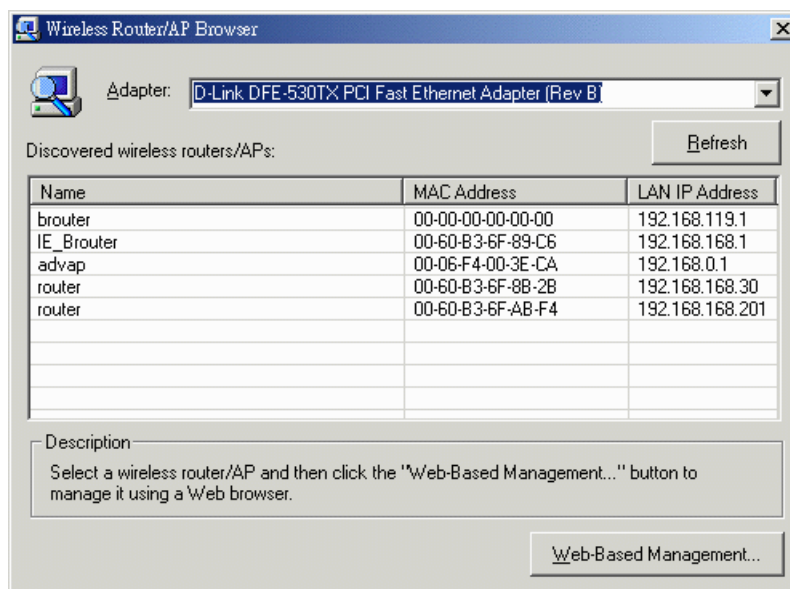


Fig. 122. Wireless Gateway/AP Browse.

- My IWE3200 stops working and does not respond to Web management requests.
 - The firmware of the **IWE3200** may be stuck in an incorrect state.
 - ◆ Unplug the power connector from the power jack, and then re-plug the connector to restart the **IWE3200**.
 - ◆ Contact our technical support representatives to report this problem, If this happens after a failed firmware upgrade process, the firmware of the **IWE3200** may have been corrupted.
 - If the **IWE3200** still does not work after restarting, there may be hardware component failures in the **IWE3200**.
 - ◆ Contact our technical support representatives for repair.

Appendix C: Technical Specifications

C-1: IWE3200

Standards:

802.11b
802.11g
802.3
802.3u
802.3af

Data rate & modulation:

OFDM@54Mbps, CCK@11/5.5Mbps, DQPSK@2Mbps and DBSK@1Mbps

Radio Technology:

OFDM
DSSS

Operating Range:

Up to 1,155 feet

Channels:

USA: 1-11 (FCC),
Canada: 1-11 (IC),
Europe: 1-13 (ETSI),
Japan: 1-14

Frequency range:

2.402 ~ 2.472 GHz (North America)
2.402 ~ 2.4970 GHz (Japan)
2.402 ~ 2.4835 GHz (Europe ETSI)
2.4465 ~ 2.4835 GHz (France)

Transmission output Power:

Typ. 19dBm@11Mbps, 15dBm@54Mbps

Receiving Sensitivity:

Typ. -81dBm@11Mbps, -68dBm@54Mbps

Antenna:

Removable Antenna with R-SMA connector ; antenna connector is "unique"

Operational Modes:

Wireless:

- Access Point / WDS Static Wireless Bridge

Gateway:

- Router with PPPoE-based DSL/Cable connection.
- Router with DHCP-based DSL/Cable connection.
- Router with Static-IP DSL/Cable connection.
- Router with nWAN DSL/Cable connection (n = 2)

Interface:

10/100 Mbps RJ-45 Connector
RS-232c Serial Connector
802.11b/g WLAN

Security:

64/128-bit WEP
802.1x
WPA
MAC address filtering
Disabled SSID broadcast
Wireless client isolation

Configuration and Management:

Web-browser
TFTP
SNMP
Syslog
Event Logging

LEDs:

Power
LAN/WAN
WLAN
Alive

Environmental:

Temperature: Operating (0~55C), storage (-20~70C)
Humidity: 5% to 95% non-condensing in storage

Electromagnetic Compatibility:

FCC Class B
Industry Canada
CE
ETS 300.328; ETS 300 826

Power Supply:

Input: 100VAC 60Hz
Output: 12VDC, 1A

Dimensions (without antenna):

8.5" x 5.5 " x 1.25"

Weight:

0.96 lbs

C-2: IWE500-INJ Power Injector

Input Power Requirements

AC Input Voltage	: 90 – 264Vac
AC Frequency	: 47 – 63 Hz
AC Input Current	: 2A at 100Vac, 1A at 240Vac, (-48Vdc)

Power over LAN output Specification

Pin Assignments and Polarity:	(+) 4/5 (–) 7/8
Output Voltage	: Aggregate Power:50W (48Vdc)

Mechanical Requirement

Dimensions	: 4" x 5.5" x 1.5"
Weight	: 1.38 Lbs
Indicators	
System Indicator	: AC Power (Green) Power Active (Red) $0.05\text{ A} < I_o < 0.8\text{ A}$ Over Current Protection (Red, Flash) $I_o > 1.0\text{ A}$

Connectors Shielded Rj-45

Environmental Conditions

Operating Temperature	: 32° to 104° F (0° to 40° C)
Operating Humidity	: Maximum 90% Non-condensing
Storage Temperature	: -13° to 185° F (-25° to 85° C)
Storage Humidity	: Maximum 95%, Non-condensing
Operating Altitude	: -1000 to 10,000 ft. (-304.8 to 3048 m)

Safety Approval

UL 1950
CSA A22.2 No. 950
EN 60950
CB

Regulatory Compliance

CE Compliance

Electromagnetic Emission and Immunity

A. FCC Part 15 Class B

C-3: IWE810-POS mini-POS Ticket Printer

Printing Method	Direct Thermal
Printing Speed	150 mm/sec (5.905 inch/sec)
Dot Density	180 x 180 DPI
Dot Pitch	0.141 mm, 0.125 mm
Effective Printing Width	72mm, 552 dots/line
Character Per Line	- Font A : 46 columns - Font B : 61 columns - Korea : 21 columns
Paper Type	Thermal Paper, Roll type
Paper Width	80 mm (+/-0.1)
Paper Thickness	0.06 ~ 0.09 mm
Paper Roll Diameter	83.0 mm (max)
Roll Core Inner Diameter	12.5 mm (+/-0.5)
Paper Supply Method	D&P(Drop and Print) Mechanism
Reliability TPH Life	100 km
Character Set	- 95 alphanumeric characters - 128 x 7 page(1 space page) extended graphic - 32 international characters
Barcode	Ean-8, Ean-13, Code 39, Code 93, Code 128, ITF, UPC-A, UPC-E, Codabar
Emulation	ESC/POS Command Compatible; TM-T88(II), TSP600(Epson mode), iDP-3540
Driver	Epson driver compatible, RP-200 driver (Win2000/XP)
Draw Port	2 ports
Interface	RS-232 Serial (optional Centronics Parallel or USB)
Power Adapter	External AC 100V ~ 250V, 50~60 Hz
Environment	- Operating Temperature : 5 ~ 40 degree - Operating Humidity : 35 ~ 80% - Storage Temperature : -20 ~ 60 degree - Storage Humidity : 10 ~ 90%
Auto cutter	- Type : Guillotine - Life : 10,000,000 cuts - Paper Thickness : 0.06 ~ 0.09 mm - Cutting Method : Full/Partial Cut (controlled by swith)
Weight	1.6 kg (include auto cutter)
Dimension	152 x 194 x 148 mm (5.984" x 7.638" x 5.826")
Certification	UL, CUL, FCC Class A