HD COM

IN WALL BOX ACCESS POINT

Model :

HD28650

Copyright Notice

Protected by TW patent 223184, JPN patent 3099924 and China patent ZL 03 2 04640.5.

Disclaimer

We shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from furnishing this material, or the performance or use of this product. We reserve the right to change the product specification without notice. Information in this document may change without notice.

Trademarks

Microsoft Win98, Windows 2000 and WinXP are registered trademarks of Microsoft Corporation.

General: All other brand and product names mentioned herein may be registered trademarks of their respective owners. Customers should ensure that their use of this product does not infringe upon any patent rights. Trademarks mentioned in this publication are used for identification purposes only and are properties of their respective companies.

Table of Contents

1 Introduction

The HD28650 Access Device revolutionizes the way wireless and wired IP-based services are delivered to hospitality and residential properties. The HD28650 integrates wired and wireless connectivity into a small unit that can be quickly and discretely installed in a standard wall box. The HD28650 provides **One** Ethernet ports, a 2.4GHz 802.11b/g/n wireless access point. The HD28650 requires a single powered cable drop to unlock its utility and, through the reduction in cabling, switch ports, and power-sourcing equipment, the HD28650 represents the best value for the delivery of next generation entertainment services.

1-1 Package Contents

Please inspect your package. The following items should be included:

◎ ***HD28650***

- One In Wall Access Pointt
- One Telephone Cable (10cm)
- One UTP Ethernet/Fast Ethernet cable (Cat.5 Twisted-pair)
- One Wall Faceplate(Top and Bottom)
- Bracket (EU STD*2/Set JPN STD*1/Set)
- One Quick Installation Guide

If any of the above items are damaged or missing, please contact your dealer immediately.

1-2 Features

- Wireless data rates up to 150Mbps
- Comprehensive security

  64/128-bit WEP encryption

  WPA encryption

  WPA2 encryption
- Intelligent Management

1-3 Precautions

- Never remove or open the cover. You may suffer serious injury if you touch these parts.
- Never install the system in the wet locations.

1-4 Outlook

Figure 1 In Wall Box Access PointOutlook

1-4-1 Top Panel

The top panel of the In Wall Box Access Pointis shown below.

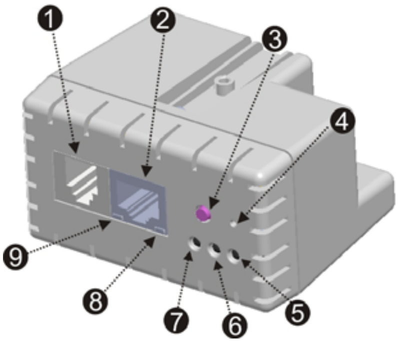
Figure 2 In Wall Box Access PointTop Panel

LEDs Indication

LED	State	Description
PWR	Off	The In Wall Box Access Pointis not receiving electrical power.
	Green	The In Wall Box Access Pointis receiving electrical power.
SYS	Off	The In Wall Box Access Pointstatus is defective.
	Green	The In Wall Box Access Pointstatus is complete.
	Green (Blinking)	During firmware upgrades, this system LED will blink.
LINK / WAN	Off	Port has not established any network connection.
	Yellow	A port has established a valid 10/100Mbps network connection.
	Yellow (Blinking)	10/100Mbps traffic is traversing the port.
LAN	Off	Port has not established any network connection.
	Green	A port has established a valid 10/100Mbps network connection.
	Green (Blinking)	10/100Mbps traffic is traversing the port.
WLAN	Off	The Wireless is not ready.
	Green	The In Wall Box Access Pointhas established a valid wireless connection.
	Green (Blinking)	The Wireless connection is active.

1-4-2 Rear Panel

The rear panel of the In Wall Access Pointt



1. RJ-11 Telephone Connector
2. RJ-45 Ethernet Connector
3. WPS Button
4. Reset Button
5. WLAN
6. SYSTEM
7. POWER
8. LAN Port
9. LINK Port

Figure 3 In Wall Box Access PointRear Panel

1-5 Technical Specifications

1-5-1 Hardware Specifications

Network Specification

IEEE802.3 10 Base TX Ethernet

IEEE802.3u 100 Base TX Fast Ethernet

IEEE802.3af Power over Ethernet

IEEE802.11b Wireless LAN

IEEE802.11g Wireless LAN

IEEE802.11n Wireless LAN

ANSI/IEEE 802.3 NWay auto-negotiation

Static IP Client

DHCP Client

Wi-Fi Compatible

Connectors

One LAN Ports (10BaseT/100BaseTX Auto cross-over)

One LINK Port (10BaseT/100BaseTX Auto cross-over)

Two Tel Port (Telephone Line transparent used)

Encryption

WEP (Wired Equivalent Privacy) 64/128-bit RC4

WPA (Wi-Fi Protected Access)

WPA2 (Wi-Fi Protected Access)

WPS (Wi-Fi Protected Setup)

LED Indicators

One POWER LED

One Link 10/100M Link/Activity LED

One LAN 10M/100M Link/Activity LEDs

One Wireless Link/Activity LED

One System LED

Environment Conditions

Operating Temperature: 0 to 50°C

Storage Temperature: -10 to 60°C

Operating Humidity: 10~80% non-condensing

Storage Humidity: 10% to 90% non-condensing

Certifications

FCC part 15 Class B, CE, NCC

Dimension

Size: 39.3(W) x 71.6(L)x 55(H)/ mm

Weight: About 85g (Net)

1-5-2 Software Specifications

Networking

- IEEE802.3 10BaseT Ethernet
- IEEE802.3u 100BaseTX Fast Ethernet
- IEEE802.3af Power over Ethernet
- IEEE802.11b Wireless LAN

- IEEE802.11g Wireless LAN
- IEEE802.11n Wireless LAN
- Static IP WAN Client
- DHCP WAN Client

Security and Firewall

- WEP
- WPA
- WPA2
- WPS

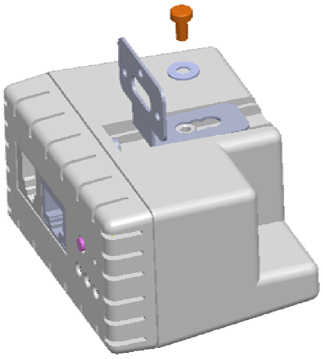
Management

- Web-based Management Tool
- Firmware Upgrade via HTTP/TFTP
- Backup/Restore/Factory Default Setting
- Remote Authorized Management
- SNMP v1/v2 (MIB II, Private MIB)
- System Information Table

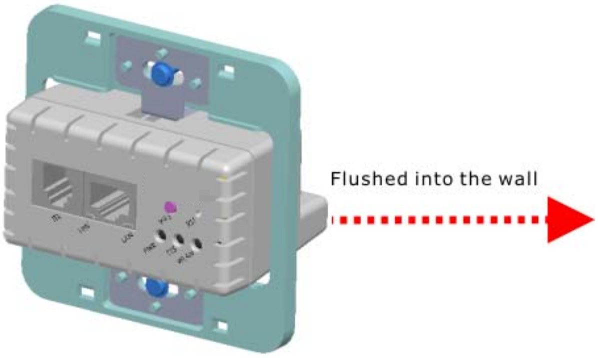
2 Installation

The followings are instructions for setting up the In Wall Access Point. Refer to the illustration and follow the simple steps below to quickly install your In Wall Access Point.

Step 1：Slide the Bracket to align with screw holes on the HD28650, and fasten the Bracket tightly with screws on the HD28650.



Step 2：Slide the HD28650 into the Bottom Faceplate and fasten tightly into the Bottom Faceplate until it's flushed into the wall.



Step 3：Line-up and push the Top faceplate onto Bottom faceplate until snaps securely into place.

2-1 Installation Requirements

Before installing the In Wall Access Point, make sure your network meets the following requirements.

System Requirements

The In Wall Box Access Pointrequires one of the following types of software:

- Windows 98 Second Edition/NT/2000/XP
- Red Hat Linux 7.3 or later version
- MAC OS X 10.2.4 or later version
- Any TCP/IP-enabled systems like Mac OS and UNIX (TCP/IP protocol installed)
- Standard phone line for xDSL modem

  Or

  Coaxial cable for Cable modem
- Web Browser Software (Microsoft I.E 5.0 or later version or Netscape Navigator 5.0 or later version)
- One computer with an installed 10Mbps, 100Mbps or 10/100Mbps Ethernet card
- UTP network Cable with a RJ-45 connection (Package contents)

Note: *Prepare twisted-pair cables with RJ-45 plugs. Use Cat.5 cable for all connections. Make sure each cable not exceed 328 feet (Approximately 100 meters).*

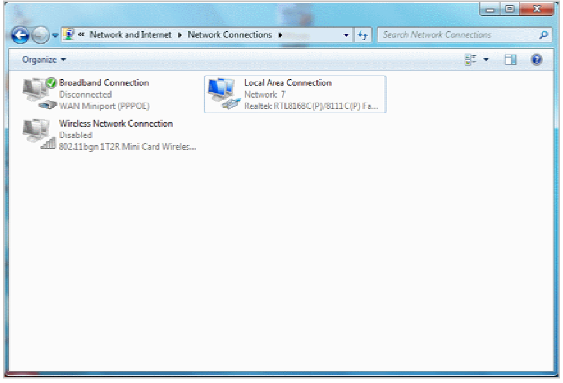
2-2 Getting Start

HD28650 support web-based configuration. Upon the completion of hardware installation, can be configured through PC/NB by web browser such as Internet Explorer, Firefox, and Opera.

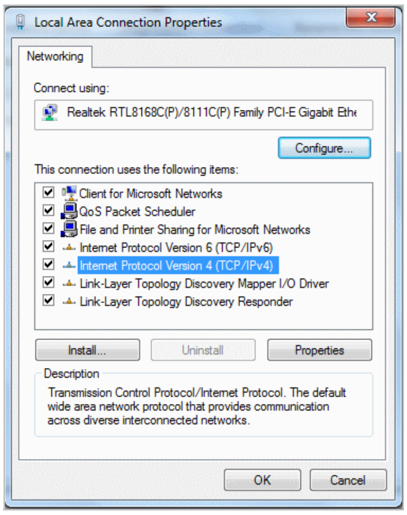
- **Default IP Address:**10.59.1.254
- **Default Subnet Mask:**255.255.255.0
- **Default Username and Password:** admin/admin

> ***Note*** *：Set the IP segment of the administrator's computer to be in the same range as HD28650 for accessing the system.* ***Do not duplicate*** *the IP address used here with IP address of HD28650 or any other device within the network.*

Step1：Click **Start→Setting→Control Panel,** and then "Control Panel" window appears, Click on "**Network connection**" window appears.


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Broadband Connection
Disconnected
WAN Miniport (PPPOE)
Local Area Connection
Network 7
Realtek RTL8168C(P)/8111C(P) Fa...
Wireless Network Connection
Disabled
802.11bgn 1T2R Mini Card Wireles...

Step2：In **"Local Area Connection properties"** window, select **"Internet Protocol (TCP/IPv4)"** and click on **"properties"** button.



Local Area Connection Properties

Networking

Connect using:

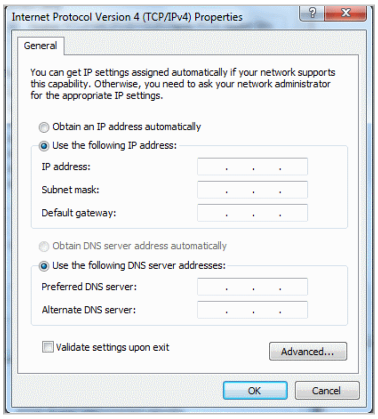
Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethe

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

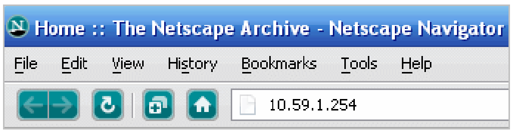
□ Validate settings upon exit

Example:

IP Address:10.59.1.109

Subnet Mask:255.255.255.0

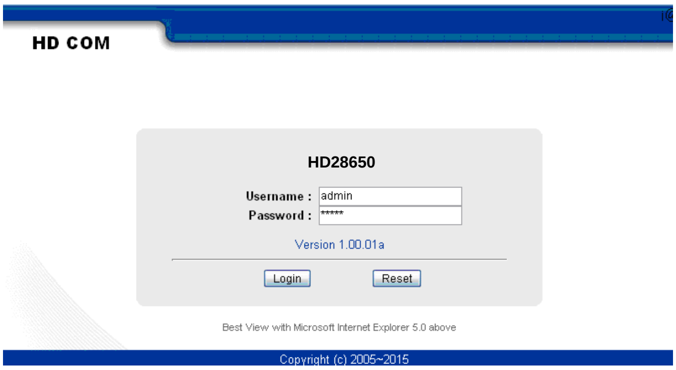
Step 3：Launch your browser, and then enter the factory default IP address **10.59.1.254** in your browser's location box. Press **Enter**.



Home :: The Netscape Archive - Netscape Navigator

10.59.1.254

Step 4：.The HD28650 login screen will appear. In the Username and Password field, type the factory default user name **admin** and password **admin** and click Setup. The HD28650 setup screen will appear.



HD COM

HD28650

Username : admin

Password : *****

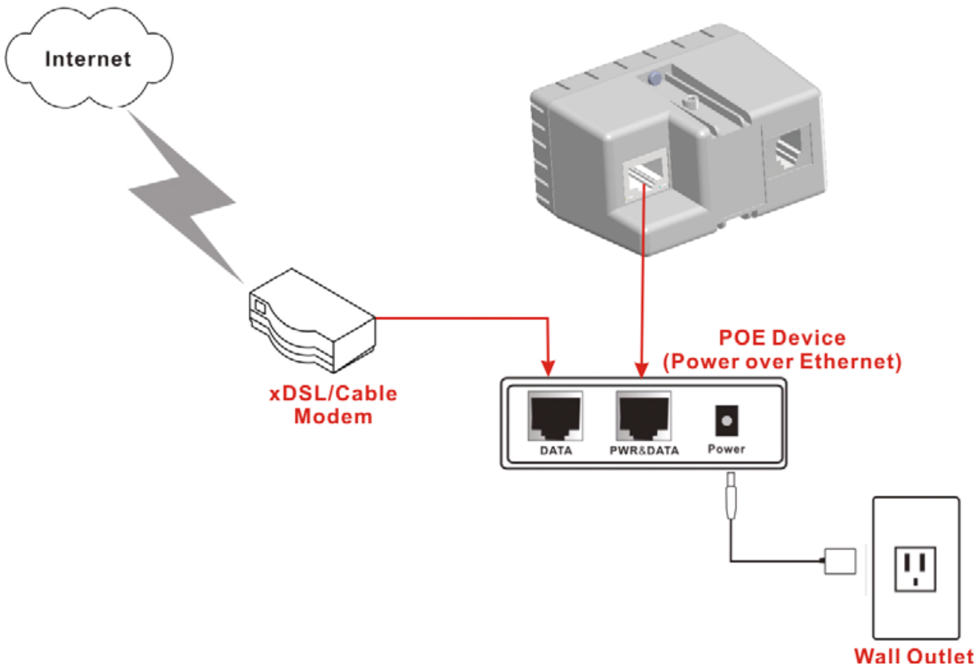
Version 1.00.01a

Best View with Microsoft Internet Explorer 5.0 above

Copyright (c) 2005~2015

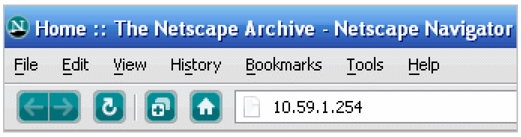
Note: It is important to remember your password. If for any reason you lose or forget your password, press the reset button located on the top of the device. Reset action will re-initialize the settings. All configurations, including username, password and IP address(s), will be reset, and requires re-entering.

POE (Power over Ethernet) Application



Note: *To use the HD28650's POE feature, follow the instructions for your specific POE device.*

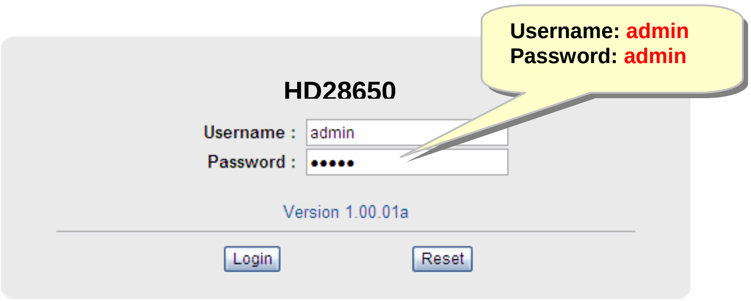
Step 1: Start your browser, and then enter the factory default IP address **10.59.1.254** in your browser's location box. Press **Enter**.


Home :: The Netscape Archive - Netscape Navigator
File Edit View History Bookmarks Tools Help

10.59.1.254

Figure 4 Web Browser Location Field (Factory Default)

Step 2: The In Wall Box Access Pointconfiguration tools menu will appear. In the Username and Password field, type the factory default user name **admin** and password **admin** and click **Login**. If you are first time setting the system, the wizard setup screen will appear. You will be guided, step-by-step, through a basic setup procedure.



Username : admin
Password : ●●●●●

Username: admin
Password: admin

Figure 5 Configuration Tools Menu

Note:

☞ *This Web agent is best viewed with IE 5.0 or Netscape 6.0 and above browsers.*

☞ *Username and Password can consist of up to 20 alphanumeric characters and are case sensitive.*

☞ *If for some reason your password is lost or you cannot gain access to the In Wall Box Access PointConfiguration Program, please press the reset button to load the device to manufacturer defaults.*

☞ *If the In Wall Box Access Pointdoesn't send packet in 5 minutes (default), the In Wall Box Access Pointwills logout automatically.*

☞ Proxy needs to set disable first when administrator accesses admin UI

The Setting enables you to configure advanced settings related to accessing the Internet；display In Wall Box Access Pointbasic status and process Firmware upgrade, change password and backup or restore configuration.　Including,

- **Internet Setting**
  - Link
- **Wireless**
  - Basic
  - Advanced
  - Security
  - WPS
- **Administration**
  - Management
  - Firmware
  - Configuration
  - SNMP
  - System Status
  - Ping Command
- **System Tool**
  - Restart
  - Logout

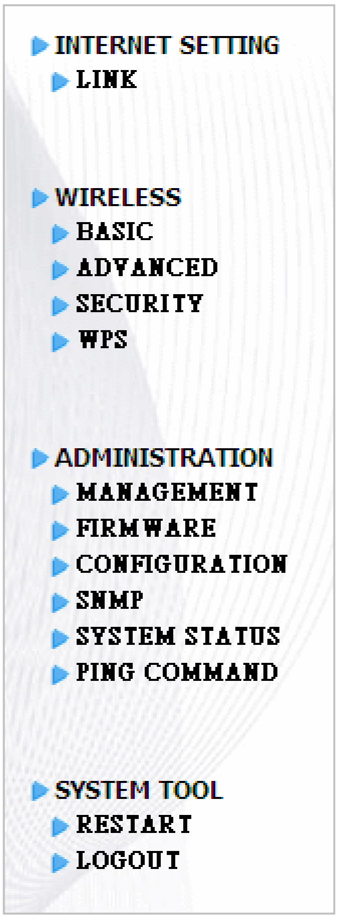
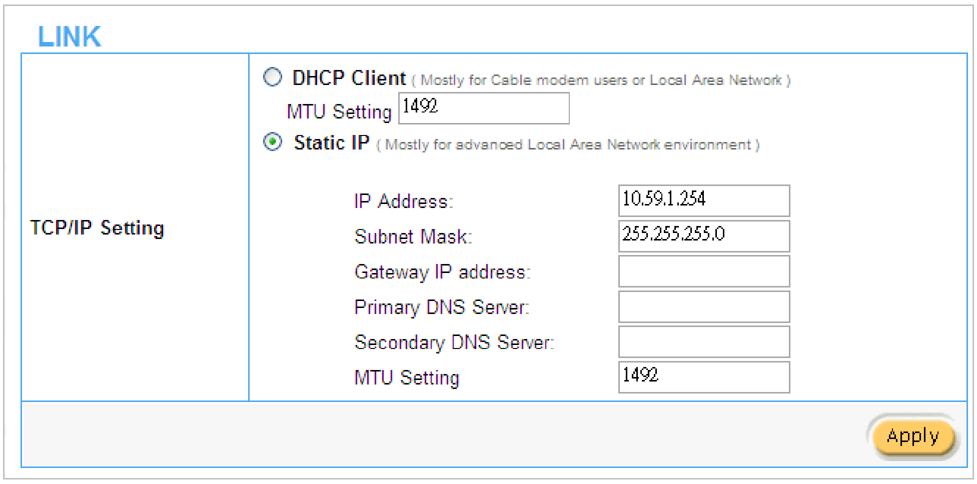


Figure 6 Configuration Tools Menu

3-1 Internet Setting

3-1-1 TCP/IP Setting

The IP address can be manually set or automatically assigned by a DHCP server on the LAN. If you are manually setting the **IP address**, **Subnet mask**, and **Gateway IP address** settings, set them appropriately, so that they comply with your LAN environment.



LINK

TCP/IP Setting

○ DHCP Client (Mostly for Cable modem users or Local Area Network)

MTU Setting 1492

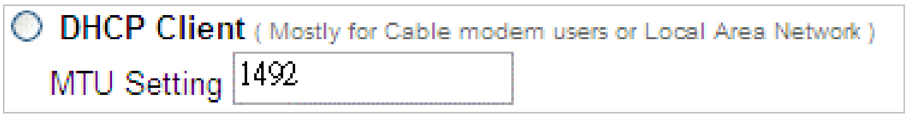
● Static IP (Mostly for advanced Local Area Network environment)

IP Address:	10.59.1.254
Subnet Mask:	255.255.255.0
Gateway IP address:	
Primary DNS Server:	
Secondary DNS Server:	
MTU Setting	1492

Figure 7 the TCP/IP Setting

<u>DHCP Client</u>

The device can work as a DHCP client. This allows the device to obtain the IP address and other TCP/IP settings from your switch or IP router. If your device comes with this feature, please enable Use DHCP Client.



○ DHCP Client (Mostly for Cable modem users or Local Area Network)

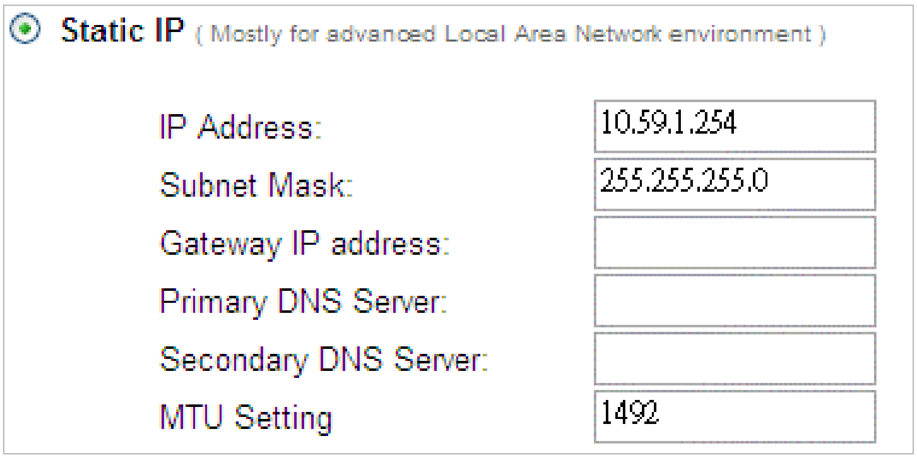
MTU Setting 1492

Figure 8 DHCP Client Setting Screen

Item	Default	Descriptior
MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum

		transmission unit size.

Static IP



● Static IP (Mostly for advanced Local Area Network environment)

IP Address: 10.59.1.254

Subnet Mask: 255.255.255.0

Gateway IP address:

Primary DNS Server:

Secondary DNS Server:

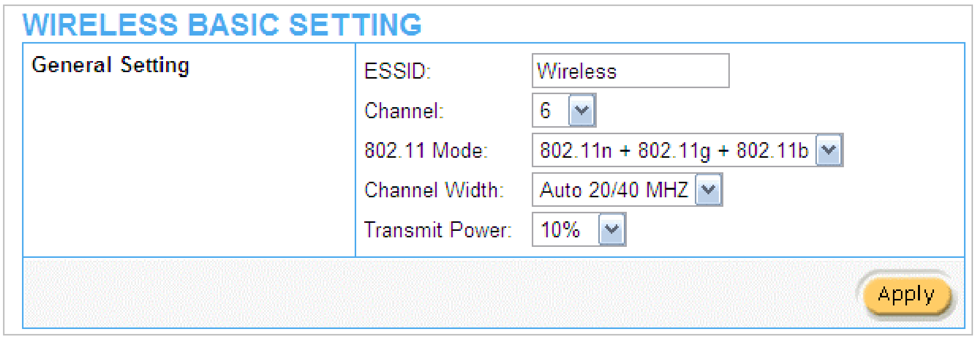
MTU Setting 1492

Figure 9 Static IP Setting Screen

Item		Description
IP Address	10.59.1.254	Enter the IP address for the xDSL/Cable connection (provided by your ISP).
Subnet Mask	255.255.255.0	Enter the subnet mask for the IP address.
Gateway IP Gateway		Enter the Gateway IP address for the xDSL/Cable connection
Primary DNS Server		A primary DNS server IP address for the xDSL/Cable connection
Secondary DNS Server		A secondary DNS server IP address for the xDSL/Cable connection. If the primary DNS Server IP were not available, meanwhile, Secondary DNS Server IP would start in the same time.
MTU Setting	1492	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.

3-2 Wireless

3-2-1 Wireless Basic Setting



WIRELESS BASIC SETTING

General Setting

ESSID: Wireless

Channel: 6

802.11 Mode: 802.11n + 802.11g + 802.11b

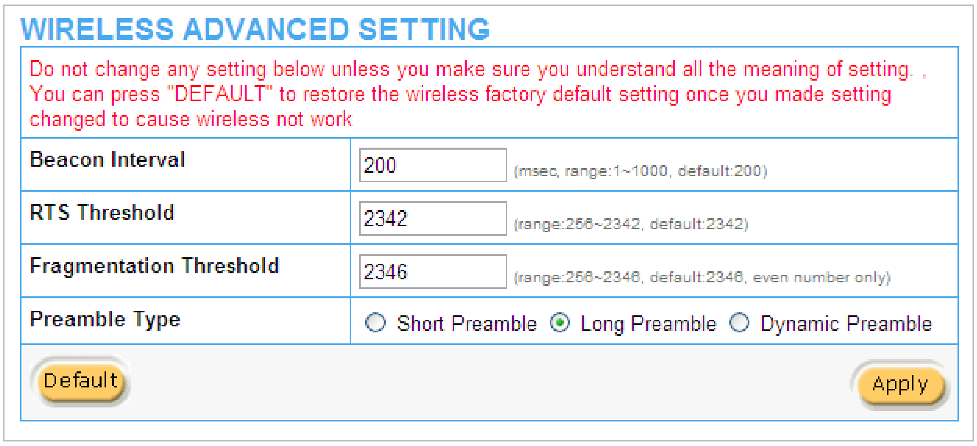
Channel Width: Auto 20/40 MHZ

Transmit Power: 10%

Figure 10 Wireless Basic Setting Screen

Item	Default	Description
General Settings		
ESSID	Wireless	The ESSID is the unique name that is shared among all points in a wireless network. It is case sensitive and must not exceed 32 characters.
Channel	6	Select the channel ID for wireless connection.
802.11 Mode	802.11g+802.11b	Select the 802.11 mode of following: : -802.11n+802.11g+802.11b -802.11n+802.11g -802.11g+802.11n -802.11n only -802.11g only -802.11b only
Channel Width	Auto 20/40MHz	Select of channel width of Auto 20/40 MHz or 20MHz
Transmit Power	10%	To Adjust the output power of the system to get the appropriate coverage of your wireless network. Select the 10% to 100% that you needed for your environment.

3-2-2 Wireless Advanced Setting



WIRELESS ADVANCED SETTING

Do not change any setting below unless you make sure you understand all the meaning of setting. , You can press "DEFAULT" to restore the wireless factory default setting once you made setting changed to cause wireless not work

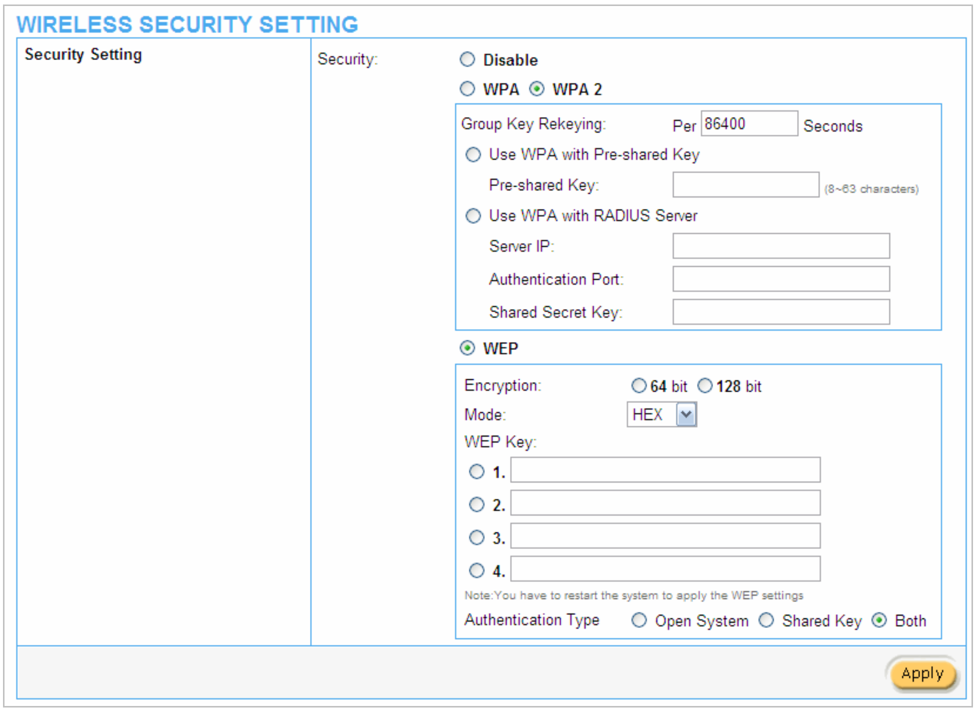
Beacon Interval	200 (msec, range:1~1000, default:200)
RTS Threshold	2342 (range:256~2342, default:2342)
Fragmentation Threshold	2346 (range:256~2346, default:2346, even number only)
Preamble Type	○ Short Preamble ● Long Preamble ○ Dynamic Preamble

Figure 11 Wireless Advanced Setting Screen

Item	Default	Description
Beacon Interval	200	This value valid range is 1 to 1000 indicates the frequency interval of the beacon.
RTS Threshold	2347	This value valid range is 256-2342. This setting determines the packet size at which the Wireless Subscriber Gateway issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the Wireless Subscriber Gateway, or in areas where the clients are far apart and can detect only the Wireless Subscriber Gateway and not each other.
Fragmentation Threshold	2432	This setting determines the size at which packets are fragmented. Enter a setting ranging from 256 to 2432 bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
Preamble Type	Long Preamble	The preamble type is a section of data at the head of a packet that contains information the Wireless Subscriber Gateway and client devices need when sending and receiving packets. The setting menu allows you to select a long, short or dynamic preamble type.

Apply Click Apply button to save the new settings.

3-2-3 Wireless Security Setting



WIRELESS SECURITY SETTING

Security Setting

Security: ○ Disable

○ WPA ● WPA 2

Group Key Rekeying: Per 86400 Seconds

○ Use WPA with Pre-shared Key

Pre-shared Key: (8~63 characters)

○ Use WPA with RADIUS Server

Server IP:

Authentication Port:

Shared Secret Key:

● WEP

Encryption: ○ 64 bit ○ 128 bit

Mode: HEX

WEP Key:

○ 1.

○ 2.

○ 3.

○ 4.

Note:You have to restart the system to apply the WEP settings

Authentication Type ○ Open System ○ Shared Key ● Both

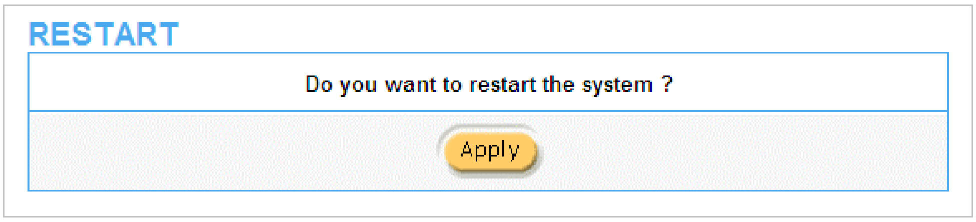
Figure 12 Wireless Security Setting Screen

Item	Default	Descriptio
Security	Disable	Select disable to allow wireless station to communicate with the device without any data encryption. Select enable to enable WPA or WEP data encryption.
WPA2 Encryption	Wi-Fi Protected Access Encryption	
Pre-shared Key	Empty	Enter a pre-shared key from 8 to 63 case sensitive ASCII characters.
Group Key Re-Keying	86400 Seconds	Enter a number in the field to set the force re-keying interval.
WPA Encryption	Wi-Fi Protected Access Encryption	

Pre-shared Key	Empty	Enter a pre-shared key from 8 to 63 case sensitive ASCII characters.
Group Key Re-Keying	86400 Seconds	Enter a number in the field to set the force re-keying interval.

Item	Default	Descriptior
WEP Key	1	This selects which of the Keys the In Wall Box Access Pointuses when it transmits. You can change the selected encryption key every now and then to increase the security of your network. Note: You have to configure all WEP keys (1~4), and select one of the four WEP key. Enter 5 characters (case sensitive) for ASCII 64-bit WEP Key. Enter 10 characters (case sensitive) for Hex 64-bit WEP Key. Enter 13 characters (case sensitive) for ASCII 128-bit WEP Key. Enter 26 characters (case sensitive) for Hex 128-bit WEP Key.

Apply *Click **Apply** button to save the new settings.*



RESTART

Do you want to restart the system ?

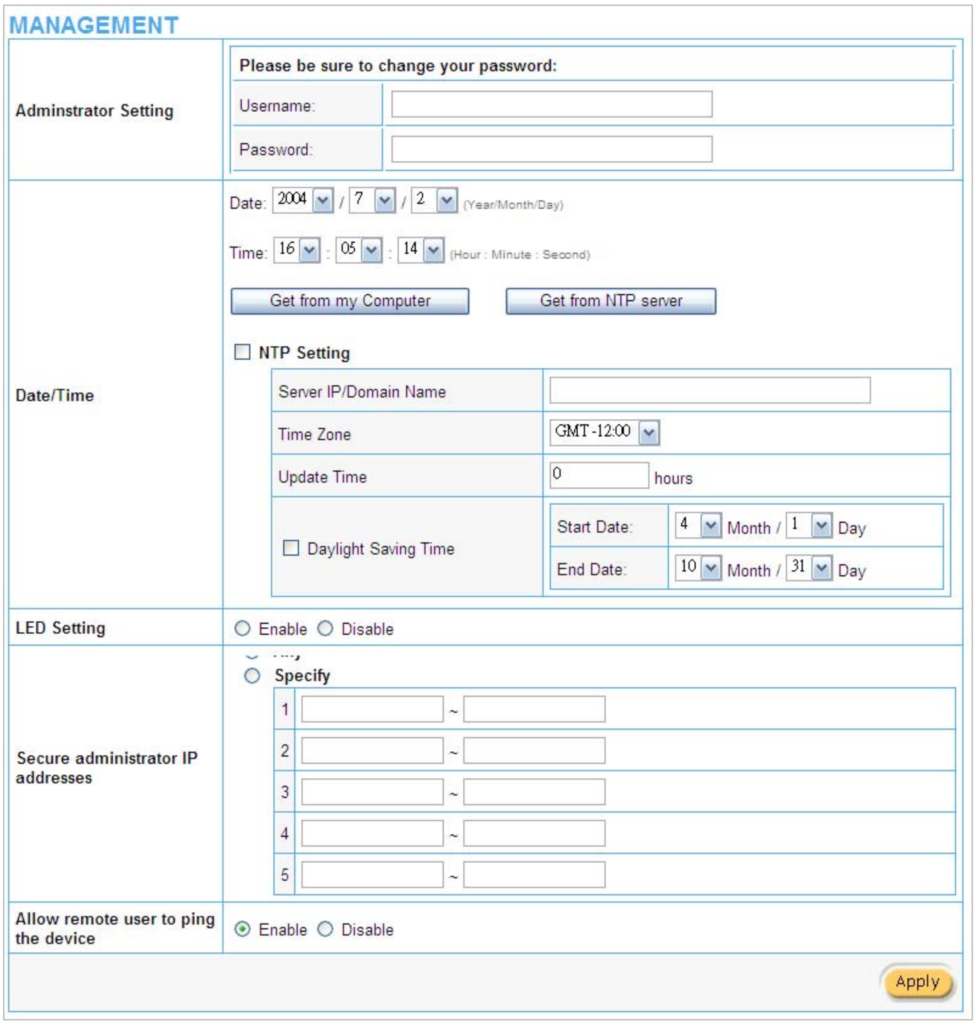
Figure 13 Restart Dialog Box

Click **Apply** button, the restart dialog box appears. Click on **Apply** to restart the system.

3-3 Advanced

3-3-1 *Management*

Define the In Wall Box Access PointManagement configuration



MANAGEMENT

Adminstrator Setting

Please be sure to change your password:

Username:

Password:

Date/Time

Date: 2004 / 7 / 2 (Year/Month/Day)

Time: 16 : 05 : 14 (Hour : Minute : Second)

□ **NTP Setting**

Server IP/Domain Name	
Time Zone	GMT -12:00
Update Time	0 hours
□ Daylight Saving Time	Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day

LED Setting ○ Enable ○ Disable

Secure administrator IP addresses

○ **Specify**

1		~	
2		~	
3		~	
4		~	
5		~	

Allow remote user to ping the device ● Enable ○ Disable

Figure 14 Management Setting Screen

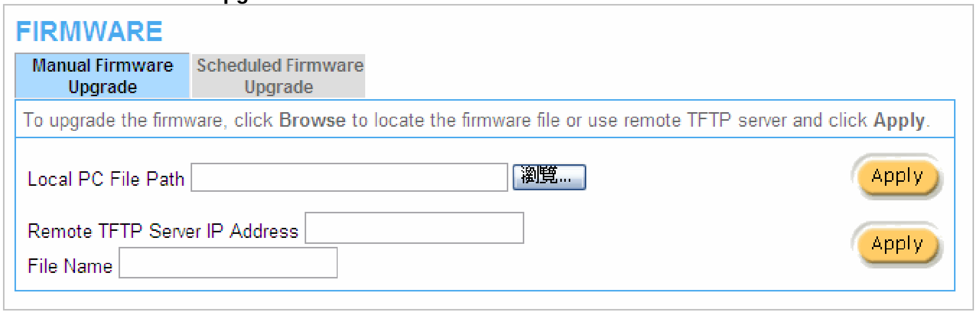
Item	Default	Description
Administrator Setting	Username	The username can consist of up to 20 alphanumeric characters and is sensitive.
	Password	The password can consist of up to 20 alphanumeric characters and is sensitive.
Date/Time		
Date (Year/Month/Day)	System Date	The system date of the In Wall Access Point. The valid setting of year is from 2002 to 2035.
Time (Hour:Minute:Second)	System Time	The system time of the In Wall Access Point.
Get from my Computer	-	Click “Get from my Computer” button to correct the system date and time.
Get from NTP server	-	Click “Get from NTP server” button to correct the system date and time.
NTP Setting	Disable	Enables or disables NTP (Network Time Protocol) Time Server. Network Time Protocol can be utilized to synchronize the time on devices across a network. A NTP Time Server is utilized to obtain the correct time from a time source and adjust the local time.
Server IP/Domain Name	Empty	Enter the IP address/domain name of NTP server. The maximum allowed characters length is 100.
Time Zone	GMT-12:00	Select the appropriate time zone for your location.
Update Time	0 hours	Enter the number of hours for update time.
Daylight Saving Time	Disable	Enables or disables Daylight Saving Time (DST).
	Month/Day	Set the Daylight Saving Time (DST) on the In Wall Access Point. Adjust the begin time and end time.
LED Setting	Disable	Enable or Disable Device LED lighting.
Secure administrator IP Addresses	Any	Options: Any and Specify. Administrator can specify 5 IP addresses or a range to allow remote control access from network.
Allow remote user to ping the device	Enable	This function allows remote user to ping the In Wall Box Access Pointthrough Internet. Ping is normally used to test the physical connection between two

		devices, to ensure that everything is working correctly.

3-3-2 Firmware

The Firmware Upgrade menu loads updated firmware to be permanent in flash ROM. The download file should be a binary file from factory; otherwise the agent will not accept it. After downloading the new firmware, the agent will automatically restart it.

● **Manual Firmware Upgrade**



To upgrade the firmware, click **Browse** to locate the firmware file or use remote TFTP server and click **Apply**.

Local PC File Path

Remote TFTP Server IP Address

File Name

Figure 15 Manual Firmware Upgrade Setting Screen

Item	Default	Description
This allow administrator to upgrade the firmware via HTTP.		
Local PC File Path	Empty	Enter the file name and location in the Local PC File Path field.
This allows administrator use TFTP server to upgrade firmware.		
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.

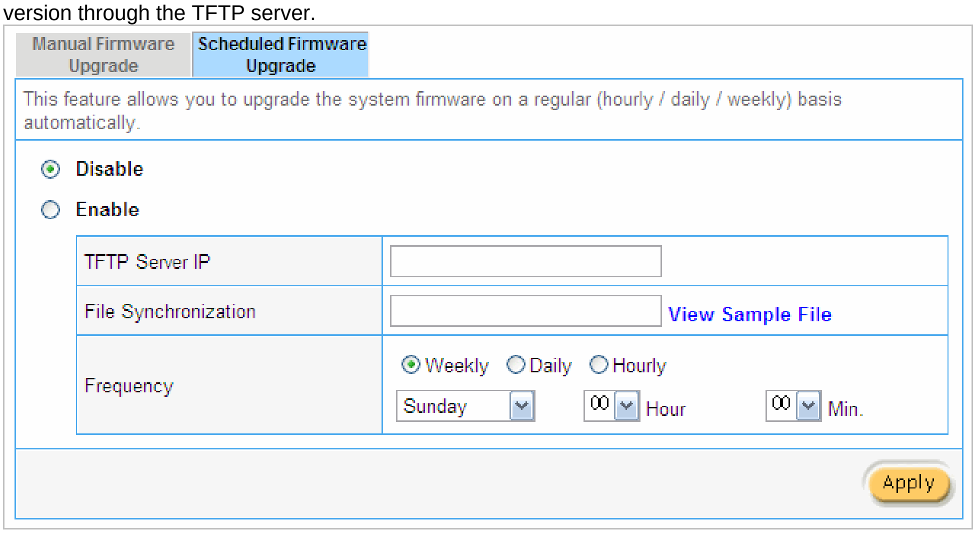
Note:

1. Before downloading the new firmware, users must save the configuration file for restore configuration parameters of the device.

2. Do not turn the power off during the upgrade process. This will damage the unit.

● Scheduled Firmware Upgrade

Scheduled Firmware Upgrade is a program that enables an automatic upgrade to the latest firmware version through the TFTP server.



This feature allows you to upgrade the system firmware on a regular (hourly / daily / weekly) basis automatically.

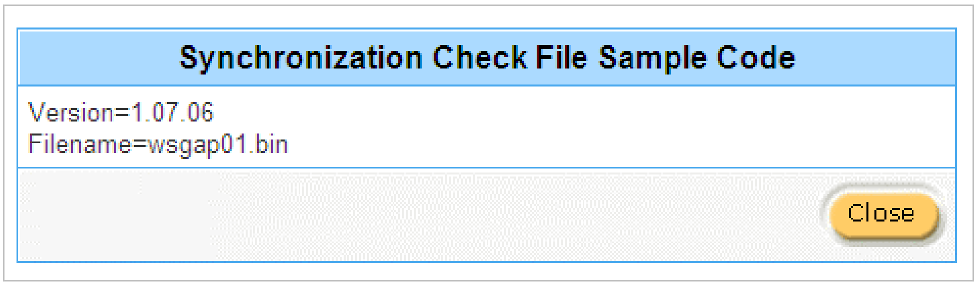
● Disable

○ Enable

TFTP Server IP	
File Synchronization	View Sample File
Frequency	● Weekly ○ Daily ○ Hourly Sunday 00 Hour 00 Min.

Figure 16 Scheduled Firmware Upgrade Setting Screen

Item	Default	Description
Disable/Enable	Disables or enables the scheduled firmware upgrade function.	
TFTP Server IP	Empty	Enter the IP address of TFTP Server.
File Synchronization	Empty	Enter the file name and location in the File Synchronization field.
View Sample File	Click the button to display synchronization file example.	
Frequency	Weekly	Set the firmware upgrade time. The default value is "Weekly".



Synchronization Check File Sample Code

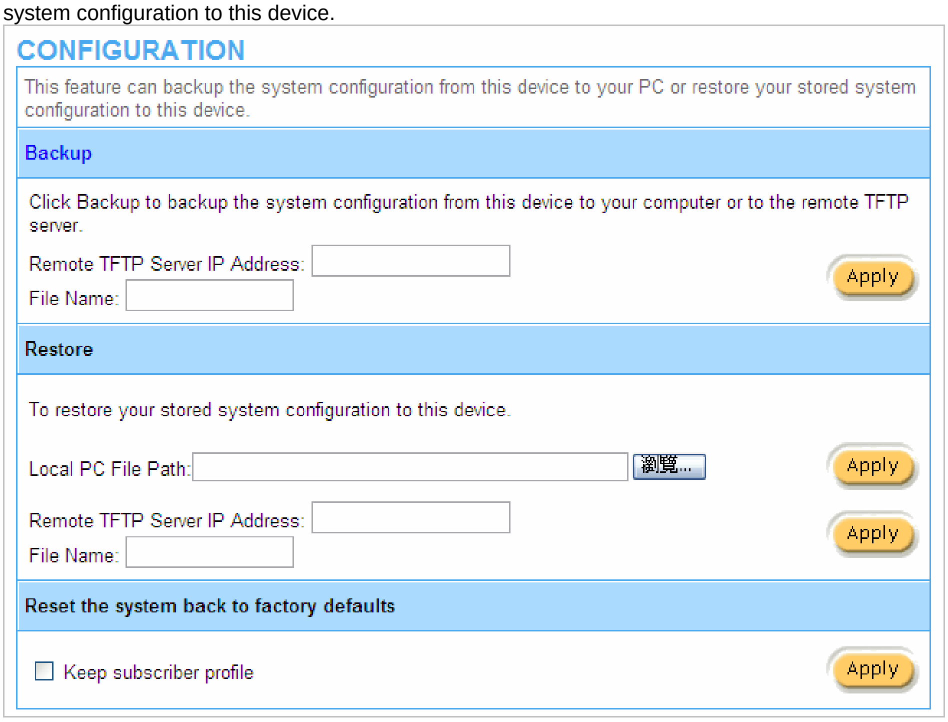
Version=1.07.06
Filename=wsgap01.bin

Figure 17 Synchronization File Sample Code

Note: *Do not turn the power off during the upgrade process. This will damage the unit.*

3-3-3 Configuration

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.



CONFIGURATION

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.

Backup

Click Backup to backup the system configuration from this device to your computer or to the remote TFTP server.

Remote TFTP Server IP Address:

File Name:

Restore

To restore your stored system configuration to this device.

Local PC File Path:

Remote TFTP Server IP Address:

File Name:

Reset the system back to factory defaults

□ Keep subscriber profile

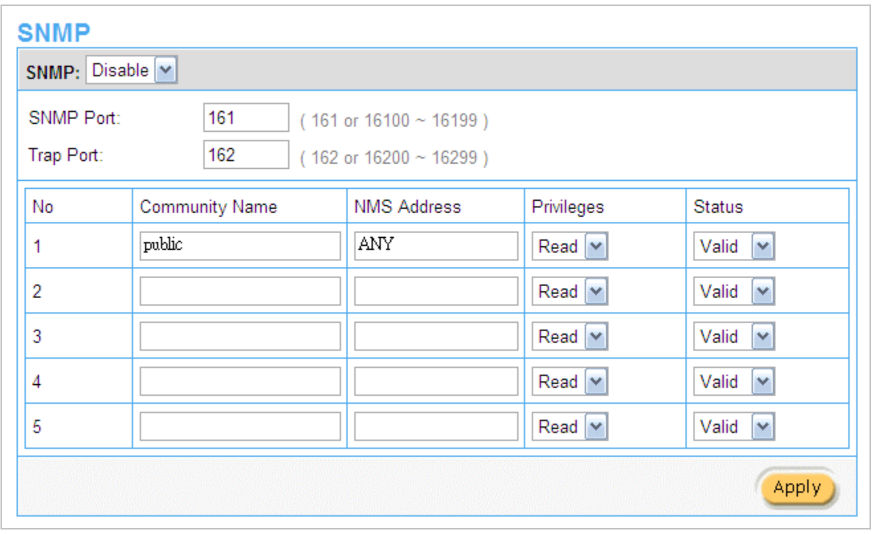
Figure 18 Configuration Setting Screen

Item	Default	Description
Backup	Click it to save the system configuration to your computer. (export.cfg)	
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Restore	Click it to restore your system configuration.	
Local PC File Path	Empty	Enter the file pathname of the system configuration file in the Local PC File Path field.
Remote TFTP Server IP Address	Empty	Enter the IP address of TFTP Server.
File Name	Empty	Enter the file name in the File Name field.
Reset the system back to factory defaults	Erase all setting and back to factory setting.	
Keep subscriber profile	Disable	Click the keep subscriber profile to change all the parameters

		into factory setting but still reserve the subscriber profiles.

3-3-4 SNMP

The SNMP Agent Configuration screen enables you to access to your device via Simple Network Management Protocol. If you are not familiar with SNMP, please consult your Network Administrator or consult SNMP reference material. You must first enable SNMP on the SNMP Agent Configuration screen.



SNMP

SNMP: Disable

SNMP Port: 161 (161 or 16100 ~ 16199)

Trap Port: 162 (162 or 16200 ~ 16299)

No	Community Name	NMS Address	Privileges	Status
1	public	ANY	Read	Valid
2			Read	Valid
3			Read	Valid
4			Read	Valid
5			Read	Valid

Figure 19 SNMP Setting Screen

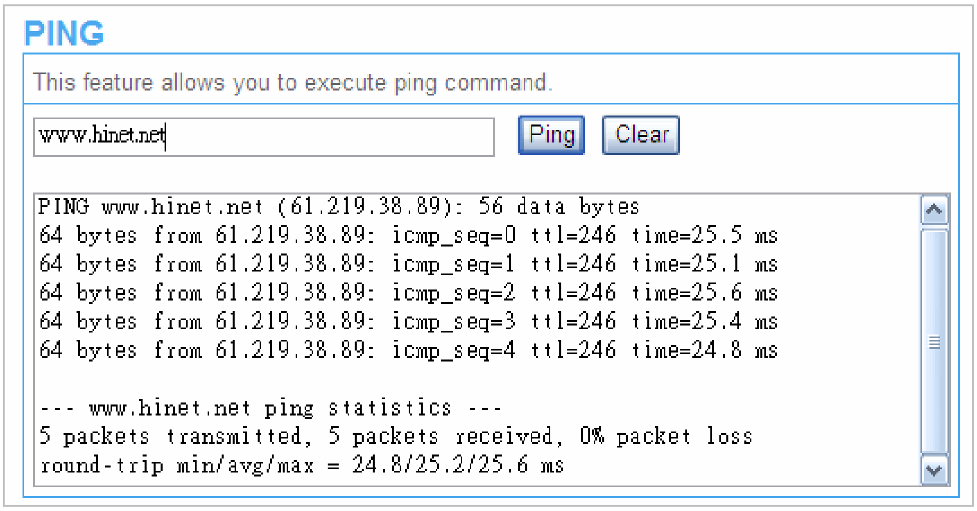
Item	Default	Description
SNMP	Disable	Disables or enables the SNMP management.
SNMP Port	161	If the SNMP enables, also allowed to specific the SNMP port number via NAT. The allowed SNMP port numbers are 161 (default), 16100-16199 and Trap port numbers are 162 (default), 16200-16299. This Port setting is useful for remote control via NAT network.
Trap Port	162	
Configuration		
Community Name	public/private	Every unit with SNMP enable must be configured to recognize one or more community names up to 20 characters. The default setting for the community of entry 1 is “public” and for the entry 2 is “private” and others are empty.
NMS Address	ANY	The address of the NMS. The default settings for the NMS Networking are “ANY”.
Privileges	Read/Write	Choose “Read”, “Write”, “Trap Recipients” and “All” for different privileges. The default setting of the entry 2 is “write” and others are “read”.
Status	Valid/Invalid	Chosen “Valid” or “Invalid”. The default setting of entry 1, 2 are valid

		and others are invalid.

3-3-5 System

3-3-6 Ping Command

The Ping function can check the Wireless Subscriber Gateway networking connective or not.



```
PING www.hinet.net (61.219.38.89): 56 data bytes
64 bytes from 61.219.38.89: icmp_seq=0 ttl=246 time=25.5 ms
64 bytes from 61.219.38.89: icmp_seq=1 ttl=246 time=25.1 ms
64 bytes from 61.219.38.89: icmp_seq=2 ttl=246 time=25.6 ms
64 bytes from 61.219.38.89: icmp_seq=3 ttl=246 time=25.4 ms
64 bytes from 61.219.38.89: icmp_seq=4 ttl=246 time=24.8 ms

--- www.hinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 24.8/25.2/25.6 ms
```

Figure 20 Ping Command Screen

Item	Description
IP or URL	Enter the IP address or the URL link.

3-4 Advanced

3-4-1 Restart

If your In Wall Box Access Pointis not operating correctly, you can choose this option to display the restart Wireless Subscriber Gateway screen. Clicking the apply button restart the In Wall Access Point, with all of your settings remaining intact.

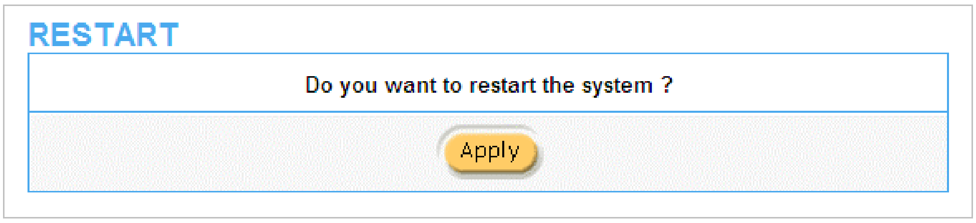
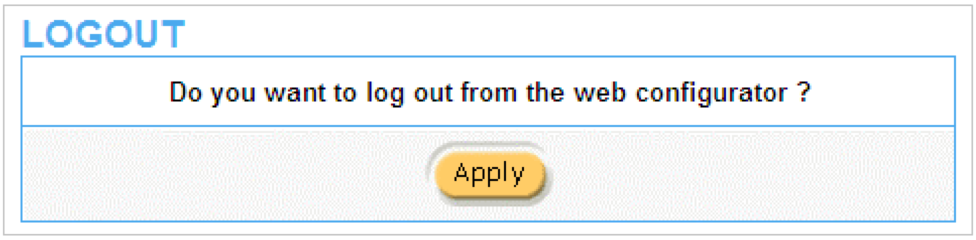


Figure 21 Restart Screen

3-4-2 Logout

If you would like to leave the configuration page, please click apply to exit.



LOGOUT

Do you want to log out from the web configurator ?

Figure 22 Restart Screen

Appendix A Signal Connection Arrangem :nts

RJ-45 Ethernet Port

The In Wall Box Access PointRJ-45 Ethernet port can connect to any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

10Mbps: Use EIA/TIA-568-100-Category 3, 4 or 5 cable.
100Mbps: Use EIA/TIA-568-100-Category 5 cable.

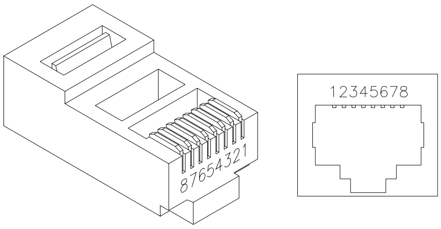


Figure 23 RJ-45 Connector and Cable Pins

Note: *To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 meters.*

Appendix B Regulations/EMI Complian e

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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

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 20cm between the radiator & your body. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

NCC警語:

(1)「經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能」警語以及(2)「低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾」警語。

LIMITED WARRANTY

In Wall Access Point

What the warranty covers:

We warrant its products to be free from defects in material and workmanship during the warranty period. If a product proves to be defective in material or workmanship during the warranty period, we will at its sole option repair or replace the product with a like product with a like product. Replacement product or parts may include remanufactured or refurbished parts or components.

How long the warranty is effective:

The Easy Hotspot Kit is warranted for one year for all parts and one year for all labor from the date of the first consumer purchase.

Who the warranty protects:

This warranty is valid only for the first consumer purchaser.

What the warranty does not cover:

1. Any product, on which the serial number has been defaced, modified or removed.
2. Damage, deterioration or malfunction resulting from:
   a. Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
   b. Repair or attempted repair by anyone not authorized by us.
   c. Any damage of the product due to shipment.
   d. Removal or installation of the product.
   e. Causes external to the product, such as electric power fluctuations or failure.
   f. Use of supplies or parts not meeting our specifications.
   g. Normal wears and tear.
   h. Any other cause that does not relate to a product defect.
3. Removal, installation, and set-up service charges.

How to get service:

1. For information about receiving service under warranty, contact our **Customer Support**.
2. To obtain warranted service, you will be required to provide (a) the original dated sales slip, (b) your name, (c) your address (d) a description of the problem and (e) the serial number of the product.
3. Take or ship the product prepaid in the original container to your dealer, and our service center.
4. For additional information, contact your dealer or our **Customer Service Center**.

Limitation of implied warranties:

THERE ARE NOWARRANTIED, EXPRESSED OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION CONTAINED HEREIN INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Exclusion of damages:

Our LIABILITY IS LIMITED TO THE COST OF REPAIR OR REPLACEMENT OF THE PRODUCT. We SHALL NOT BE LIABLE FOR:

1. DAMAGE TO OTHER PROPERTY CAUSED BY ANY DEFECTS IN THE PRODUCT, DAMAGES BASED UPON INCONVENCE, LOSS OF USE OF THE PRODUCT, LOSS OF TIME, LOSS OF PROFITS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, INTERFERENCE WITH BUSINESS RELATIONSHIPS, OR OTHER COMMERCIAL LOSS, EVEN IF ADVISED OF THE POSSIBLITY OF SUCH DAMAGES.
2. ANY OTHER DAMAGES, WHETHER INCIDENTAL, CONSEQUENTIAL OR OTHERWISE.

3. ANY CLAIM AGAINST THE CUSOMER BY ANY OTHER PARTY.