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 Windows 98, Windows 2000, Windows XP, Windows 7 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 EW28650 In Wall Access Point revolutionizes the way wireless and wired IP-based services are delivered to hospitality, enterprise, and residential properties. The EW28650 integrates wired and wireless connectivity into a small unit that can be quickly and discretely installed in a single gang wall box. The EW28650 provides an Ethernet port, telephone jack, and a 2.4GHz 802.11b/g/n wireless access point. The EW28650 requires a single power over ethernet cable drop to unlock its functionality and, through the reduction in cabling, switch ports, and power-sourcing equipment, the EW28650 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:

◎ ***EW28650***

- One In Wall Access Point
- One Telephone Cable (3.9 in / 10 cm)
- One UTP Ethernet/Fast Ethernet cable (Cat.5 Twisted-pair) (3.9 in / 10 cm)
- One Wall Faceplate (Top and Bottom)
- One Mounting Bracket
- One Quick Installation Guide
- One CD

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 wet locations.

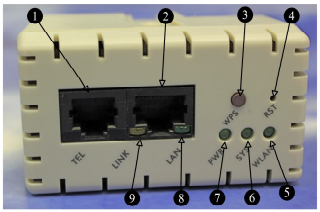
1-4 Aspects

Figure 1 In Wall Access Point Aspect

1-4-1 Front Panel

The Front panel of the In Wall Access Point shown below.

Figure 2 In Wall Access Point Front Panel



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

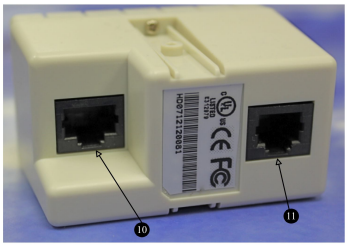
Figure 3 In-Wall Point Front Panel

LEDs Indication

LED	State	Description
PWR	Off	The In Wall Access Point not receiving electrical power.
	Green	The In Wall Access Point receiving electrical power.
SYS	Off	The In Wall Access Point status is defective.
	Green	The In Wall Access Point status 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 Access Point has 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 Point



10. RJ-45 Ethernet Connector(802.3af PoE)
11. RJ-11 Telephone Connector

Figure 4 In Wall Access Point Rear 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 Port (10BaseT/100BaseTX Auto cross-over)

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

Two Tel Ports (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 LED

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: 1.3” (W) x 2.8” (L) x 2.2” (H)/ Inches

Weight: About 3.0 Oz/85 g (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

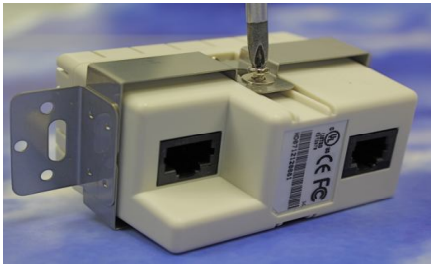
Management

- 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 following are instructions for the hardware assembly and installation of the In Wall Wireless Access Point. Refer to the illustrations and follow the simple steps below to quickly install your EW28650.

Step 1： Slide the Bracket to align with the screw holes on the In Wall Access Point, and fasten the Bracket tightly with the screws.



Step 2： Slide the EW28650 into the Bottom Faceplate and fasten tightly into the Bottom Faceplate until it is flush with the wall.

Step 3： Line-up and push the Top faceplate onto Bottom faceplate until it 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 Access Point requires one of the following types of software:

- Windows 98 Second Edition/NT/2000/XP/Vista/Windows 7
- 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)
- Web Browser Software (Microsoft Internet Explorer 6.0 or Mozilla Firefox 3.5)
- 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 that each cable does not exceed 328 feet (Approximately 100 meters).*

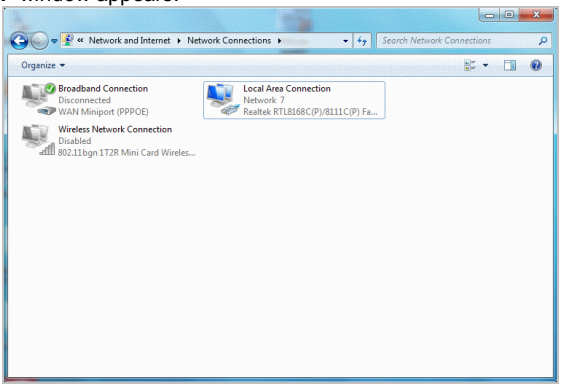
2-2 Getting Started

The EW28650 supports web-based configuration. Upon the completion of the hardware installation, it can be configured using a web browser such as Internet Explorer, Firefox, or Safari.

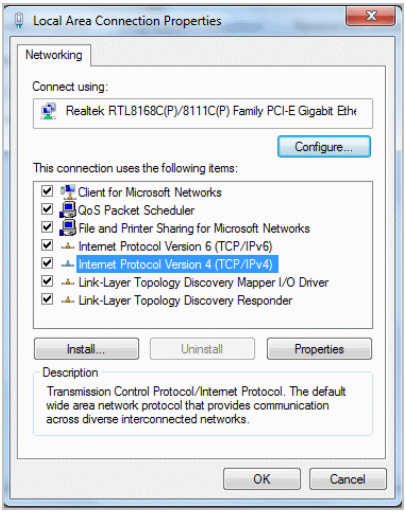
- **Default IP Address:** 192.168.10.1
- **Default Subnet Mask:** 255.255.255.0
- **Default Username and Password:** root/root

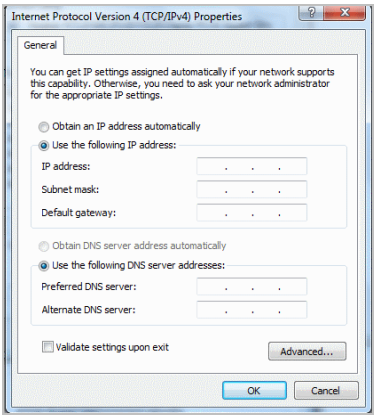
Note *: Set the IP segment of the administrator's computer to be in the same range as EW28650 for accessing the system.* ***Do not duplicate*** *the IP address used here with the IP address of EW28650 or any other device within the network.*

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



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

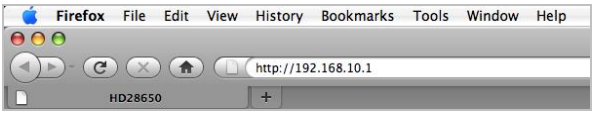




Example:

IP Address:192.168.10.5
Subnet Mask:255.255.255.0

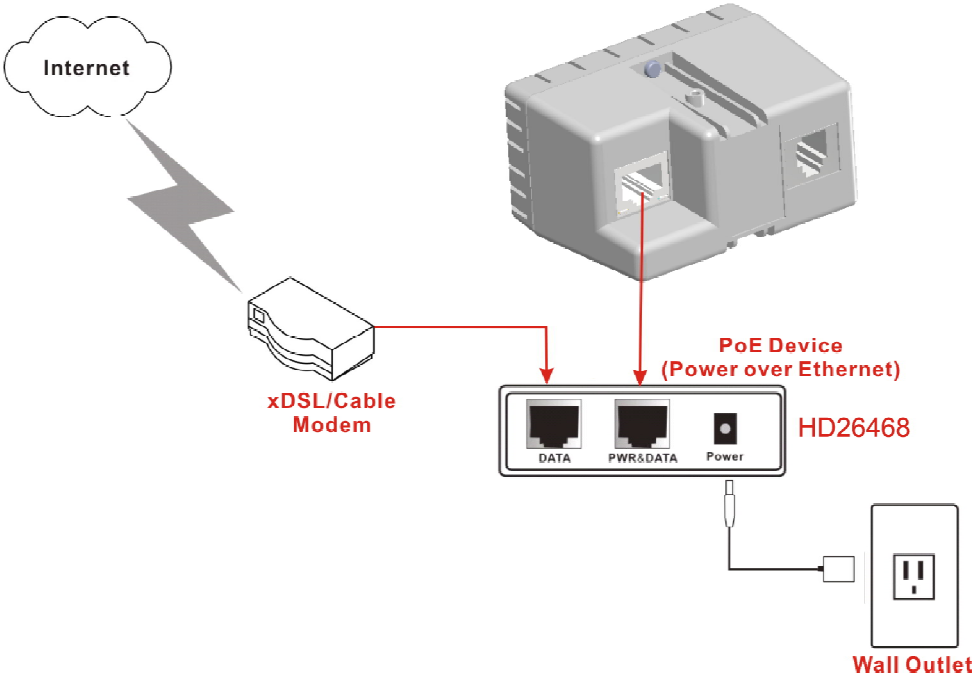
Step 3 : Launch your web browser, and then enter the factory default IP address **192.168.10.1** in your browser's location box. Press **Enter**.



Step 4 : The EW28650 login screen will appear. In the Username and Password field, type the factory default user name **root** and password **root** and click **Submit**. The EW28650 setup screen will appear.

Note: *It is important to remember your password. If for any reason you lose or forget your password, press the reset button located inside of a recessed hole on the front of the device. Using a paperclip or similar instrument, depress and hold the reset button for 15 seconds. Performing a Reset will reboot the device and will re-initialize the settings back to factory default. All configurations, including username, password and IP address(es), will be reset, and requires re-entering that information.*

PoE (Power over Ethernet) Application



Note: *To use the EW28650's PoE feature, follow the instructions for your specific PoE device.*

3 Configuring the In Wall Access Point

Step 1: Start your browser, and then enter the factory default IP address **192.168.10.1** in your browser's location box. Press **Enter**.

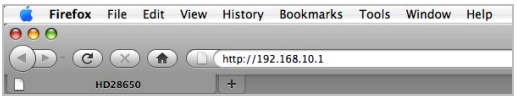


Figure 5 Web Browser Location Field (Factory Default)

Step 2: The In Wall Access Point configuration tools menu will appear. In the Username and Password field, type the factory default user name **root** and password **root** and click **Submit**.

Figure 6 Configuration Tools Menu

Note:

- ☞ *This Web Configuration Utility is best viewed with IE 6.0 or Firefox 3.5 or higher versions.*
- ☞ *Username and Password can consist of up to 20 alphanumeric characters (case sensitive).*
- ☞ *If for some reason your password is lost or you cannot gain access to the In Wall Access Point Configuration Program, please press the reset button to load the device to manufacturer defaults.*
- ☞ *If the In Wall Access Point doesn't send any packets within 5 minutes (default), the In Wall Access Point will logout automatically.*
- ☞ *Proxy needs to set disable first when administrator accesses admin User Interface*

The following settings enable you to configure advanced settings related to accessing the Internet； Display in Wall Access Point basic status; process Firmware upgrade; change password; and backup or restore configuration. Including,

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

Figure 7 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.

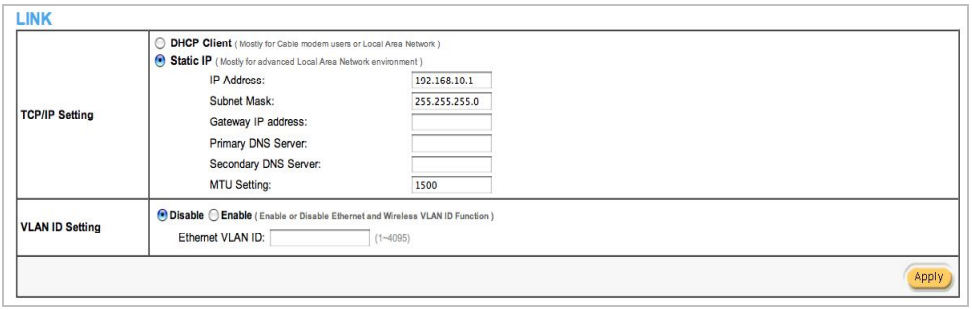


Figure 8 the TCP/IP Setting

DHCP Client

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

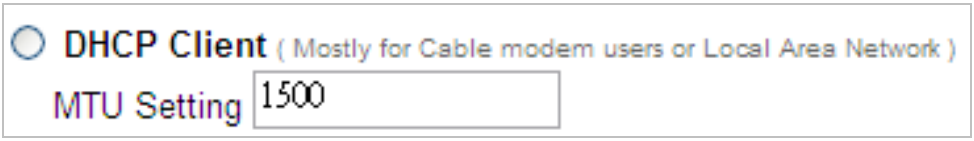


Figure 9 DHCP Client Setting Screen

Item	Default	Description
MTU Setting	1500	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.

Static IP

Figure 10 Static IP Setting Screen

Item	Default	Description
IP Address	192.168.10.1	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	Empty	Enter the Gateway IP address for the xDSL/Cable connection
Primary DNS Server	Empty	A primary DNS server IP address for the xDSL/Cable connection
Secondary DNS Server	Empty	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	1500	MTU (Maximum Transfer Unit) specifies maximum transmission unit size.

3-2 Wireless

3-2-1 Wireless Basic Settings

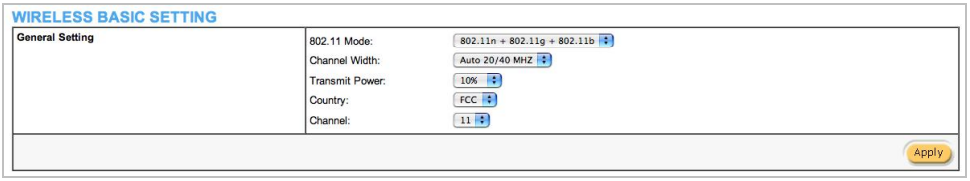


Figure 11 Wireless Basic Setting Screen

Item	Default	Description
General Settings		
ESSID	In Room WiFi	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+802.11b -802.11n only -802.11g only -802.11b only
Channel Width	20 MHz	Select of channel width of Auto 20/40 MHz or 20MHz
Transmit Power	25%	To Adjust the output power of the system to get the appropriate coverage of your wireless network. Select the 10% to 100% that you need for your environment.

3-2-2 Wireless Advanced Setting

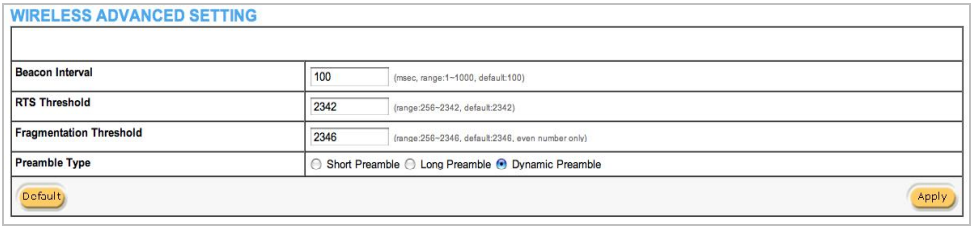


Figure 12 Wireless Advanced Setting Screen

Item	Default	Description
Beacon Interval	100	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 In Wall Access Point 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 In Wall Access Point, or in areas where the clients are far apart and can detect only the In Wall Access Point, 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	Dynamic preamble	The preamble type is a section of data at the head of a packet that contains information and client devices need when sending and receiving packets. The setting menu allows you to select a long, short or dynamic preamble type.

Click Apply button to save the new settings.

3-2-3 MULTI-ESSID Setting

MULTI-ESSID Setting

Multiple SSIDs (Service Set Identifier) logically divide the access point into several virtual access points, and allow users to access different networks through the single Access Point. The ability to create and configure Multiple SSIDs can be performed within the "**MULTI-ESSID"** tab within the **Wireless** menu setting. You can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure. They can be named differently, with separate security options and settings. For example, Multiple SSIDs are commonly configured for creating public and private networks within the same access point.

MULTI-ESSID SETTINGS

Item	ESSID	Status	VLAN ID	Security	Edit
1	802.11N INWALL	Active	Disable	**WPA2**	Edit
2	In Room WiFi2	Inactive	Disable	**Disable**	Edit

VLAN Setting

Virtual Local Area Network (VLAN). This enables the separation of wireless applications based on security and performance requirements. If your network uses VLANs, you can assign an SSID to a VLAN ID (range from 1 - 4095), and the access point will group client devices (and network traffic) using that SSID into that specific VLAN ID. For example, you could enable encryption and authentication on one SSID to protect private applications, and no security on another SSID to maximize open connectivity for public usage.

Wireless Security Settings are configured within the edited fields of the **MULTI-ESSID** tab.

See Figure 13

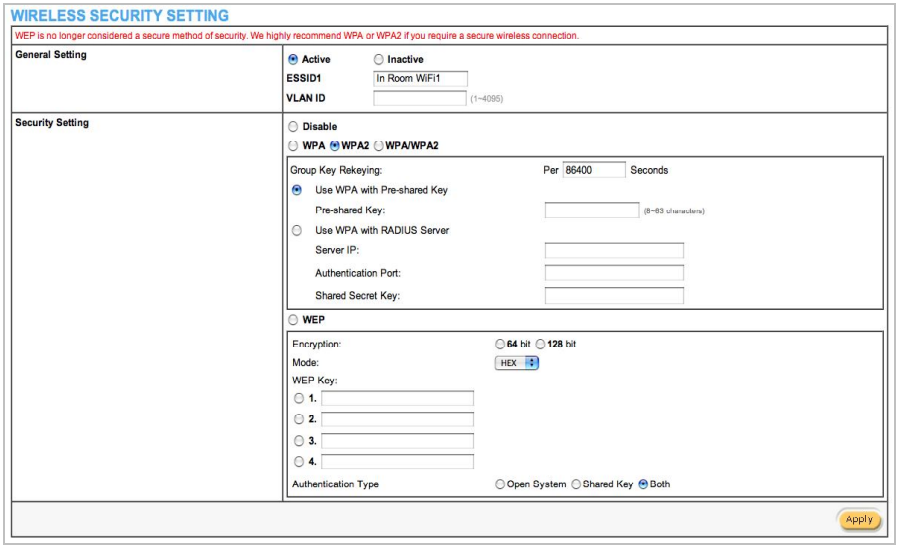


Figure 13 Wireless Security Setting Screen

Item	Default	Description
Security	Disable	Select disable to allow wireless stations 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	Description
WEP Key	1	This selects which of the Keys the In Wall Access Point uses when it transmits. You can change the selected encryption key periodically 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.

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

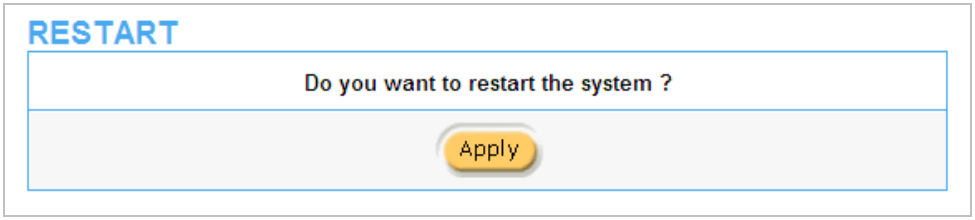


Figure 14 Restart Dialog Box

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 Access Point Management configuration

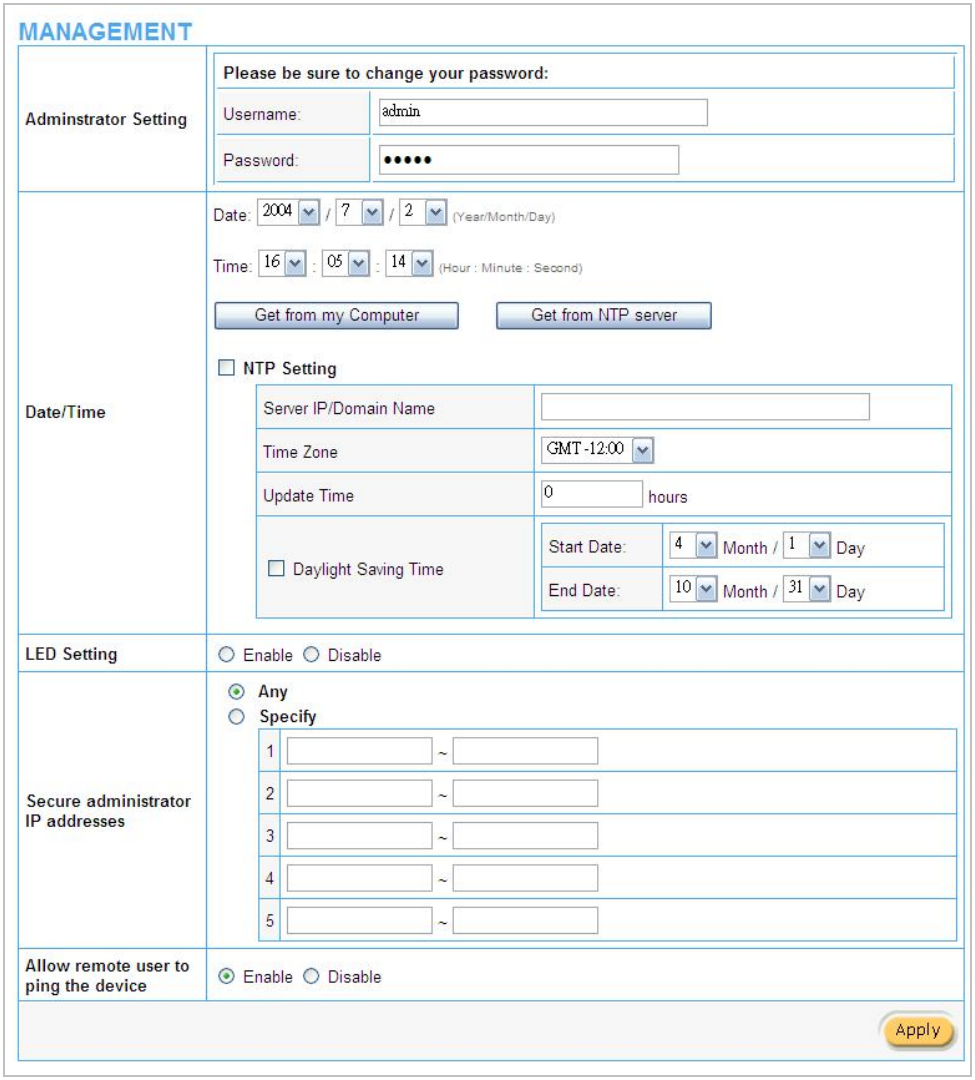


Figure 15 Management Setting Screen

Item		Default	Description
Administrator Setting	Username	root	The username can consist of up to 20 alphanumeric characters and is sensitive.
	Password	root	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 2010 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 Access Point through the 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**

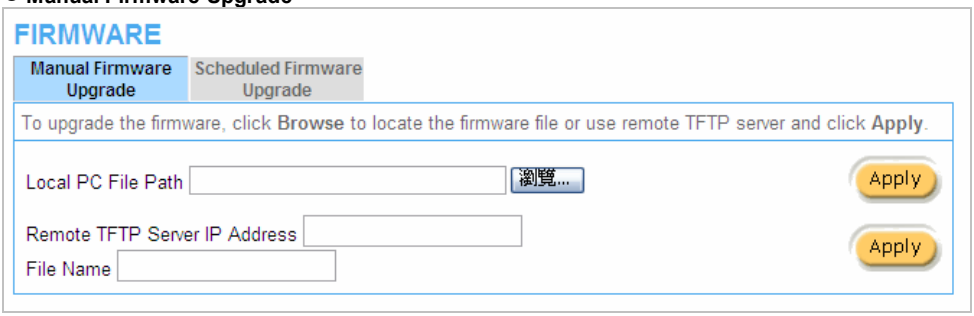


Figure 16 Manual Firmware Upgrade Setting Screen

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 to restore the 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.

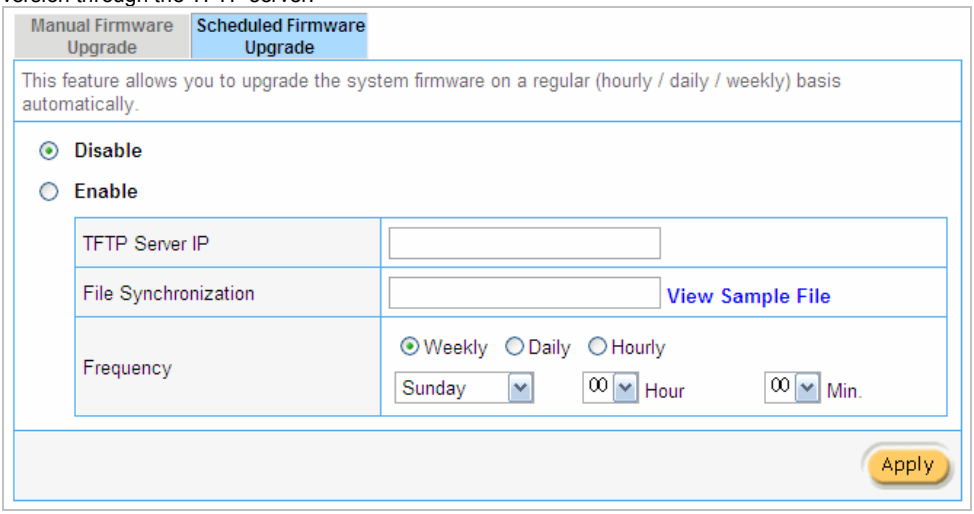


Figure 17 Scheduled Firmware Upgrade Setting Screen

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".

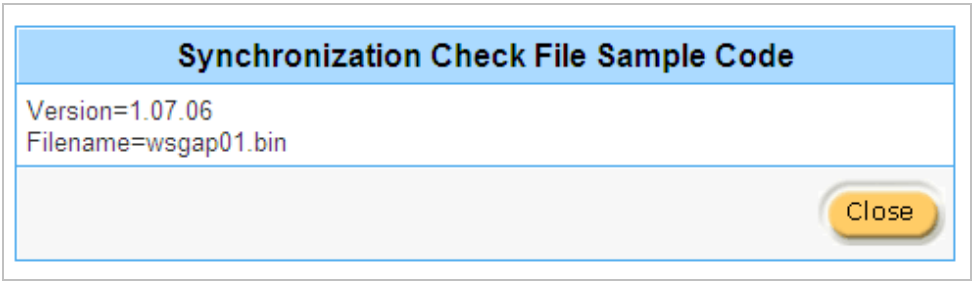


Figure 18 Synchronization File Sample Code

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.

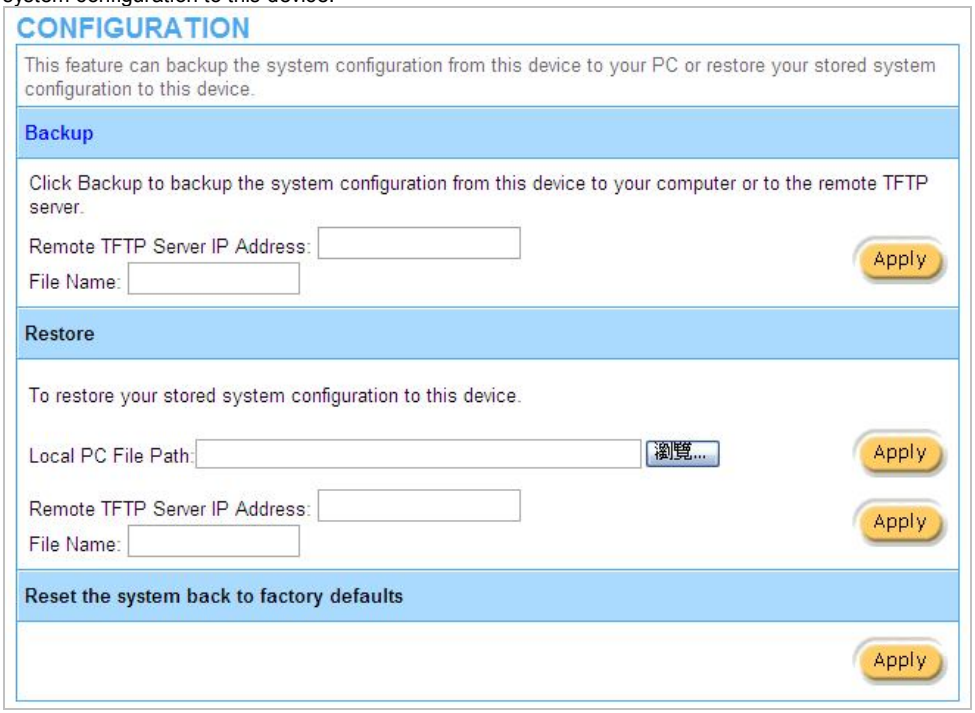


Figure 19 Configuration Setting Screen

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.	

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.

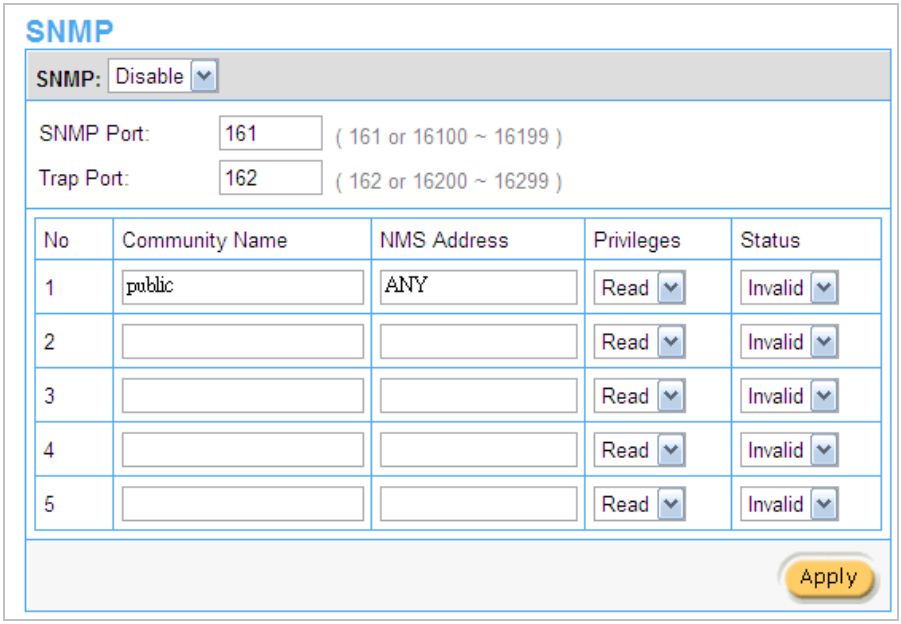


Figure 20 SNMP Setting Screen

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 is “public”
NMS Address	ANY	The address of the NMS. The default settings for the NMS Networking are “ANY”.
Privileges	Read	Choose “Read”, “Write”, “Trap Recipients” and “All” for different privileges. The defaults are all “read”.
Status	Valid/Invalid	Chosen “Valid” or “Invalid”. The default setting of entry is all invalid.

3-3-5 System

3-3-6 Ping Command

The Ping function can determine if the In Wall Access Point's network is connected or not.

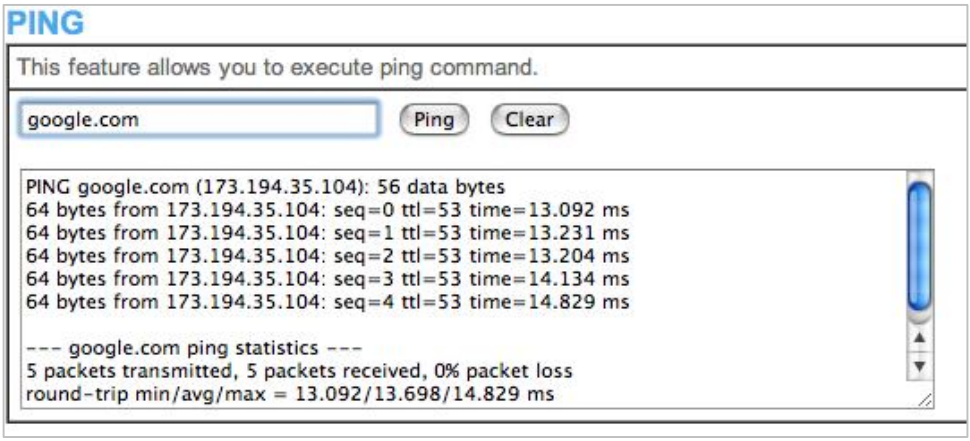


Figure 21 Ping Command Screen

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

3-4 Advanced

3-4-1 Restart

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

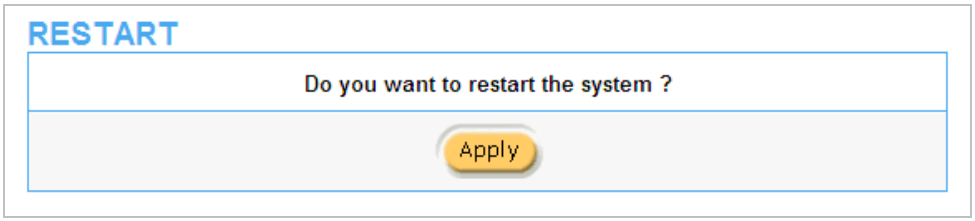


Figure 22 Restart Screen

3-4-2 Logout

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

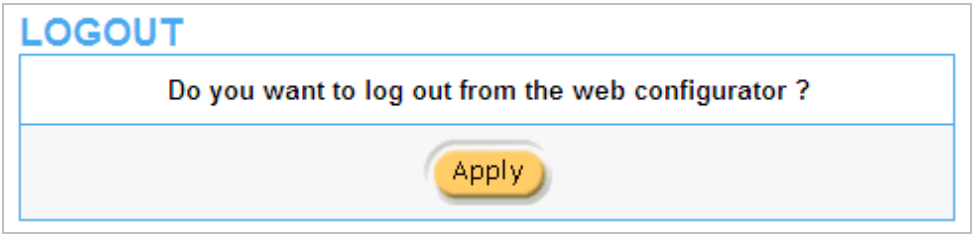


Figure 23 Logout Screen

Appendix A Signal Connection Arrangements

RJ-45 Ethernet Port

The In Wall Access Point RJ-45 Ethernet port can connect to any networking devices that use a standard LAN interface, such as a Hub/Switch or Router. Use unshielded twisted-pair (UTP) or shielded 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 cables.
100Mbps: Use EIA/TIA-568-100-Category 5 cable.

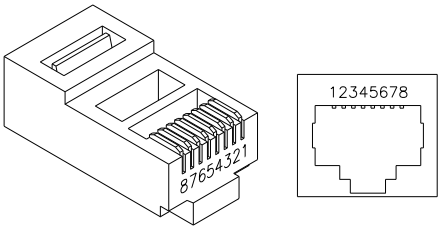


Figure 24 RJ-45 Connector and Cable Pins

Note: *To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 meters (approximately 328 feet).*

Appendix B Regulations/EMI Compliance

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 operating 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.

LIMITED WARRANTY

EW28650 In Wall Wireless Access Point

What the warranty covers:

We warrant this product 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 EW28650 is warranted for one (1) year for all parts and labor from the date of receipt.

Who the warranty protects:

This warranty is valid only for the original 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 wear 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 **Technical 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, or point of purchase.
4. For additional information, contact your dealer or:

HD Communications Technical Support Team @ (888) 588-3800 / (631) 588-3877
techs@hdcom.com

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 CUSTOMER BY ANY OTHER PARTY.