11Mb High Gain Smart Ethernet Client

T-311

User's Guide

Version 1.0 Nov. 2004

www.gemtek-systems.com

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.

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.

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.

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

Gemtek systems declares that T-311 (FCC ID: MXF-A930923B) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

1. Before You Start

1.1 Notice

Gemtek Systems, Inc. reserves the right to change specifications without prior notice. While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Gemtek Systems, Inc. shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Gemtek Systems, Inc.

1.2 Trademarks

The product described in this book is a licensed product of Gemtek Systems, Inc.

Microsoft, Windows 95, Windows 98, Windows Millennium Edition, Windows NT, Windows 2000, Windows XP, and MS-DOS are registered trademarks of the Microsoft Corporation.

All other brand and product names are trademarks or registered trademarks of their respective holders.

1.3 National Radio Regulations

Please note:

The usage of wireless network components is subject to national and or regional regulations and laws.

Administrator must ensure that they select the correct radio settings according to their regulatory domain. Refer to the regulatory domains chapter in the appendix to get more information on regulatory domains. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values!

Channel and output power settings may be modified by experienced service person only!

The default channel numbers for this product, T-311 High Gain Smart Ethernet Client are only available from 1~11.

2. Table of Contents

3. About this Guide

3.1 Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the Gemtek Systems High Gain Smart Ethernet Client T-311.

3.2 Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.

- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium Edition, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

3.3 Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

⚡ *Very important information. Failure to observe this may result in damage!*

❗ *Important information that should be observed.*

ℹ *Additional information that may be helpful but which is not required.*

Bold Menu commands, buttons and input fields are displayed in bold

Code File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type

<value> Placeholder for certain values, e.g. user inputs

[value] Comments or hints

3.4 Help us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to: support@gemtek-systems.com

3.5 Gemtek Systems Technical Support

If you encounter problems when installing or using this product, please consult the Gemtek Systems website at

http://www.gemtek-systems.com

for

- The latest software, user documentation and product updates.
- Frequently Asked Questions (FAQ).
- Direct contact to the Gemtek Systems support centers.

4. Introduction

Thank you for choosing the Gemtek Systems T-311 11Mb High Gain Smart Ethernet Client.

This manual will assist you with the installation procedure.

4.1 Overview

T-311 allows for one Ethernet-enable device (e.g., Windows/MAC/Linux/UNIX Desktop PC or laptop) to be instantly connected to an existing 802.11b wireless network. Taking full advantage of the integrated Web server capability, T-311 is performed through a simple Web browser user interface for easy configuration.

Besides laptop or desktop environment, T-311 is also the ideal solution to make other network device such as network printer or camera becomes a wireless station.

4.2 Scope of Delivery

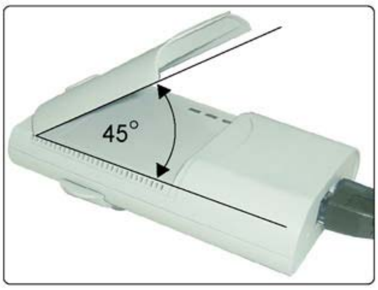
Please ensure that the package is complete before beginning with the installation. The package should include the following components:

- T-311 11Mbps High Gain Smart Ethernet Client
- Dual purposes cable USB/Ethernet with movable SR.
- Universal Sucking Disk (USD)
- CD (includes user's manual and quick guide)
- Warranty Card

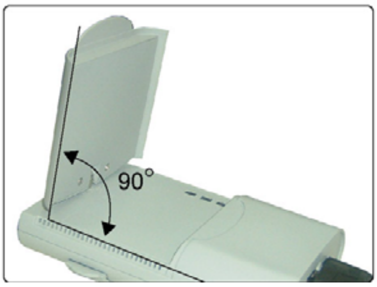
4.3 The Usage of Antenna Housing

When lift the antenna lid, it will be locked/lodged in 45 degrees and 90 degrees (See pictures A and B).

A.

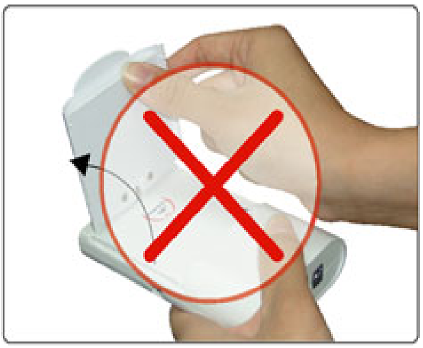


B.



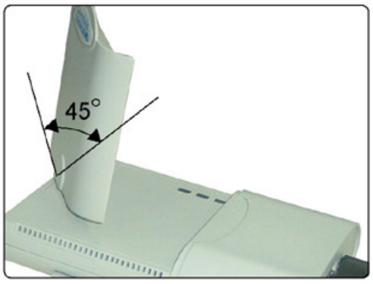
Please do not lifted the antenna over 90 degrees (See Picture C), otherwise it will cause damage to antenna.

C.

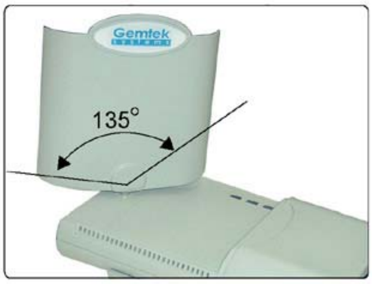


The antenna housing can rotate up to 135 degrees clockwise/counter-clockwise (See pictures D~G). It will be locked /lodged in every increment of 45 degrees in position.

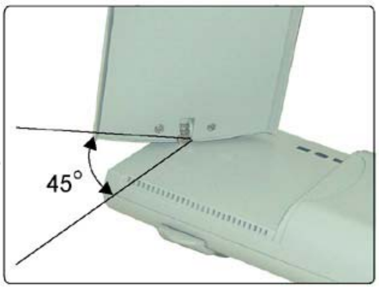
D.



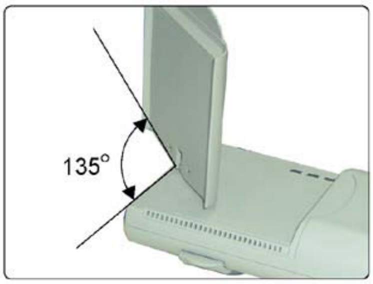
E.



F.



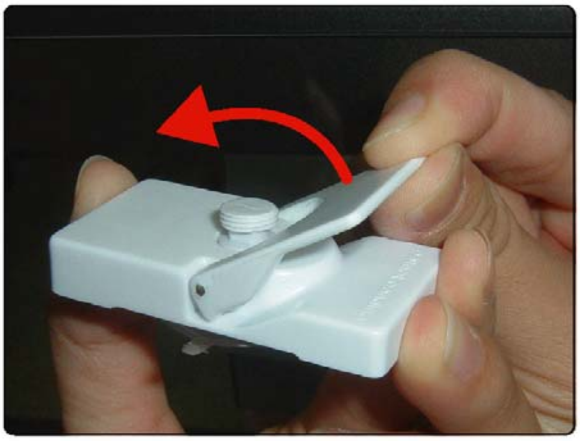
G.



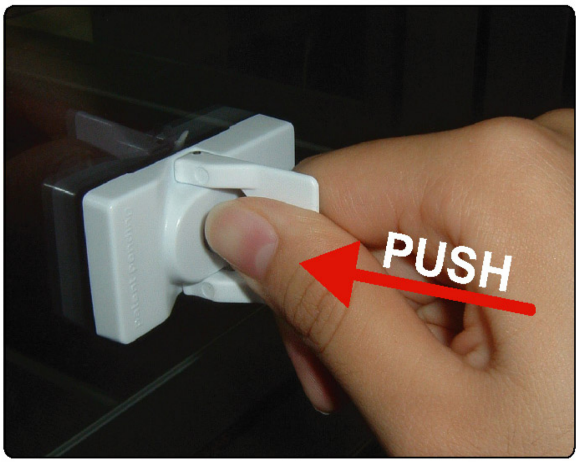
4.4 The Usage of Universal Sucking Disk (U.S.D)

1. To pull and rotate USD's shaft into 90 degrees, then, press it against the surface to make exhausted its air out. (See pictures A&B)

A

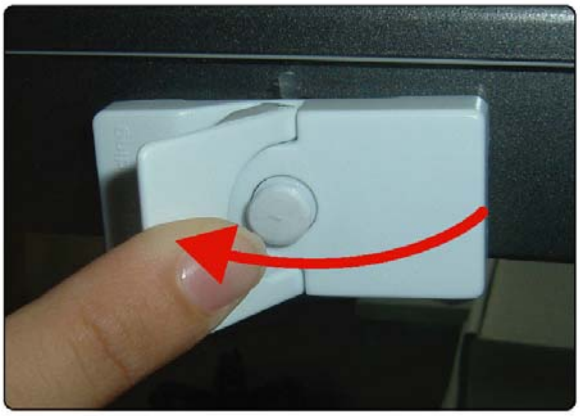


B



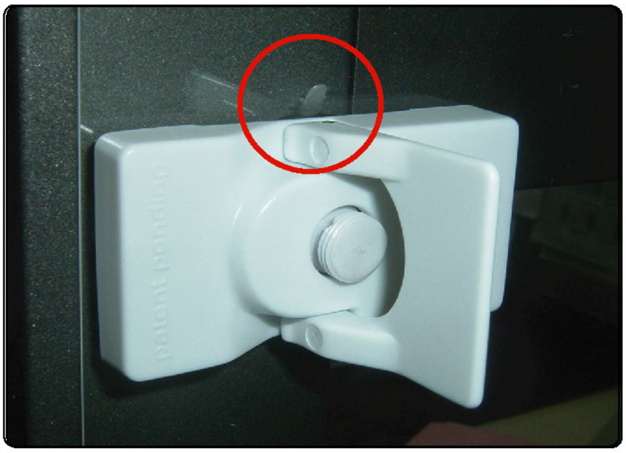
2. Return shaft into original position on USD. (See picture C)

C

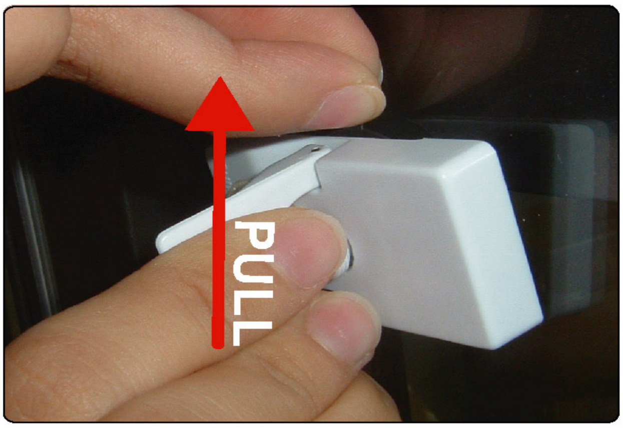


3. To Grasp and lift the salient part of the suction cap to allow ventilated. So, USD can be easily torn off. (See pictures D&E)

D

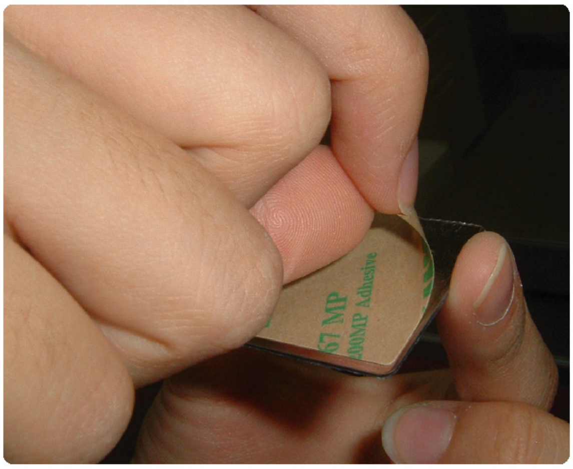


E



4. Besides the suction cap, the USD kit also equips with magnet and a metal plate to adhere on the surface. It simply tears off sticker on the back of metal plate and places USD unit on it. (See picture F)

F



Please apply suction cap and metal plate on any smooth surface. Any method/usage does not follow this instruction may cause USD cannot hold T-311 unit properly.

5. Installation

5.1 Installation

1. Insert circular power and Ethernet plug into the appropriate connector on T-311.

2. Connect power connector and Ethernet cable into a (power) USB port and Ethernet connector (RJ45) on your systems, respectively.

3. Open and/or adjust lid (external patch antenna) to aim at Access Point for T-311's best performance.

5.2 LED Indicators

At the front of the T-311 High Gain Smart Ethernet Client you will see three LEDs.

If all go well, the Power LED is red and the LINK LED is green. It will be blinking whenever there is traffic on the wired networks. The Orange LED indicates WLAN signal and represents traffic wireless networks.

5.3 Reset the High Gain Smart Ethernet Client

If you press the reset button for more than five seconds, the High Gain Smart Ethernet Client will be reset to the default factory settings. All changes you made to the configuration will be lost.

1. Insert one end of a paper clip into the hole of reset button and keep it pressed for more than five seconds. LINK LED will be blinking during the process.

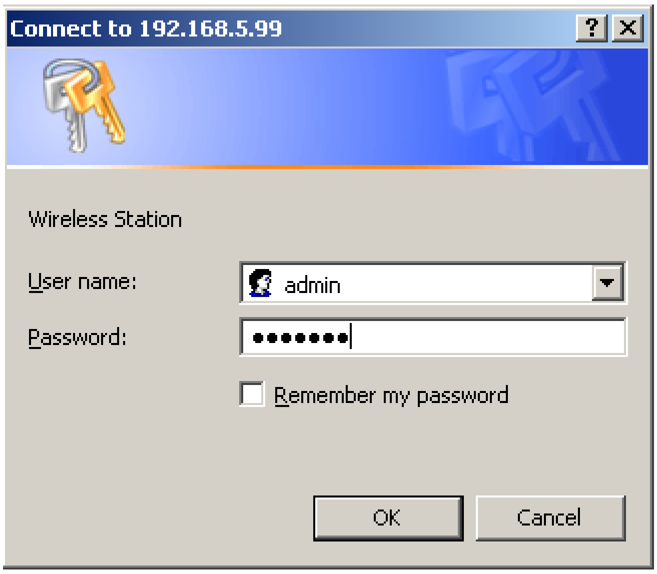
2. Release the reset button after WLAN LED goes off. All settings will be deleted and back to the default. You can refer to this manual again and reconfigure the High Gain Smart Ethernet Client by yourself.

5.4 Configuring the High Gain Smart Ethernet Client

The High Gain Smart Ethernet Client is a ready-to-use device. It is delivered with default settings that allow you to have access to it without configuration. The default IP address is "192.168.5.99", so enter http://192.168.5.99 in the address table of web browser then the User

Login Window pops up (See *Figure 1-User Login*). Input the default user name (admin) and password (admin01) and click OK to affirm.

Getting through the step above, the main frame of configuration displays and you can configure the High Gain Smart Ethernet Client via a JavaScript-enabled web-browser such as Internet Explorer 4.0 or higher, or Netscape Navigator 4.0 or higher.



Connect to 192.168.5.99

Wireless Station

User name: admin

Password: •••••••

□ Remember my password

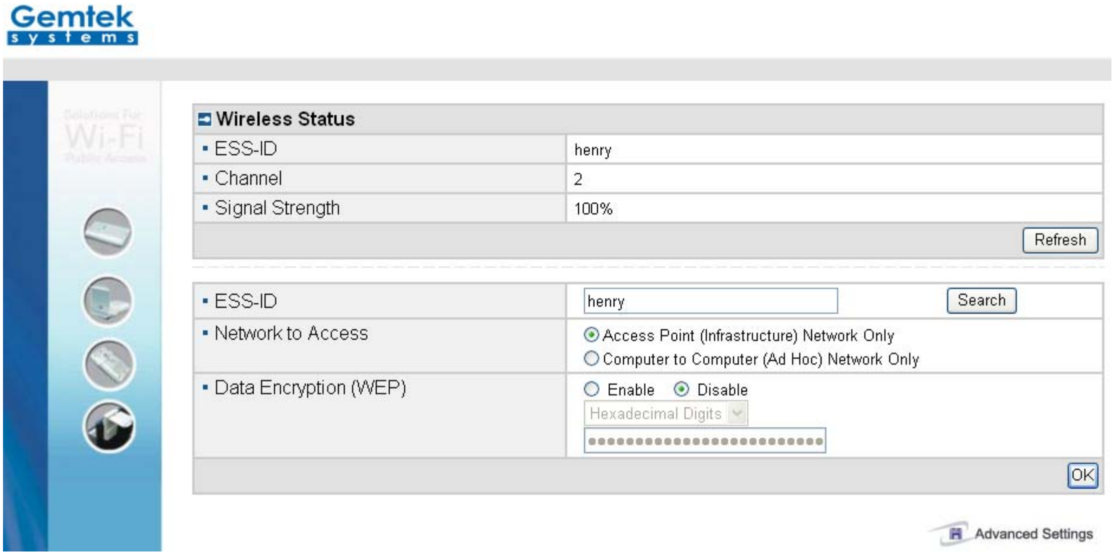
Figure 1 – User Login

The computer that you are using for initial configuration must have an IP Address within the same sub-network as the IP Address of the High Gain Smart Ethernet Client. The High Gain Smart Ethernet Client has a default IP Address of 192.168.5.99 with a subnet mask of 255.255.255.0.

6. Contents of Web Interface

6.1 Top Page

The **Top page** displays the current setup status of the T-311 11Mb High Gain Smart Ethernet Client.



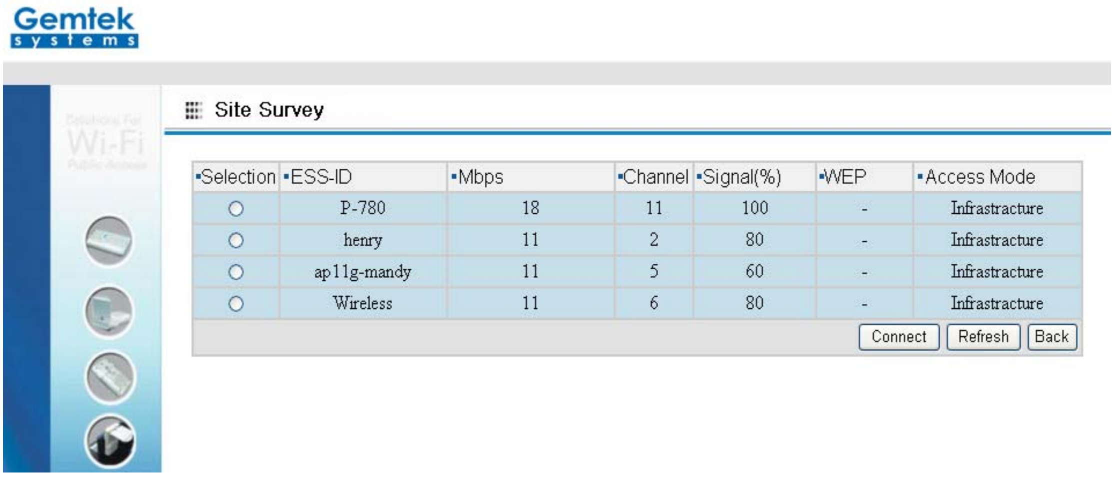
Wireless Status	
▪ ESS-ID	henry
▪ Channel	2
▪ Signal Strength	100%

▪ ESS-ID	henry
▪ Network to Access	● Access Point (Infrastructure) Network Only ○ Computer to Computer (Ad Hoc) Network Only
▪ Data Encryption (WEP)	○ Enable ● Disable Hexadecimal Digits ●●●●●●●●●●●●●●●●●●●●●●●●●●

Figure 2 – Top Page

ESS-ID

The ESS-ID is also known as Extended Service Set Identify. It is a special case of SSID used to identify a wireless network that includes access points. SSID is the short for the Service Set Identifier that identifies a wireless network. All wireless devices on one network must use the same SSID. Only High Gain Smart Ethernet Clients and clients that share the same ESS-ID are able to communicate with each other. Click **Search** to scan the environment and a site pops up to show the available networks around you. (*See Figure 3 - Site survey*). Then you can select the network you want to connect and click **Connect** to affirm and apply the configuration. Click **Refresh** to restart scan and if you click **Back**, it will go back to the top page.



Site Survey

▪Selection	▪ESS-ID	▪Mbps	▪Channel	▪Signal(%)	▪WEP	▪Access Mode
○	P-780	18	11	100	-	Infrastracture
○	henry	11	2	80	-	Infrastracture
○	ap11g-mandy	11	5	60	-	Infrastracture
○	Wireless	11	6	80	-	Infrastracture

Figure 3 – Site Survey

Network to Access

T-311 can operate with or without access point and have two corresponding modes. One is the infrastructure mode and the other is ad hoc mode, also called peer-to-peer mode.

Infrastructure mode uses access points to allow wireless computers to send and receive information. Wireless computers transmit to the access point that receives the information and rebroadcasts it to other computers. The access point can also connect to a wired network onto the Internet. Multiple access points can work together to provide coverage over a wide area.

Ad-hoc mode works without access points and allows wireless computers to send information directly to other wireless computers. You can use ad-hoc mode to network computers in a home or small office that contains fewer computers.

To connect a wireless network with a different mode, make sure to select the mode correctly before scanning and connecting. For example, now you are in an infrastructure network, when you want to connect an ad-hoc network, select the **Computer-to-Computer (ad-hoc) Network Only** before doing anything else.

Data Encryption (WEP)

Overview

Wired equivalent privacy encryption (**WEP**) provides protect for your data on the network. **WEP** uses an encryption key to encrypt data before transmitting it. Only computers using the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. You could select one of the radio buttons to enable or disable this function and if it is enabled, a key is needed.

Under 802.11 a wireless station can be configured with up to four keys (the key index vales are 1, 2, 3 and 4). When an access point or a wireless station transmits an encrypted message using a key that is stored in a specific key index, the transmitted message indicates the key index that was used to encrypt the message body. The receiving access point or wireless station can then retrieve the key that is stored at the key index and use it to decode the encrypted message body.

How to enable WEP Encryption

Select **Enable** button and chose the encryption mode from the pull-down menu.

- **Use ASCII Text**

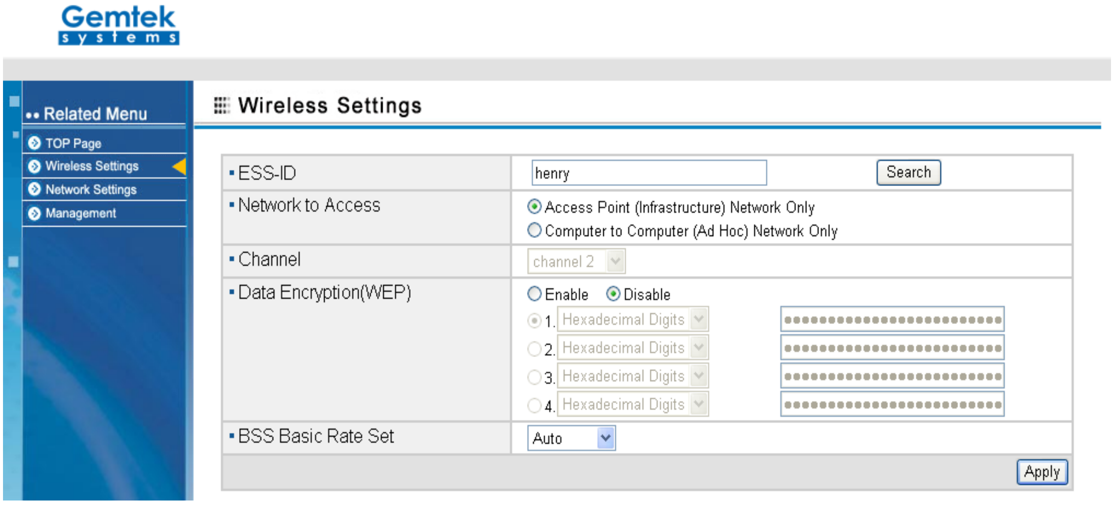
  Select **ASCII Characters** to enable. Enter a text, up to five (using 64-bit) or thirteen (using 128-bits) characters in the text field.

- **Use Hexadecimal Digits**

  Select **Hexadecimal Digits** to enable. Enter up to ten (using 64-bit) characters, or twenty -six (using 128-bit) characters (0-9,A-F), in the text filed.

6.2 Advanced Settings

Top page only includes the basic information about the network you connected to. To further configure the network, click the **Advanced Settings** on the bottom of the top page and a more complex page pops up. (*See Figure-4 Further Configuration*) In the left column of this page, there are four items related to the corresponding configuration for the smart Ethernet client. Click one item to enter into the frame it represents and do the related configuration if you want.



Wireless Settings

ESS-ID	henry
Network to Access	● Access Point (Infrastructure) Network Only ○ Computer to Computer (Ad Hoc) Network Only
Channel	channel 2
Data Encryption(WEP)	○ Enable ● Disable ● 1. Hexadecimal Digits ●●●●●●●●●●●●●●●●●●●●●●●●●● ○ 2. Hexadecimal Digits ●●●●●●●●●●●●●●●●●●●●●●●●●● ○ 3. Hexadecimal Digits ●●●●●●●●●●●●●●●●●●●●●●●●●● ○ 4. Hexadecimal Digits ●●●●●●●●●●●●●●●●●●●●●●●●●●
BSS Basic Rate Set	Auto

Figure-4 Further Configuration

6.3 Wireless Settings

The wireless settings page contains more information about the smart Ethernet client and you could change some of the attributes to connect to a network properly. (*See Figure-4 Further Configuration*)

ESS-ID

The ESS-ID is also known as Extended Service Set Identify. It is a special case of SSID used to identify a wireless network that includes access points. SSID is the short for the Service Set Identifier who identifies a wireless network. All wireless devices on one network must use the same SSID. You can type the ESS-ID in the text filed manually or click **Search** to scan the available networks around you automatically. The process to configure the ESS-ID is the same as described in the Top Page and you can see more specification there.

Network to Access

T-311 can operate with or without access point and have two corresponding modes. One is the infrastructure mode and the other is ad hoc mode, also called peer-to-peer mode.

- **Access Point (infrastructure) mode**
  In access point wireless networks, T-311 connects to wireless access points. These access points function as bridges between wireless stations and the existing network distribution system (network backbone).
- **Computer-to-computer (ad hoc) mode**

In *computer-to-computer* wireless networks, T-311 connects to each other directly, rather than through wireless access points. For example, if you are in a meeting with co-workers, your wireless device can connect to the wireless devices of your co-workers, and you can form a temporary network.

Choose one of the two modes from the field and if you select the ad-hoc mode, then you must specify a channel, refer to the Channel for more information.

Channel

In ad hoc mode, you can send and receive information to other computers without using an access point. All wireless clients in the ad hoc network must use the same network name (SSID) and channel number. The channel number is ranging from 1 to 11 and you can choose a right one in the poll-down menu in the filed. If you are not sure about the channel number, click **Search** to scan the network first and the channel number will be showed in the corresponding column in the Site Survey page.

Data Encryption (WEP)

The same as described in the Top Page, the data encryption is used to encrypt the transmitted data and provide the security in WLAN. You can enable the Data Encryption feature by click the Enable radio box.

If you enable Data Encryption, you should select a key index from 1 to 4 and input the key in the input box. You can choose to use **ASCII Characters** mode or **Hexadecimal Digits** mode to input the key. There are two types of keys that one is 64-bits long and the other one is 128-bits. Using the 64-bits, you have to enter 5 characters or 10 Hexadecimal numbers (0-9,a-f) in the field. The amount of character or number for 128-bits ASCII and Hexadecimal are respectively 13 and 26.

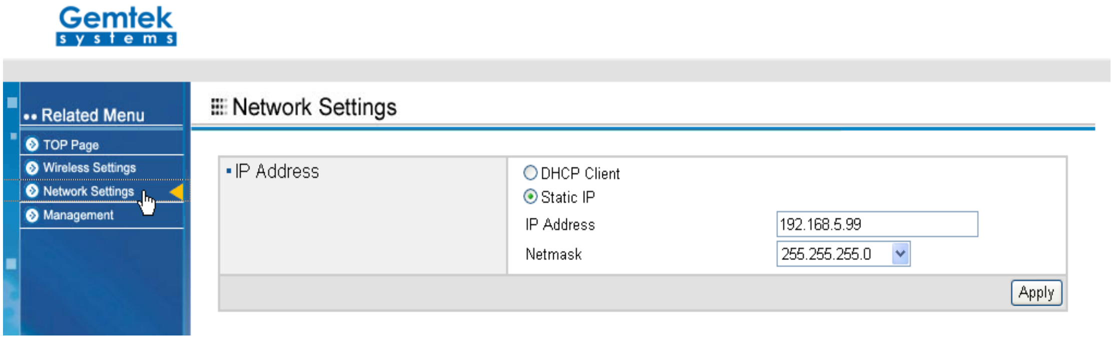
BSS Basic Rate Set

The BSS Basic Rate is the speed at which the client transmits the data to the AP or other computers or receives data from them. All the computers in a network must have the same rate to communicate the others well. If you are not sure about the rate of the network you want to connect, use **Auto** as default. The **Mbps** column in the page displays the rate speed at which the network transmits the data. Make sure to keep the rate speed of the smart Ethernet client synchronous to the networks'. One of the five speed rates could be configured in the pull-down menu and the **Auto** represents the auto-negotiation mechanism that each client has an ability to negotiate its rate speed with the AP and others computers automatically and the **Auto** is the default configuration for the T-311 11Mb high gain smart Ethernet client.

*To connect a wireless network, using **Auto*** is recommended unless you know the rate of the network you want to connect.

6.4 Network Settings

In Network Settings page, you could configure the IP-related attributes of the smart Ethernet client such as the netmask (See *Figure-5 Network Settings*). There are two methods to define the client IP --- the static and the DCHP. When select the DCHP mode, the client will get the IP from DHCP server on the same LAN. In the case of selecting the **Static IP** mode, you have to define the IP Address and the netmask by yourself. If the above steps are over, click **Apply** button to affirm and apply this new configuration.



IP Address

○ DHCP Client
● Static IP

IP Address 192.168.5.99

Netmask 255.255.255.0

Figure-5 Network Settings

Note: the IP configuration here is not the IP of PC you are using, but it is the address of the T-311 11Mb high gain smart Ethernet client. Once you configure a new IP for the client, if the new address is not in the same sub-network as the old is, the logic connection between your pc and the client will be cut off and you can't further configure it. To recover it, configure your own pc in the sub-network that the client is in and login the client again to continue configuration. See 5.4 for more information about login.

6.5 Management

Management is the last item in the left column of the Advanced Settings page. When place the cursor over the Management, a menu that has four items pops up (*See Figure-6 Pop-up Menu*). The four items are System Info, Administration, Configuration and Firmware Upgrade. Most of them execute the management of the firmware in the smart Ethernet client. Specific descriptions are described as below:

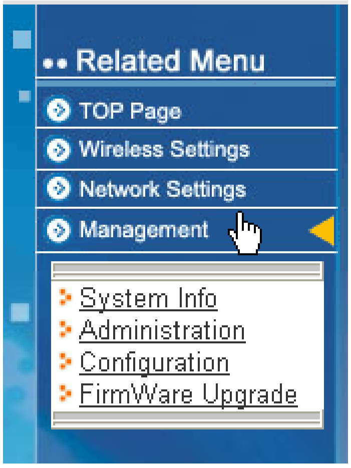
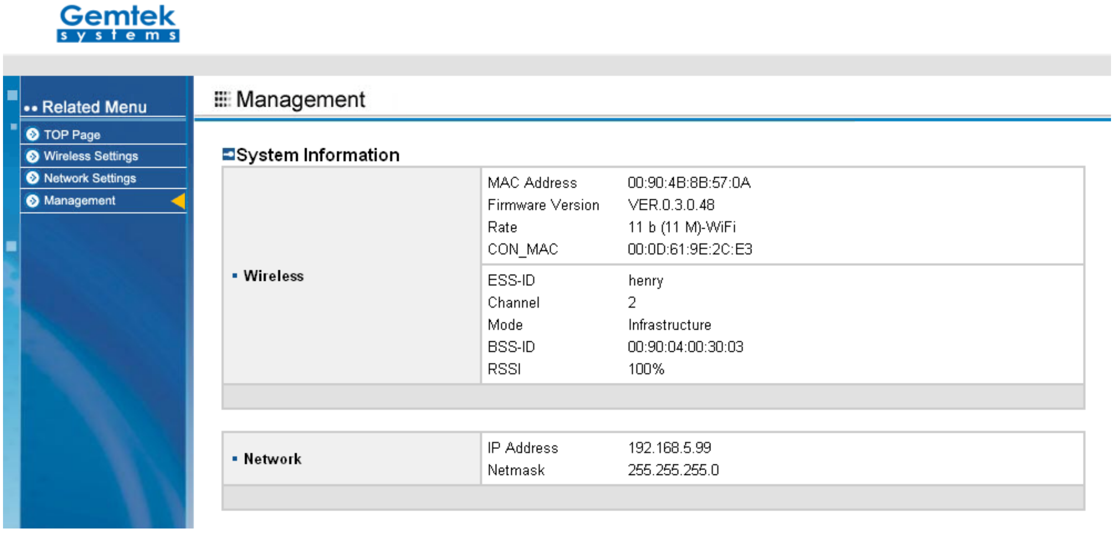


Figure-6 Pop-up Menu

System Info

System Info page contains all the basic configuration information and you can get an overview of the configuration from the System Info. page (*See Figure-7 System Info*).



Management

System Information

Wireless	MAC Address	00:90:4B:8B:57:0A
	Firmware Version	VER.0.3.0.48
	Rate	11 b (11 M)-WiFi
	CON_MAC	00:0D:61:9E:2C:E3
	ESS-ID	henry
	Channel	2
	Mode	Infrastructure
	BSS-ID	00:90:04:00:30:03
	RSSI	100%
Network	IP Address	192.168.5.99
	Netmask	255.255.255.0

Figure-7 System Info

MAC Address

The MAC address of T-311

Firmware Version

Current firmware version of the system.

Rate

The current speed at which the client transmits and receives data, see BSS Basic Rate Set for more information.

CON_MAC

The MAC address of the pc connected with the client.

ESS-ID

ESS-ID of the network. See ESS-ID in top page for more information.

Channel

The channel in which the client runs. See Channel for more information.

Mode

Network mode that the smart Ethernet client is using. See Network to Access for more information.

BSS-ID

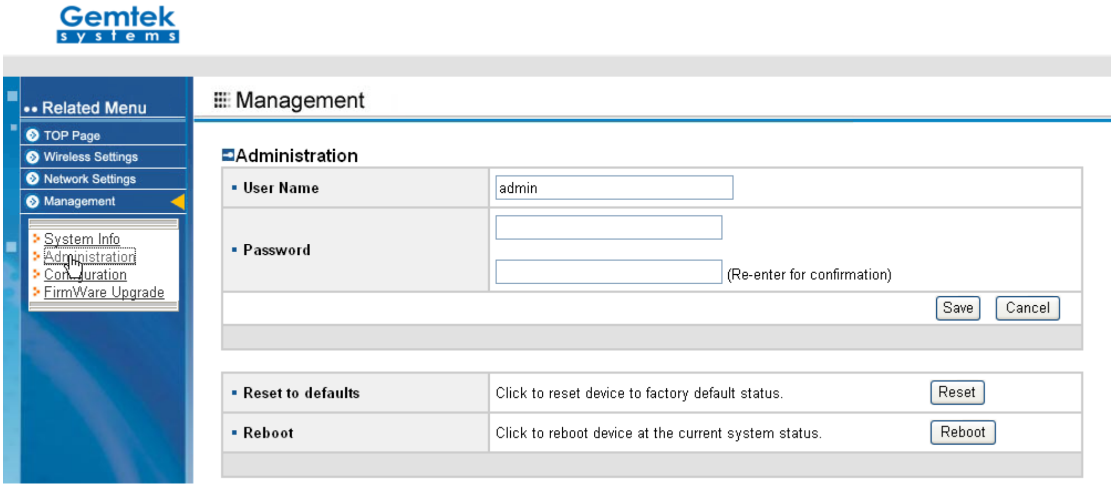
An unique identifier that AP used to identify the wireless network.

RSSI

Received signal strength indication.

Administration

In the firmware, there is a server to authenticate the user via the password. To configure the client, you have to enter the username and the corresponding password so a more security is supplied by this mechanism.



Administration

▪ User Name	admin
▪ Password	(Re-enter for confirmation)
	Save Cancel

▪ Reset to defaults	Click to reset device to factory default status.	Reset
▪ Reboot	Click to reboot device at the current system status.	Reboot

Figure-8 Management

Username and Password

You can use a password to prevent tampering with the configuration of the High Gain Smart Ethernet Client. By default, the username is "admin" and password is "admin01". However, if you want to renew the username/password, you can enter your new username and password in the field, and click **Save** for the configuration to take effect.

Reset to Defaults

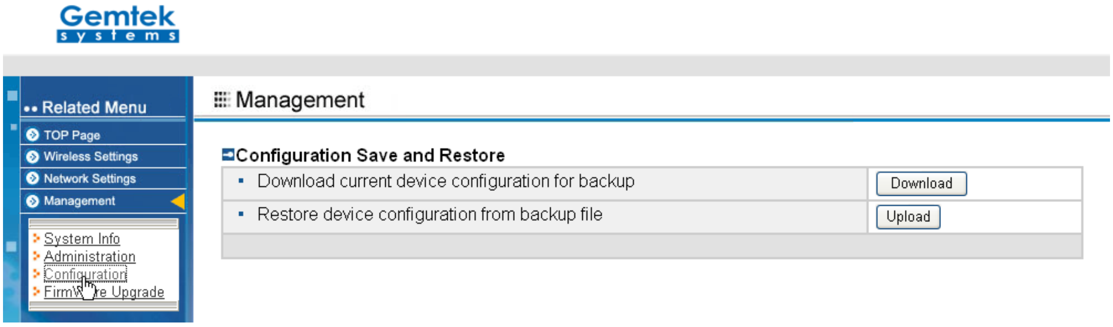
Click on **Reset to Defaults** to return all settings to the Factory Default values.

Reboot

Click **Reboot** to restart the High Gain Smart Ethernet Client.

Configuration

This page is to save or restore the configuration.



Configuration Save and Restore

▪ Download current device configuration for backup	Download
▪ Restore device configuration from backup file	Upload

Figure-9 Configuration Save and Restore

To download current device configuration for backup, click **Download** and a **Save As** message box pops up. Specify the file name to backup the configuration and click **OK** to complete it.

To restore device configuration from backup file, click **Upload** and go forward to Upload page to identify the backup file to be restored. See the Figure-10.

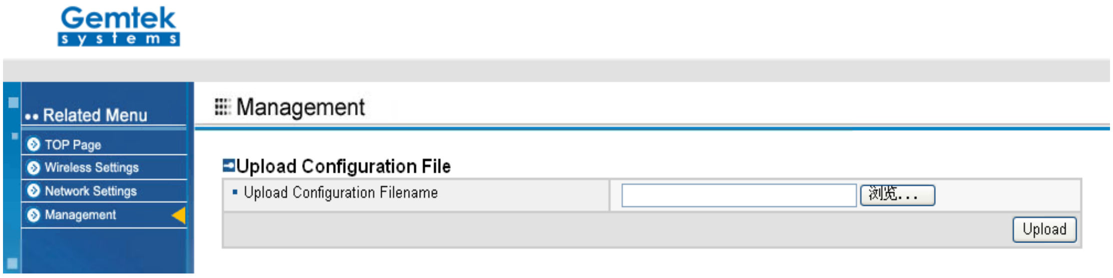


Figure-10 Upload

Firmware Upgrade

Click **FirmWare Upgrade** to enter the Firmware Upgrade Page:

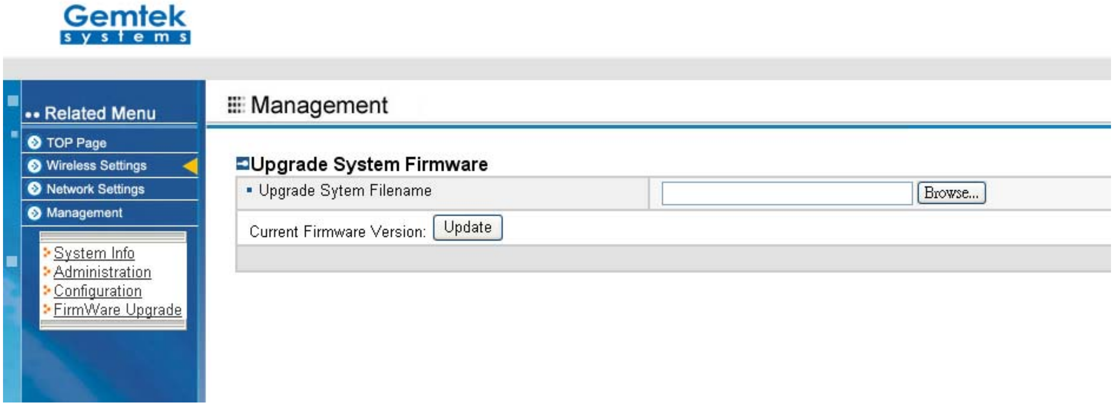


Figure 11 – Upgrade System Firmware

To change the firmware, a valid firmware file must be selected at first by clicking the **Browse** button.

After selecting the valid firmware version, click the **Upgrade** button to complete.

7.Troubleshooting

Q: It’s difficult to connect this device with exist wireless network.

A: There are several possible causes based on the way the High Gain Smart Ethernet Client is connected to the network.

a. Problems on the wireless side

Always check the status of the LEDs to verify if you have:

- ♦ Electricity problems,
- ♦ Radio signal problems,
- ♦ Networking problems

1. **Possible cause:** Is the High Gain Smart Ethernet Client powered up?

   Solution: Check the power LED. Check if the High Gain Smart Ethernet Client is connected.

2. **Possible cause:** Is the High Gain Smart Ethernet Client is in range of the Access Point?

   Solution: Check the WLAN signal LED. Check for possible problems with respect to range.

3. **Possible cause:** Is there a network connection? Check the network LINK LED.

   Solution: The High Gain Smart Ethernet Client may take up to a minute to find an IP address.

b. Problems on the wired side

Always check if your cables and connections are in good order and properly installed.

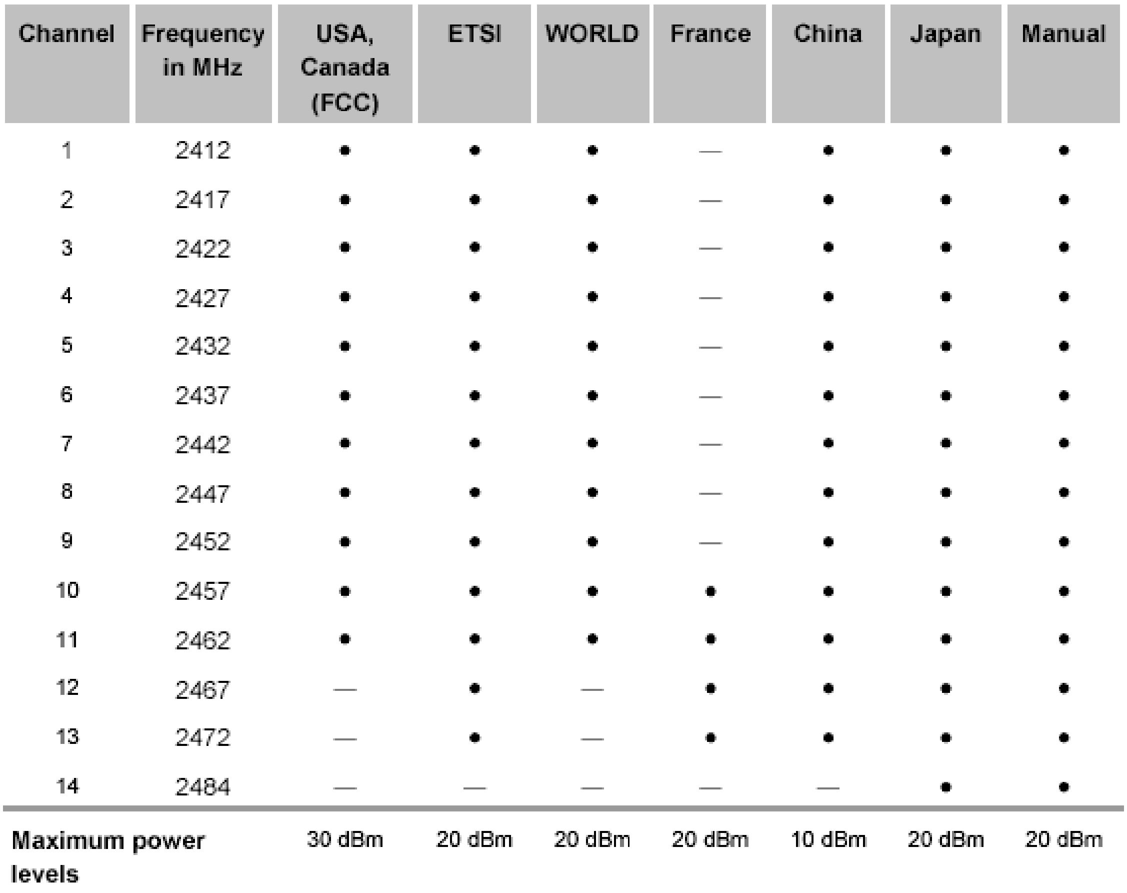
1. **Possible cause:** Has the proper cable been used?

   Solution: • If the High Gain Smart Ethernet Client connects to a HUB, a 'normal' (not a crossover) cable must be used.

- If the High Gain Smart Ethernet Client connects directly to a computer, a crossover cable must be used.

8. Appendix

8.1 Regulatory domains



Channel	Frequency in MHz	USA, Canada (FCC)	ETSI	WORLD	France	China	Japan	Manual
1	2412	•	•	•	—	•	•	•
2	2417	•	•	•	—	•	•	•
3	2422	•	•	•	—	•	•	•
4	2427	•	•	•	—	•	•	•
5	2432	•	•	•	—	•	•	•
6	2437	•	•	•	—	•	•	•
7	2442	•	•	•	—	•	•	•
8	2447	•	•	•	—	•	•	•
9	2452	•	•	•	—	•	•	•
10	2457	•	•	•	•	•	•	•
11	2462	•	•	•	•	•	•	•
12	2467	—	•	—	•	•	•	•
13	2472	—	•	—	•	•	•	•
14	2484	—	—	—	—	—	•	•
Maximum power levels		30 dBm	20 dBm	20 dBm	20 dBm	10 dBm	20 dBm	20 dBm

Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration compiles with the regulatory standards of Mexico.

France is included in the EMEA regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration compiles with the regulatory standards of France.

8.2 Device configuration default values

Parameter	Default Value
SSID	[Blank]
WEP enable	No
IP Address mode	Static
IP Address	192.168.5.99
Subnet mask	255.255.255.0
Default Gateway	192.168.5.1
User Name	Admin
Administrator or password	Admin01

8.4 Hardware Specification

Interface			
System Interface	IEEE 802.3 10/100Base_T Ethernet Port (RJ45)		
Wireless			
Standard	IEEE 802.11b DSSS (2.4GHz ISM radio band)		
Data Rate	11Mbps, 5.5Mbps, 2 Mbps, 1Mbps (Auto scaling)		
Transmit Power	+14dBm (typical)		
Sensitivity	Data Rate	Sensitivity	Modulation
	11Mbps	-79dBm	CCK
External Patch Antenna	5.5 dBi		
Physical Specification			
Dimension	114 x 72 x 23mm (L x W x H)		
Weight	115g		
Environment Specification			
Temperature	0℃ to 40℃		
Humidity	10% to 95%, non-condensing		
Power Supply			
Operating Voltage	5.0V ± 5%		
Current Consumption	500mA (maximum)		
Regulatory Compliance			
FCC			
LEDs			
3 LEDs	WLAN, Link, Power		
Warranty			
1 year (limited)			

9. Glossary

Symbols:

802.11: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become "industry standards".

802.11b adds CCK modulation enabling data rates of up to 11Mbps, and 802.11a specifies OFDM modulation in frequency bands in the 5 to 6GHz range, and enables data rates up to 54Mbps.

A

AAA: Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password), service authorization, and session accounting details between devices and networks in a real-time manner.

authentication: The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

B

backbone: The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

Bandwidth: Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communication circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps: bits per second. A measure of the data transmission rate.

D

DHCP: Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DNS: Domain Name Service. An Internet service that translates a domain name such as gemtek-systems.com to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hex number.

E

EAP: Extensible Authentication Protocol. Defined in [RFC2284] and used by IEEE 802.1x Port Based Authentication Protocol [8021x] that provides additional authentication methods. EAP-TLS (Transport Level Security) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints [RFC2716]. EAP-TTLS (Tunneled TLS Authentication Protocol) provides an authentication negotiation enhancement to TLS (see Internet-Draft <draft-ietf-pppext-eap-ttls-00.txt>).

G

gateway: A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

H

hot-spot: A hot-spot is wireless public access system that allows subscribers to be connected to a wireless network in order to access the Internet or other devices, such as printers. Hot-spots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

hot-spot operator: An entity that operates a facility consisting of a Wi-Fi public access network and participates in the authentication.

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

HTTPS: HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

I

ICMP: ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

IEEE: Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world's largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

IP: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IPsec: IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPsec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

ISP: An ISP (Internet Service Provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

L

LAN: A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

M

MAC: Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

N

NAT: NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

NAT is included as part of a router and is often part of a corporate firewall.

P

POP3: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

PPP: PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

PPPoE: PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on." Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses (during an initial exchange called "discovery"). Once a session is established between an individual user and the remote site (for example, an Internet service provider), the session can be monitored for billing purposes.

PPTP: Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. This kind of interconnection is known as a virtual private network (VPN).

R

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

S

SNMP: Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

SSL: The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

T

TCP: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Telnet: Telnet is the way to access someone else's computer, assuming they have given permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow to request specific files from remote computers, but not to actually be logged on as a user of that computer.

U

UAM: Universal Access Method is the current recommended methodology for providing secure web-based service presentment, authentication, authorization and accounting of users is a WISP network. This methodology enables any standard Wi-Fi enabled TCP/IP device with a browser to gain access to the WISP network.

W

WAN: A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN).

X

XSL (Extensible Style sheet Language), formerly called Extensible Style Language, is a language for creating a style sheet that describes how data sent over the Web using the Extensible Markup Language (XML) is to be presented to the user.