300N Wireless LAN
Home Networking Solution

Video Bridge Kit

User's Manual

Version 1.0

(February, 2011)

COPYRIGHT

Copyright ©2011/2012 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

Federal Communication Commission Interference Statement

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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 or more of the following measures:

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

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person’s body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

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.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

This device is restricted to indoor use when operated in the 5.15 to 5.25 GHz frequency range.

R&TTE Compliance Statement

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

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

Safety

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

EU Countries Intended for Use

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

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

EU Countries Not intended for use

None.

CATALOG

Chapter I: Product Information

1-1 Product Introduction

Thank you for purchasing this 300N Wireless LAN Home Networking Solution! This wireless video bridge kit consisting of one wireless access point and one wireless client, which is a wireless HD video system designed to distribute High Definition IP Video Streams (IPTV) throughout the home wirelessly. Connecting the access point to the video source that can be an Ethernet-equipped broadband gateway, a cable/DSL modem or DVR/PVR devices and then connecting the client to the video receiving set top box device, the wireless kit is able to transmit the HD or SD IPTV streams robustly and reliably.

Up to four clients could be supported for multiple video streaming transmissions by the access point.

Easy install procedures allows any users to setup a wireless video network environment in very short time. With this wireless kit, you will immediately enjoy the convenience of the cable-less video streaming environment.

Other features of this wireless kit including:

IPTV Features

- Any packetized video stream is supported. This includes but not limited to MPEG2, MPEG4, H.264 encapsulated in MPEG2 Transport Streams.
- Any kind of video service is supported. This includes but not limited to Live Video, VOD and recorded streams coming out of DVR and NAS devices.
- The underlying transport protocols for the video streams can be both TCP and UDP.
- Up to 3 video clients can be supported simultaneously by an access point.
- IGMP (v2, v3) snooping and Multicast to Unicast conversions.

- Employs WDS (Wireless Distribution System) and therefore functions as a truly transparent layer 2 bridge, thus eliminating MAC cloning related problems and incompatibilities.
- Uses DLS (Direct Link Setup) to facilitate direct client to client communication for efficient support of multi room DVR network topologies.

Wireless Features

- Complies with IEEE 802.11a/n standards.
- Operates in the 5GHz band, frequency range is from 5.15GHz to 5.85GHz.
- High speed data rate – up to 300Mbps.
- Supports 64/128-bit WEP, WPA and WPA2 security.
- Supports advanced 2T3R MIMO technology, enhancing the throughput and coverage range significantly.
- Support explicit beam forming, enhancing the performance for long range transmission.
- Support dynamic antenna selection in transmit and receive directions to further increase range and robustness and overcome channel fading.
- Supports WPS function for easy wireless association.
- Supports WMM wireless QoS feature.

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the following safety instructions:

1. This wireless kit is designed for indoor use only; DO NOT place this access point outdoor.

2. DO NOT put this wireless kit at or near hot or humid places, like kitchen or bathroom. Also, do not left this wireless kit in the car in summer.

3. If you want to place this wireless kit at high places or hang on the wall, please make sure the wireless kit is firmly secured. Falling from high places would damage this wireless kit and the accessories, and warranty will be void.

4. Accessories of this wireless kit, like power supply, are danger to small children under 3 years old. They may put the small parts in their nose or month and it could cause serious damage to them. KEEP THIS ACCESS POINT OUT THE REACH OF CHILDREN!

5. The wireless kit will become hot when being used for long time (***This is normal and is not a malfunction).*** DO NOT put this wireless kit on paper, cloth, or other flammable materials.

6. There's no user-serviceable part inside the wireless kit. If you found that the wireless kit is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the wireless kit, warranty will be void.

7. If the wireless kit falls into water when it's powered, DO NOT use your hand to pick it up. Switch the electrical power off before you do anything, or contact an experienced electrical technician for help.

8. If you smell something strange or even see some smoke coming out from the wireless kit or power supply, remove the power supply or switch the electrical power off immediately, and call dealer of purchase for help.

1-3 System Requirements for Configuration

- Computer or network devices with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser).*
- An available AC power socket (100 – 240 V, 50/60Hz)

1-4 Package Contents

Before you starting to use this wireless kit, please check if there’s anything missing in the package, and contact your dealer of purchase to claim for missing items:

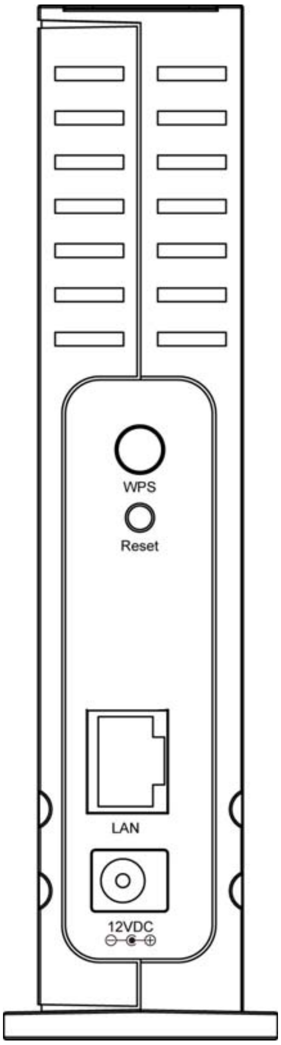
□ Wireless Access Point (main body, 1 pcs)
□ Wireless Client (main body, 1 pcs)
□ Quick Installation Guide (1 pcs)
□ User Manual CD (1 pcs)
□ A/C Power Adapter (2 pcs)

1-5 Familiar with your new wireless access point

Front Panel

LED Name	Light Status	Description
WLAN	On	**Access Point Behavior** - At least one Client is associated with the Access Point. **Client Behavior** － The Client is associated with an Access Point at higher data rate (able to transfer HD streaming).
	Flashing	**Client Behavior –** The client is associated with an access point at lower data rate (able to transfer SD streaming).
	Off	**Access Point Behavior** - No Clients are associated with the Access Point. **Client Behavior** － The Client is not associated with an Access Point.
WPS	On	WPS pairing has finished successfully. This is a temporary state that lasts for 2 minutes.
	Flashing	WPS pairing is in progress. This is a temporary state that lasts for 2 minutes or until WPS pairing.
	Off	WPS function is not enabled.
LAN	Flashing	Activity on the wired network interface.
	Off	The LAN port is either not connected or there is no activity on the link.
Power/Standby	Green On	The device is powered on.
	Red On	The device is in standby mode which means there is no traffic on Ethernet port.

Back Panel



Item Name	Description
Power	Power connector, connects to A/C power adapter.
LAN	Local Area Network (LAN) port.
Reset	This button is for you to restart the router or reset the router to factory default settings (clear all settings). Press this button less than 5 seconds to restart the router; and press this button and hold for 10 seconds to restore all settings to factory defaults.
WPS	Press this button to enable WPS connection. WPS paring will be activated during two minutes.

Chapter II: System and Network Setup

2-1 Installing the access point and client to your network

Please follow the following instruction to build the network connection with the wireless access point and the wireless client to your home:

1. Powering up the wireless access point and the wireless client. (Please go to Section 2-1-1)
2. Paring the wireless access point and the wireless client (Please go to Section 2-1-2)
3. Placing and connecting the wireless access point and the wireless client (Please go to Section 2-1-3)

2-1-1 Powering up the devices

To power up the two devices, please follow the procedures as below.

1. Plug in the two A/C adapters supplied with the package and connect the adapters to the wireless access point and the wireless client.
2. Wait several seconds while the two devices are reset.

Note: You must use the power adapters shipped along with the wireless access point and the wireless client, do NOT use any other power adapter from other sources.

2-1-2 Paring your devices

To pair the two devices, please follow the procedures as below.

1. Place the wireless access point and the wireless client between 1 to 3 meters from each other.
2. Pair the devices by pressing the WPS button on the front panel of each device. You can release the button as soon as the WPS LED begins flashing.
3. Wait for the pairing process to complete by watching the LEDs on the devices:

   - While pairing is in progress, the WPS LED is flashing.
   - After successful pairing, the WPS LED stays on for two minutes.

Note: WPS Pairing is in progress during two minutes after pressing the WPS button.

2-1-3 Placing and connecting your devices

To place and connect the wireless access point, please follow the procedures as below.

1. Place the wireless access point on an easily accessible surface near the home gateway, Cable/DSL Modem or DVR/PVT device.
2. Plug one end of the Ethernet cable into the LAN port of the gateway device and the other end into the Ethernet port of the wireless access point.

To place and connect the wireless client, please follow the procedures as below.

1. Place the wireless client on an easily-accessible surface near the set top box.
2. Plug one end of the Ethernet cable into the LAN port of the set top box device and the other end into the Ethernet port of the wireless client.

3. Make sure that the WLAN LED is solid green.

If the WLAN LED is turned off, try to reposition the device to a more elevated location and as far as possible from large metallic objects.

If the WLAN LED is solid green, you have finished installing your devices. To test your connectivity, turn on the TV and set top box and watch any available channel.

Note: To install additional wireless client, repeat the above procedure for each new wireless client.

2-2 Connecting to the wireless devices by web browser

After the network connection is built, the next step you should do is setup the access point or client with proper network parameters, so it can work properly in your network environment.

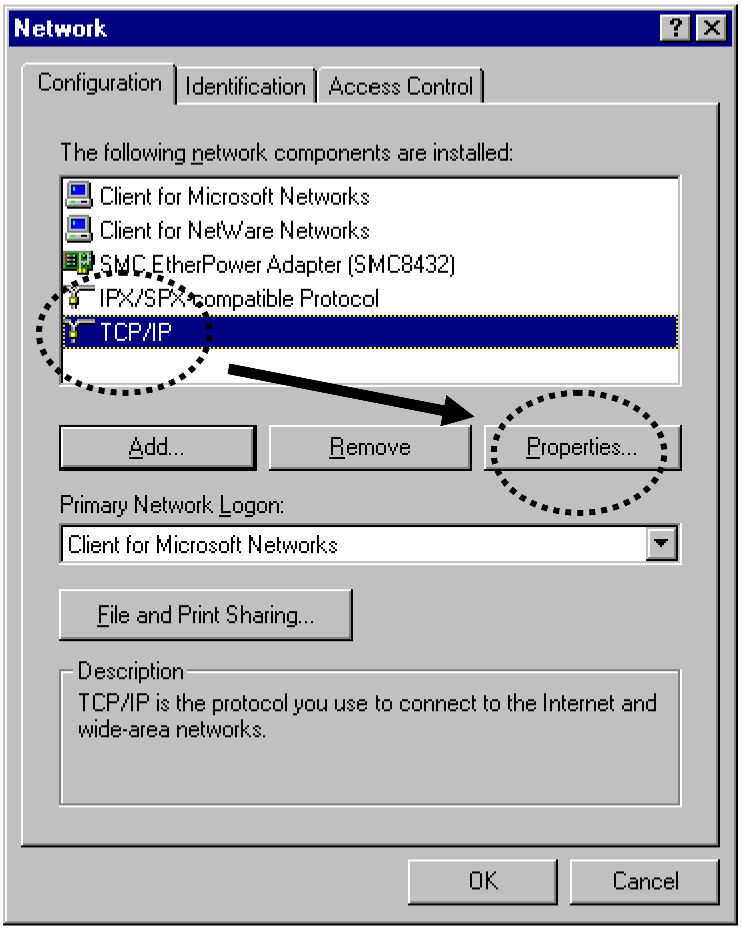
Before you can connect to the access point or client and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address:

If the operating system of your computer is….

Windows 95/98/Me	**- please go to section 2-2-1**
Windows 2000	**- please go to section 2-2-2**
Windows XP	**- please go to section 2-2-3**
Windows Vista	**please go to section 2-2-4**

2-2-1 Windows 95/98/Me IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network*** icon, and ***Network*** window will appear. Select 'TCP/IP', then click 'Properties'.



The following network components are installed:

- Client for Microsoft Networks
- Client for NetWare Networks
- SMC EtherPower Adapter (SMC8432)
- IPX/SPX-compatible Protocol
- TCP/IP

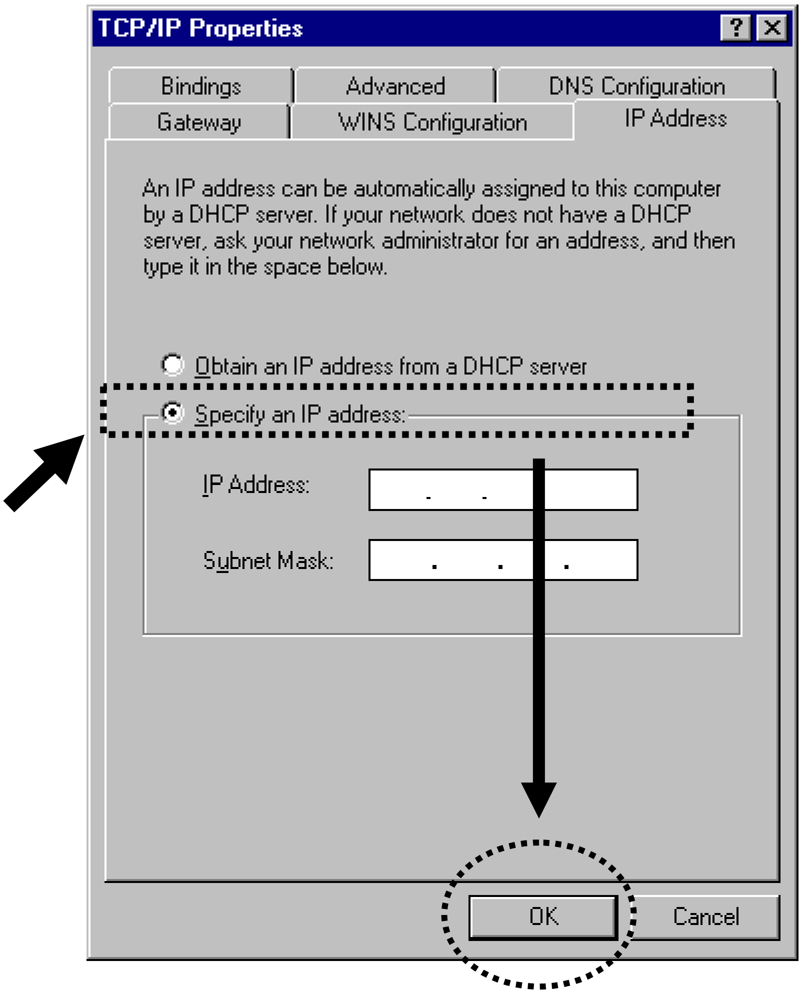
Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

2. Select ‘Specify an IP address’, then input the following settings in respective field:

IP address: 192.168.2.2
Subnet Mask: 255.255.255.0

click ‘OK’ when finish.



An IP address can be automatically assigned to this computer by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address from a DHCP server

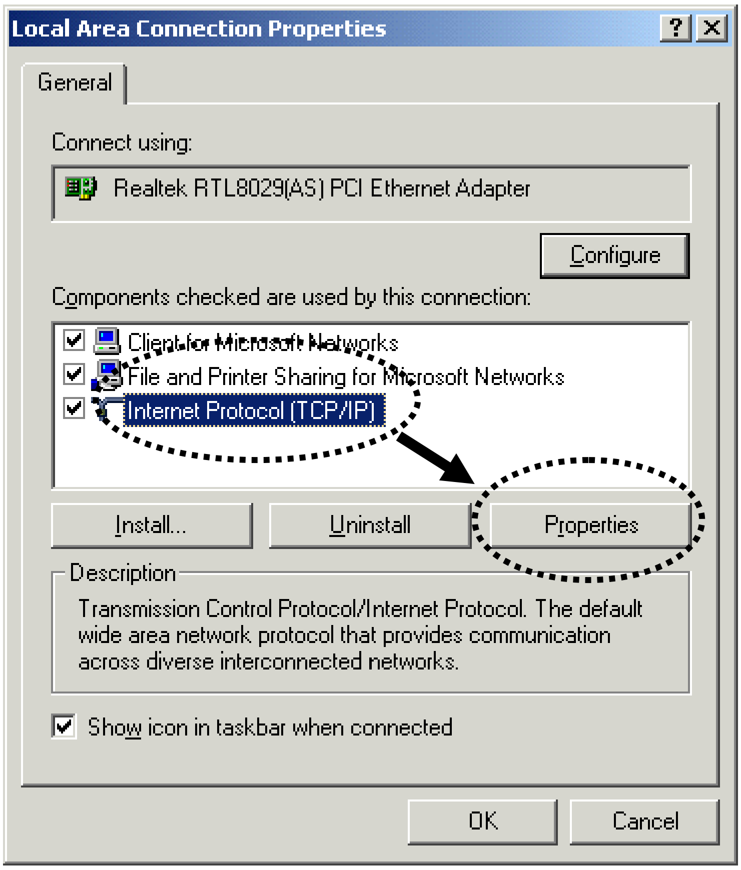
● Specify an IP address:

IP Address: . .

Subnet Mask: . . .

2-2-2 Windows 2000 IP address setup

1. Click ‘Start’ button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network and Dial-up Connections*** icon, double click ***Local Area Connection,*** and ***Local Area Connection Properties*** window will appear. Select ‘Internet Protocol (TCP/IP)’, then click ‘Properties’



Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

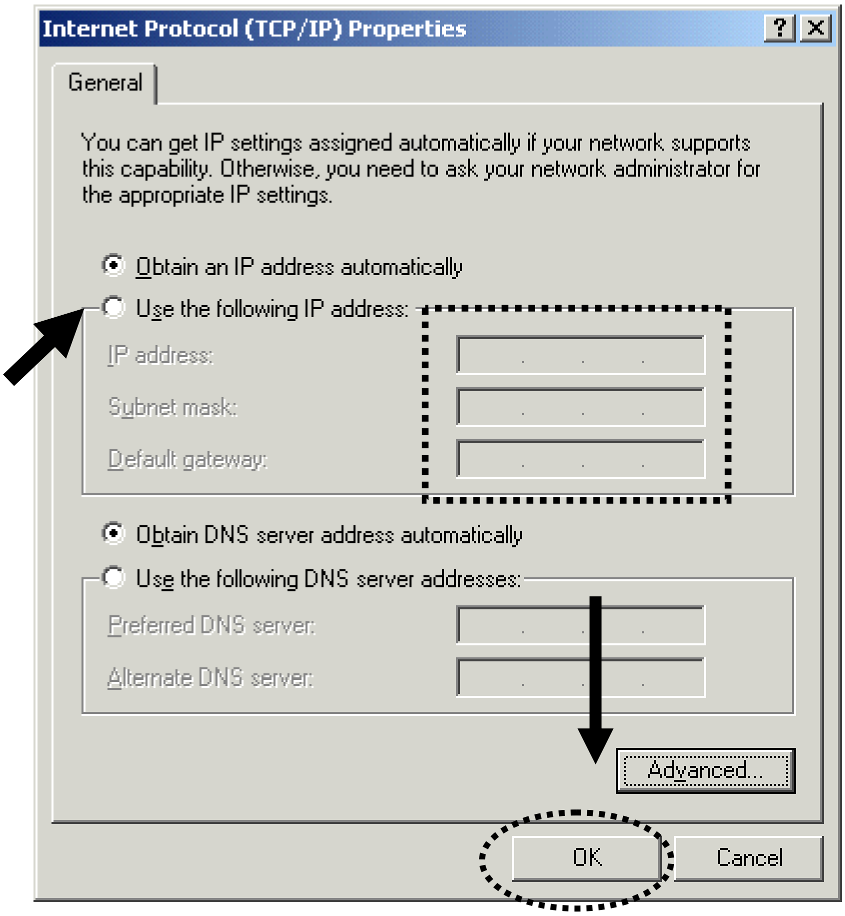
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

2. Select ‘Use the following IP address’, then input the following settings in respective field:

IP address: 192.168.2.2
Subnet Mask: 255.255.255.0

click ‘OK’ when finish.



Internet Protocol (TCP/IP) 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

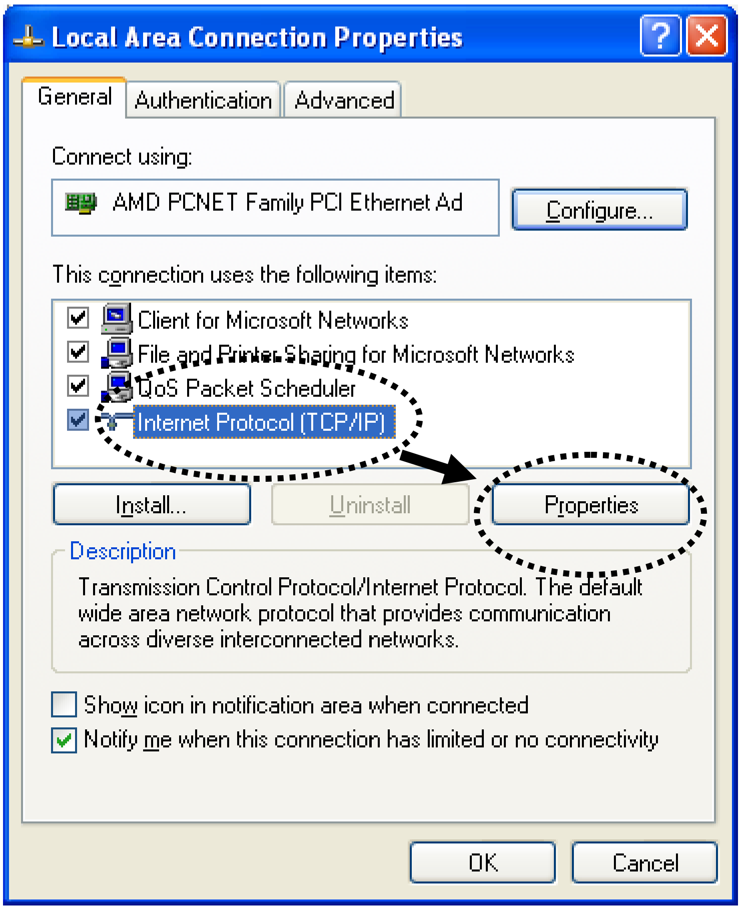
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

2-2-3 Windows XP IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Click ***Network and Internet Connections*** icon, click ***Network Connections,*** and then double-click ***Local Area Connection, Local Area Connection Status*** window will appear, and then click 'Properties'



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

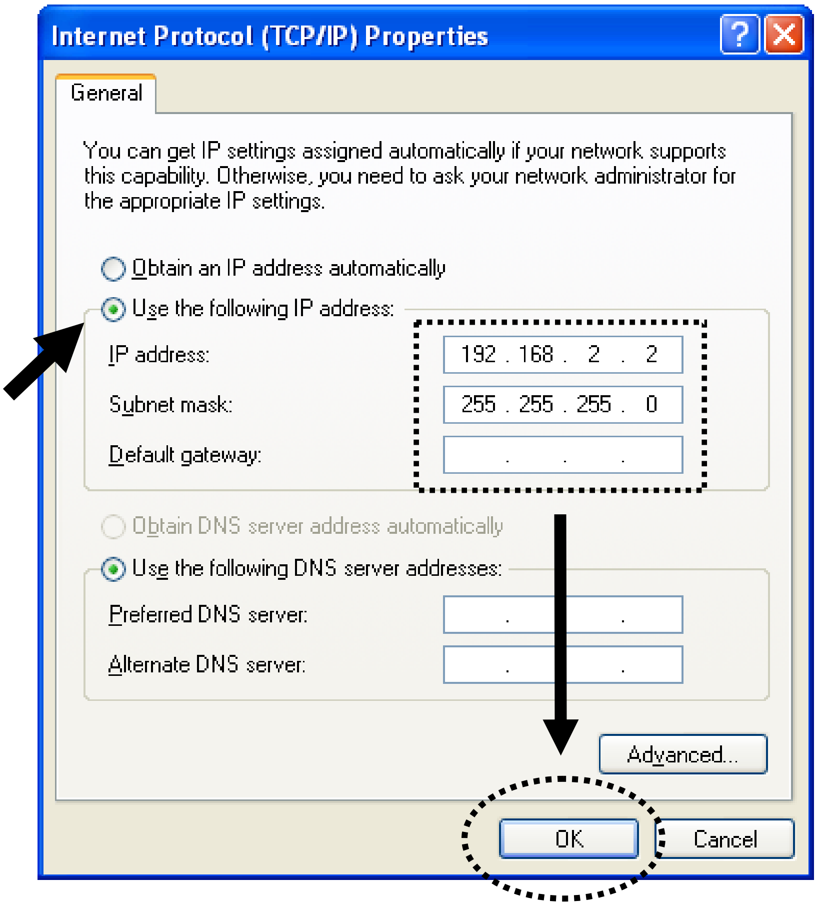
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

2. Select ‘Use the following IP address’, then input the following settings in respective field:

IP address: 192.168.2.2
Subnet Mask: 255.255.255.0

click ‘OK’ when finish.



Internet Protocol (TCP/IP) Properties

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: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

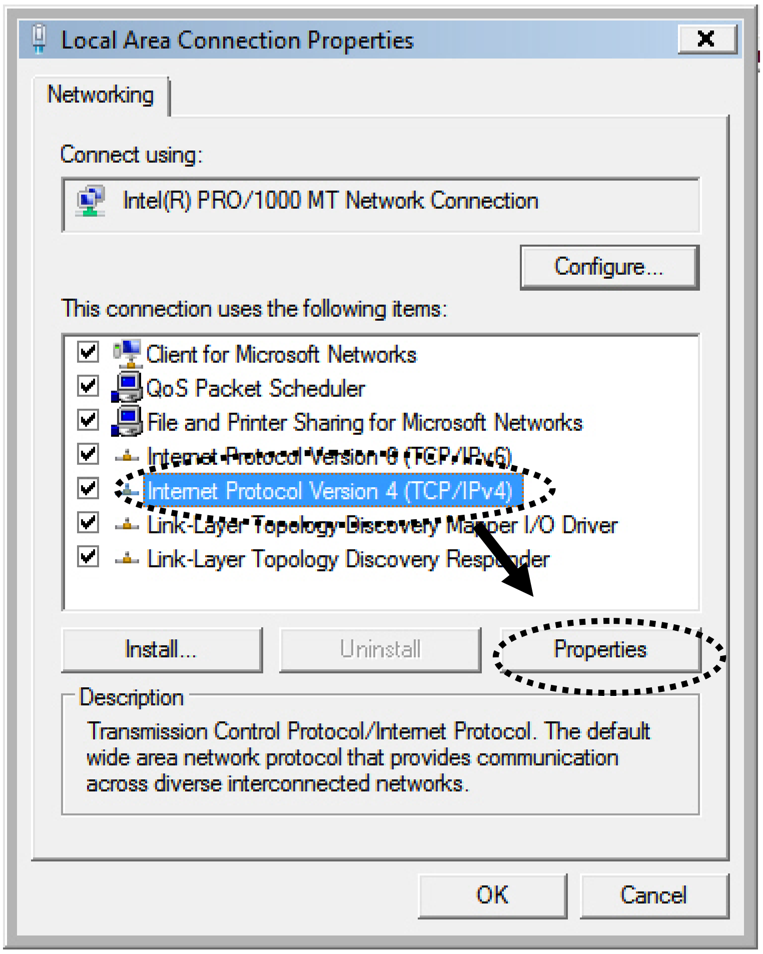
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

2-2-4 Windows Vista IP address setup

1. Click ‘Start’ button (it should be located at lower-left corner of your computer), then click control panel. Click ***View Network Status and Tasks***, then click ***Manage Network Connections***. Right-click ***Local Area Network, then select ‘Properties’***. ***Local Area Connection Properties*** window will appear, select ‘Internet Protocol Version 4 (TCP / IPv4), and then click ‘Properties’



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

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

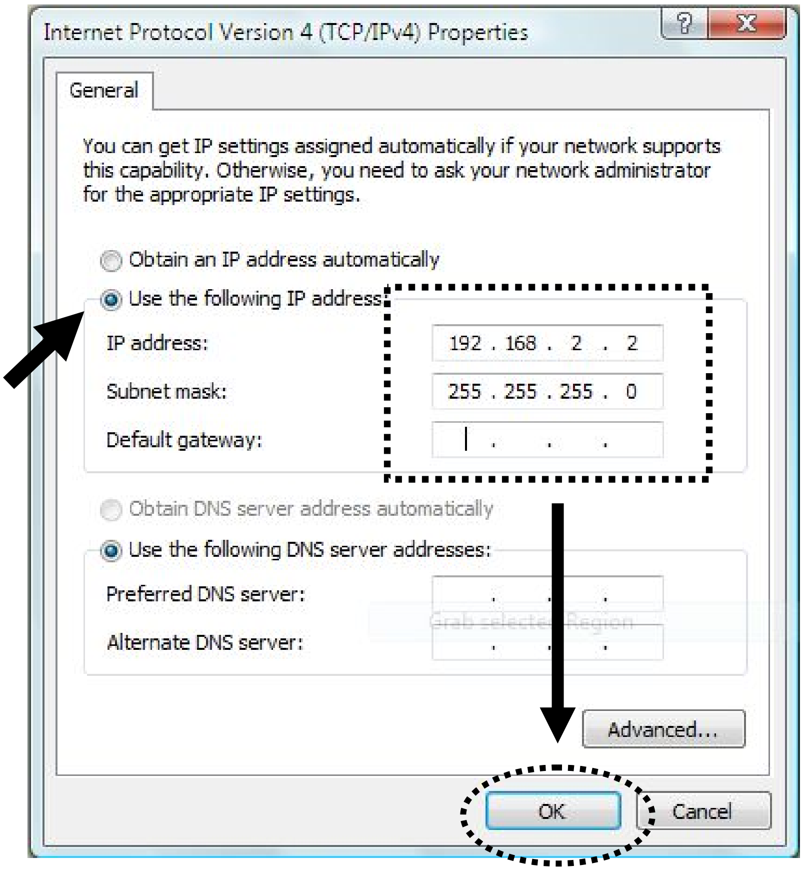
Description

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

2. Select ‘Use the following IP address’, then input the following settings in respective field:

IP address: 192.168.2.2
Subnet Mask: 255.255.255.0

click ‘OK’ when finish.



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: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

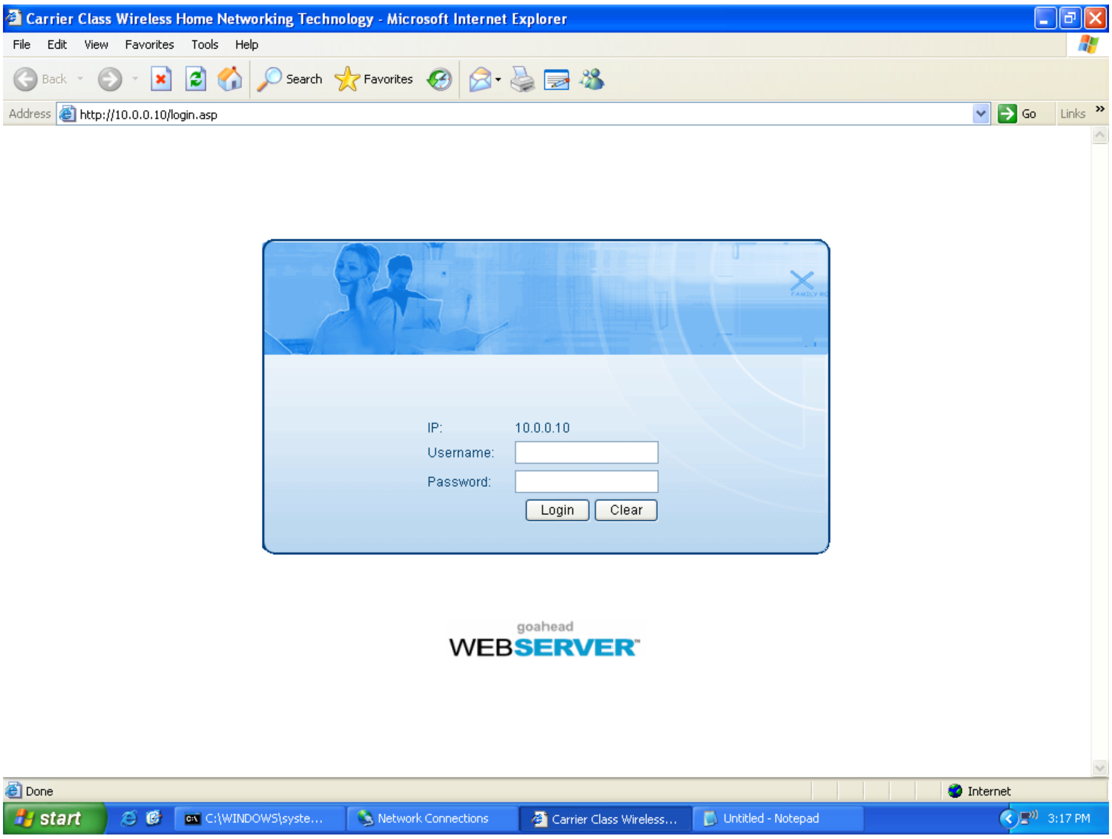
Alternate DNS server: . . .

2-2-5 Connecting to Web Management Interface

All functions and settings of the wireless access point and the wireless client must be configured via web management interface. Please start your web browser, and input the IP address in address bar, then press the 'Enter' key. The following message should be shown:

The default IP address of the wireless access Point and the wireless client are listed as below.

Access Point IP Address: 192.168.2.1
Client IP Address: 192.168.2.10

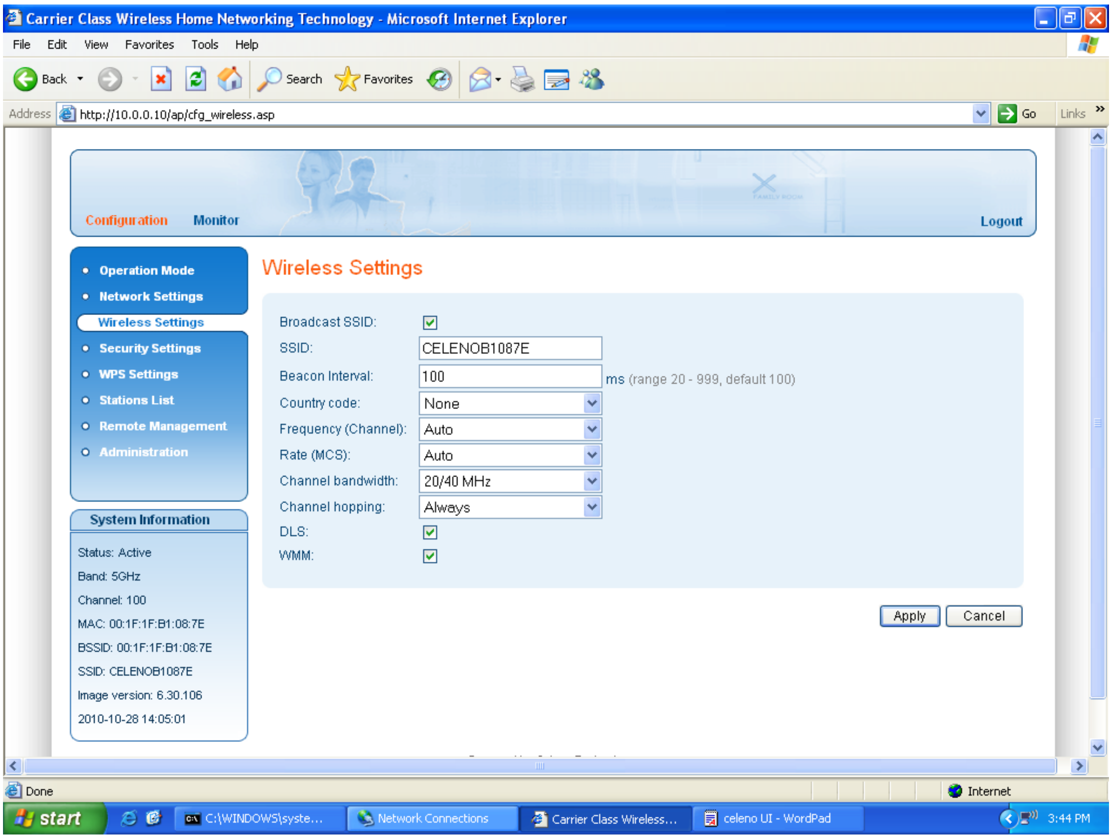


Carrier Class Wireless Home Networking Technology - Microsoft Internet Explorer

Address http://10.0.0.10/login.asp

IP: 10.0.0.10
Username:
Password:

Please input user name and password in the field respectively, default user name is 'admin', and default password is '1234', then press 'OK' button, and you can see the web management interface of this access point:


Carrier Class Wireless Home Networking Technology - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.0.0.10/ap/cfg_wireless.asp
Go Links
Configuration Monitor Logout
Operation Mode
Network Settings
Wireless Settings
Security Settings
WPS Settings
Stations List
Remote Management
Administration
Apply Cancel
Done Internet
start C:\WINDOWS\syste... Network Connections Carrier Class Wireless... celeno UI - WordPad 3:44 PM

Wireless Settings

Broadcast SSID:	☑
SSID:	CELENOB1087E
Beacon Interval:	100 ms (range 20 - 999, default 100)
Country code:	None
Frequency (Channel):	Auto
Rate (MCS):	Auto
Channel bandwidth:	20/40 MHz
Channel hopping:	Always
DLS:	☑
WMM:	☑

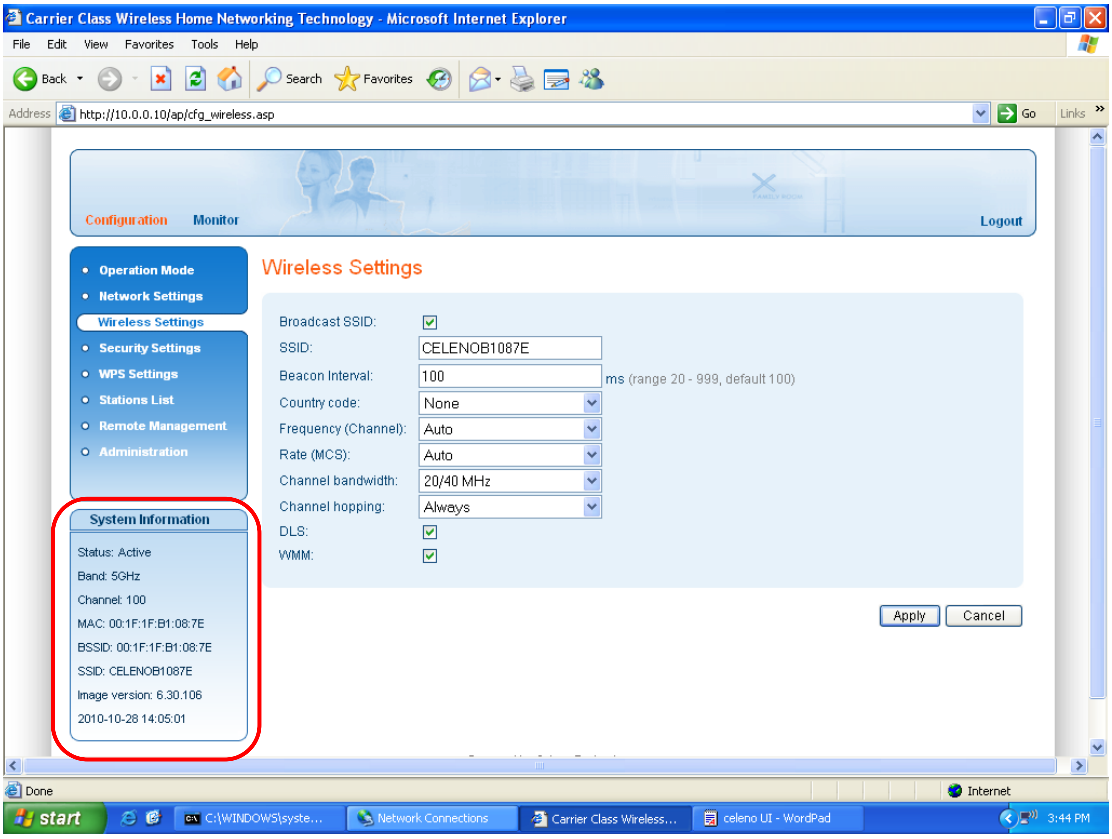
System Information

Status: Active
Band: 5GHz
Channel: 100
MAC: 00:1F:1F:B1:08:7E
BSSID: 00:1F:1F:B1:08:7E
SSID: CELENOB1087E
Image version: 6.30.106
2010-10-28 14:05:01

NOTE: If you can’t see the web management interface, and you’re being prompted to input user name and password again, it means you didn’t input username and password correctly. Please retype user name and password again. If you’re certain about the user name and password you type are correct, please go to ‘4-2 Troubleshooting’ to perform a factory reset, to set the password back to default value.

2-3 View system information

After you connected to the access point or client by web browser, you will see the web management interface. In the web management interface, you can view the system information of the device.



Wireless Settings

Broadcast SSID: ☑
SSID: CELENOB1087E
Beacon Interval: 100 ms (range 20 - 999, default 100)
Country code: None
Frequency (Channel): Auto
Rate (MCS): Auto
Channel bandwidth: 20/40 MHz
Channel hopping: Always
DLS: ☑
WMM: ☑

System Information

Status: Active
Band: 5GHz
Channel: 100
MAC: 00:1F:1F:B1:08:7E
BSSID: 00:1F:1F:B1:08:7E
SSID: CELENOB1087E
Image version: 6.30.106
2010-10-28 14:05:01

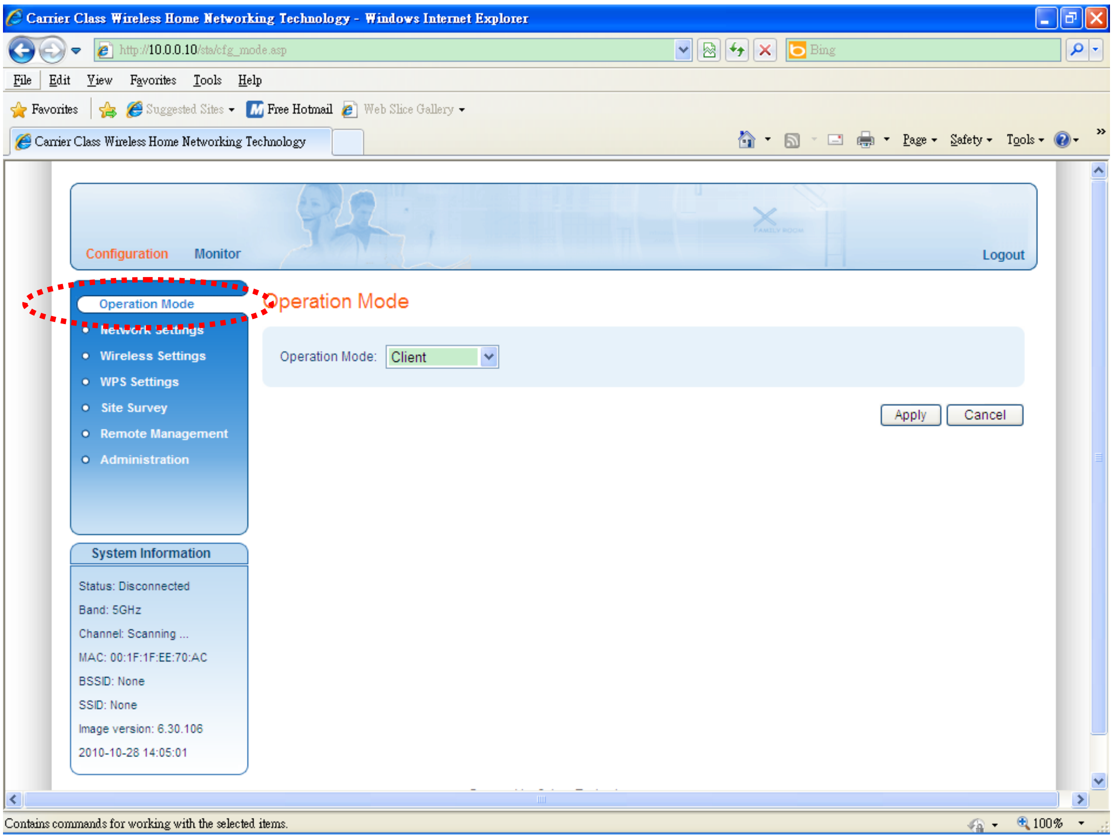
Here are descriptions of every item:

Item	Description
Mode	*Displays current wireless operating mode, for example: AP or Client mode.*
Status	*Display the status of the device.*
Band	*Indicates that the system is currently transmitting in the 5Ghz radio band.*
Channel	*Displays current wireless channel number*
MAC	*Displays the MAC address of LAN interface*
BSSID	*Displays current BSSID (a set of unique identification name of this device, it can not be modified by user)*
SSID	*Displays current SSID (the name used to identify*

	this wireless access point or client)
Image Version	*Displays the current firmware version of the device.*

2-4 Select an Operating Mode for the device

This wireless access point or wireless client can be operated in different modes; you can click ‘Operation Mode’ on the left of web management interface to select an operating mode you want to meet for different needs:


Carrier Class Wireless Home Networking Technology - Windows Internet Explorer
http://10.0.0.10/sta/cfg_mode.asp
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Free Hotmail
Web Slice Gallery
Carrier Class Wireless Home Networking Technology
Page Safety Tools
Configuration
Monitor
Logout
Operation Mode
Network Settings
Wireless Settings
WPS Settings
Site Survey
Remote Management
Administration
System Information
Apply
Cancel
Contains commands for working with the selected items.
100%

Operation Mode

Operation Mode: Client

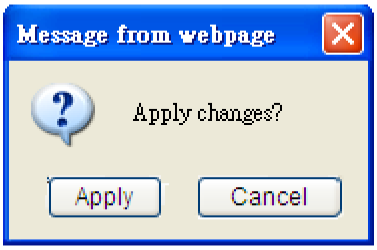
System Information

Status: Disconnected
Band: 5GHz
Channel: Scanning ...
MAC: 00:1F:1F:EE:70:AC
BSSID: None
SSID: None
Image version: 6.30.106
2010-10-28 14:05:01

There are two modes can be selected. Here is the description for these two modes.

Item	Description
AP	*Access point mode, allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.*
Client	*Select this mode and the TV or Set top box connected to the wireless device is able to connect to the access point wirelessly.*

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



Message from webpage

Apply changes?

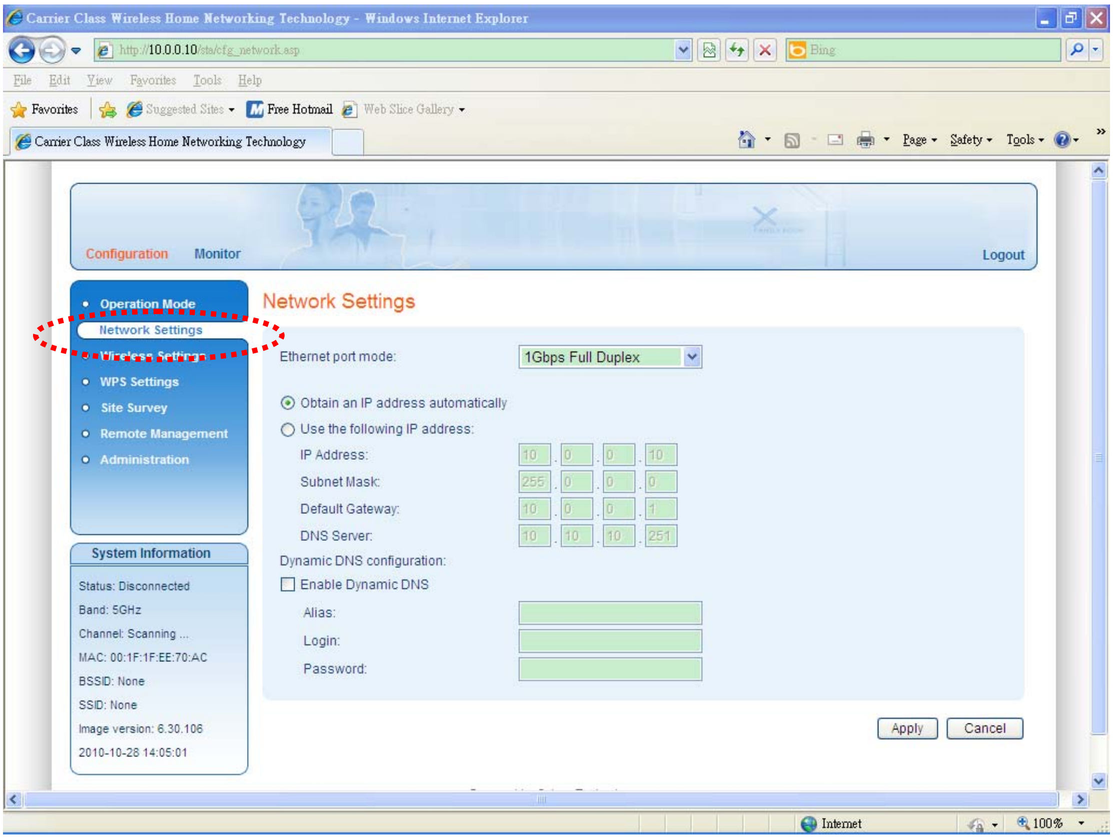
When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-5 Network Settings

You can change the IP address of this wireless access point or wireless client, so it can become a part of your local network. Please remember this address or you will not be able to connect the configuration menu of this wireless access point or wireless client.

Default IP address of access point is: 192.168.2.1 / Subnet Mask 255.255.255.0, and default IP address of wireless client is 192.168.2.10 / Subnet Mask 255.255.255.0, you can press and hold 'Reset' button over 10 seconds to change the IP address back to default value if you forget the IP address you set.

To change IP address, please click 'Network Settings' on the left of web management interface, and the following web page will be displayed:



Network Settings

Ethernet port mode: 1Gbps Full Duplex

● Obtain an IP address automatically

○ Use the following IP address:

IP Address: 10 . 0 . 0 . 10

Subnet Mask: 255 . 0 . 0 . 0

Default Gateway: 10 . 0 . 0 . 1

DNS Server: 10 . 10 . 10 . 251

Dynamic DNS configuration:

□ Enable Dynamic DNS

Alias:

Login:

Password:

System Information

Status: Disconnected

Band: 5GHz

Channel: Scanning ...

MAC: 00:1F:1F:EE:70:AC

BSSID: None

SSID: None

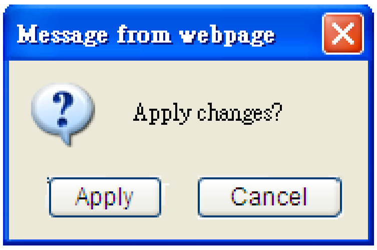
Image version: 6.30.106

2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Ethernet Port Mode	*The Ethernet Port of the device is fixed in 100Mbps.*
Obtain an IP address automatically	*When selected this item, the device acts as a DHCP client and obtains its IP properties automatically.*
Use the following IP address	*When selected this item, you have to fill the IP address settings in the following field.*
IP Address	*Please input the IP address of the device.*
Subnet Mask	*Please input the subnet mask of the device.*
Default Gateway	*Please input the default gateway of the device.*
DNS Server	*Please input the IP address of the DNS server for the device.*
Enable Dynamic DNS	*DDNS (Dynamic DNS) is an IP-to-Hostname mapping service for those Internet users who don't have a static (fixed) IP address. It will be a problem when such user wants to provide services to other users on Internet, because their IP address will vary every time when connected to Internet, and other user will not be able to know the IP address they're using at a certain time.* *If you have applied for a dynamic DNS account for the device, please select this item.*
Alias	*Please input the alias name for the dynamic DNS account.*
Login	*Input account or email of DDNS registration.*
Password	*Input the password to login for the DDNS service.*

After you finish with setting, please click 'Apply', and the following message will be displayed:



Message from webpage

Apply changes?

When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-6 Wireless Settings

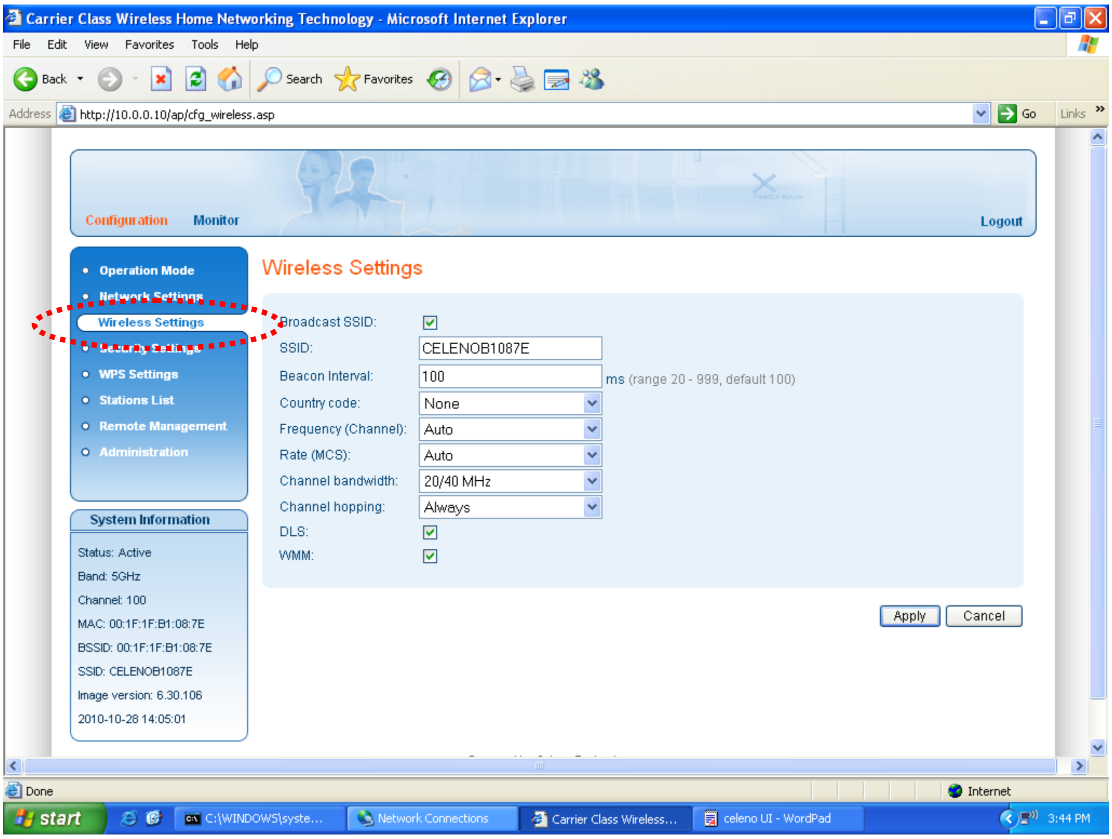
This wireless access point and the wireless client have many advanced wireless features. Please note that all settings listed here are for experienced users only, if you’re not sure about the meaning and function of these settings, please don’t modify them, or the wireless performance will be reduced.

The wireless settings for wireless access point and the wireless client are different. Please refer to the following two sections.

Wireless Access Point	**- please go to section 2-6-1**
Wireless Client	**- please go to section 2-6-2**

2-6-1 Wireless Access Point

You can click ‘Wireless Settings’ on the left of web management interface, and the following web page will be displayed:



http://10.0.0.10/ap/cfg_wireless.asp

Wireless Settings

Broadcast SSID: ☑

SSID: CELENOB1087E

Beacon Interval: 100 ms (range 20 - 999, default 100)

Country code: None

Frequency (Channel): Auto

Rate (MCS): Auto

Channel bandwidth: 20/40 MHz

Channel hopping: Always

DLS: ☑

WMM: ☑

Apply Cancel

System Information

Status: Active

Band: 5GHz

Channel: 100

MAC: 00:1F:1F:B1:08:7E

BSSID: 00:1F:1F:B1:08:7E

SSID: CELENOB1087E

Image version: 6.30.106

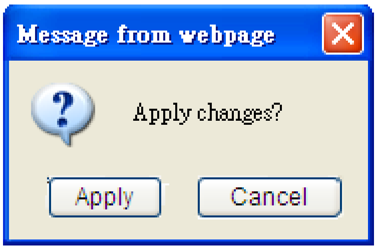
2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Broadcast SSID	*Decide if the wireless access point will broadcast its own SSID or not. You can hide the SSID of your wireless access point (set the option to 'Disable'), so only people those who know the SSID of your wireless access point can get connected.*
SSID	*Please input the SSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters.* ***PLEASE NOTE THAT ESSID IS CASE SENSITIVE.***
Beacon Interval	*Set the beacon interval of wireless radio.* ***Do not modify default value if you don't know what it is, default value is 100***
Country Code	*The available channels are different from countries. If you are in different country, please select the country code where you are located.* *Note: This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems.*
Frequency (Channel)	*Please select a channel number you wish to use. If you know a certain channel number is being used by other wireless access points nearby, please refrain from using the same channel number*
Rate(MCS)	*Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically,* ***it's not necessary to change this value unless you know what will happen after modification.***
Channel Bandwidth	*Select wireless channel bandwidth (bandwidth taken by wireless signals of this access point). It's suggested to select '20/40MHz'. Do not change*

	to '20 MHz' unless you know what it is.
Channel Hopping	*Determines the system behavior when interference is detected:* *Always – Change channel as soon as interference is detected on the current radio channel.* *Conditional – Change channel as soon as interference is detected only if no video is being streamed through the system.*
DLS	*When checked the system employs the direct link protocol to enable direct client to client communication. Use this option when client devices in your network can stream video to each other, such as in a Multi-Room DVR deployment.*

After you finish with setting, please click 'Apply', and the following message will be displayed:

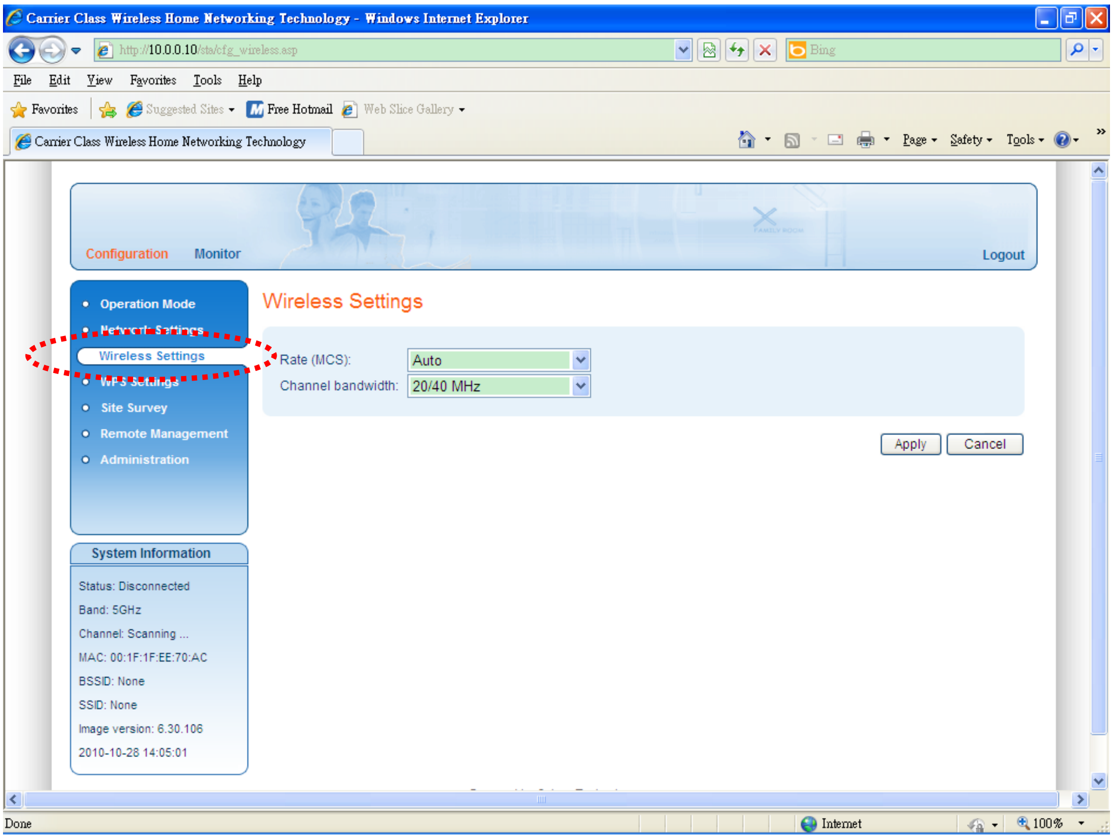

Message from webpage

Apply changes?

When you see this message, the settings you made is temporarily save. You can click 'Cancel' button to back to previous page, or click 'Apply' button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-6-2 Wireless Client

You can click ‘Wireless Settings’ on the left of web management interface, and the following web page will be displayed:



Wireless Settings

Rate (MCS): Auto

Channel bandwidth: 20/40 MHz

System Information

Status: Disconnected

Band: 5GHz

Channel: Scanning ...

MAC: 00:1F:1F:EE:70:AC

BSSID: None

SSID: None

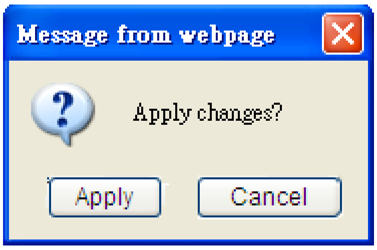
Image version: 6.30.106

2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Rate(MCS)	*Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically,* ***it’s not necessary to change this value unless you know what will happen after modification.***
Channel Bandwidth	*Select wireless channel bandwidth (bandwidth taken by wireless signals of this access point). It’s suggested to select ‘20/40MHz’. Do not change to ’20 MHz’ unless you know what it is.*

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



Message from webpage

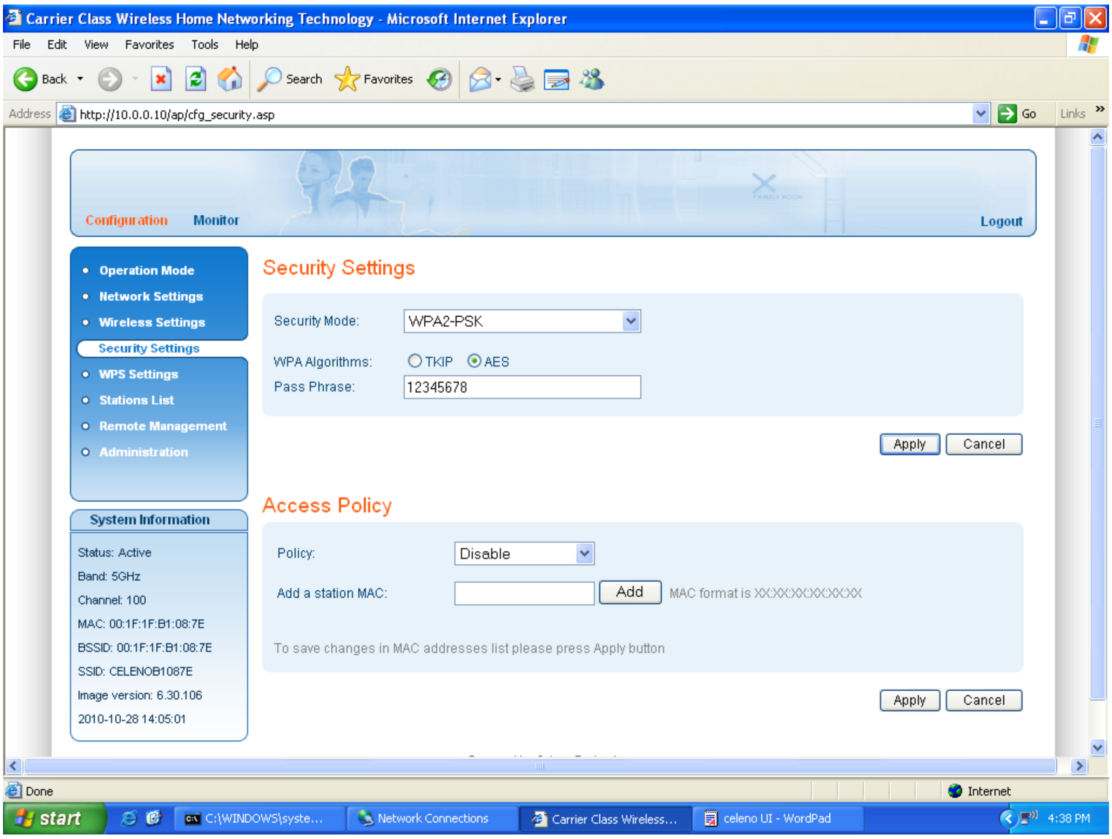
Apply changes?

When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-7 Security Settings (Access Point Only)

This wireless access point provides many types of wireless security (wireless data encryption). When you use data encryption, data transferred by radio signals in the air will become unreadable for those people who don’t know correct encryption key (encryption password). Besides security settings, you can also configure the access policy to filter the clients to connect to the access point.

You can click ‘Security Settings’ on the left of web management interface, and the following web page will be displayed:



Carrier Class Wireless Home Networking Technology - Microsoft Internet Explorer

Address: http://10.0.0.10/ap/cfg_security.asp

Security Settings

Security Mode: WPA2-PSK

WPA Algorithms: ○ TKIP ● AES

Pass Phrase: 12345678

Access Policy

Policy: Disable

Add a station MAC: MAC format is XX:XX:XX:XX:XX:XX

To save changes in MAC addresses list please press Apply button

System Information

Status: Active
Band: 5GHz
Channel: 100
MAC: 00:1F:1F:B1:08:7E
BSSID: 00:1F:1F:B1:08:7E
SSID: CELENOB1087E
Image version: 6.30.106
2010-10-28 14:05:01

There are three types of security levels you can select: Disable (no security - data encryption disabled), WEP, and WPA2 Pre-shared Key. Please refer to the following sections for detailed instructions.

Note: To be able to use Wireless Protected Setup (WPS) features (refer to Section 2-8), it is required that you enable the WPA2

Please remember it’s very important to set wireless security settings properly! Without a proper setting, hackers and intruders may gain access to your local network and do something bad to your computers and servers, which could cause serious problem.

There are several things you can do to improve wireless security:

1. Always enable data encryption. Only disable it when you want to open your wireless access point to the public.

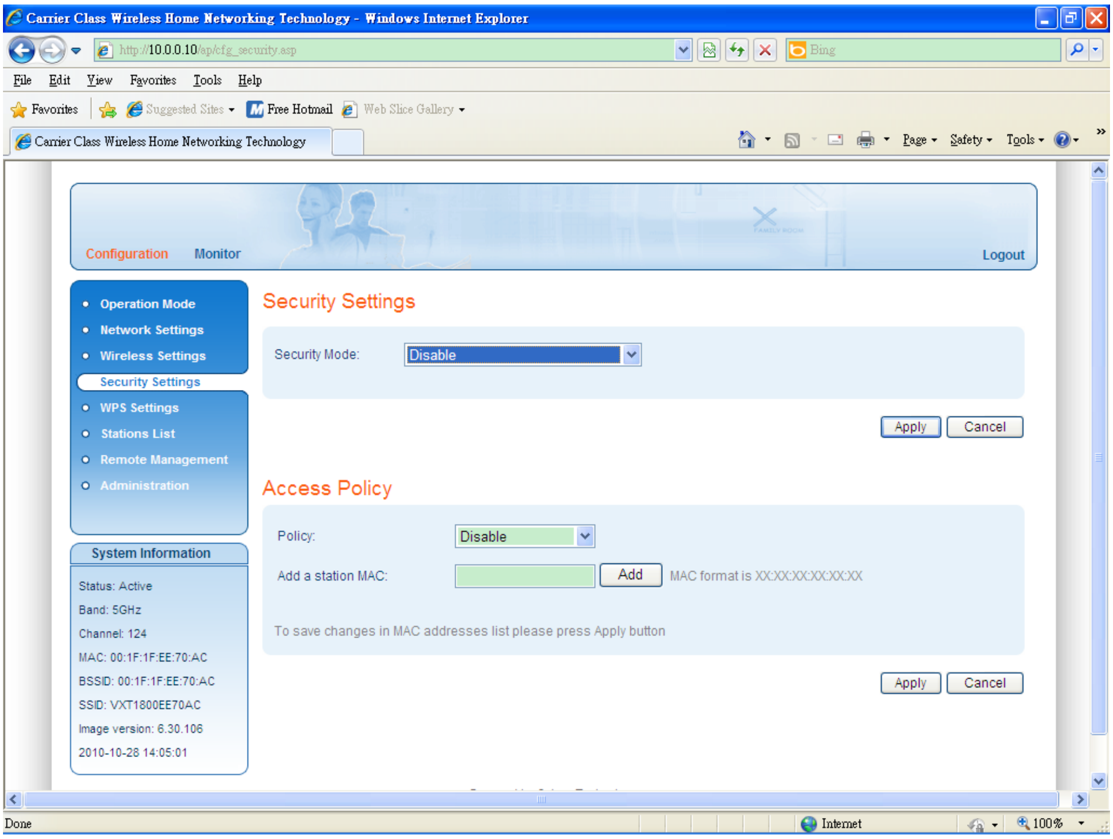
2. Never use simple words as encryption password. Use the random combination of symbols, numbers, and alphabets will greatly improve security.

3. Use WPA when possible - it's much safer than WEP.

4. Change encryption password when you’ve used it for too long time.

2-7-1 Disable Security

When you select ‘Disable’, wireless encryption for the network is disabled.



Security Settings

Security Mode: Disable

Access Policy

Policy: Disable

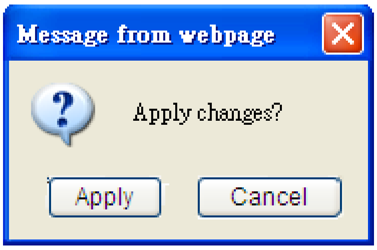
Add a station MAC: MAC format is XX:XX:XX:XX:XX:XX

To save changes in MAC addresses list please press Apply button

System Information

Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



Apply changes?

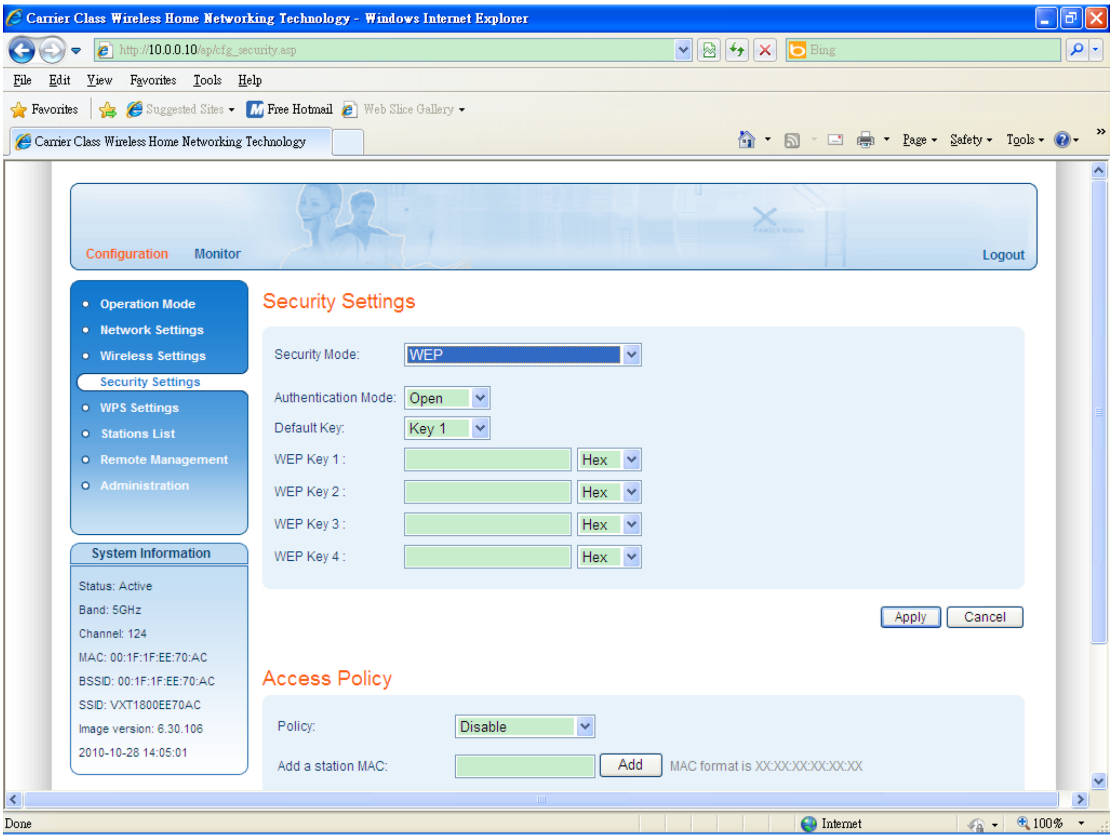
When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-7-2 WEP

WEP (Wired Equivalent Privacy) is a common encryption mode, it’s safe enough for home and personal use. But if you need higher level of security, please consider using WPA encryption (see next Section).

However, some wireless clients don’t support WPA, but only support WEP, so WEP is still a good choice for you if you have such kind of client in your network environment.

When you select ‘WEP’ as encryption type, the following messages will be displayed:



Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Security Settings

Security Mode: WEP
Authentication Mode: Open
Default Key: Key 1
WEP Key 1 : Hex
WEP Key 2 : Hex
WEP Key 3 : Hex
WEP Key 4 : Hex

Access Policy

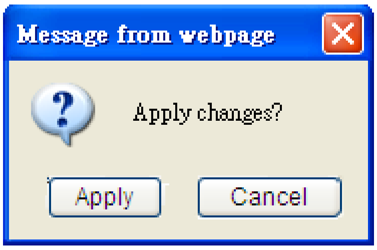
Policy: Disable
Add a station MAC: MAC format is XX:XX:XX:XX:XX:XX

Here are descriptions of every setup item:

Item	Description
Authentication Mode	*There are two authentication modes: Open and Shared. If ‘Open’ is selected, any device can authenticate to the AP without checking the WEP*

	key. If 'Shared' is selected, only devices with the WEP key can successfully authenticate to the access point.
Default Key	*You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***
WEP Key 1 to 4	*Input WEP key characters here, you can use any alphanumerical characters (0-9, a-z, and A-Z) and the key length is 5 or 13 characters if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f, and A-F and the key length is 10 or 26 characters Hex keys. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same with each other.*

After you finish with setting, please click 'Apply', and the following message will be displayed:



Message from webpage

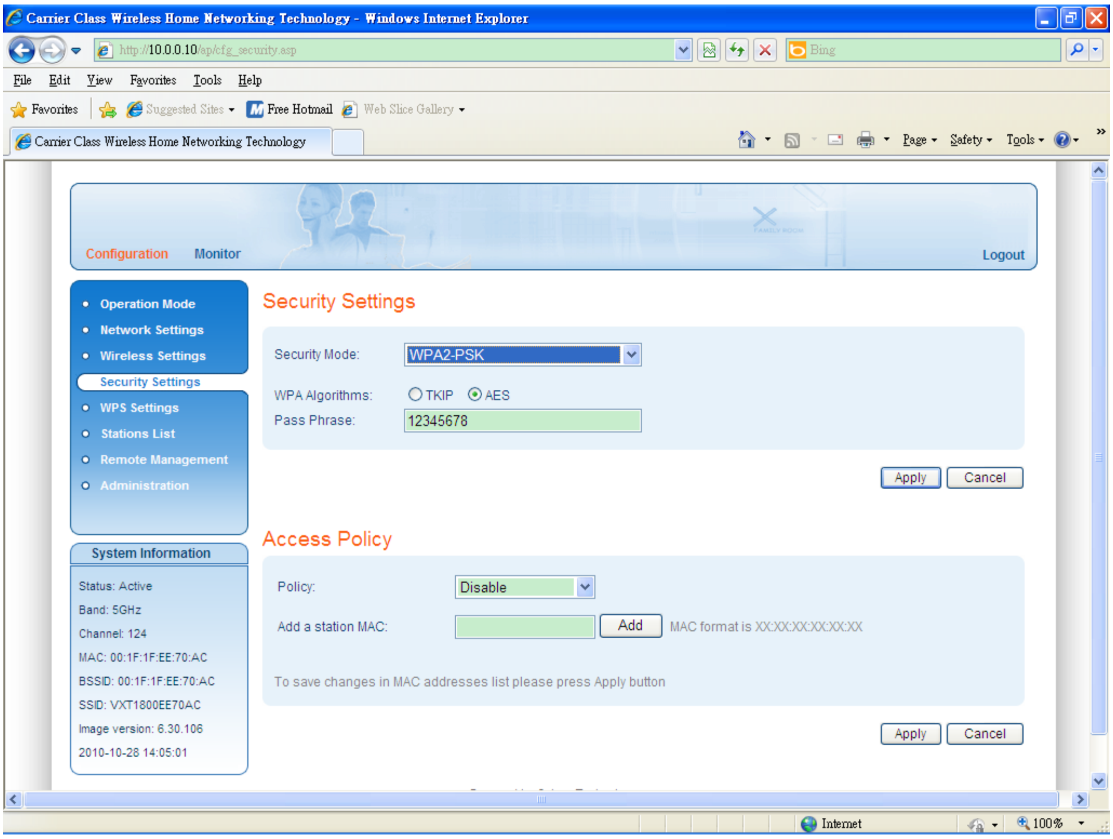
Apply changes?

When you see this message, the settings you made is temporarily save. You can click 'Cancel' button to back to previous page, or click 'Apply' button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-7-3 WPA2 Pre-shared Key

WPA2 Pre-shared key is the safest encryption method currently, and it’s recommended to use this encryption method to ensure the safety of your data.

When you select ‘WPA2 pre-shared key’ as encryption type, the following messages will be displayed:



Security Settings

Security Mode: WPA2-PSK

WPA Algorithms: ○ TKIP ● AES

Pass Phrase: 12345678

Access Policy

Policy: Disable

Add a station MAC:

MAC format is XX:XX:XX:XX:XX:XX

To save changes in MAC addresses list please press Apply button

System Information

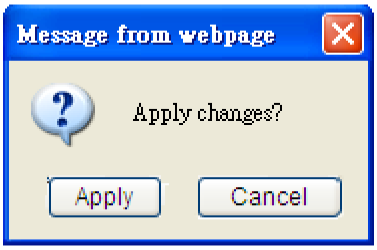
Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
WPS Algorithms	*Available options are: TKIP and AES. ‘AES’ is much safer for the network. You can select one of them, but you have to make sure your wireless client support the algorithms you selected.*
Pre-shared Key Format	*Please select the format of pre-shared key here, available options are ‘Passphrase’ (8 to 63 alphanumerical characters) and ‘Hex (64*

	hexadecimal characters – 0 to 9 and a to f).
Pass Phrase	*Please input 8 to 63 alphanumerical characters as the pass phrase key. For security reason, don't use simple words).*

After you finish with setting, please click 'Apply', and the following message will be displayed:



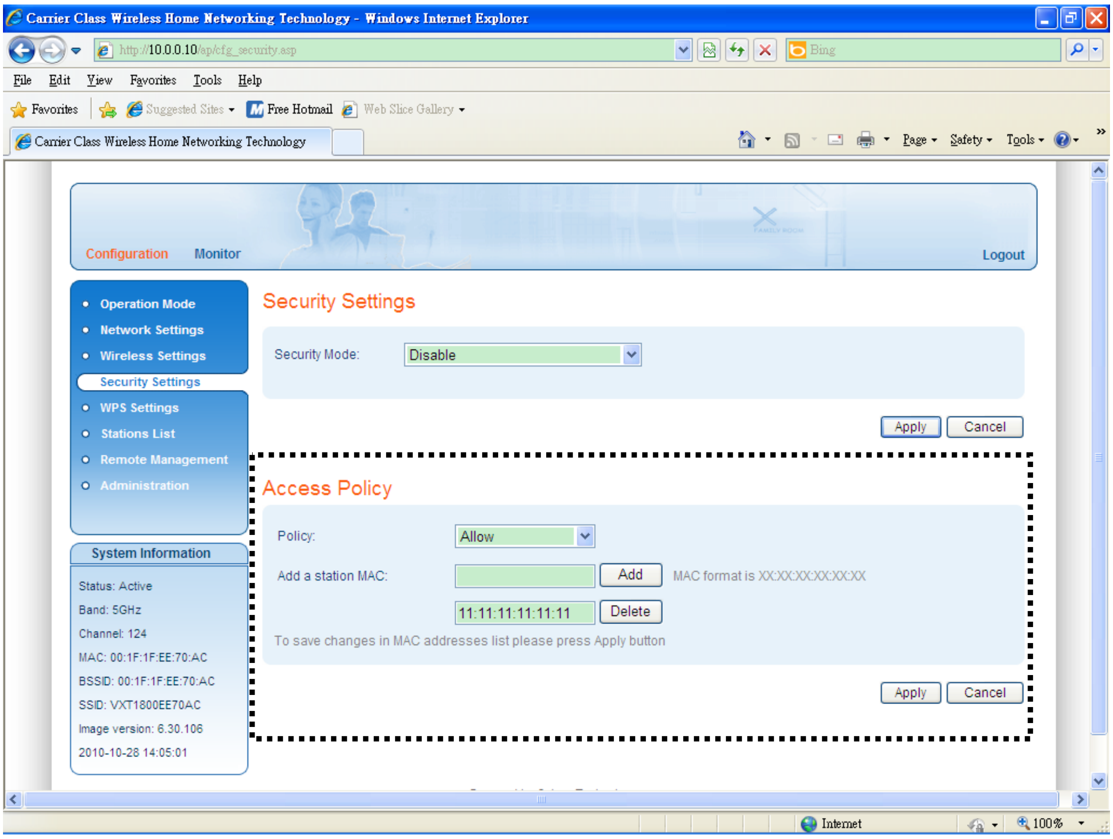
Message from webpage

Apply changes?

When you see this message, the settings you made is temporarily save. You can click 'Cancel' button to back to previous page, or click 'Apply' button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-7-4 Access Policy

Another security measure you can use to keep hackers and intruders away is ‘Access Policy’. You can pre-define a list, which contains MAC addresses of the wireless clients you want to deny accessing or allow to access.



Carrier Class Wireless Home Networking Technology - Windows Internet Explorer

http://10.0.0.10/ap/cfg_security.asp

Security Settings

Security Mode: Disable

Access Policy

Policy: Allow

Add a station MAC: MAC format is XX:XX:XX:XX:XX:XX

11:11:11:11:11:11

To save changes in MAC addresses list please press Apply button

System Information

Status: Active

Band: 5GHz

Channel: 124

MAC: 00:1F:1F:EE:70:AC

BSSID: 00:1F:1F:EE:70:AC

SSID: VXT1800EE70AC

Image version: 6.30.106

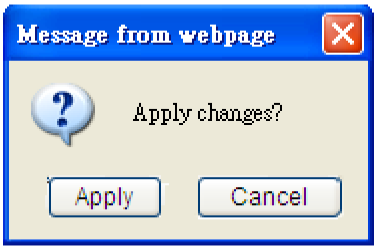
2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Policy	*There are three policies including Disable, Allow and Reject. When ‘Disable’ is selected, all wireless clients can access to the access point. When ‘Allow’ is selected, only the wireless clients contain MAC address in the list are allowing to access the access point. When ‘Reject’ is selected, the wireless clients contain MAC address in the list will be rejected to access the access point.*
Add a Station MAC	*Input the MAC address of the wireless client into the field and then click ‘Add’ button to add to the*

	list. MAC address format is 12 digits of hexadecimal key. Only characters 0-9, a-f, and A-F are allowed. *If you want to delete one of the MAC addresses, click 'Delete' button by the side of the selected column.*

After you finish with setting, please click 'Apply', and the following message will be displayed:



Apply changes?

When you see this message, the settings you made is temporarily save. You can click 'Cancel' button to back to previous page, or click 'Apply' button to restart the wireless access point or the wireless client and the changes will take effect after about 30 seconds.

2-8 WPS Settings

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and the wireless access point. You don't have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client, you only have to press a button on wireless client and this access point, and the WPS will do the setup for you.

The WPS settings for wireless access point and the wireless client are different. Please refer to the following two sections.

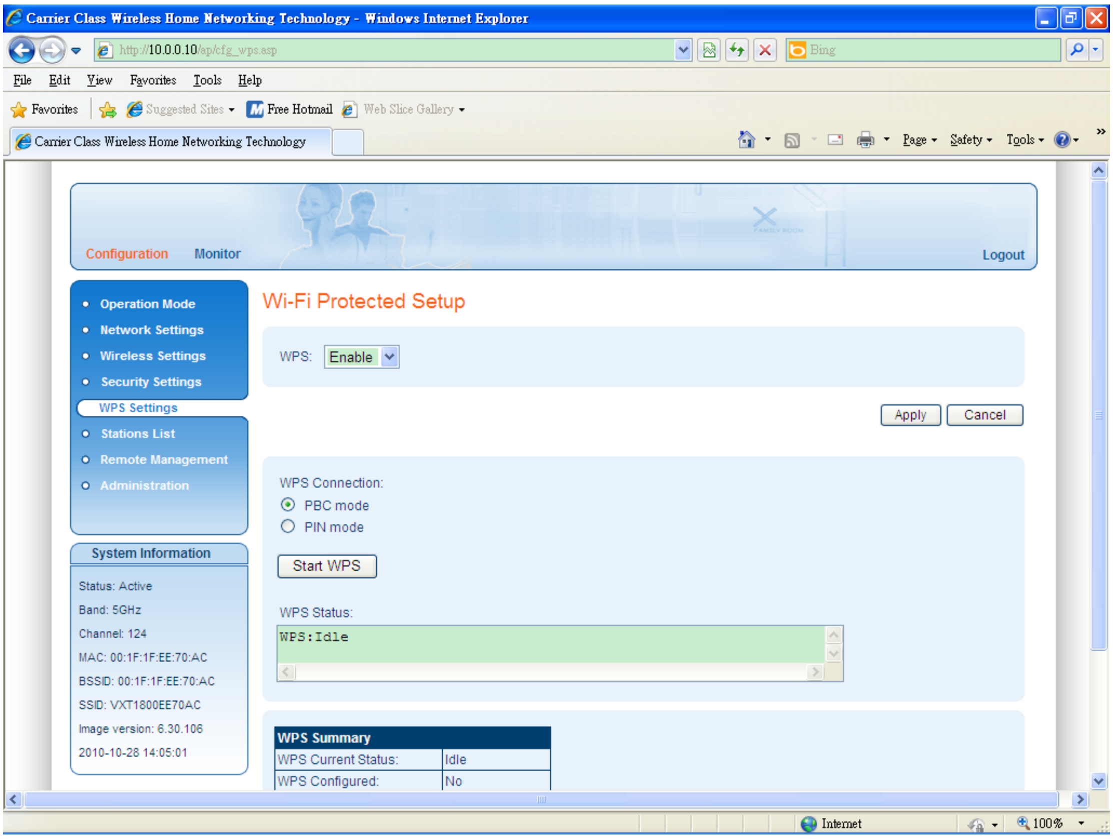
Wireless Access Point	**- please go to section 2-8-1**
Wireless Client	**- please go to section 2-8-2**

2-8-1 Wireless Access Point

This access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch this access point to WPS mode and push a specific button on the wireless client to start WPS mode. You can push WPS button of this access point, or click 'Start WPS' button in the web configuration interface to do this; if you want to use PIN code, you have to provide the PIN code of the wireless client you wish to connect to this access point and then switch the wireless client to WPS mode.

Note: WPS function of this access point will not work for those wireless clients do not support WPS.

To use WPS function to set encrypted connection between this access point and WPS-enabled wireless client by WPS, click 'WPS Settings' on the left of web management menu, and the following information will be displayed:



Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Wi-Fi Protected Setup

WPS: Enable

WPS Connection:
● PBC mode
○ PIN mode

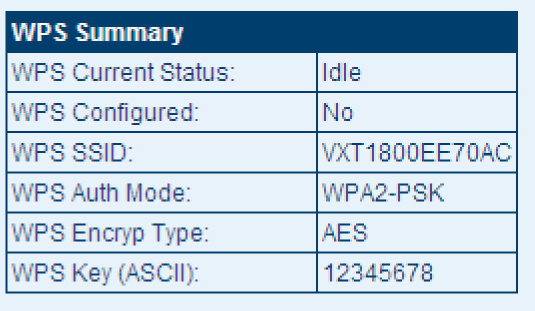
WPS Status:

```
WPS:Idle
```

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No

Here are descriptions of every setup item:

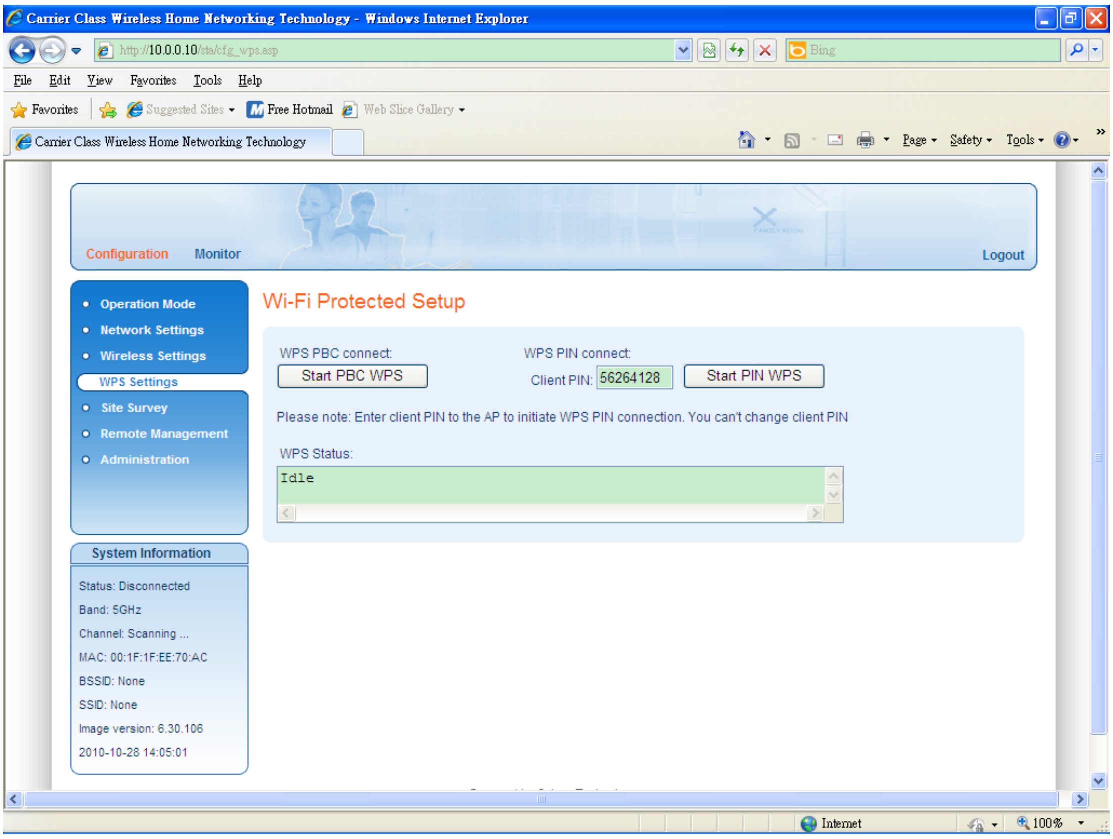
Item	Description
WPS	*Select 'Enable' or 'Disable' to activate or deactivate WPS function.*
PBC mode	*When you select 'PBC mode', click 'Start WPS' to start Push-Button style WPS setup procedure. This access point will wait for WPS requests from wireless clients for 2 minutes. The 'WPS' LED on the access point will be kept flashing for 2 minutes when this access point is waiting for incoming WPS request.*
PIN mode	*Please input the PIN code of the wireless client you wish to connect, and click 'Start WPS' button. The 'WPS' LED on the access point will be kept flashing when this access point is waiting for incoming WPS request.*
WPS Status	*All information related to WPS will be displayed here, they're helpful when you're setting up*

	connections by WPS.
WPS Summary	*The WPS Summary table displays the WPS status for the access point.* *WPS Current Status: Display if the WPS function is in process or in idle status.* *WPS Configured: If you have set the security before WPS process, here will display 'Yes' and the security settings of the WPS connection will follow your settings. If not, here will display 'No' and the access point will random generate a set of security settings for the WPS connection.* *WPS SSID: Display the SSID setting for the WPS connection.* *WPS Auth Mode: Display the authentication setting for the WPS connection.* *WPS Encryp Type: Display the encryption setting for the WPS connection.* *WPS Key (ASCII): Display the WPS key setting for the WPS connection.*  WPS Summary WPS Current Status: Idle WPS Configured: No WPS SSID: VXT1800EE70AC WPS Auth Mode: WPA2-PSK WPS Encryp Type: AES WPS Key (ASCII): 12345678

NOTE: When you're using PBC type WPS setup, you must press 'PBC or WPS' button (hardware or software) of wireless client within 120 seconds; if you didn't press PBC or WPS button of wireless client within this time period, please activate PBC WPS function of this access point again.

2-8-2 Wireless Client

This wireless client supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch the WPS-enabled access point to WPS mode and push a specific button on the access point and the wireless client to start WPS connection. You can push WPS button of this client, or click 'Start PBC WPS' button in the web configuration interface to do this. If you want to use PIN code, you have to provide the PIN code number of the wireless client to the access point as the WPS PIN code (Please refer to section 2-8-1 for the instructions about how to do this in access point) and then click 'Start PIN WPS' button in the web configuration interface to do this.



Wi-Fi Protected Setup

WPS PBC connect:

WPS PIN connect:

Client PIN: 56264128

Please note: Enter client PIN to the AP to initiate WPS PIN connection. You can't change client PIN

WPS Status:

Idle

System Information

Status: Disconnected

Band: 5GHz

Channel: Scanning ...

MAC: 00:1F:1F:EE:70:AC

BSSID: None

SSID: None

Image version: 6.30.106

2010-10-28 14:05:01

Here are descriptions of every setup item:

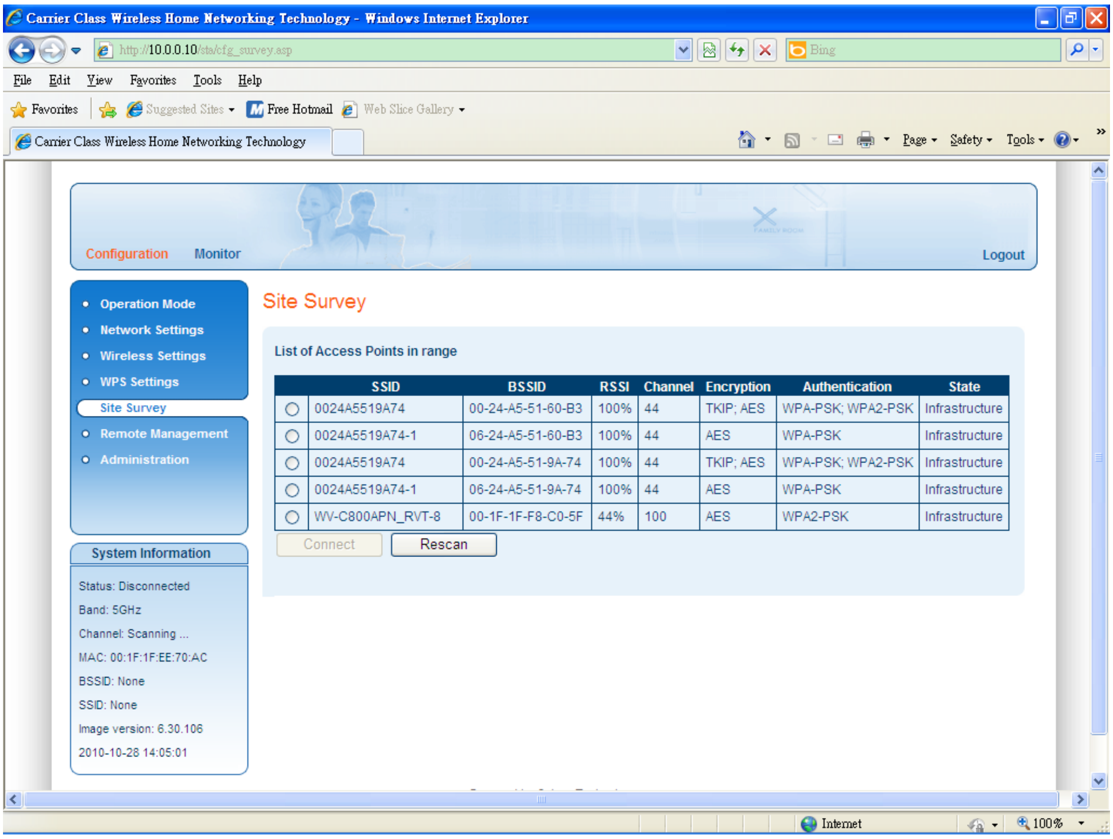
Item	Description
Start PBC WPS	*Click the 'Start PCB WPS' button to enable PBC WPS connection of the wireless client.*
Client PIN	*Here displays the PIN number of the wireless*

	client. Please remember the PIN number and input it in the access point while you want to enable PIN WPS connection.
Start PIN WPS	*Click the 'Start PIN WPS' button to enable PIN WPS connection of the wireless client.*
WPS Status	*Display the current WPS status of the wireless client.*

2-9 Site Survey (Client Only)

The site survey page allows you to find the access points or routers nearby. You can choose one of the access points or routers you wish to connect and then click ‘Connect’ button to build up the wireless connection. If you do not find the devices you wish to connect, move closer to the device and click ‘Prescan’ to research again.

To do site survey, please click ‘Site Survey’ on the left of web management menu, and the following information will be displayed:



Site Survey

List of Access Points in range

	SSID	BSSID	RSSI	Channel	Encryption	Authentication	State
○	0024A5519A74	00-24-A5-51-60-B3	100%	44	TKIP; AES	WPA-PSK; WPA2-PSK	Infrastructure
○	0024A5519A74-1	06-24-A5-51-60-B3	100%	44	AES	WPA-PSK	Infrastructure
○	0024A5519A74	00-24-A5-51-9A-74	100%	44	TKIP; AES	WPA-PSK; WPA2-PSK	Infrastructure
○	0024A5519A74-1	06-24-A5-51-9A-74	100%	44	AES	WPA-PSK	Infrastructure
○	WV-C800APN_RVT-8	00-1F-1F-F8-C0-5F	44%	100	AES	WPA2-PSK	Infrastructure

System Information

Status: Disconnected
Band: 5GHz
Channel: Scanning ...
MAC: 00:1F:1F:EE:70:AC
BSSID: None
SSID: None
Image version: 6.30.106
2010-10-28 14:05:01

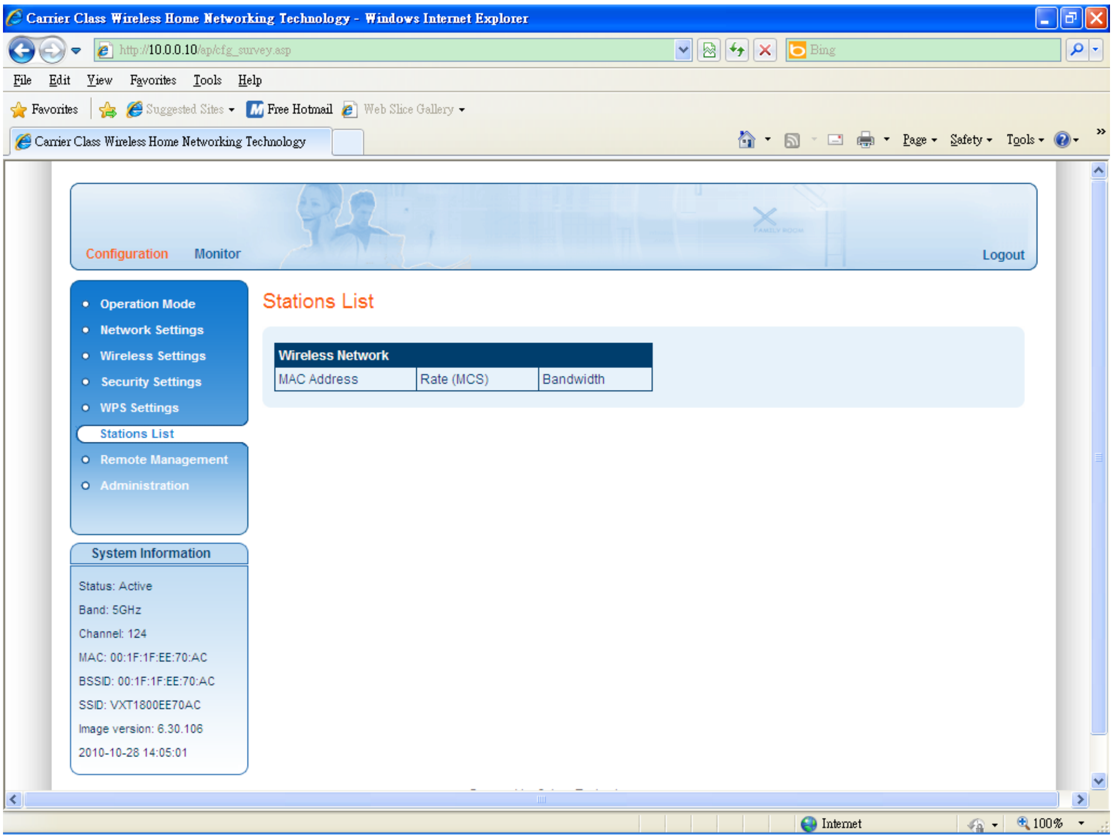
Here are descriptions of every setup item on the list:

Item	Description
SSID	*Display the SSID of the access points or routers.*
BSSID	*Display the BSSID of the access points or routers.*
RSSI	*RSSI indicates the signal strength of the access points or routers. The percentage number is higher means the signal strength is better.*

Channel	*Display the channel setting of the access points or routers.*
Authentication	*Display the authentication setting of the access points or routers.*
State	*It indicates if the access point or router is an 'Infrastructure' or 'Ad Hoc' network connection.*

2-10 Stations List (Access Point Only)

The station list page presents a list of wireless clients connected to the access point. To check the station list, please click ‘Station List’ on the left of the web management menu, and the following information will be displayed:



Stations List

Wireless Network		
MAC Address	Rate (MCS)	Bandwidth

System Information

Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Mac Address	*Display the Mac address of the associated client.*
Rate (MCS)	*Display the data rate that the wireless client is connecting to the access point.*
Bandwidth	*Display the bandwidth that the access point uses while sending data to the wireless client.*

2-11 Remote Management

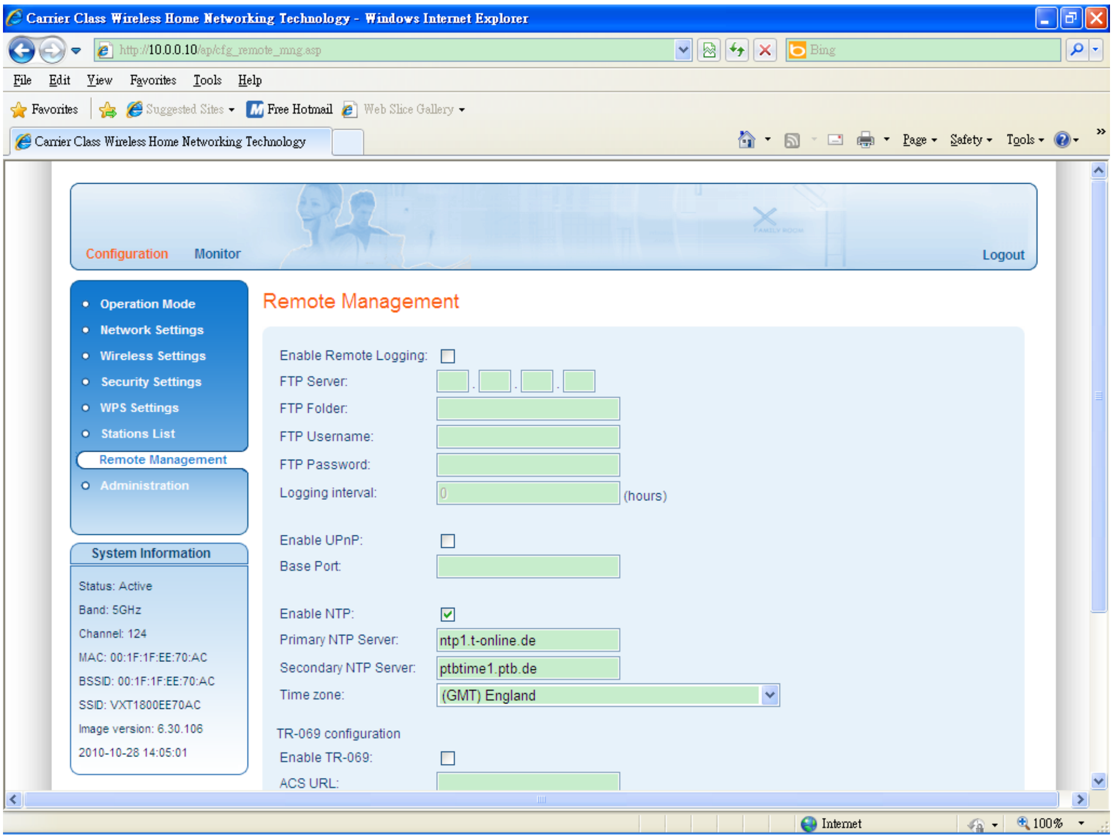
The wireless access point and the wireless client are able to support remote management which is allowing access the device from Internet.

The remote management settings for wireless access point and the wireless client are different. Please refer to the following two sections.

Wireless Access Point	**- please go to section 2-11-1**
Wireless Client	**- please go to section 2-11-2**

2-11-1 Wireless Access Point

This wireless access point supports record logs in FTP server, UPnP, NTP server and TR-069 features for remote management. Click 'Remote Management' on the left of the web management menu and the following information will be displayed:



System Information

Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Remote Management

Enable Remote Logging: ☐
FTP Server: . . .
FTP Folder:
FTP Username:
FTP Password:
Logging interval: 0 (hours)

Enable UPnP: ☐
Base Port:

Enable NTP: ☑
Primary NTP Server: ntp1.t-online.de
Secondary NTP Server: ptbtime1.ptb.de
Time zone: (GMT) England

TR-069 configuration
Enable TR-069: ☐
ACS URL:

Here are descriptions of every setup item:

Item	Description
Enable Remote Logging	*Enable or disable remote logging to the FTP Server you have assigned.*
FTP Server	*Please input the IP address of the FTP server onto which the logs of the access point will be uploaded.*
FTP Folder	*Please input the folder name into which the logs will be uploaded.*
FTP Username	*Please input the FTP username for logging.*
FTP Password	*Please input the FTP password for logging.*
Logging Interval	*The period in hours of the scheduled log uploads.*
Enable UPnP	*When you enable UPnP function, you are able to access the home gateway device and configure its port mapping table to enable accessing the access point remotely.*
Base Port	*The port at the Home Gateway that the device will be mapped to. In case that the selected port is already mapped in the gateway, the next available port will be used. When you want to access the access point remotely, you can enter 'http://the router's public IP address: port number'.*
Enable NTP	*When the function is enabled, the access point uses NTP protocol to obtain date & time.*
NTP Server	*There are several NTP servers are available on Internet. It is able to provide the date and time information to the device through NTP protocol. Please input the IP address of the NTP server here.*
Time Zone	*Please press* ⌄ *button, a drop-down list will be shown, and you can choose a time zone of the location you live.*
Enable TR-069	*TR-069 is a management protocol using by ISP service provider to management the end-user network devices remotely. You can enable this function if it is required by your ISP service provider.*
ACS URL	*ACS server is a device deployed at ISP service*

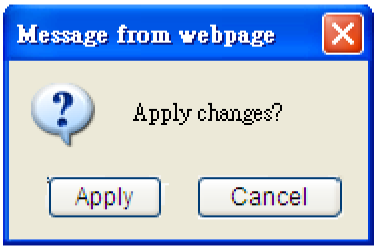
	provider and it includes auto-provisioning and remote management features for the residential devices. Please input the IP address of the ACS Server.
ACS Username	*Please input the username for ACS server authentication.*
ACS Password	*Please input the password for ACS server authentication.*
Periodic Inform Enable	*Enable or disable to receive the information from ACS server.*
Periodic Inform Interval	*The period in seconds of receiving the information from ACS server.*

NOTE: Following are some available NTP servers on internet:

129.6.15.28 (time-a.nist.gov)
132.163.4.101 (time-a.timefreq.bldrdoc.gov)
131.107.1.10 (time-nw.nist.gov)

If you found that the time of access point is incorrect, try another one.

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



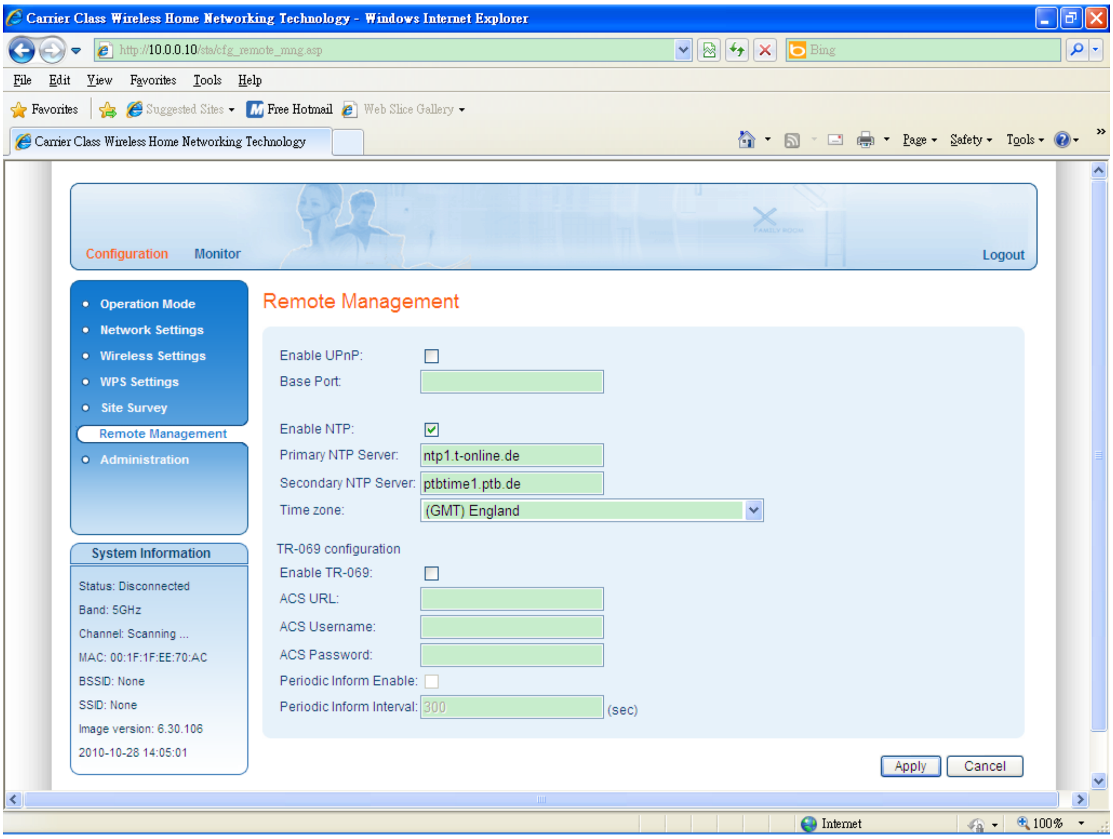
Message from webpage

Apply changes?

When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-11-2 Wireless Client

This wireless client supports UPnP, NTP server and TR-069 features for remote management. Click ‘Remote Management’ on the left of the web management menu and the following information will be displayed:


Carrier Class Wireless Home Networking Technology - Windows Internet Explorer
http://10.0.0.10/sta/cfg_remote_mng.asp
File Edit View Favorites Tools Help
Configuration
Monitor
Logout
Operation Mode
Network Settings
Wireless Settings
WPS Settings
Site Survey
Remote Management
Administration
Internet
100%

Remote Management

Enable UPnP: □
Base Port:

Enable NTP: ☑
Primary NTP Server: ntp1.t-online.de
Secondary NTP Server: ptbtime1.ptb.de
Time zone: (GMT) England

TR-069 configuration
Enable TR-069: □
ACS URL:
ACS Username:
ACS Password:
Periodic Inform Enable: □
Periodic Inform Interval: 300 (sec)

Apply Cancel

System Information
Status: Disconnected
Band: 5GHz
Channel: Scanning ...
MAC: 00:1F:1F:EE:70:AC
BSSID: None
SSID: None
Image version: 6.30.106
2010-10-28 14:05:01

Here are descriptions of every setup item:

Item	Description
Enable UPnP	*When you enable UPnP function, you are able to access the home gateway device and configure its port mapping table to enable accessing the wireless client remotely.*
Base Port	*The port at the Home Gateway that the device will be mapped to. In case that the selected port is already mapped in the gateway, the next available port will be used. When you want to access the wireless client remotely, you can enter ‘http://the router’s public IP address: port number’.*

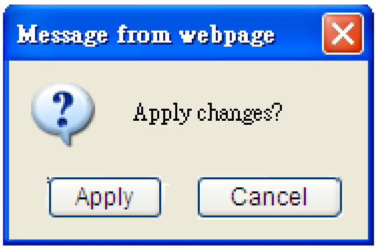
Enable NTP	*When the function is enabled, the wireless client uses NTP protocol to obtain date & time.*
NTP Server	*There are several NTP servers are available on Internet. It is able to provide the date and time information to the device through NTP protocol. Please input the IP address of the NTP server here.*
Time Zone	*Please press* ▼ *button, a drop-down list will be shown, and you can choose a time zone of the location you live.*
Enable TR-069	*TR-069 is a management protocol using by ISP service provider to management the end-user network devices remotely. You can enable this function if it is required by your ISP service provider.*
ACS URL	*ACS server is a device deployed at ISP service provider and it includes auto-provisioning and remote management features for the residential devices. Please input the IP address of the ACS Server.*
ACS Username	*Please input the username for ACS server authentication.*
ACS Password	*Please input the password for ACS server authentication.*
Periodic Inform Enable	*Enable or disable to receive the information from ACS server.*
Periodic Inform Interval	*The period in seconds of receiving the information from ACS server.*

NOTE: Following are some available NTP servers on internet:

129.6.15.28 (time-a.nist.gov)
132.163.4.101 (time-a.timefreq.bldrdoc.gov)
131.107.1.10 (time-nw.nist.gov)

If you found that the time of wireless client is incorrect, try another one.

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



Message from webpage

Apply changes?

When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless client and the changes will take effect after about 30 seconds.

Chapter III: Advanced Configuration

This wireless access point and wireless client support some advanced features for administration. Click ‘Administration’ on the left of web management menu, the following web page will be displayed. Please refer to the following sections for more details.

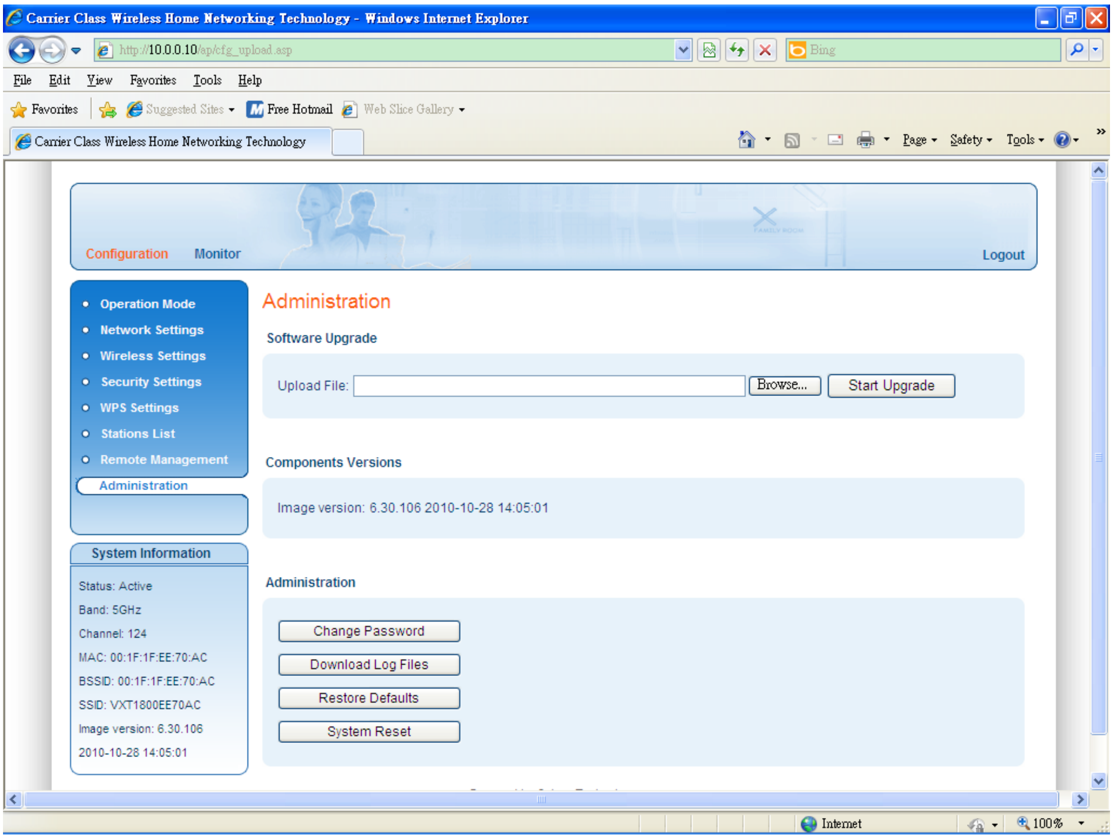


Image version: 6.30.106 2010-10-28 14:05:01

Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

3-1 Software Upgrade

If there are new firmware of this wireless access point or wireless client available, you can upload the firmware to the access point or wireless client to change the firmware with new one, to get extra functions or problem fix.

To perform firmware upgrade, please click ‘Browse’ button first, you’ll be prompted to provide the filename of firmware upgrade file. Please download the latest firmware file from our website, and use it to upgrade your access point or wireless client.

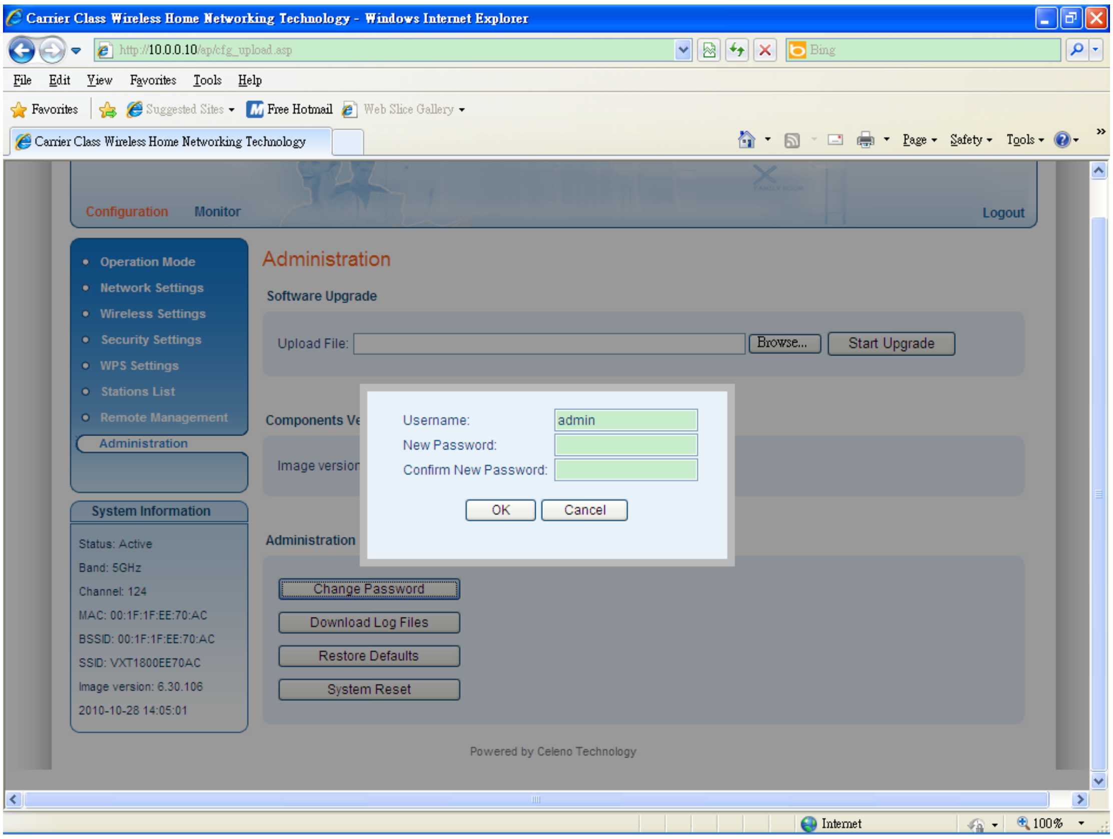
After a firmware upgrade file is selected, click ‘Start Upgrade’ button, and the access point or wireless client will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnect your computer from access point or wireless client. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this access point or wireless client to the dealer of purchase to ask for help. (Warranty voids if you interrupted the upgrade procedure).

3-2 Change Password

You can change the password used to enter the web configuration menu of this wireless access point or wireless client.

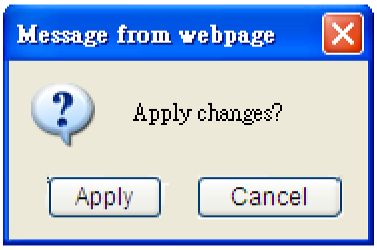
Please click ‘Change Password’ button and the following message will be displayed:



Username: admin
New Password:
Confirm New Password:
OK Cancel

Status: Active
Band: 5GHz
Channel: 124
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Please input user name and, then input new password in both ‘New Password’ and ‘Confirm New Password’ fields. After you finish, please click ‘OK’, and the following message will be displayed:



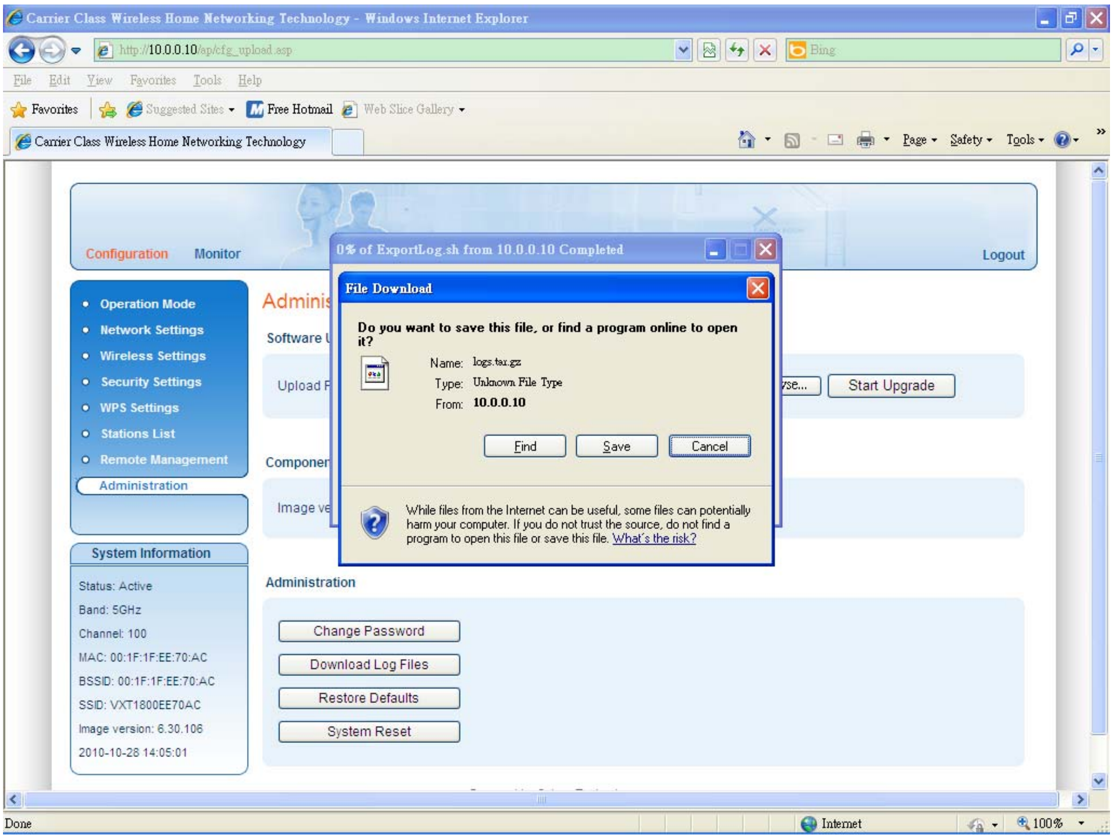
Apply changes?

When you see this message, the settings you made is temporarily save. You can click ‘Cancel’ button to back to previous page, or click ‘Apply’ button to restart the wireless access point or the wireless client and the password changes will take effect after about 30 seconds.

3-3 Download Log Files

To download log files from the wireless access point or wireless client, click ‘Download Log Files’ button and then a confirmation window will prompt you to confirm the download.

Click ‘Save’ button in the window and then save the log files to the folder you designate. If you want to find a program to open the log files, please click ‘Find’ button.



Status: Active
Band: 5GHz
Channel: 100
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

0% of ExportLog.sh from 10.0.0.10 Completed

File Download

Do you want to save this file, or find a program online to open it?

Name: logs.tar.gz
Type: Unknown File Type
From: 10.0.0.10

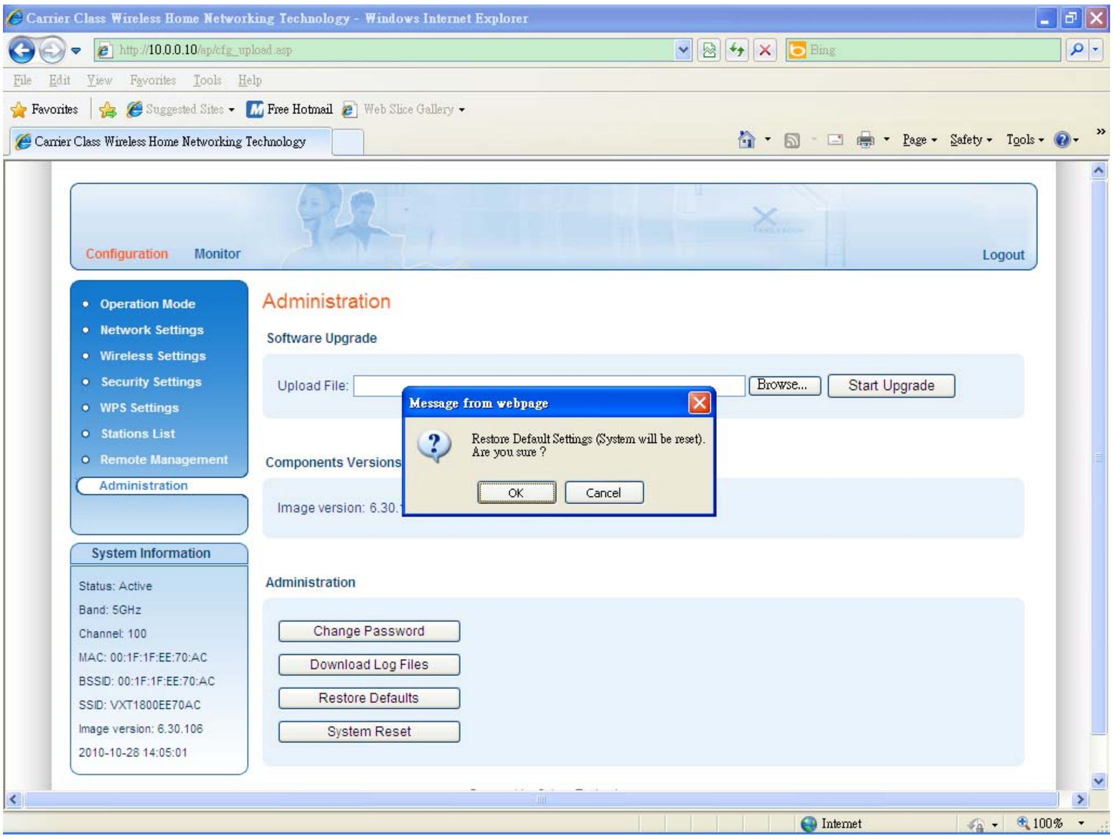
Find Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

3-4 Restore to defaults

To restore the wireless access point or wireless client configurations, please follow the following instructions:

Please click ‘Reset Defaults’ button and then the following message will be displayed on your web browser.



Administration

Software Upgrade

Upload File:

Components Versions

Image version: 6.30.1

Message from webpage

Restore Default Settings (System will be reset).
Are you sure ?

OK Cancel

System Information

Status: Active
Band: 5GHz
Channel: 100
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Administration

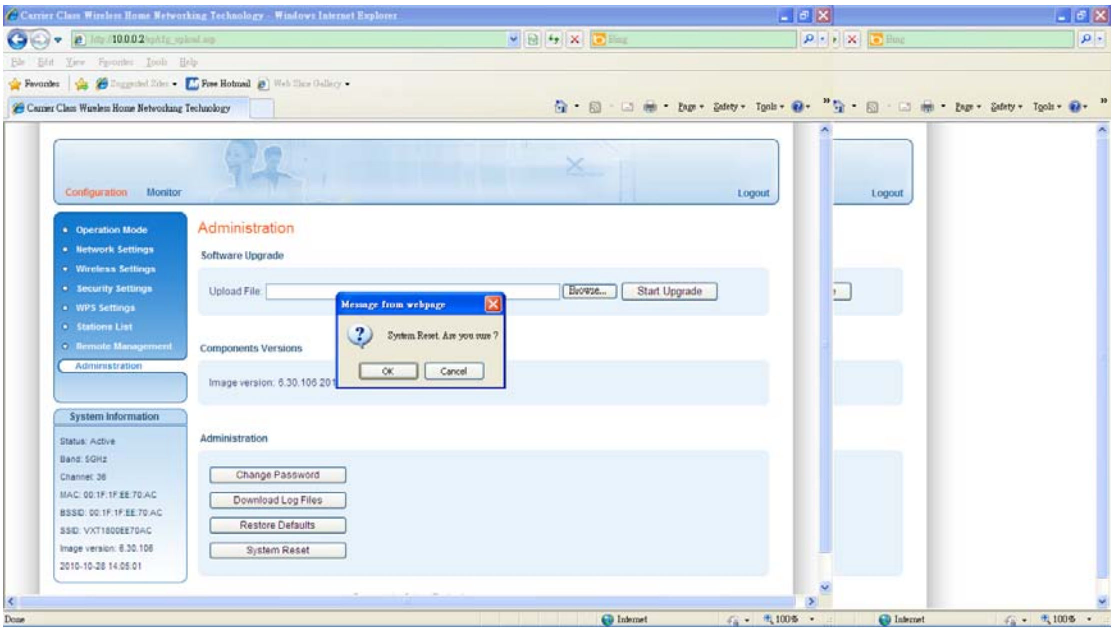
Click ‘OK’ and the wireless access point or the wireless client will be restarted and the setting changes will take effect after about 30 seconds.

3-5 System Reset

When you think the wireless access point or wireless client is not working properly, you can use this function to restart the access point or wireless client; this may help and solve the problem.

This function is useful when the access point or wireless client is far from you or unreachable. However, if the access point or wireless client is not responding, you may have to switch it off by unplug the power plug and plug it back again after 10 seconds.

To reset your access point or wireless client, please click ‘System Reset’ button and the following message will be displayed:



Administration

Software Upgrade

Upload File:

Message from webpage

System Reset. Are you sure ?

Components Versions

Image version: 6.30.106 201

Administration

System Information

Status: Active
Band: 5GHz
Channel: 36
MAC: 00:1F:1F:EE:70:AC
BSSID: 00:1F:1F:EE:70:AC
SSID: VXT1800EE70AC
Image version: 6.30.106
2010-10-28 14:05:01

Click ‘OK’ to reset the access point or wireless client, or click ‘Cancel’ to abort. Please remember all connections between wireless client and access point will be disconnected.

Chapter IV: Appendix

4-1 Hardware Specification

SoC: Celeno CL1820

Flash: 4MB

DDR2 RAM: 64MB

Frequency Band:

FCC: 5.15~5.25GHz, 5.725~5.85GHz

CE: 5.15~5.25GHz, 5.25~5.35GHz, 5.47~5.725GHz

LAN Port: 10/100M UTP Port x 1

Antenna: 3dBi Printed Antenna x 4 (2T3R MIMO Technology)

Power: 12VDC, 1A Switching Power Adapter

Dimension: 46(H) x 130(W) x 153(D) mm

Transmit Power:

11a:17dBm+/-1dBm for CH36~140, 16+/-1dBm for CH149~165

11n:17dBm+/-1dBm for CH36~140, 16+/-1dBm for CH149~165

Temperature: 32~104°F (0 ~ 40°C)

Humidity: 10-90% (NonCondensing)

Certification: FCC, CE

4-2 Troubleshooting

If you found the wireless access point or the wireless client is working improperly or stop responding to you, don’t panic! Before you contact your dealer of purchase for help, please read this troubleshooting first. Some problems can be solved by yourself within very short time!

Scenario	Solution
Access point or wireless client is not responding to me when I want to access it by web browser	a. Please check the connection of power cord and network cable of this access point or wireless client. All cords and cables should be correctly and firmly inserted to the access point or wireless client. b. If all LEDs on this access point or wireless client are off, please check the status of A/C power adapter, and make sure it’s correctly powered. c. You must use the same IP address section which access point or wireless client uses. d. Are you using MAC or IP address filter? Try to connect the access point by another wireless client and see if it works; if not, please perform a hard reset (pressing ‘reset’ button). e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all above solutions don’t work, contact the dealer of purchase for help.
Wireless Client can’t get connected to wireless access point	a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client. b. Try to move closer to wireless access point. c. Unplug the power plug of access point, and plug it back again after 10 seconds.

	d. If all LEDs on this access point are off, please check the status of A/C power adapter, and make sure it's correctly powered.
I can't locate my access point by my wireless client	a. Check if 'Broadcast SSID' of the access point set to off? b. Is Antenna properly installed and secured? c. Are you too far from your access point? Try to get closer. d. Please remember that you have to input SSID on your wireless client manually, if SSID broadcast is disabled.
File download is very slow or breaks frequently	a. Try to reset the access point and see if it's better after that. b. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. c. Change channel number and see if this works.
I can't log onto web management interface: password is wrong	a. Make sure you're connecting to the correct IP address of the access point or the wireless client! b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard restore to defaults.
Access point become hot	a. This is not a malfunction, if you can keep your hand on the access point's case. b. If you smell something wrong or see the smoke coming out from access point or A/C power adapter, please disconnect the access point and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

4-3 Glossary

Default Gateway (Access point): Every non-access point IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandaccess point.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading

1’s followed by consecutive trailing 0’s, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as “x” number of leading 1’s.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1’s in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device’s network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product’s serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point’s NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Access point: An access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and

Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.