Compal Broadband Networks

CH6643E
Wireless Gateway Series

User Guide

Table of Contents

1.Overview

The CBN CH6643E Wireless Gateway is designed for your home, home office, or small business/enterprise. It can be used in households with one or more computers capable of wireless connectivity for remote access to the wireless gateway.

This user guide provides product overview and setup information for the CH6643E. It also provides instructions for installing the wireless gateway and configuring the wireless LAN, Ethernet, router, DHCP, and security settings.

Contact Information

- For any questions or assistance with the CH6643E Wireless Gateway, contact your Internet Service provider.
- For information on customer service, technical support, or warranty claims; see the CBN CH6643E Software License, Warranty, Safety, and Regulatory Information card provided with the CH6643E Wireless Gateway.

Standard Features

The CH6643E Wireless Gateway combines high-speed Internet access, networking, and computer security for a home or small-office LAN. It offers the following features:

- Combination of five separate products in one compact unit — an EURO/ DOCSIS® 3.0 cable modem, IEEE 802.11b/g/n/a wireless access point, Ethernet 10/100/1000 Base-T connections, two VoIP Internet telephone connections, and firewall.
- An integrated high-speed cable modem for continuous broadband access to the Internet and other online services with much faster data transfer than traditional dial-up or ISDN modems.
- Advanced firewall for enhanced network security from undesired attacks over the Internet. It supports stateful-inspection, intrusion detection, DMZ, denial-of-service attack prevention, and Network Address Translation (NAT).
- One broadband connection for up to 253 computers to surf the web; all computers on the LAN communicate as if they were connected to the same physical network.
- Four 10/100/1000Base-T Ethernet uplink ports supporting half- or full-duplex connections with auto-MDIX capability.
- An IEEE 802.11n wireless access point to enable laptop users to remain connected while moving around the home or small office or to connect desktop computers without installing network wiring. Depending on distance, wireless connection speeds can vary.
- CH6643E wireless function supports Wi-Fi 2.4G and 5G dual-band mode. You can either select 2.4G or 5G single mode or select dual-band concurrent mode to adapt to a wide variety of environment.

- A secure Wireless Fidelity (Wi-Fi) broadband connection for Wi-Fi enabled devices on your network, such as your cellular telephone, laptops, printers, PDAs, and desktops.
- Routing for a wireless LAN (WLAN) or a wired Ethernet LAN; you can connect more than four computers using hubs and/or switches
- A built-in DHCP server to easily configure a combined wired and/or wireless Class C private LAN.
- Virtual private network (VPN) pass-through operation supporting IPSec, PPTP, or L2TP to securely connect remote computers over the Internet.
- CH6643E Configuration Manager (CMGR) which provides a graphical user interface (GUI) for easy configuration of necessary wireless, Ethernet, router, DHCP, and security settings.
- USB 2.0 host port is provided to support print server and network storage function with FTP server and Samba server which file system supported are FAT16, FAT32, and NTFS. You can plug in an USB memory stick then access it via FTP client or Windows Explorer.

CH6643E LAN Choices

You can connect up to 253 client computers to the CH6643E using one or any combination of the following network connections:

- Wi-Fi wireless LAN (WLAN)
- Ethernet local area network (LAN)

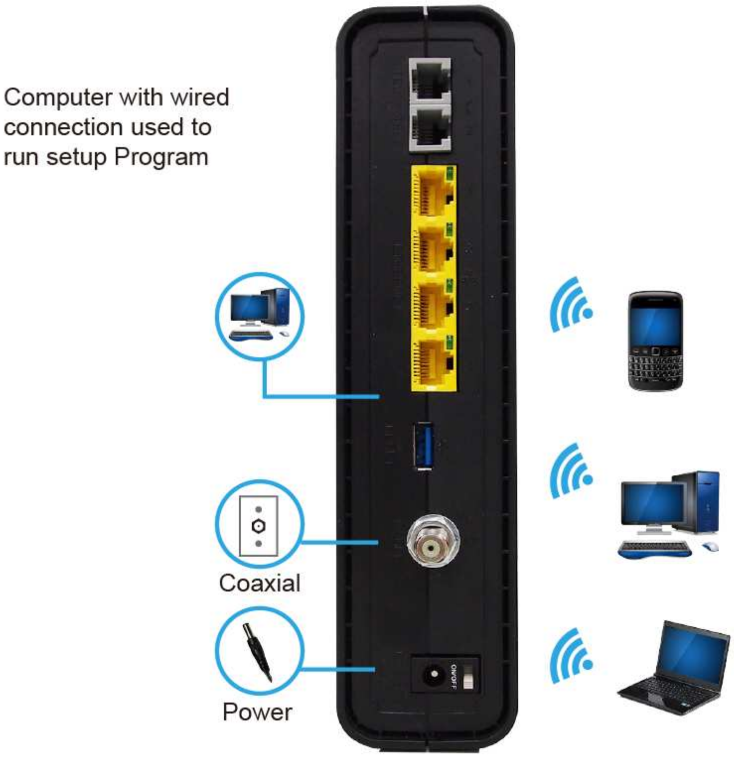
Wireless LAN

Wireless communication occurs over radio waves rather than a wire. Like a cordless telephone, a WLAN uses radio signals instead of wires to exchange data. A wireless network eliminates the need for expensive and intrusive wiring to connect computers throughout the home or office. Mobile users can remain connected to the network even when carrying their laptop to different locations in the home or office.

Each computer or other device on a WLAN must be Wi-Fi enabled with either a built-in or external wireless adapter.

Laptops — Use a built-in wireless notebook adapter, a wireless PCMCIA slot adapter, or a wireless USB adapter.

Desktops — Use a wireless PCI adapter, wireless USB adapter, or compatible product in the PCI slot or USB port, respectively.



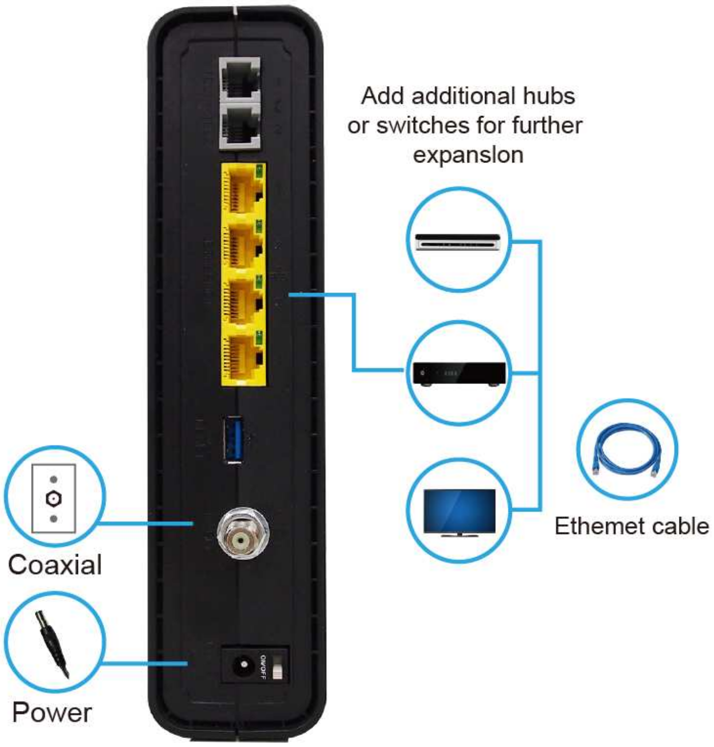
Sample Wireless Network Connections (CH6643E model shown)

Your maximum wireless operation distance depends on the type of materials through which the signal must pass and the location of your CH6643E and clients (stations). CBN cannot guarantee wireless operation for all supported distances in all environments.

> ***Note: To get better wireless coverage, please put your CH6643E wireless gateway vertically.***

Wired Ethernet LAN

You can easily connect any PC with an Ethernet cable to the CH6643E Ethernet port. Because the CH6643E Ethernet port supports auto-MDIX, you can use a straight-through or cross-over cable to connect a hub, switch, or computer. Use category 5, or better, cabling for all Ethernet connections.



Sample Ethernet to Computer Connection (CH6643E model shown)

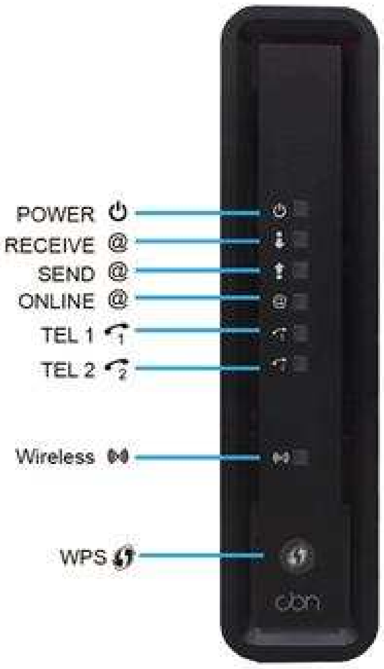
A wired Ethernet LAN with more than four computers requires one or more hubs, switches, or routers. You can:

- Connect a hub or switch to any Ethernet port on the CH6643E.
- Use Ethernet hubs, switches, or routers to connect up to any combination of 253 computers and wireless clients to the CH6643E.

More detailed information on Ethernet cabling is beyond the scope of this document.

Front Panel

The CH6643E front panel contains indicator lights and the **WPS button** which is used to configure Wi-Fi Protected Security (WPS) on compatible clients connected to the CH6643E network.

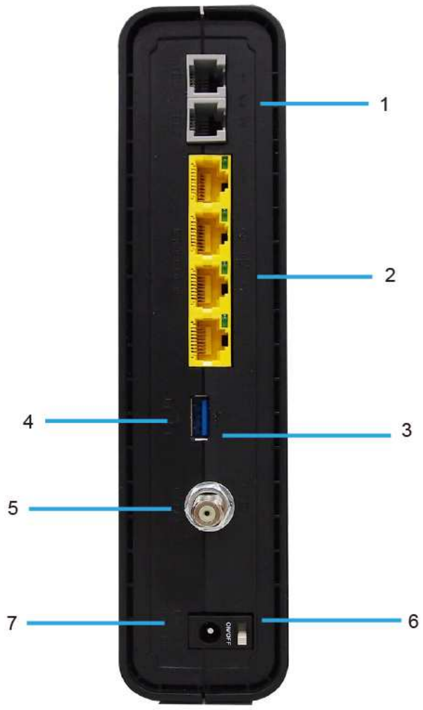


The CH6643E front panel LED indicators provide the following status information for power, communications, and errors:

	LED	Flashing	On
1	**POWER**	Not applicable — LED does not flash	**Green**: Power is properly connected
2	**RECEIVE**	Scanning for a downstream channel connection	**Green**: Downstream channel is connected **Blue**: Downstream channel is connected with bonded channels
3	**SEND**	Scanning for an upstream channel connection	**Green**: Upstream channel is connected **Blue**: Upstream channel is connected with bonded channels
4	**ONLINE**	Scanning for Internet connection: Transmitting or receiving data over the Internet	**Green**: Connected to Internet
5	**TEL1** **TEL 2**	Telephone is off-hook: Dialing or call in progress	**Green**: Telephone is connected and activated: on-hook

	LED	Flashing	On
6	**WIRELESS**	**Amber**: WPS function is enabled.	**Green**: Wi-Fi wireless interface is active now.

Rear Panel



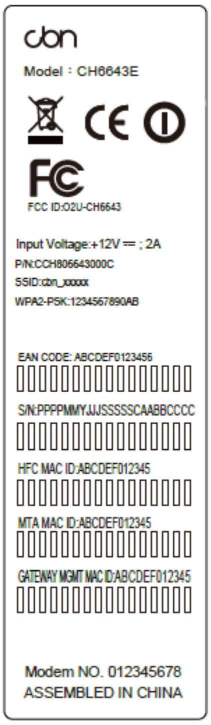
The CH6643E (shown above) rear panel contains the following cabling port and connectors:

	Item	Description
1	**TEL 1** **TEL 2**	VoIP connection for a single telephone. Two sets of telephone can be supported.
2	**ETHERNET** **1 2 3 4**	Use any Ethernet port to connect an Ethernet-equipped computer, hub, bridge, or switch using an RJ-45 cable. **Activity LED** - Green LED defines the activity of the Ethernet connector. When LED is ON, this indicates that there is no data traffic and a connection is stabilized. When LED is FLASHING, this indicates that there is data being transmitted upstream or downstream. When LED is OFF, this indicates that the unit is not powered or

Item		Description
		there is no Ethernet connection.
3	**USB**	USB host port for print server or network storage function
4	**RESET**	Press and hold the RESET button for five seconds or longer to restore CH6643E to factory default settings. After factory default settings are restored, the gateway will restart and may take 5 to 30 minutes to find and lock on the appropriate communication channels.
5	**CABLE**	Connect the CH6643E to a cable wall outlet.
6	**POWER SWITCH**	Switch gear for power on/off the CH6643E.
7	**POWER**	Provide power to the CH6643E.

MAC Label

The CH6643E Media Access Control (MAC) label is located on the bottom of the CH6643E. The label contains the MAC address which is a unique, 48-bit value that identifies each Ethernet network device. To receive data service, you will need to provide the MAC address marked **HFC MAC ID** to your Internet Service provider.”



cbn

Model：CH6643E

FCC ID:O2U-CH6643

Input Voltage:+12V ⎓ ; 2A
P/N:CCH806643000C
SSID:cbn_xxxxx
WPA2-PSK:1234567890AB

EAN CODE: ABCDEF0123456

S/N:PPPPMMYJJJSSSSSCAABBCCCC

HFC MAC ID:ABCDEF012345

MTA MAC ID:ABCDEF012345

GATEWAY MGMT MAC ID:ABCDEF012345

Modem NO. 012345678
ASSEMBLED IN CHINA

2. Getting Started

Inside the Box

Before you install the CH6643E Wireless Gateway, verify that the following items are included in the box with the CH6643E:

Item		Description
Power cord		Connects the CH6643E to an AC electrical outlet
Software License & Regulatory Card		Contains software license, warranty, and safety information for the CH6643E.
CH6643E Install Sheet		Provides basic information for setting up the CH6643E

You must have the latest service packs and patches installed on your computer for your operating system.

You will need a 75-ohm coaxial cable with F-type connectors to connect the CH6643E to the nearest cable outlet. If a TV is connected to the cable outlet, you may need a 5 to 900 MHz RF splitter and two additional coaxial cables to use the TV and the CH6643E.

Before You Begin

Take the following precautions before installing the CH6643E:

- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- To avoid potential shock, always unplug the power cord from the wall outlet or other power source before disconnecting it from the CH6643E rear panel.
- To prevent overheating the CH6643E, do not block the ventilation holes on the sides of the unit. Do not open the unit. Refer all service to your Internet Service provider.

Check that you have the required cables, adapters, and adapter software. Verify that the proper drivers are installed for the Ethernet adapter on each networked computer. For information on WLAN setup, see Setting Up Your Wireless LAN.

System Requirements

Your computer must meet the following minimum requirements:

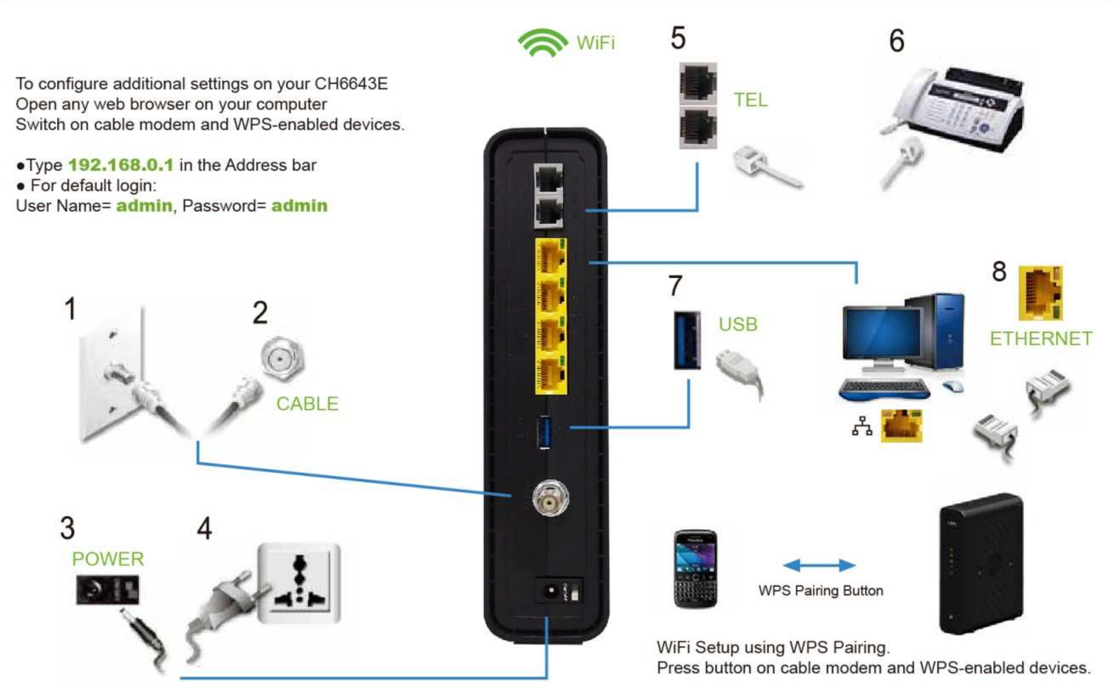
- Computer with Pentium© class or better processor
- Windows XP, Windows 7, Windows 8, Macintosh, or UNIX operating system with available operating system CD-ROM
- Any web browser, such as Microsoft Internet Explorer, Netscape Navigator®, or Mozilla® Firefox®

Connecting the CH6643E

Before starting, be sure the computer is turned on and the CH6643E power cord is unplugged.

1. Connect one end of the coaxial cable to the cable outlet or splitter.
2. Connect the other end of the coaxial cable to the Cable connector on the CH6643E. Hand-tighten the connectors to avoid damaging them.
3. Plug the power cord into the Power port on the CH6643E.
4. Plug the other end of the power cord into an electrical wall outlet.

   This automatically powers on the gateway. You do not need to unplug the gateway when it is not in use. The first time you plug in the CH6643E, allow it 5 to 30 minutes to find and lock on the appropriate communications channels.
5. Plug the other end of the telephone cord of a single or two-line telephone into the TEL 1/2 port on the rear of the CH6643E.
6. Plug the telephone cord of a single or two-line telephone into the telephone.
7. (optional step) Plug USB memory stick or hard-disk drive into USB port on CH6643E.
8. Connect the Ethernet cable to the Ethernet port on the computer, and connect the other end of the Ethernet cable to the Ethernet port on the gateway.
9. For a second telephone, plug the telephone wire of a single-line telephone into the TEL 2 port on the rear of the CH6643E.



To configure additional settings on your CH6643E
Open any web browser on your computer
Switch on cable modem and WPS-enabled devices.

- Type **192.168.0.1** in the Address bar
- For default login:
User Name= **admin**, Password= **admin**

WiFi Setup using WPS Pairing.
Press button on cable modem and WPS-enabled devices.

10. Check that the LEDs on the front panel cycle through the following sequence:

CH6643E LED Activity During Startup

LED	Description
POWER	Turns on when AC power is connected to the CH6643E. Indicates that the power is connected properly.
RECEIVE	Flashes while scanning for the downstream receive channel. Changes to solid green when single downstream channel is locked. Changes to solid blue when multiple downstream channels are locked.
SEND	Flashes while scanning for the upstream send channel. Changes to solid green when single upstream channel is locked. Changes to solid blue when multiple upstream channels are locked.
ONLINE	Flashes during CH6643E registration and configuration. Changes to solid green when the CH6643E is registered successfully and ready for Internet access

Wall Mounting the CH6643E

You have the option to wall mount the CH6643E. Do the following before mounting the CH6643E on the wall:

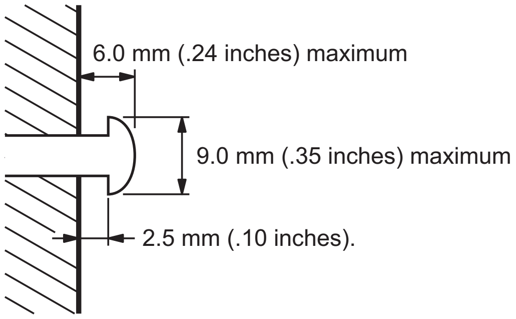
- Locate the unit as specified by the local or national codes governing residential or business cable TV and communications services.
- Follow all local standards for installing a network interface unit/network interface device (NIU/NID).
- Make sure the AC power plug is disconnected from the wall outlet and all cables are removed from the back of the CH6643E before starting the installation.
- Decide if you want to mount the CH6643E horizontally or vertically.

If possible, mount the unit to concrete, masonry, a wooden stud, or some other very solid wall material. Use anchors if necessary (for example, if you must mount the unit on drywall).

> ***CAUTION:*** *Before drilling holes, check the structure for potential damage to water, gas, or electrical lines.*

Do the following to mount your CH6643E on the wall:

1. Print a copy of the Wall Mounting Template.
2. Measure the printed template with a ruler to ensure that it is the correct size.
3. Use a center punch to mark the center of the holes.
4. On the wall, locate the marks for the mounting holes.
5. Drill the holes to a depth of at least 1 1/2 inches (3.8 cm). Use M3.5 x 38 mm (#6 x 11/2 inch) screws with a flat underside and maximum screw head diameter of 9.0 mm to mount the CH6643E.
6. Using a screwdriver, turn each screw until part of it protrudes from the wall, as shown in the following wall mounting screw dimensions illustration.



   There must be .10 inches (2.5 mm) between the wall and the underside of the screw head.

7. Place the CH6643E so the keyholes on the back of the unit are aligned above the mounting screws.

8. Slide the CH6643E down until it stops against the top of the keyhole opening.
9. After mounting, reconnect the coaxial cable input and Ethernet connection.
10. Plug the power cord into the +12VDC connector on the gateway and the electrical outlet.
11. Route the cables to avoid any safety hazards.

Wall Mounting Template

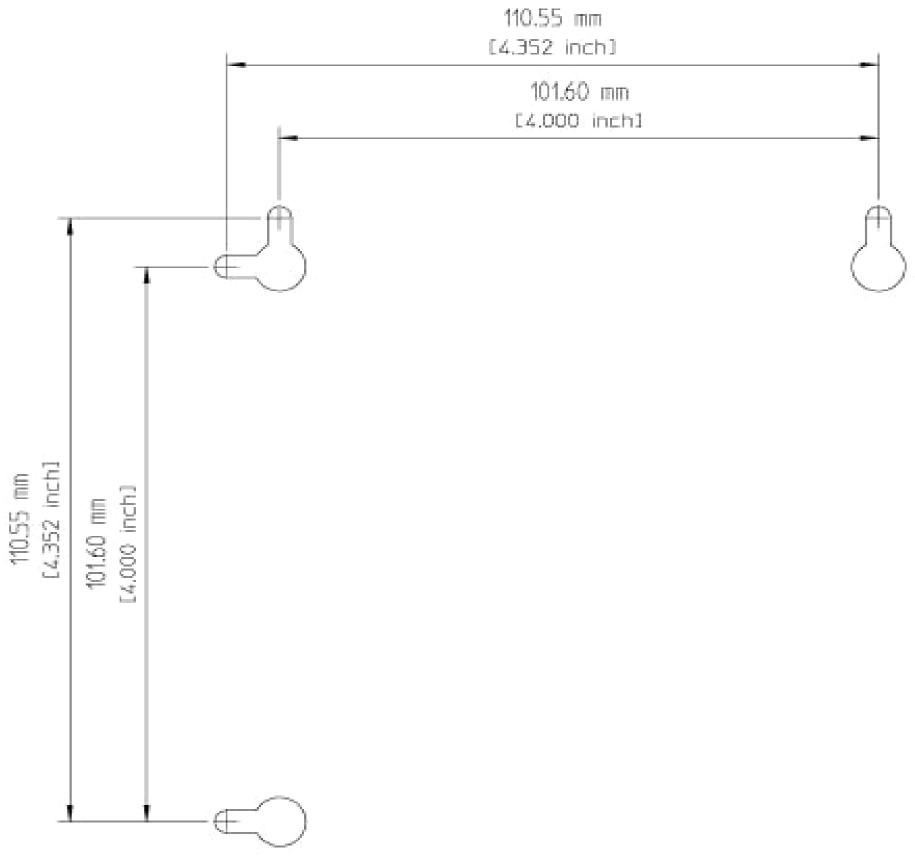


Figure 1 Wall Mounting Template

Setting Up Internet Access

After installing the CH6643E, check that you can connect to the Internet. You can retrieve an IP address for your computer's network interface using one of the following options:

- Retrieve the statically defined IP address and DNS address
- Automatically retrieve the IP address using the Network DHCP server

The CBN CH6643E Wireless Gateway provides a DHCP server on its LAN. It is recommended that you configure your LAN to obtain the IPs for the LAN and DNS server automatically.

Make sure all computers on your LAN are configured for TCP/IP. After configuring TCP/IP on your computer, you should verify the IP address.

> ***Note**: For UNIX or Linux systems, follow the instructions in the applicable user documentation.*

Configuring TCP/IP in Windows XP

1. Open the Control Panel.
2. Double-click Network Connections to list the Dial-up and LAN or High-Speed Internet connections.
3. Right-click the network connection for your network interface.
4. Select Properties from the drop-down menu to display the Local Area Connection Properties window. Be sure Internet Protocol (TCP/IP) is checked.
5. Select Internet Protocol (TCP/IP) and click Properties to display the Internet Protocol (TCP/IP) Properties window.
6. Select Obtain an IP address automatically and Obtain DNS server address automatically.
7. Click OK to save the TCP/IP settings and exit the TCP/IP Properties window.
8. Close the Local Area Connection Properties window and then exit the Control Panel.
9. When you complete the TCP/IP configuration, continue with Verifying the IP Address in Windows XP

Verifying the IP Address for Windows XP

1. On the Windows taskbar, click Start.
2. Select Run to open the Run window.
3. Type cmd and click OK.
4. Type ipconfig and press Enter to display your IP configuration.

Configuring TCP/IP in Windows 7

1. Open the Control Panel.
2. Click Network and Internet to display the Network and Internet window.
3. Click Network and Sharing Center to display the Network and Sharing Center window.
4. Click change adapter settings
5. Right-click the network connection for the network interface you want to change.

6. Click Properties to display the Local Area Connection Properties window
7. Select Internet Protocol Version 4(TCP/IPv4), double click it or click Properties
8. Select Obtain an IP address automatically and Obtain DNS server address automatically**.**
9. Click OK to save the TCP/IP settings and close the Internet Protocol Version 4 (TCP/IPv4) Properties window.
10. Click OK to close the Local Area Connection Properties window.
11. Close the remaining windows and exit the Control Panel.
12. When you complete the TCP/IP configuration, continue with Verifying the IP Address in Windows 7

Verifying the IP Address for Windows 7

1. On the Windows taskbar, click Start.
2. Click All Programs.
3. Click Accessories.
4. Click Run to open the Run window.
5. Type cmd and click OK to open a command prompt window.
6. Type ipconfig and press Enter to display the IP Configuration.

Configuring TCP/IP in windows 8

1. Press Windows key on the keyboard to go into Desktop mode.
2. Move the mouse's cursor to the lower right corner of the screen. A right pane will now appear. Click the settings icon. The settings pane will now appear.
3. On the settings pane, click the Control panel link.
4. Open The Control Panel.
5. Click Network and internet to display the Network and Internet window.
6. Click Network and sharing center to dsiplay the Network and Sharing Centre window.
7. Click change adapter settings.

. 8. Right click the network connection for the network interface you want to
. change.

9. Click Properties to display the Local Area Connection properties window.
10. Select Internet Protocol Version 4 (TCP/IPv4),double click it or click properties.
11. Select obtain IP address automatically and obtain DNS server address automatically.
12. Click ok to save the TCP/IP settings and close the internet Protocol Version 4 (TCP/IPV4) properties window.
13. Click ok to close the Local Area Connection Properties window.
14. Close the remaining windows and exit the control panel.
15. When you complete the TCP/IP configuration. Continue with verifying the IP Address in windows 8.

Verifying the IP Address in Windows 8

1. Press the Windows ⊞ key on your keyboard and then enter "command prompt" to display the Command Prompt shortcut. A search box on right side of the screen will appear.
2. Click Command Prompt
3. In the Command Prompt, Type ipconfig and press Enter to display the IP Configuration

Renewing the IP Address for Windows XP, Windows 7& Windows 8

1. Open a command prompt window.
A. From the Windows taskbar, click Start.
B. Select *Run* to open the Run window.
C. Type cmd and click OK to open a command prompt window.
2. Type ipconfig /renew and press Enter. A valid IP address should appear indicating that Internet access is available.
3. Type exit and press Enter to close the command prompt window.
If, after performing this procedure, your computer still cannot access the Internet, call your service provider.

Setting Up a Wi-Fi Network

Do the following to set up a Wi-Fi network using the WPS button on the CH6643E:

1. Power on the CH6643E.
2. Power on the WPS-enabled devices you want to have access to the network, such as a PC, router, or telephone.

   The Wi-Fi network will automatically detect the WPS devices.
3. Press WPS button on the CH6643E.
4. If applicable, press WPS button on the other WPS devices.

3.Basic Configuration

For normal operation, you do not need to change most default settings. Carefully consider the following caution statements:

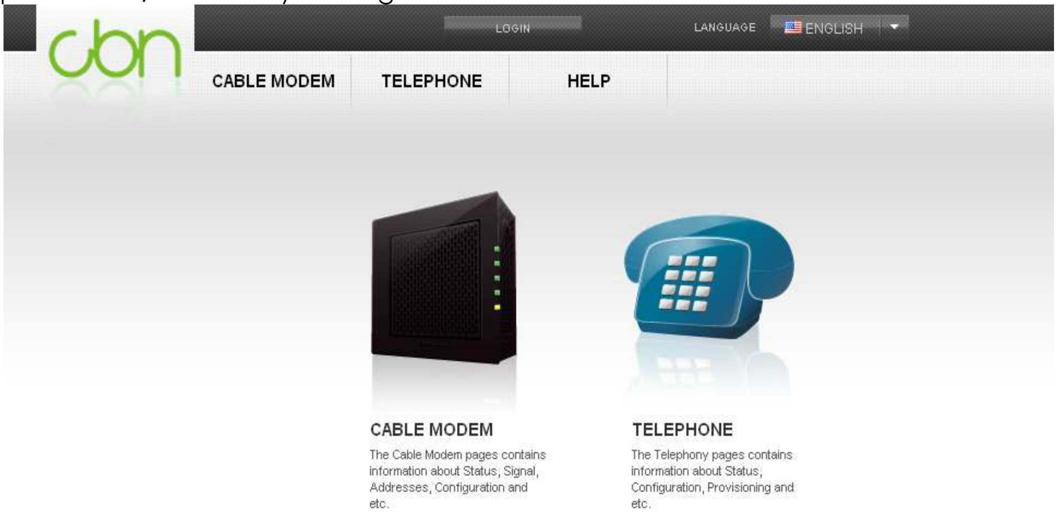
Starting the CH6643E Configuration Manager (CMGR)

The CH6643E Configuration Manager (CMGR) allows you to change and view the settings on your CH6643E.

1. Open the web browser on a computer connected to the CH6643E over an Ethernet connection.

> ***Note: Do not attempt to configure the CH6643E over a wireless connection.***

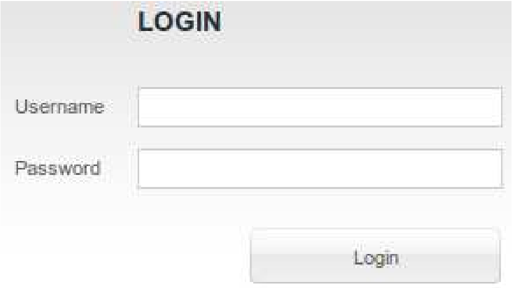
2. In the Address or Location field of your browser, type **http://192.168.0.1** and press **ENTER,** and then you will get into homesection.



The Cable Modem pages contains information about Status, Signal, Addresses, Configuration and etc.

The Telephony pages contains information about Status, Configuration, Provisioning and etc.

CMGR provide more information and gateway functions for experienced users in privileged mode, you can login by click the "LOGIN" button on the top of window then input Username and Password.

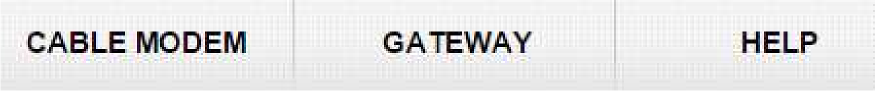


There are is a default privileged account in CH6643E:

Username	Password	Privilege
admin	**admin**	Allow access gateway sections

CH6643E Menu Options Bar

The CH6643E Menu Options bar is displayed at the top of the CH6643E Configuration Manager window.

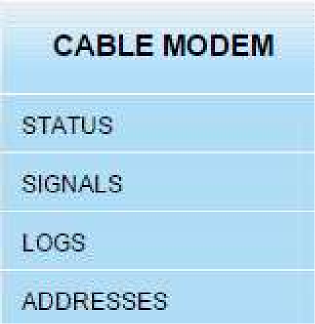


Configuration Manager Menu Options Bar

Menu Option Sections	Function
CABLE MODEM	The Cable Modem sections contain information about Status, Signals, Logs and Addresses.
GATEWAY	The Gateway sections contain information about LAN, Firewall, Wireless configuration, and etc.
HELP	This section provides an overview of the Modem Configuration Manager, and brief troubleshooting information.

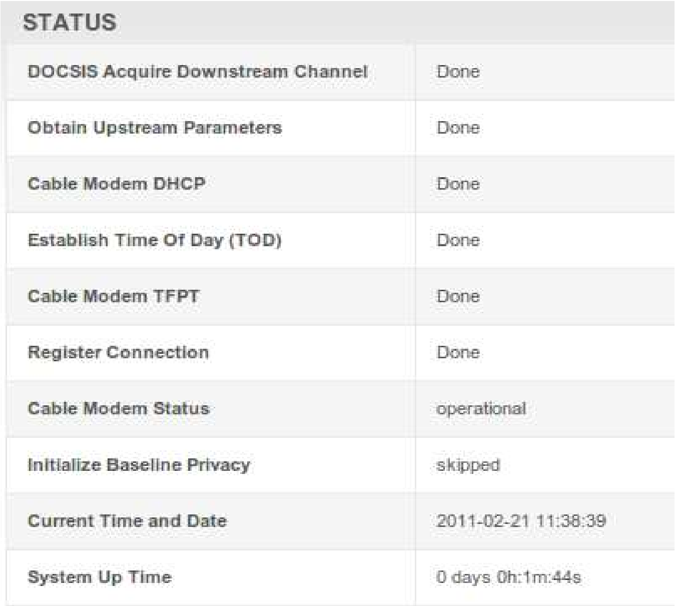
4.CABLE MODEM

The CABLE MODEM section provide the information of cable connection status, channel signals, network IP address, and system logs during the establishment of cable connection to cable service provider's CMTS.



CABLE MODEM Status Section

This section provides information about the startup process of the Cable Modem.

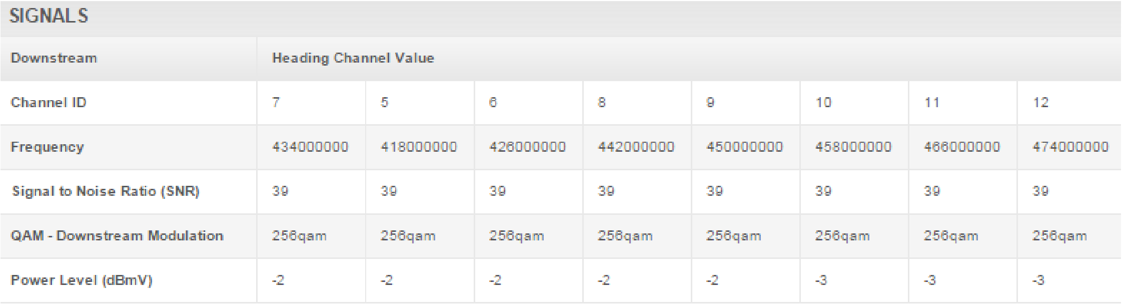


STATUS

DOCSIS Acquire Downstream Channel	Done
Obtain Upstream Parameters	Done
Cable Modem DHCP	Done
Establish Time Of Day (TOD)	Done
Cable Modem TFPT	Done
Register Connection	Done
Cable Modem Status	operational
Initialize Baseline Privacy	skipped
Current Time and Date	2011-02-21 11:38:39
System Up Time	0 days 0h:1m:44s

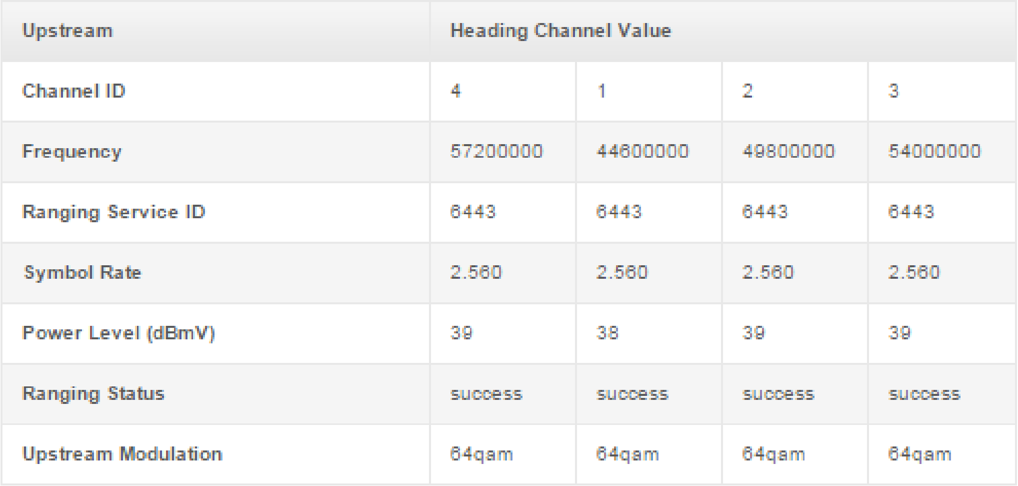
CABLE MODEM Signals Section

This section provides information about the connection between the Cable Modem and the CMTS of cable service provider.

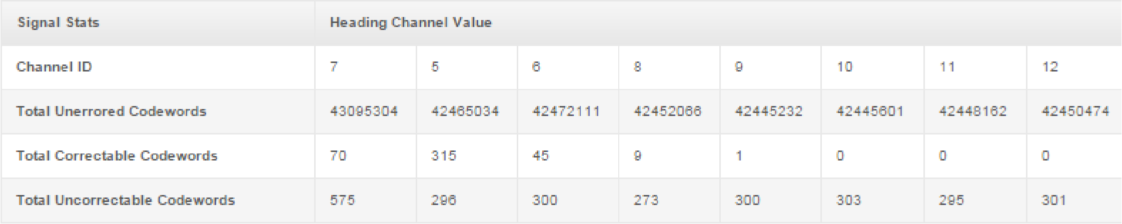


SIGNALS

Downstream	Heading Channel Value							
Channel ID	7	5	6	8	9	10	11	12
Frequency	434000000	418000000	426000000	442000000	450000000	458000000	466000000	474000000
Signal to Noise Ratio (SNR)	39	39	39	39	39	39	39	39
QAM - Downstream Modulation	256qam	256qam	256qam	256qam	256qam	256qam	256qam	256qam
Power Level (dBmV)	-2	-2	-2	-2	-2	-3	-3	-3



Upstream	Heading Channel Value			
Channel ID	4	1	2	3
Frequency	57200000	44600000	49800000	54000000
Ranging Service ID	6443	6443	6443	6443
Symbol Rate	2.560	2.560	2.560	2.560
Power Level (dBmV)	39	38	39	39
Ranging Status	success	success	success	success
Upstream Modulation	64qam	64qam	64qam	64qam



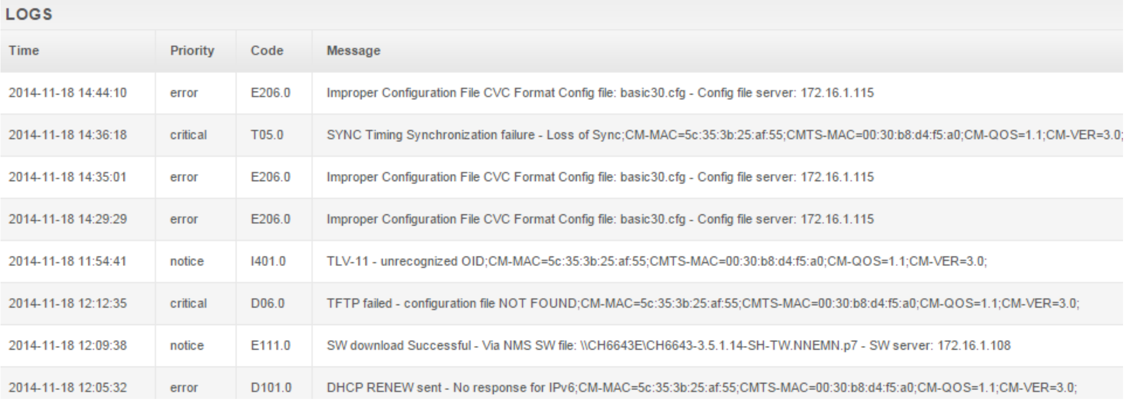
Signal Stats	Heading Channel Value							
Channel ID	7	5	6	8	9	10	11	12
Total Unerrored Codewords	43095304	42465034	42472111	42452066	42445232	42445601	42448162	42450474
Total Correctable Codewords	70	315	45	9	1	0	0	0
Total Uncorrectable Codewords	575	296	300	273	300	303	295	301

Field Descriptions for the Status Connection Section

Field	Description
Downstream	Status information about the RF downstream channels, including downstream channel frequency and downstream signal power and modulation.
Upstream	Status information about the RF upstream channels, including upstream channel ID and upstream signal power and modulation.

CABLE MODEM Logs Section

This section lists the critical system events in chronological order. A sample event log is shown below:



LOGS

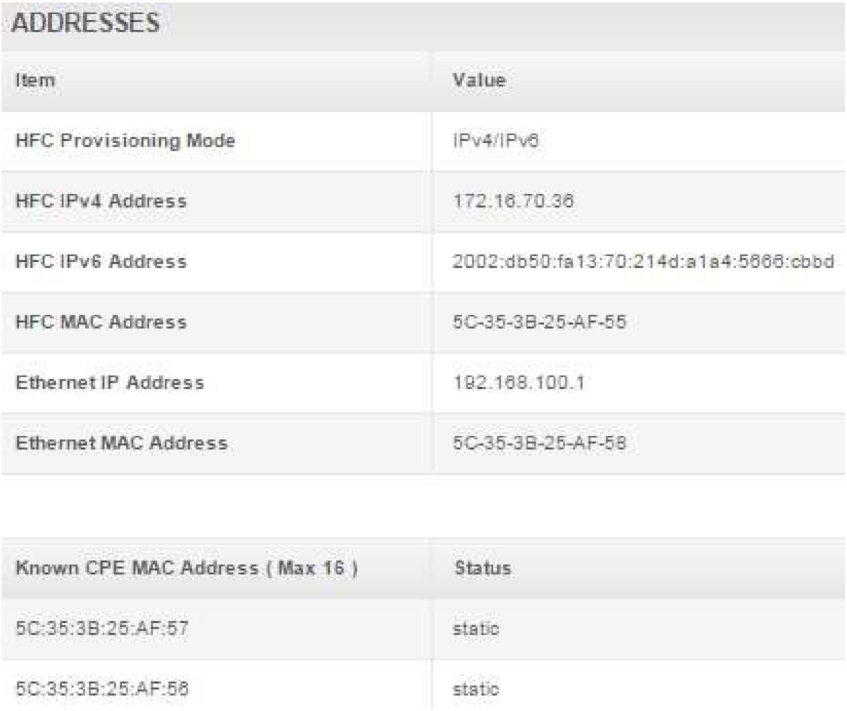
Time	Priority	Code	Message
2014-11-18 14:44:10	error	E206.0	Improper Configuration File CVC Format Config file: basic30.cfg - Config file server: 172.16.1.115
2014-11-18 14:36:18	critical	T05.0	SYNC Timing Synchronization failure - Loss of Sync;CM-MAC=5c:35:3b:25:af:55;CMTS-MAC=00:30:b8:d4:f5:a0;CM-QOS=1.1;CM-VER=3.0;
2014-11-18 14:35:01	error	E206.0	Improper Configuration File CVC Format Config file: basic30.cfg - Config file server: 172.16.1.115
2014-11-18 14:29:29	error	E206.0	Improper Configuration File CVC Format Config file: basic30.cfg - Config file server: 172.16.1.115
2014-11-18 11:54:41	notice	I401.0	TLV-11 - unrecognized OID;CM-MAC=5c:35:3b:25:af:55;CMTS-MAC=00:30:b8:d4:f5:a0;CM-QOS=1.1;CM-VER=3.0;
2014-11-18 12:12:35	critical	D06.0	TFTP failed - configuration file NOT FOUND;CM-MAC=5c:35:3b:25:af:55;CMTS-MAC=00:30:b8:d4:f5:a0;CM-QOS=1.1;CM-VER=3.0;
2014-11-18 12:09:38	notice	E111.0	SW download Successful - Via NMS SW file: \\CH6643E\CH6643-3.5.1.14-SH-TW.NNEMN.p7 - SW server: 172.16.1.108
2014-11-18 12:05:32	error	D101.0	DHCP RENEW sent - No response for IPv6;CM-MAC=5c:35:3b:25:af:55;CMTS-MAC=00:30:b8:d4:f5:a0;CM-QOS=1.1;CM-VER=3.0;

Field Descriptions for the Status Event Log Section

Field	Description
Time	Indicates the date and time the error occurred
Priority	Indicates the level of importance of the error
Code	The Error Code field provides a value, represented as a decimal, that the described event encountered.
Message	A brief definition of the error

CABLE MODEM Addresses Section

This section provides information about the IPV4/IPV6 address, MAC address etc.



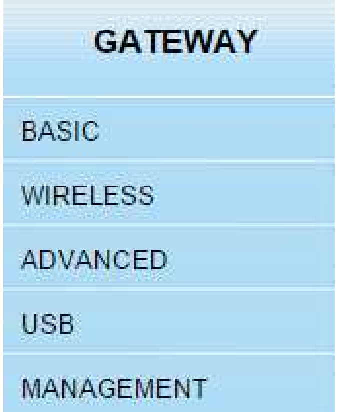
ADDRESSES

Item	Value
HFC Provisioning Mode	IPv4/IPv6
HFC IPv4 Address	172.16.70.36
HFC IPv6 Address	2002:db50:fa13:70:214d:a1a4:5666:cbbd
HFC MAC Address	5C-35-3B-25-AF-55
Ethernet IP Address	192.168.100.1
Ethernet MAC Address	5C-35-3B-25-AF-58

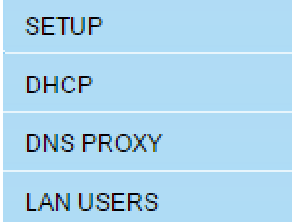
Known CPE MAC Address (Max 16)	Status
5C:35:3B:25:AF:57	static
5C:35:3B:25:AF:56	static

5.Gateway

CH6643E GATEWAY section provide six major items including BASIC Setup, WIRELESS, Advanced,USB and MANAGEMENT to control all gateway functions, describing respectively as below.

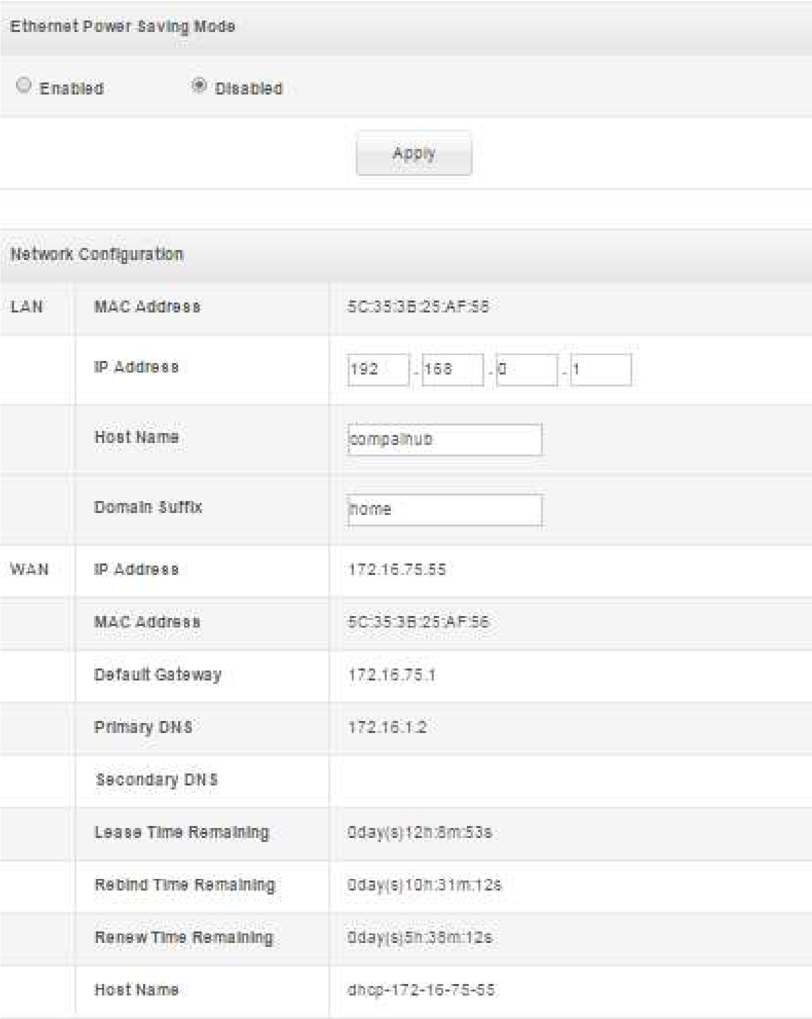


The CH6643E Basic section allows you to view and configure CH6643E IP-related configuration data, including Network Configuration, DHCP. DNS Proxy, You can click any Basic submenu option to view or change the configuration information for that option.



Basic Setup

This section allows you to configure the basic features of your CH6643E gateway related to your ISP connection.

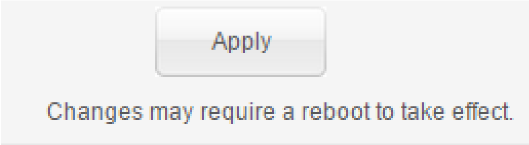


Ethernet Power Saving Mode

○ Enabled ● Disabled

Network Configuration

LAN	MAC Address	5C:35:3B:25:AF:56
	IP Address	192 . 168 . 0 . 1
	Host Name	compalhub
	Domain Suffix	home
WAN	IP Address	172.16.75.55
	MAC Address	5C:35:3B:25:AF:56
	Default Gateway	172.16.75.1
	Primary DNS	172.16.1.2
	Secondary DNS	
	Lease Time Remaining	0day(s)12h:8m:53s
	Rebind Time Remaining	0day(s)10h:31m:12s
	Renew Time Remaining	0day(s)5h:38m:12s
	Host Name	dhcp-172-16-75-55



Changes may require a reboot to take effect.

Field Descriptions for the Basic Setup Section

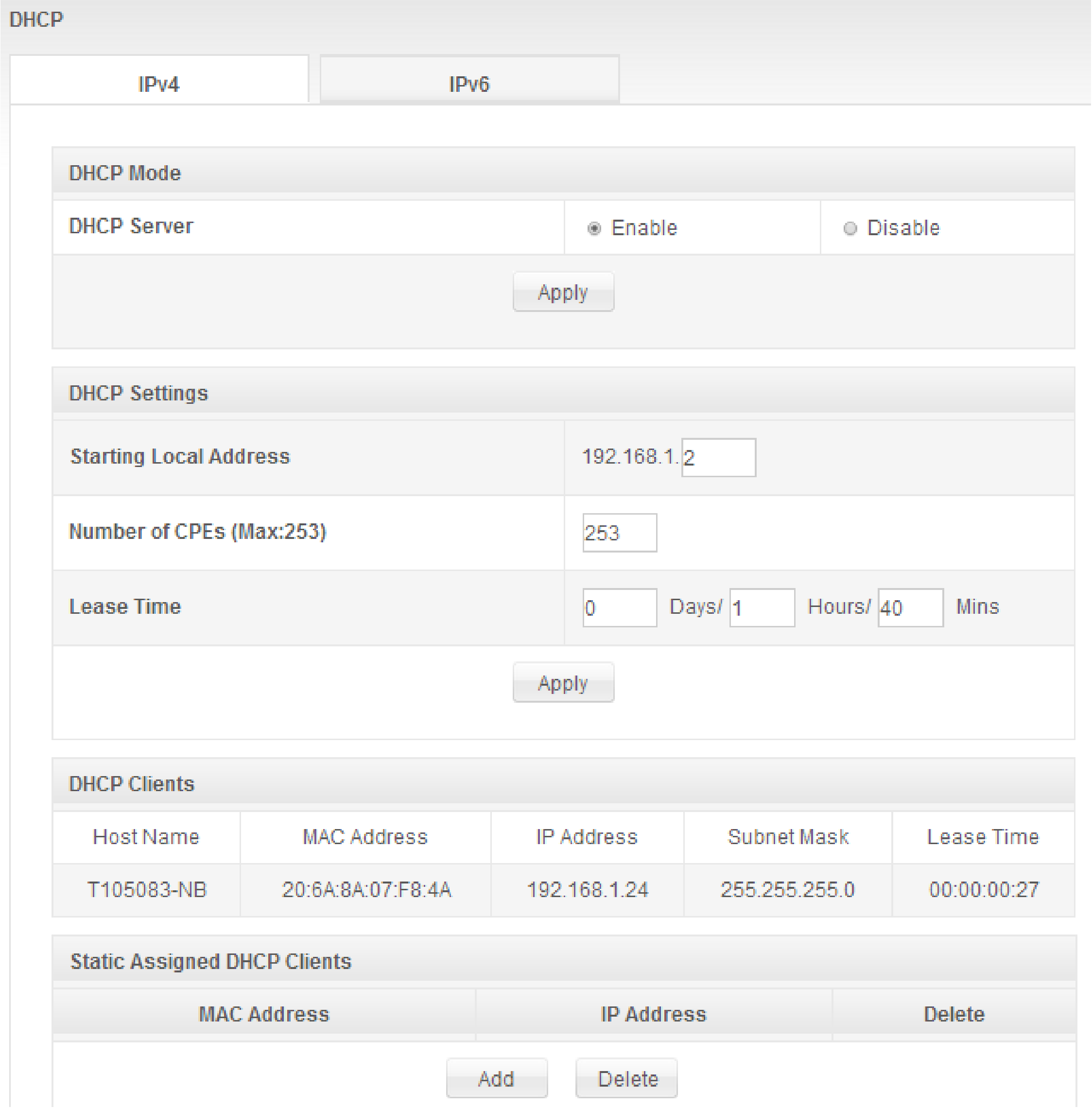
Field	Description
Ethernet Power Saving Mode	When there is no active Ethernet connection, CH6643E will enter a power-saving mode to reduce energy consumption.
Network Configuration **LAN** **IP Address**	Enter the IP address of the CH6643E on your private LAN.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the CH6643E Access Point.
Host Name	Enter Host Name is the name of your computer or server and is a unique identifier
Domain Suffix	Use this field to define the domain that you can enter into a Web browser (instead of an IP address) to reach the CH6643E on the LAN.
WAN	
IP Address	The public WAN IP address of your CH6643E device, which is either dynamically or statically assigned by your ISP.
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the CH6643E Access Point.
Default Gateway	The address of the default gateway on the internet
Primary DNS	The address of the primary domain name server (provided by your ISP).
Secondary DNS	Optional (In case your primary DNS server is unreachable)
Lease Time Remaining	This displays the time that elapses before your device's IP address lease expires, and a new IP address is assigned to it by the DHCP server.
Rebind Time Remaining	Describes how long before your DHCP server binding expires. The WAN lease will automatically rebind itself when it expires.

Field	Description
Renew Time Remaining	Describes how long before your Internet connection expires. The WAN lease will automatically renew itself when it expires.

When done, click **Apply** to save your changes.

Basic DHCP Section

This section allows you to configure IPv4 and view the status of the optional internal CH6643E DHCP (Dynamic Host Configuration Protocol) server for the LAN.



DHCP

IPv4 | IPv6

DHCP Mode

DHCP Server	● Enable	○ Disable

Apply

DHCP Settings

Starting Local Address	192.168.1. 2
Number of CPEs (Max:253)	253
Lease Time	0 Days/ 1 Hours/ 40 Mins

Apply

DHCP Clients

Host Name	MAC Address	IP Address	Subnet Mask	Lease Time
T105083-NB	20:6A:8A:07:F8:4A	192.168.1.24	255.255.255.0	00:00:00:27

Static Assigned DHCP Clients

MAC Address	IP Address	Delete

Add | Delete

CAUTION: *Do not modify these settings unless you are an experienced network administrator with strong knowledge of IP addressing, subnetting, and DHCP.*

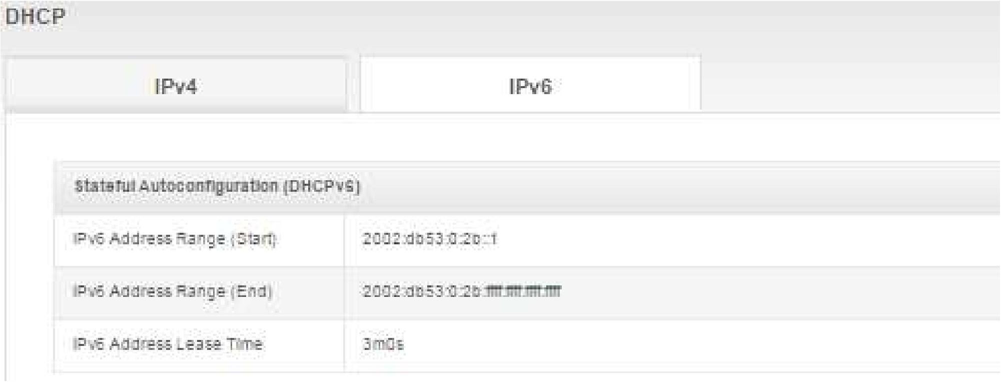
Field Descriptions for the Basic DHCP Section

Field	Description
DHCP Server	Enable / Disable DHCP function on your private LAN.
Starting Local Address	Use this field to specify the IP address at which the CH6643E begins assigning IP addresses to devices on the LAN (when DHCP is enabled).
Number of CPEs	Sets the number of clients for the CH6643E DHCP server to assign a private IP address. There are 253 possible client addresses.
Lease Time	Sets the time in seconds that the CH6643E DHCP server leases an IP address to a client.
DHCP Clients	Lists DHCP client device information.
Static Assigned DHCP clients	Reserve IP addresses assigned by the CH6643E DHCP server for specific LAN clients

When done, click **Apply** to save your changes.

DHCP IPV6

This section show IPv6 Stateful Auto configuration which allow view the status of the optional internal CH6643E IPv6/DHCPv6 (Dynamic Host Configuration Protocol) server for the LAN.



Stateful Autoconfiguration (DHCPv6)

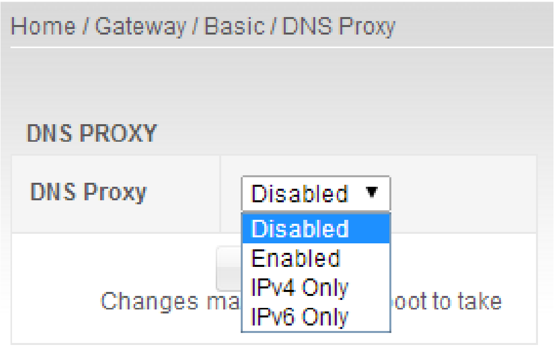
IPv6 Address Range (Start)	2002:db53:0:2b::1
IPv6 Address Range (End)	2002:db53:0:2b:ffff:ffff:ffff:ffff
IPv6 Address Lease Time	3m0s

Field Descriptions for the Basic DHCP Section – IPv6 tab

Field	Description
IPv6 Address Range (Start)	The start IPv6 addresses from delegation prefix for CH6643E DHCPv6 server to clients.
IPv6 Address Range (End)	The end IPv6 addresses from delegation prefix for CH6643E DHCPv6 server to clients.
IPv6 Address Lease Time	The lease time for IPv6 address.

Basic DNS Proxy Section

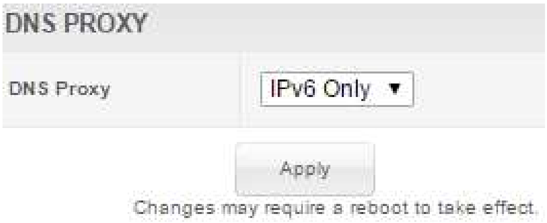
A DNS proxy server takes DNS queries from a (usually local) network and forwards them to an Internet Domain Name Server. It may also cache DNS records.



Home / Gateway / Basic / DNS Proxy

DNS PROXY

DNS Proxy: Disabled



DNS PROXY

DNS Proxy: IPv6 Only

Changes may require a reboot to take effect.

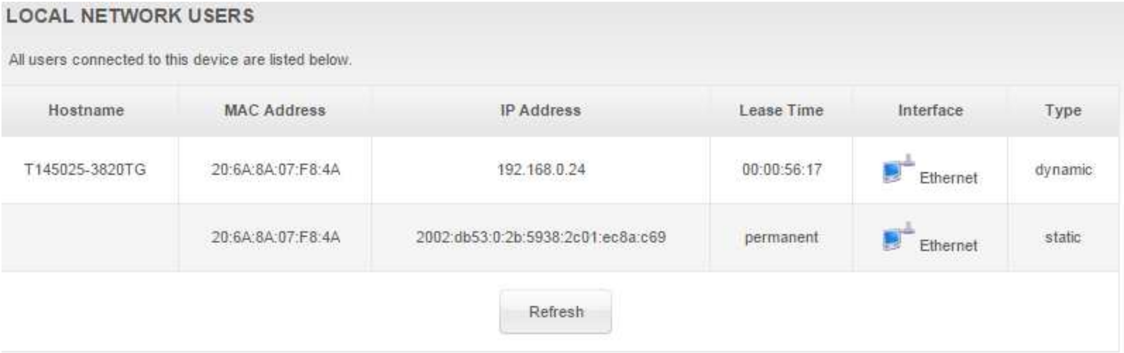
When done, click **Apply** to save your changes.

Field Descriptions for the Basic DNS PROXY Section

Field	Description
DNS Proxy	This section allow user to select basic DNS Proxy

Basic LAN Users

This section contains a list of LAN users which associated to this device.



LOCAL NETWORK USERS

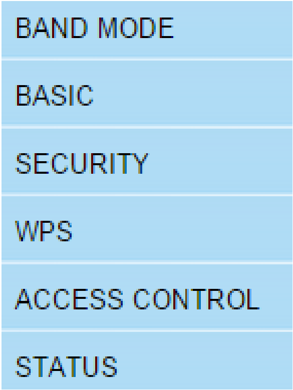
All users connected to this device are listed below.

Hostname	MAC Address	IP Address	Lease Time	Interface	Type
T145025-3820TG	20:6A:8A:07:F8:4A	192.168.0.24	00:00:56:17	Ethernet	dynamic
	20:6A:8A:07:F8:4A	2002:db53:0:2b:5938:2c01:ec8a:c69	permanent	Ethernet	static

Refresh

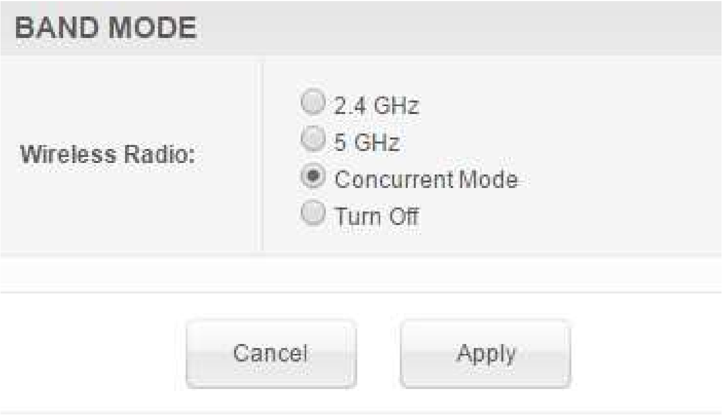
6.Gateway Wireless

The CH6643E Wireless Sections allow you to configure your wireless LAN (WLAN). You can click any Wireless submenu option to view or change the configuration information for that option. WPA or WPA2 encryption provides higher security than WEP encryption, but older wireless client cards may not support the newer WPA or WPA2 encryption methods.



Wireless Band Mode Section

CH6643E is a dual band concurrent product, therefore two wireless radio configurations are provided. This section allows you to configure the Wireless band mode, Select 2.4GHz if you want to use the 2.4GHz band only or 5GHz band if you want to use the 5GHz band only. Concurrent Mode allows you to use dual mode simultaneously. Turn Off will disable wireless, and you cannot associate with AP through wireless.

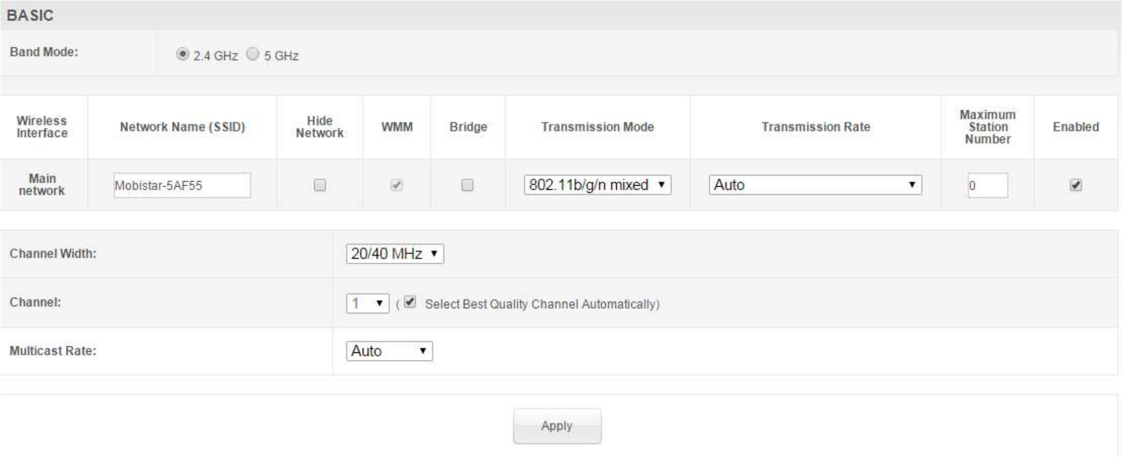


BAND MODE

Wireless Radio:	○ 2.4 GHz ○ 5 GHz ● Concurrent Mode ○ Turn Off

Wireless Basic Section

This section allows you to configure basic features of your Wi-Fi wireless network. You can enable or disable the wireless interface, hide the network from active scans, set the wireless network name (also known as SSID) and select the working channel.



BASIC

Band Mode: ● 2.4 GHz ○ 5 GHz

Wireless Interface	Network Name (SSID)	Hide Network	WMM	Bridge	Transmission Mode	Transmission Rate	Maximum Station Number	Enabled
Main network	Mobistar-5AF55	□	☑	□	802.11b/g/n mixed	Auto	0	☑

Channel Width:	20/40 MHz
Channel:	1 (☑ Select Best Quality Channel Automatically)
Multicast Rate:	Auto

Field Descriptions for the Wireless Basic Section

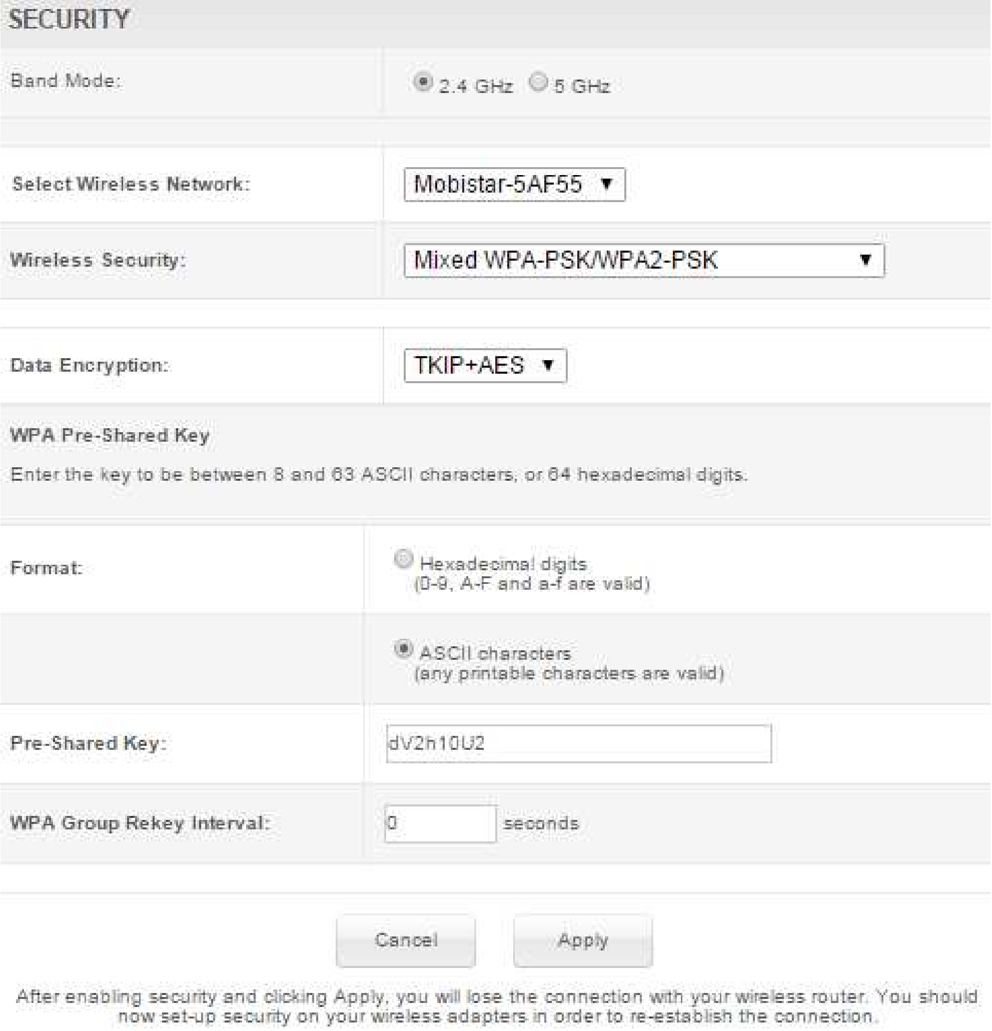
Field	Description
Band Mode	Select the band mode you want to set and this option appear only on Concurrent Mode.
SSID	Set the Network Name (also known as SSID) of the Primary wireless network. This is a 1-32 ASCII character string.
Hide Network	Users can type the SSID into the client application instead of selecting the SSID from a list. This feature

Field	Description
	makes it slightly more difficult for the user to gain access.
WMM	Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
Bridge	When the check box set, indicates network traffic from which particular wireless interface will be bridged to HFC interface. When the checkbox cleared, indicates network traffic from which particular wireless interface will be handled by Gateway routing features.
Transmission Mode	Select which 802.11 mode is used by CH6643E, including 802.11b/g/n mixed mode, 802.11g/n mixed mode, 802.11n only, 802.11b/g mixed mode, 802.11g only, for 802.11b only in 2.4G band mode, 802.11a/n mixed mode, 802.11a only, 802.11n only in 5G band mode.
Transmission Rate	Select 802.11 physical transmission rate, this value depends on Transmission Mode. If “Transmission Mode” is “802.11n only” and “802.11n Rate” is selected, the menu of MCS is provided and depends on whether a 20 MHz channel or 40 MHz channel is being used.
Maximum Station Number	Sets this field to limit the number of clients which allow connecting to this SSID and this is a number between 0 and 16. Set to 0 indicates no limitation.
Enable	Enable or disable this wireless interface.
Channel Width	Select the channel width (20 MHz or 20/40 MHz) to be used by CH6643E. When 20/40MHz is selected 802.11n clients experience improved throughput using 40 MHz, while legacy clients(either 802.11a or 802.11b/g) can still be serviced without interruption using 20MHz.
Channel	Select the current channel number or control channel, you can select “Select Best Quality Channel Automatically” check box to auto select one, this value depend on Transmission Mode.
Multicast Rate	Select the physical layer transmission rate used for Multicast traffic on the wireless interface, this value depend on Transmission Mode.

Wireless Security Section

This section allows you to protect your Wi-Fi wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security.

The default type of security is Mixed WPA-PSK/WPA2-PSK. Field of Mixed WPA-PSK/WPA2-PSK, WPA2-PSK and WPA-PSK are the same.



SECURITY

Band Mode:	● 2.4 GHz ○ 5 GHz
Select Wireless Network:	Mobistar-5AF55 ▼
Wireless Security:	Mixed WPA-PSK/WPA2-PSK ▼
Data Encryption:	TKIP+AES ▼

WPA Pre-Shared Key

Enter the key to be between 8 and 63 ASCII characters, or 64 hexadecimal digits.

Format:	○ Hexadecimal digits (0-9, A-F and a-f are valid)
	● ASCII characters (any printable characters are valid)
Pre-Shared Key:	dV2h10U2
WPA Group Rekey Interval:	0 seconds

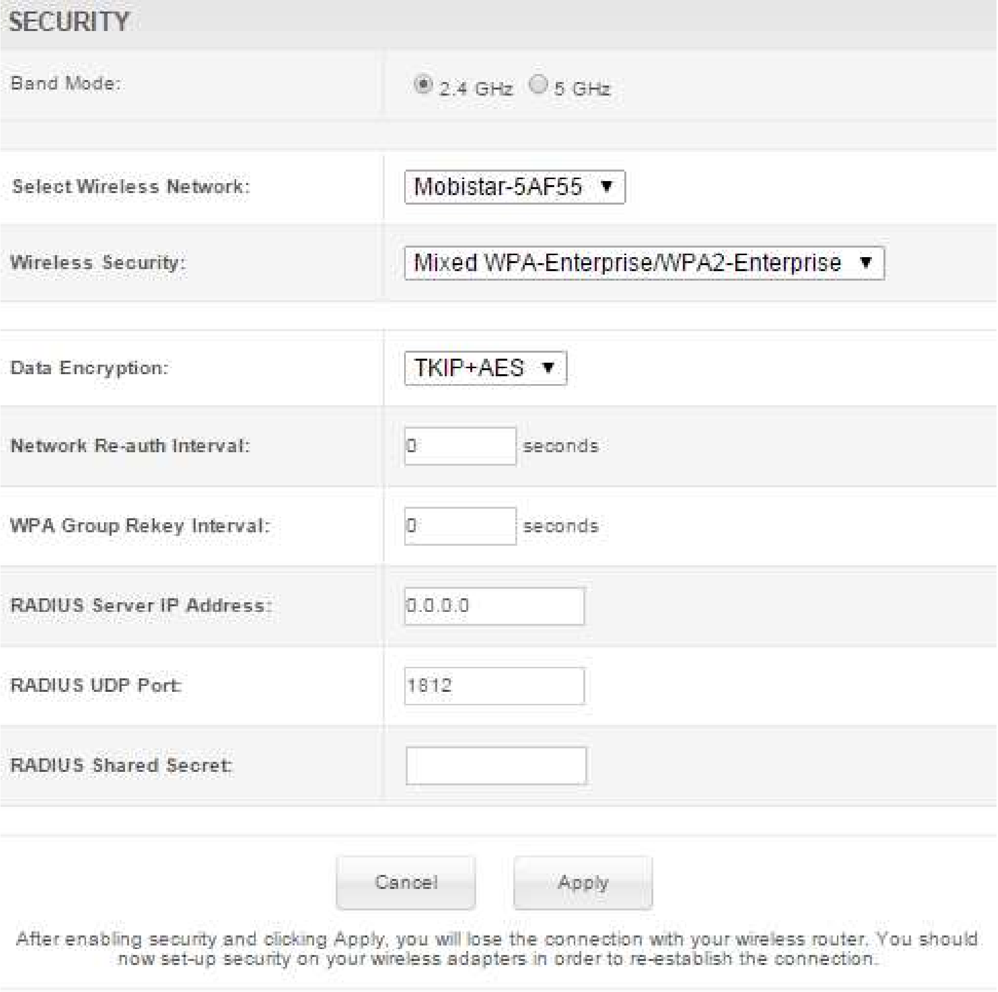
After enabling security and clicking Apply, you will lose the connection with your wireless router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Field Descriptions for Mixed WPA-PSK/WPA2-PSK, WPA2-PSK and WPA-PSK section

Field	Description
Data Encryption	When using WPA or WPA2 authentication, these WPA encryption modes can be set: TKIP, AES, or TKIP + AES. AES (Advanced Encryption Standard) provides the strongest encryption, while TKIP

Field	Description
	(Temporal Key Integrity Protocol) provides strong encryption with improved compatibility. the TKIP + AES mode allows both TKIP and AES-capable clients to connect.
Format	Sets the format of key as hexadecimal digits or ASCII character.
Pre-Shared Key	Sets the WPA/WPA2 Pre-Shared Key (PSK). This is either an 8-63 ASCII character string or 64 hexadecimal digits. This is specified when the Network Authentication method is WPA-PSK or WPA2-PSK.
WPA Group Rekey Interval	Sets the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying.

Field of Mixed WPA-Enterprise/WPA2-Enterprise, WPA-Enterprise and WPA2-Enterprise are similar.



SECURITY

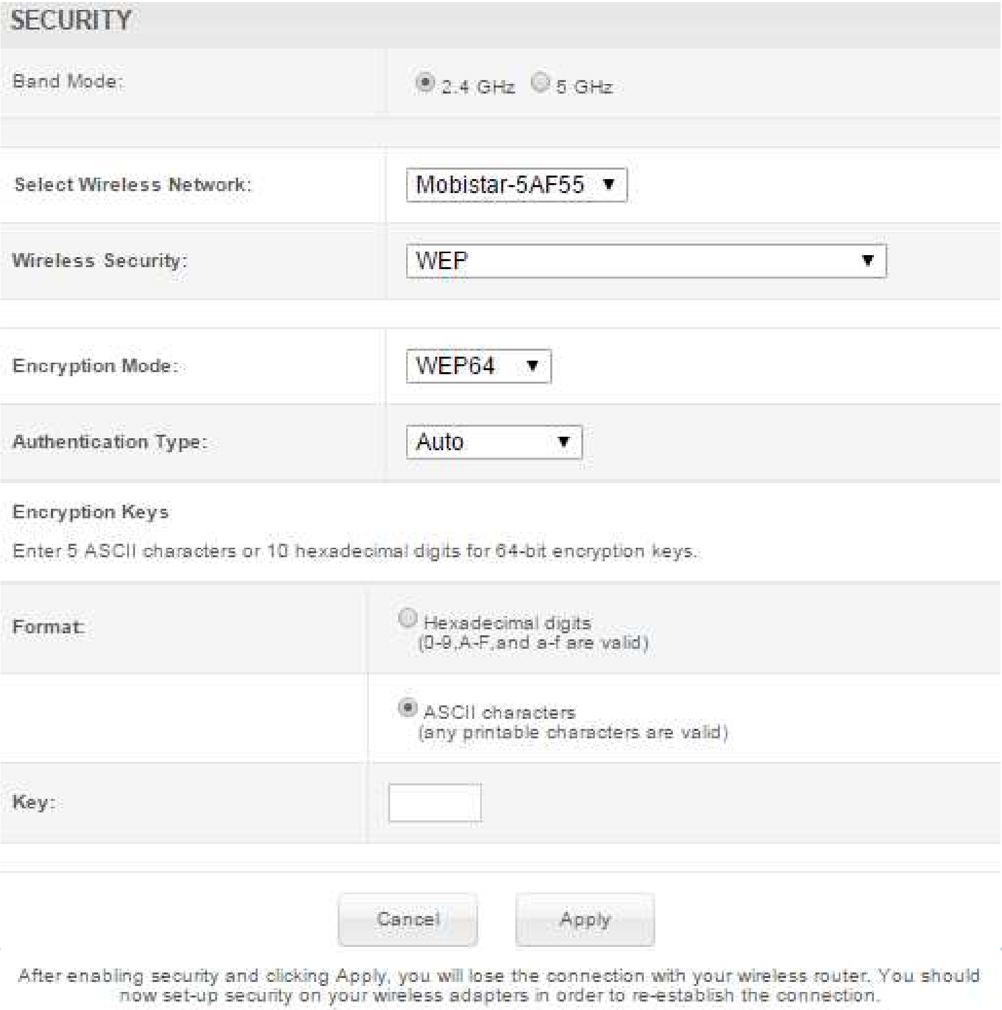
Band Mode:	● 2.4 GHz ○ 5 GHz
Select Wireless Network:	Mobistar-5AF55
Wireless Security:	Mixed WPA-Enterprise/WPA2-Enterprise
Data Encryption:	TKIP+AES
Network Re-auth Interval:	0 seconds
WPA Group Rekey Interval:	0 seconds
RADIUS Server IP Address:	0.0.0.0
RADIUS UDP Port:	1812
RADIUS Shared Secret:	

After enabling security and clicking Apply, you will lose the connection with your wireless router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Field Descriptions for WPA-Enterprise/WPA2-Enterprise, WPA-Enterprise and WPA2-Enterprise Section

Field	Description
Network Re-auth Interval	The re-authentication interval is the amount of time the wireless router can wait before re-establishing authentication with the CPE (WPA-Enterprise don't have this field).
RADIUS Server IP Address	Sets the RADIUS server IP address to use for client authentication using the dotted-decimal format (xxx.xxx.xxx.xxx).
RADIUS UDP Port	Sets the UDP port number of the RADIUS server. The default is 1812.
RADIUS Shared Secret	Sets the shared secret for the RADIUS connection. The key is a 0 to 255 character ASCII string.

WEP encryption



SECURITY

Band Mode:	● 2.4 GHz ○ 5 GHz
Select Wireless Network:	Mobistar-5AF55 ▼
Wireless Security:	WEP ▼
Encryption Mode:	WEP64 ▼
Authentication Type:	Auto ▼

Encryption Keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

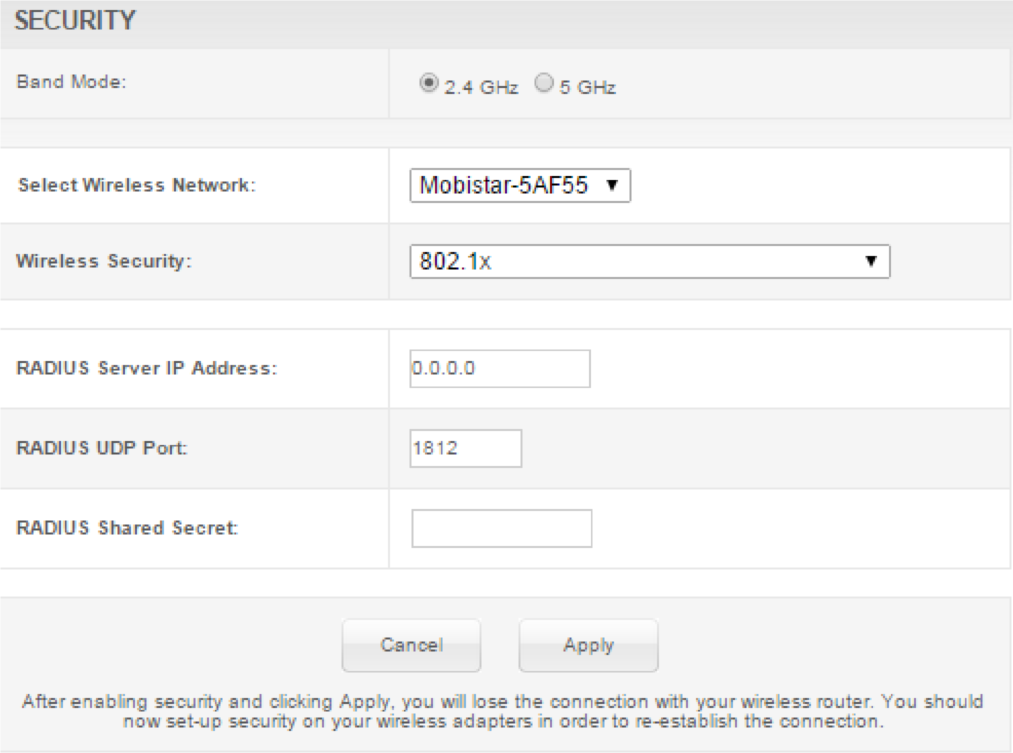
Format:	○ Hexadecimal digits (0-9,A-F,and a-f are valid)
	● ASCII characters (any printable characters are valid)
Key:	

After enabling security and clicking Apply, you will lose the connection with your wireless router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Field Descriptions for the WEP Section

Field	Description
Encryption Mode	The CPE uses either the 64-bit or 128-bit key to encrypt the challenge text and sends the encrypted text to the access point. The access point will decrypt the encrypted text and then compare the decrypted message with the original challenge text. If they are the same, the access point will let the CPE connect; if it doesn't match, then the access point does not let the CPE connect.
Authentication Type	Select the use of Shared Key authentication in WEP protocol. If select Auto, Shared Key authentication is optional. If select Shared Key, the Shared Key authentication is required for WEP.
Key 1 – 4	Sets the static WEP keys when WEP encryption is enabled. • Enter 5 ASCII characters for a 64-bit key. • Enter 13 ASCII characters for a 128-bit key.
Default Transmission Key	Selects the transmission key when WEP encryption is enabled.

802.1x encryption:



SECURITY

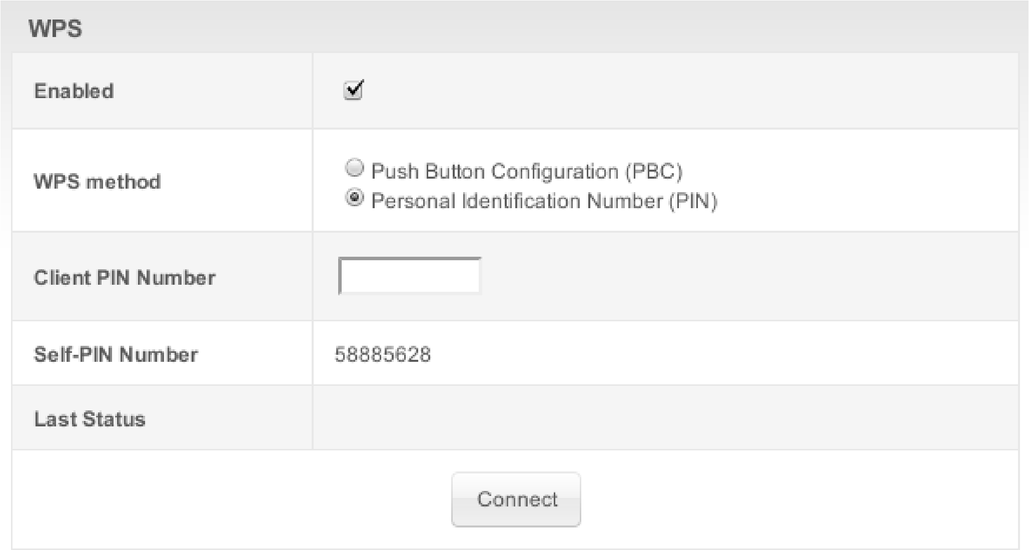
Band Mode:	● 2.4 GHz ○ 5 GHz
Select Wireless Network:	Mobistar-5AF55
Wireless Security:	802.1x
RADIUS Server IP Address:	0.0.0.0
RADIUS UDP Port:	1812
RADIUS Shared Secret:	

After enabling security and clicking Apply, you will lose the connection with your wireless router. You should now set-up security on your wireless adapters in order to re-establish the connection.

This is another type of authentication and is used on top of WEP. 802.1x Authentication is a much stronger type of authentication than WEP. About field description you can refer to tables above.

Wireless WPS Section

CH6643E provide WPS (Wi-Fi Protected Setup) function, with it enable will support WPS clients to join the network very easily. It is a standard for easy and secure establishment of a wireless network. With WPS you can setup and protect your wireless network in just a few easy steps.



WPS

Enabled	☑
WPS method	○ Push Button Configuration (PBC) ● Personal Identification Number (PIN)
Client PIN Number	
Self-PIN Number	58885628
Last Status	

Field Descriptions for the Wireless WPS Control Section

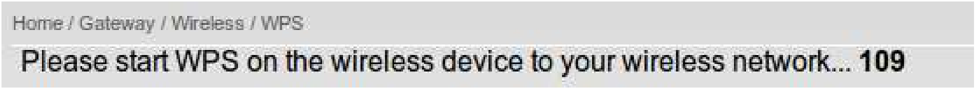
Field	Description
Enable	Enable or disable WPS.
WPS method	There are two common ways to establish WPS connection in CH6643E: 1. Push Button Configuration (PBC): If this option selected, you can press the "Connect" button below then push the WPS button on your wireless device (either an actual one or a virtual one) within 120 seconds to start the handshaking. 2. Personal Identification Number (PIN): A PIN filed will appear if this option selected, enter the PIN code from your wireless device and click the below "Connect" button to start the handshaking
PIN	Enter PIN code of wireless device.

Field	Description
Gateway PIN	CH6643E gateway's PIN code,

The step of WPS establishment:

- PBC
  1. Click or press the WPS button on the CH6643E's front panel or select Push Button Configuration (PBC) option radio then click "Connect" button in the web section "Home / Gateway / Wireless / WPS", the wireless LED will flash with orange color.
  2. Click or press the WPS button on the wireless device within 120 seconds.
  3. If WPS connection successfully established, the wireless LED will turn green.
- PIN
  1. In web section "Home / Gateway / Wireless / WPS", select Personal Identification Number (PIN) option radio then a "PIN" column will appear.
  2. Enter the wireless device's PIN code that is normally printed on the device's sticker or generated by connection manager of that device.
  3. Click "Connect", then the wireless LED will flash with orange color.
  4. Start PIN registration process by connection manager of that device within 120 seconds.
  5. If WPS connection successfully established, the wireless LED will turn green.

The countdown timer will start after you click "Connect" button

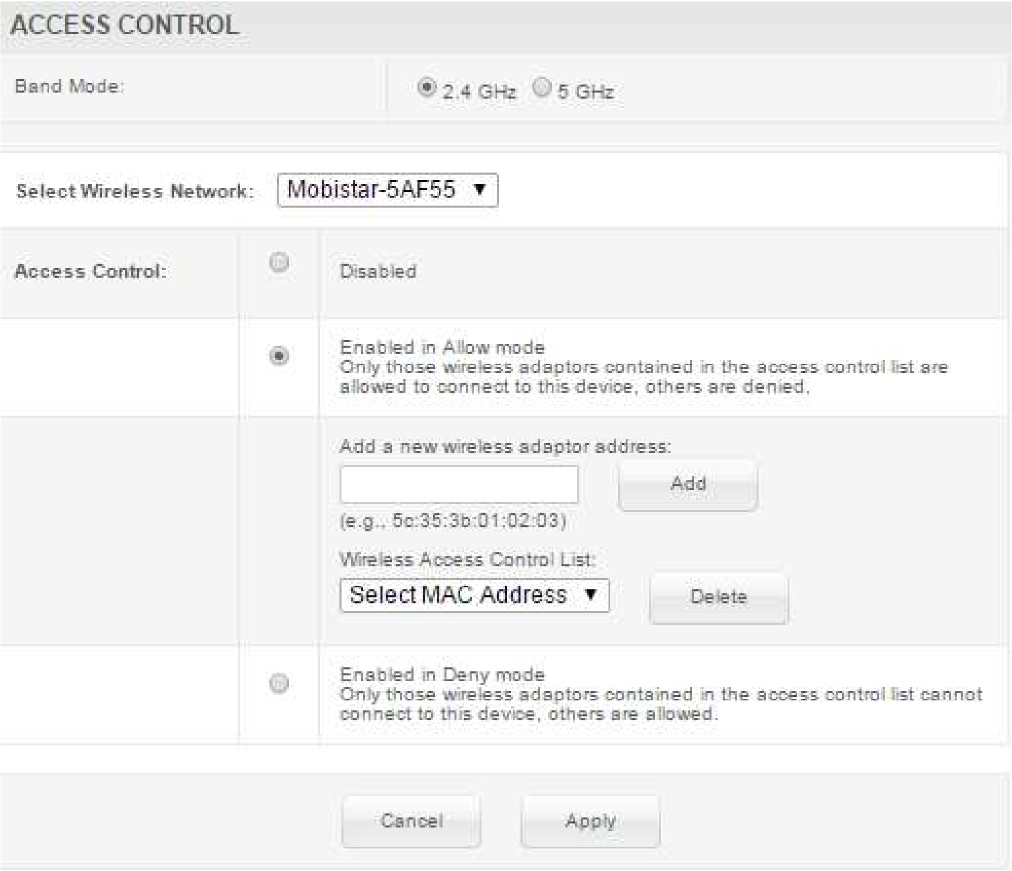


Home / Gateway / Wireless / WPS

Please start WPS on the wireless device to your wireless network... **109**

Wireless Access Control Section

This section allows you to configure the Access Control to the AP on the connected clients.



ACCESS CONTROL

Band Mode: ● 2.4 GHz ○ 5 GHz

Select Wireless Network: Mobistar-5AF55 ▼

Access Control:

○ Disabled

● Enabled in Allow mode
Only those wireless adaptors contained in the access control list are allowed to connect to this device, others are denied.

Add a new wireless adaptor address:

(e.g., 5c:35:3b:01:02:03)

Wireless Access Control List:

Select MAC Address ▼

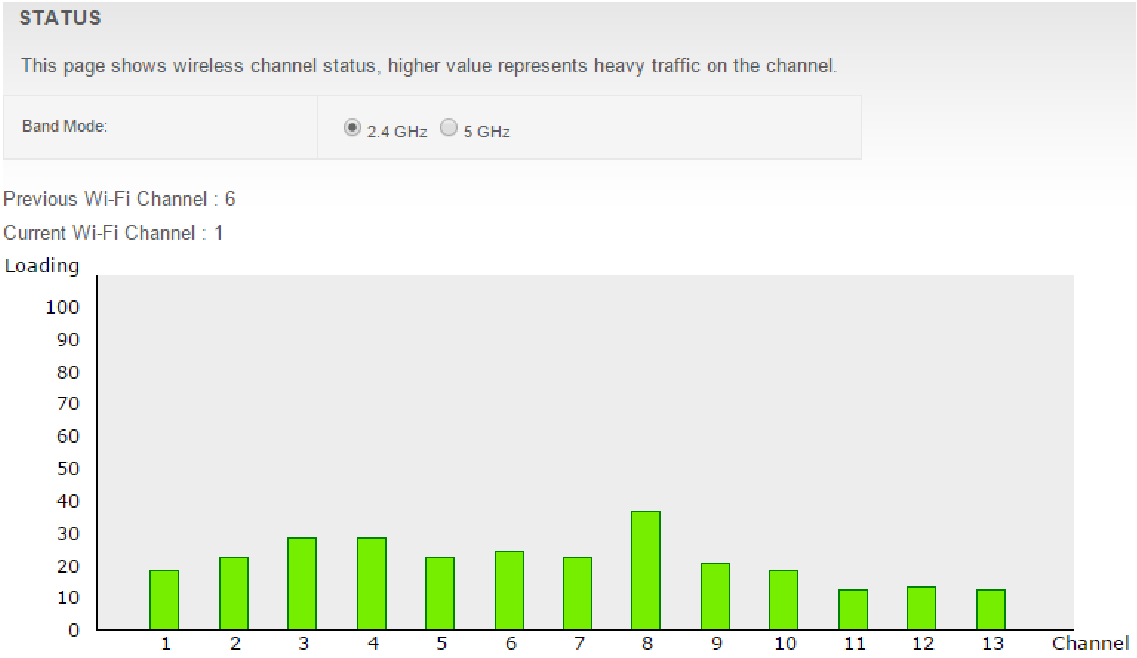
○ Enabled in Deny mode
Only those wireless adaptors contained in the access control list cannot connect to this device, others are allowed.

Field Descriptions for the Wireless Access Control Section

Field	Description
Access Control	Select “Disable” to disable access control Select Enabled in Allow mode then you can maintain a list of client allowed to connect to this device. Select Enabled in Deny mode then you can maintain a list of client cannot to connect to this device.

Wireless Status Section

This section show a histogram to represent wireless channel status on your environment, channel loading value between 0~100, higher value represents heavy traffic on this channel. For example: value 0 means no network traffic transmits on this channel, value 100 means the channel is heavy congested.



STATUS

This page shows wireless channel status, higher value represents heavy traffic on the channel.

Band Mode: ● 2.4 GHz ○ 5 GHz

Previous Wi-Fi Channel : 6

Current Wi-Fi Channel : 1

If you encounter the situation of wireless throughput degraded or slow response of network transmission, you may consider choosing a less congested channel base on the information provided by this section, and change you wireless channel on Wireless Basic Section.

Setting Up Your Wireless LAN

You can use the CH6643E as an access point for a wireless LAN (WLAN) without changing its default settings.

To enable security for your WLAN, you can do the following on the CH6643E:

- Encrypt wireless LAN transmissions
- Restrict wireless LAN access to further prevent unauthorized WLAN intrusions using the Wireless Access Control Section

> ***CAUTION:*** *Never provide your SSID, WPA or WEP passphrase, or WEP key to anyone who is not authorized to use your WLAN.*

Connect at least one computer to the CH6643E Ethernet port to perform configuration. Do not attempt to configure the CH6643E over a wireless connection.

You need to configure each wireless client (station) to access the CH6643E LAN.

Another step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.

Encrypting Wireless LAN Transmissions

To prevent unauthorized viewing of data transmitted over your WLAN, you must encrypt your wireless transmissions. Choose one of the following:

Encrypting Wireless LAN Transmissions

Configure on the CH6643E	Required on Each Wireless Client
If all of your wireless clients support Wi-Fi Protected Access (WPA), recommending configuring WPA on the CH6643E	If you use a local pre-shared key (WPA-PSK) passphrase, you must configure the identical passphrase on the CH6643E and on each wireless client. Home and small-office settings typically use a local passphrase.
Otherwise, configure WEP on the CH6643E	You must configure the identical WEP key on the CH6643E and on each wireless client.

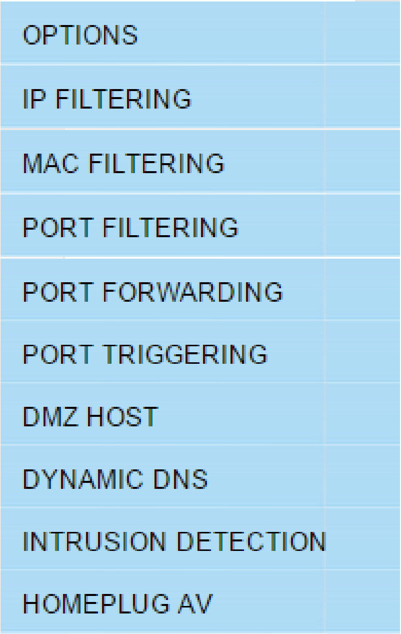
If all of your wireless clients support WPA encryption, recommending using WPA instead of WEP because WPA:

- Provides much stronger encryption and is more secure
- Provides authentication to ensure that only authorized users can log in to your WLAN
- Is much easier to configure
- Uses a standard algorithm on all compliant products to generate a key from a textual passphrase
- Will be incorporated into the new IEEE 802.11i wireless networking standard

For new wireless LANs, recommending purchasing client adapters that support WPA encryption.

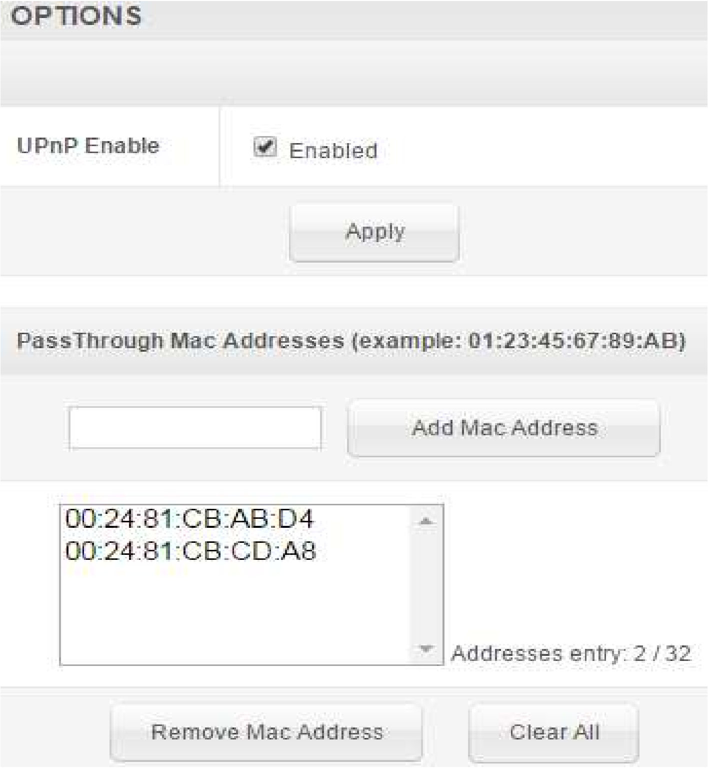
7.Gateway Advanced

The CH6643E Advanced Sections allow you to configure the advanced features of the CH6643E.You can click any Advanced submenu option to view or change the advanced configuration information for that option.



Advanced Options Section

This section allows you to set the operating modes for adjusting how the CH6643E device routes IP traffic.


OPTIONS

UPnP Enable ☑ Enabled

PassThrough Mac Addresses (example: 01:23:45:67:89:AB)

00:24:81:CB:AB:D4
00:24:81:CB:CD:A8

Addresses entry: 2 / 32

Field Descriptions for the Advanced Options Section

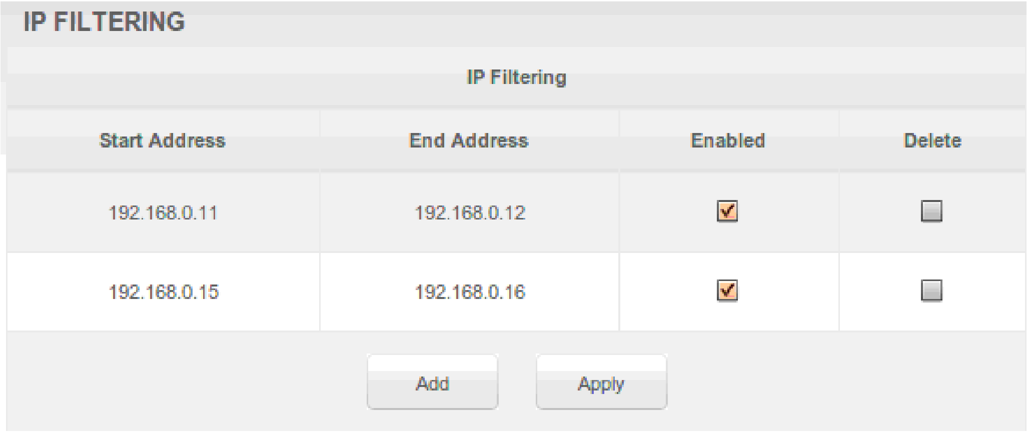
Field	Description
UPnP Enable	Turns on the Universal Plug and Play protocol (UPnP) agent in the configuration manager. If you are running a CPE (client) application that requires UPnP, select this box. Checkmark **Enable** to turn on this option.
PassThrough Mac Addresses	Specifies up to 32 computers as pass-through clients not subject to NAT, using their MAC addresses. To enable this feature, your cable operator may need to provide additional public IP addresses.

When done, click **Apply** to save your changes.

Advanced IP Filtering Section

This section allows you to define which local PCs will be denied access to the CH6643E WAN. You can configure IP address filters to block Internet traffic to specific network devices on the LAN by entering start and end IP address ranges. Note that you only need to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the CH6643E Configuration Manager's IP address.

The Enabled option allows you to store filter settings commonly used but not have them active.



IP FILTERING

IP Filtering

Start Address	End Address	Enabled	Delete
192.168.0.11	192.168.0.12	☑	□
192.168.0.15	192.168.0.16	☑	□

Field Descriptions for the Advanced IP Filtering Section

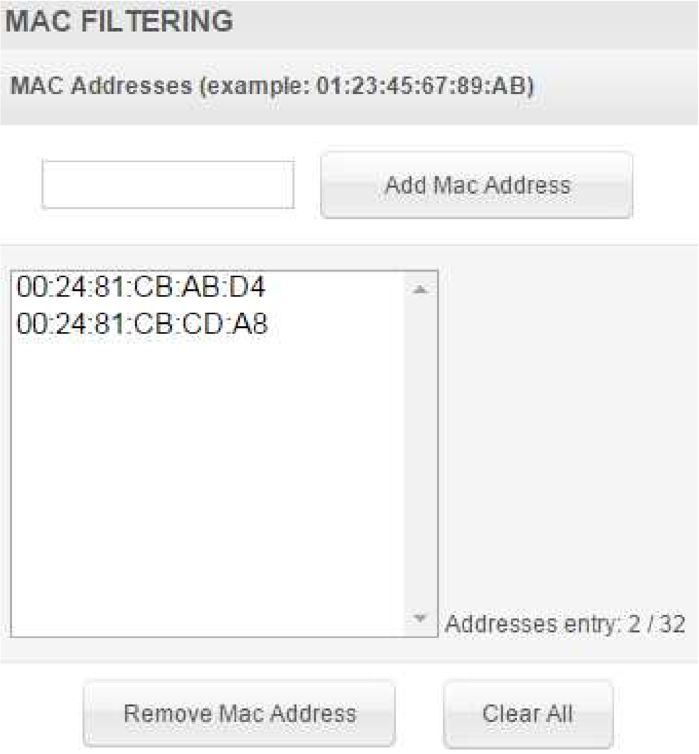
Field	Description
Start Address	Enter the start IP address range of the computers for which you want to deny access to the CH6643E WAN.

Field	Description
End Address	Enter the end IP address range of the computers you want to deny access to the CH6643E WAN.
Enabled	Activates the IP address filter, when selected. Checkmark **Enabled** for each range of IP addresses you want to deny access to the CH6643E WAN.
Delete	Remove the IP address filter, when selected. Checkmark **Delete** for each range of IP filter you want to remove.

When done, click **Apply** to activate and save your settings.

Advanced MAC Filtering Section

This section allows you to define up to twenty Media Access Control (MAC) address filters to prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. This is useful because the MAC address of a specific NIC card never changes, unlike its IP address, which can be assigned via the DHCP server or hard-coded to various addresses over time.



MAC FILTERING

MAC Addresses (example: 01:23:45:67:89:AB)

00:24:81:CB:AB:D4
00:24:81:CB:CD:A8

Addresses entry: 2 / 32

Field Descriptions for the Advanced MAC Filtering Section

Field	Description
MAC Addresses	Media Access Control address — a unique set of 12 hexadecimal digits assigned to a PC during manufacturing.

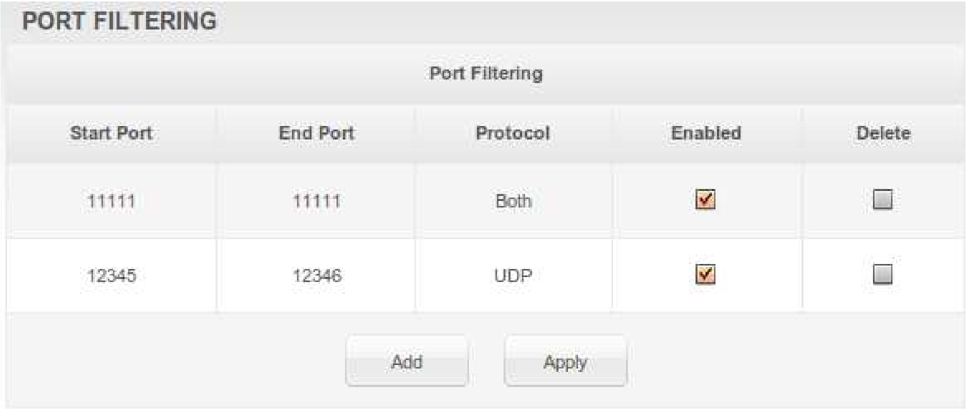
Setting a MAC Address Filter

1. Enter the MAC address in the MAC Addresses field for the PC you want to block.
2. Click **Add MAC Address**.
3. Repeat above steps for up to twenty MAC addresses.

Advanced Port Filtering Section

This section allows you to define port filters to prevent all devices from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. By specifying a starting and ending port range, you can determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis.

> ***Note:*** *The specified port ranges are blocked for ALL PCs, and this setting is not IP address or MAC address specific. For example, if you wanted to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), you would set the "Start Port" to 80, "End Port" to 80, "Protocol" to TCP, checkmark Enabled, and then click* ***Apply.***



PORT FILTERING

Port Filtering

Start Port	End Port	Protocol	Enabled	Delete
11111	11111	Both	☑	□
12345	12346	UDP	☑	□

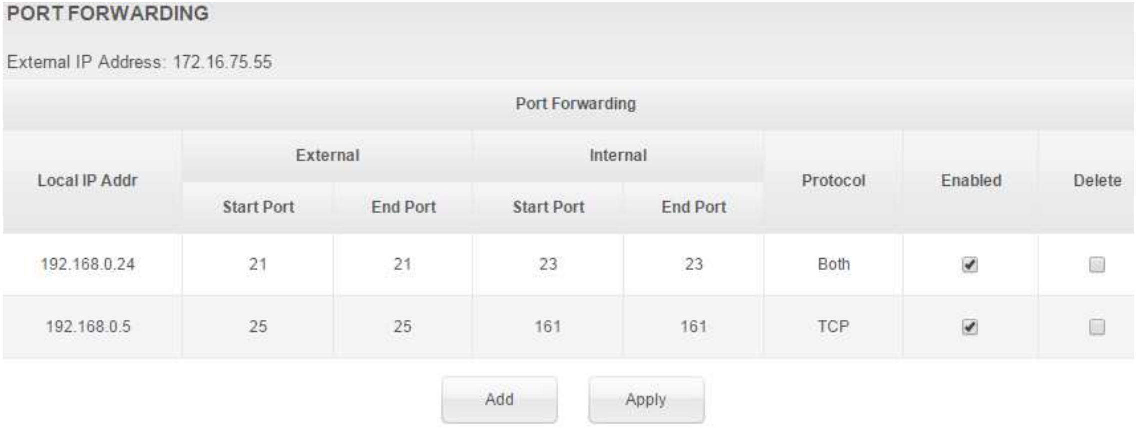
Field Descriptions for the Advanced Port Filtering Section

Field	Description
Start Port	Start port number.

Field	Description
End Port	End port number.
Protocol	TCP, UDP, or Both.
Enabled	Checkmark for each port that you want to activate the IP port filters.
Delete	Checkmark for each port that you want to remove the IP port filters.

Advanced Port Forwarding Section

This section allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC. This enables incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so that they can be accessible from the public Internet.



PORT FORWARDING

External IP Address: 172.16.75.55

Port Forwarding

Local IP Addr	External		Internal		Protocol	Enabled	Delete
	Start Port	End Port	Start Port	End Port			
192.168.0.24	21	21	23	23	Both	☑	□
192.168.0.5	25	25	161	161	TCP	☑	□

The ports used by some common applications are:

- HTTP: 80
- FTP: 20, 21
- Secure Shell: 22
- Telnet: 23
- SMTP e-mail: 25
- SNMP: 161

To map a port, you must enter the range of port numbers that should be forwarded locally and the IP address to which traffic to those ports should be sent. If only a single port specification is desired, enter the same port number in the “start” and “end” locations for that IP address.

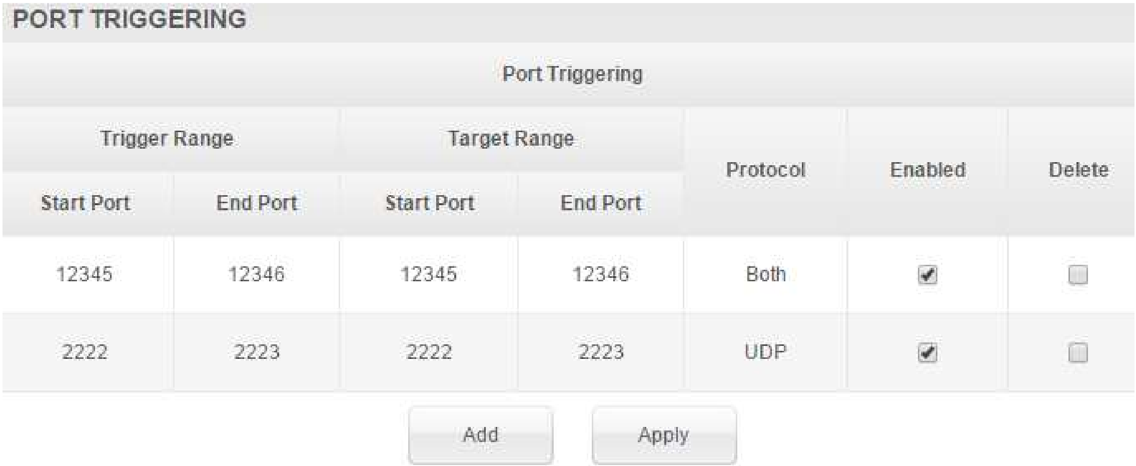
Field Descriptions for the Advanced Port Forwarding Section

Field	Description
Local IP address	Enter the IP address to which forwarded traffic should be sent.
Start Port	Start port number.
End Port	End port number.
Protocol	TCP, UDP, or Both.
Enabled	Checkmark for each port that you want to activate the IP port filters.
Delete	Checkmark for each port that you want to remove the IP port filters.

Advanced Port Triggers Section

This section allows you to configure dynamic triggers to specific devices on the LAN. This allows for special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

The Advanced Port Triggers are similar to Advanced Port Forwarding except that they are not static ports held open all the time. When the Configuration Manager detects outgoing data on a specific IP port number set in the "Trigger Range," the resulting ports set in the "Target Range" are opened for incoming (sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the "Trigger Range" ports for 10 minutes, the "Target Range" ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.



PORT TRIGGERING

Port Triggering

Trigger Range		Target Range		Protocol	Enabled	Delete
Start Port	End Port	Start Port	End Port			
12345	12346	12345	12346	Both	☑	☐
2222	2223	2222	2223	UDP	☑	☐

Field Descriptions for the Advanced Port Triggers Section

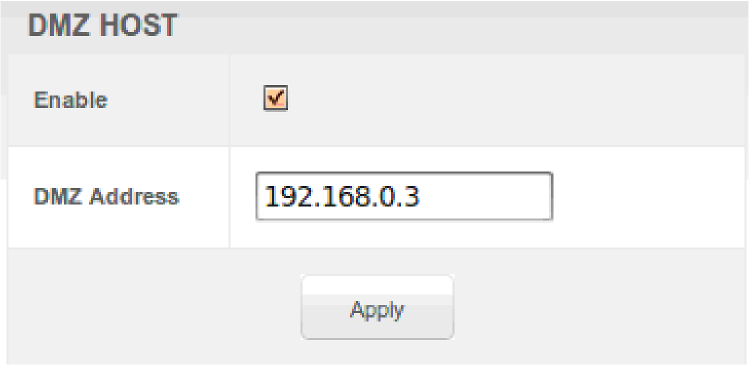
Field	Description
Trigger Range **Start Port**	The start port number of the Port Trigger range.
End Port	The end port number of the Port Trigger range.
Target Range **Start Port**	The start port number of the Port Target range.
End Port	The end port number of the Port Target range.
Protocol	TCP, UDP, or Both.
Enable	Select checkbox to activate the IP port triggers.
Delete	Select checkbox to remove the IP port triggers.

Advanced DMZ Host Section

This section allows you to specify the default recipient of WAN traffic that NAT is unable to translate to a known local PC. The DMZ (De-militarized Zone) hosting (also commonly referred to as "Exposed Host") can also be described as a computer or small sub-network that is located outside the firewall between the trusted internal private LAN and the un-trusted public Internet. It prevents direct access by outside users to private data.

For example, you can set up a web server on a DMZ computer to enable outside users to access your website without exposing confidential data on your network.

A DMZ can also be useful to play interactive games that may have a problem running through a firewall. You can leave a computer used for gaming only exposed to the Internet while protecting the rest of your network.



DMZ HOST

Enable	☑
DMZ Address	192.168.0.3

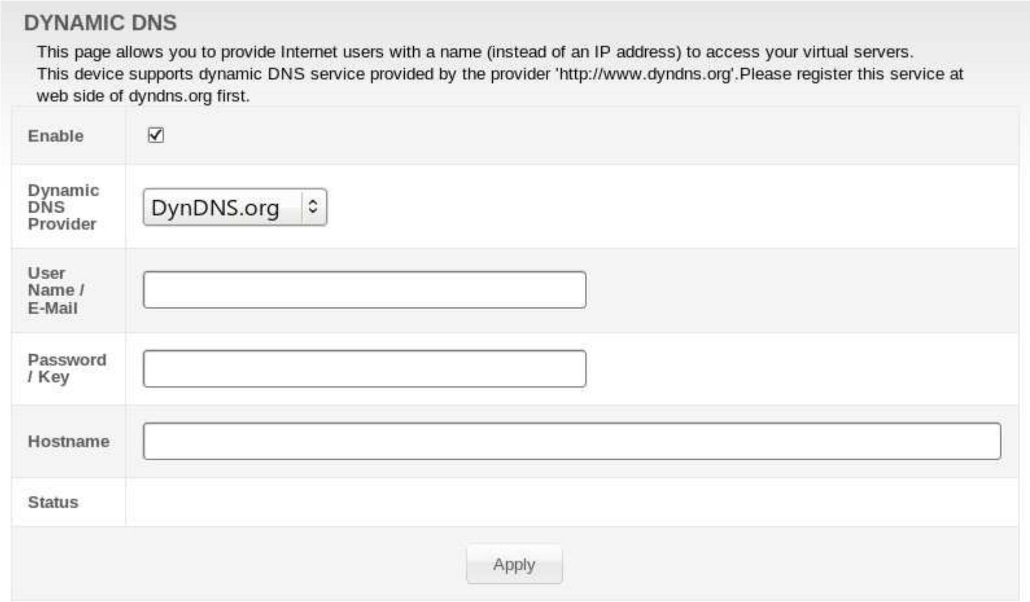
You may configure one PC to be the DMZ host. This setting is generally used for PCs using problem applications that use random port numbers and do not function correctly with specific port triggers or the port forwarding setups mentioned earlier. If a specific PC is set as a DMZ Host, remember to set this back to zero when you are finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

Setting Up the DMZ Host

1. Enter the computer's IP address and select **Enable** checkbox.
2. Click **Apply** to activate the selected computer as the DMZ host.

Advanced Dynamic DNS

This section allows you to provide Internet users with a name (instead of an IP address) to access your virtual servers. CH6643E supports dynamic DNS service provided by DynDNS.org, ChangeIP.com, No-IP.com and TZO.com. Please register this service at web site of them first.



DYNAMIC DNS

This page allows you to provide Internet users with a name (instead of an IP address) to access your virtual servers.
This device supports dynamic DNS service provided by the provider 'http://www.dyndns.org'.Please register this service at web side of dyndns.org first.

Enable	☑
Dynamic DNS Provider	DynDNS.org
User Name / E-Mail	
Password / Key	
Hostname	
Status	

Field Descriptions for the Dynamic DNS Section

Field	Description
Enable	Check the box to enable Dynamic DNS.
Dynamic DNS Provider	Choose your Dynamic DNS provider from the drop down menu.
User Name	Enter the user name for your Dynamic DNS account.
Password	Enter the password for your Dynamic DNS account.
Hostname	Enter the host name that you registered with your Dynamic DNS provider.
Status	Indicate the status of DDNS service.

Advanced Intrusion Detection Section

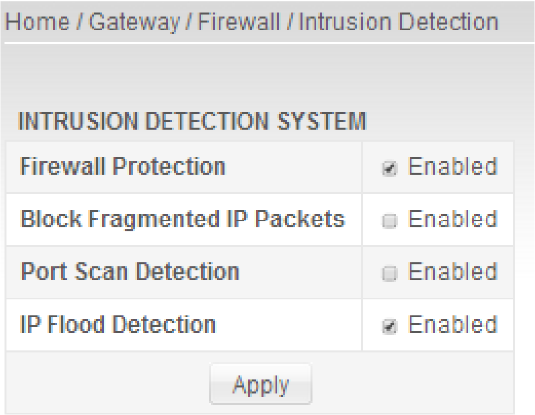
The CH6643E Intrusion Detection sections allow you to configure the CH6643E firewall filters and firewall alert notifications. The CH6643E firewall protects the CH6643E LAN from undesired attacks and other intrusions from the Internet. It provides an advanced, integrated stateful-inspection firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention. The firewall:

- Maintains state data for every TCP/IP session on the OSI network and transport layers.
- Monitors all incoming and outgoing packets, applies the firewall policy to each one, and screens for improper packets and intrusion attempts.
- Provides comprehensive logging for all
- User authentications
- Rejected internal and external connection requests
- Session creation and termination
- Outside attacks (intrusion detection)

The predefined policies provide outbound Internet access for computers on the CH6643E LAN. The CH6643E firewall uses stateful-inspection to allow inbound responses when there already is an outbound session running that corresponds to the data flow. For example, if you use a web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

When required, you can configure the CH6643E firewall to allow inbound packets without first establishing an outbound session. You also need to configure a port forwarding entry on the Advanced Port Forwarding Section or a DMZ client on the Advanced DMZ Host Section.

This section allows you to configure the firewall by enabling or disabling various protection features. Block Fragmented IP packets prevent all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN.



Home / Gateway / Firewall / Intrusion Detection

INTRUSION DETECTION SYSTEM

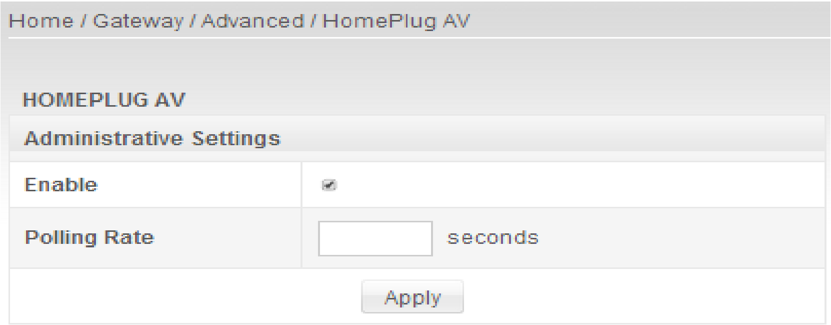
Firewall Protection	☑ Enabled
Block Fragmented IP Packets	□ Enabled
Port Scan Detection	□ Enabled
IP Flood Detection	☑ Enabled

Checkmark **Enable** for each Web filter you want to set for the firewall, and then click **Apply**. The Web filters will activate without having to reboot the CH6643E Configuration Manager.

Advanced HomePlug AV Section

This feature is to identify your HomePlug AV is functional or not when your HomePlug AV did not have response at end point. If you know the HomePlug AV's polling rate, then you can enter and apply. If you received your HomePlug AV from your service provider, please contact your service provide to obtain the polling rate for your HomePlug AV.

This section is for enable the HOMEPLUG AV function and also able to set the polling Rate (in seconds) at which the HPAV network will be polled to detect HomePlug AV devices. Polling rate of 0 indicates no polling."



Home / Gateway / Advanced / HomePlug AV

HOMEPLUG AV

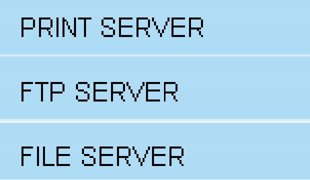
Administrative Settings

Enable	☑
Polling Rate	seconds

When done, click **Apply** to activate and save your settings.

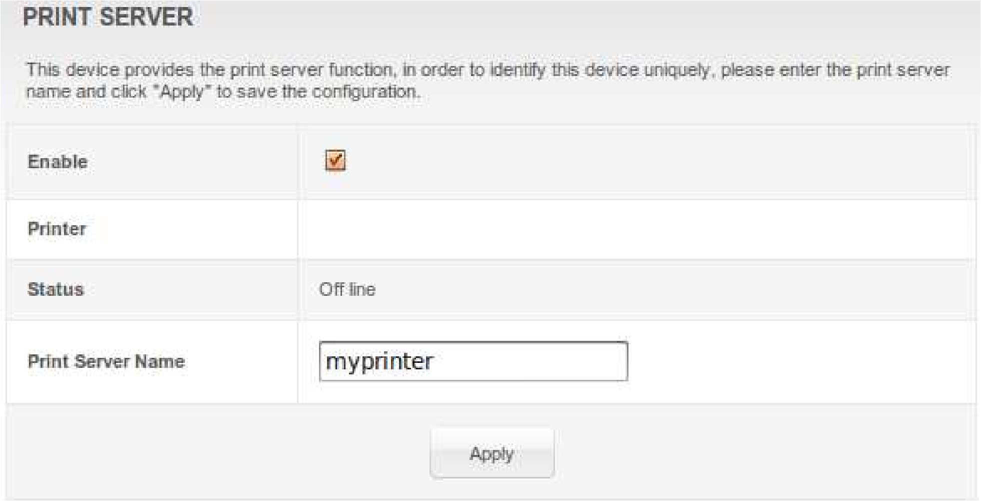
8.Gateway USB

The CH6643E support a variety of USB devices including printer and storage. You can plug USB printers and storages on the device and share them through internet.



Print Server

CH6643E support USB printer and share it based on Internet Printing Protocol (IPP) protocol that allow users connect and manage print jobs



PRINT SERVER

This device provides the print server function, in order to identify this device uniquely, please enter the print server name and click "Apply" to save the configuration.

Enable	☑
Printer	
Status	Off line
Print Server Name	myprinter

Field Descriptions for the Print Server Section

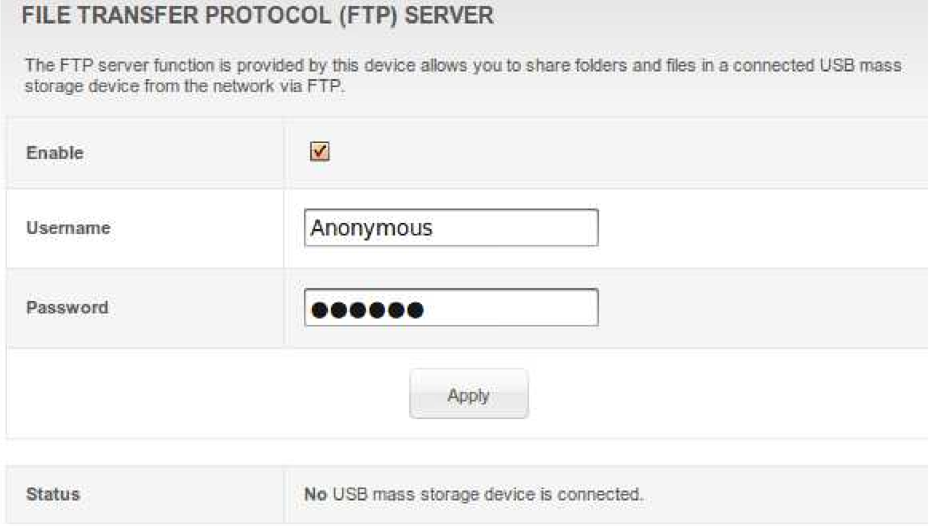
Field	Description
Enable	Enable or disable print server.
Printer	The printer's name.
Status	Status of the printer, maybe idle, busy, off-line or out-of-paper.
Print Server Name	The share name set by server let users can connect.

Steps to connect print server on windows client:

1. Open the Add Printer Wizard either by going via Start > Settings > Printers and Faxes, or by opening Printers and Faxes and clicking the add Printer icon.
2. After clicking "Add Printer", click the next button and configure this as a network printer. Click Next.
3. Click on "Connect to a printer on the Internet or on a home or office network" and set the address to "http://print:631/printers/myprinter".Click Next.
4. The wizard will prompt you to select a driver for your printer.
5. If all went well, you should see complete window. Click Finish.

FTP Server

CH6643E support USB storage and share it based on FTP (File Transfer Protocol) that allows users can login and manage it.



FILE TRANSFER PROTOCOL (FTP) SERVER

The FTP server function is provided by this device allows you to share folders and files in a connected USB mass storage device from the network via FTP.

Enable	☑
Username	Anonymous
Password	●●●●●●

Status	No USB mass storage device is connected.

Field Descriptions for the FTP Server Section

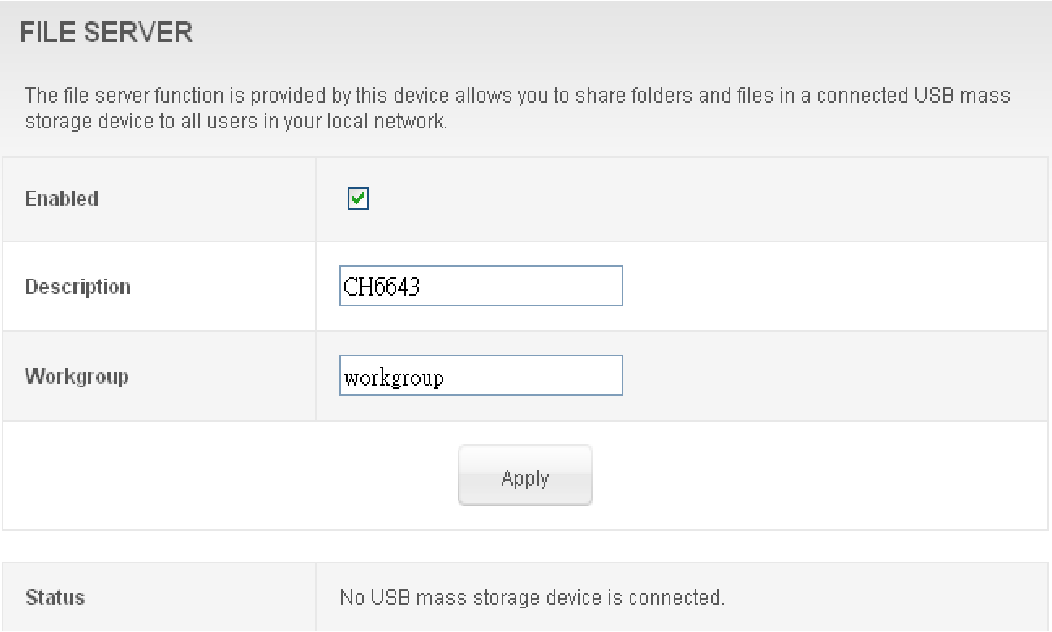
Field	Description
Enable	Enable or disable FTP server.
Username	The login username of FTP server.
Password	The login password of FTP server.
Status	Show vender and model info of the USB stick.

Steps to connect FTP server on windows client:

1. Open the “Windows Explorer” or double click “My Computer” icon on desktop.
2. Enter ftp://192.168.0.1/ in the address field and press **ENTER.**
3. Enter username and password in the prompt windows if the login username is not Anonymous.
4. The root directory of multiple USB mass storages are displayed in the browser, double click the directory you want to browser.
5. The folder structure of the USB mass storage is displayed in the file browser.

File Server

CH6643E support USB storage and share it based on Samba service that allow users can login and manage it.



FILE SERVER

The file server function is provided by this device allows you to share folders and files in a connected USB mass storage device to all users in your local network.

Enabled	☑
Description	CH6643
Workgroup	workgroup

Status	No USB mass storage device is connected.

Field Descriptions for the File Server Section

Field	Description
Enable	Enable or disable File server.
Description	The server string of samba server.
Workgroup	The workgroup name that the samba server resides on.

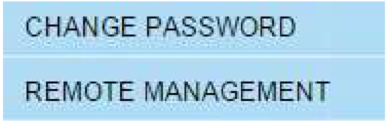
Field	Description
Status	Show information about the USB stick, including vendor name, model name, per partition size and file system type. There is a "safely remove" button after stick name column to unmount disk including all partition safely.

Step of connect file server on windows client:

1. Open the "Windows Explorer" or double click "My Computer" icon on desktop.
2. Enter \\192.168.0.1 in the address field and press **ENTER.**
3. The root directory of multiple USB mass storages are displayed in the browser, double click the directory you want to browser.
4. The folder structure of the USB mass storage is displayed in the file browser.

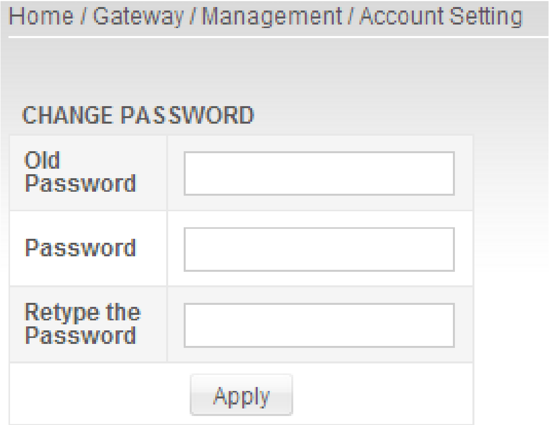
9.Gateway Management

The CH6643E support management for web browser login password, port and enable/disable web browser. These sections include change password function and Remote management.



Change Password

CH6643E allows changing admin password for web browser login. Configure Password and retype the Password again and then click Apply and when you login in next time, you must use this new password. For secure, we strongly suggest to change default password as soon as possible.



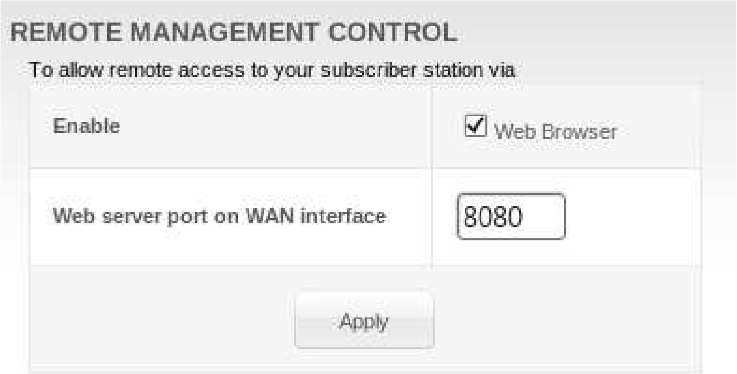
Home / Gateway / Management / Account Setting

CHANGE PASSWORD

Old Password	
Password	
Retype the Password	

Remote Management Control

Generally, only the members of your network can browse the web sections to perform administration tasks on CH6643E. Remote Management Control allows CH6643E to be configured by web browser and perform administration task from Internet.



REMOTE MANAGEMENT CONTROL

To allow remote access to your subscriber station via

Enable	☑ Web Browser
Web server port on WAN interface	8080

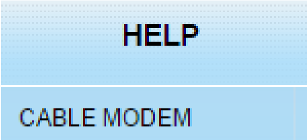
Field Descriptions for Remote Management Control

Field	Description
Enable	
Web Browser	Check the box to allow remote control by web browser.
Web server port on WAN Interface	Enter the port number of web server on WAN interface.

After apply settings, on remote host, you can browse the web section on CH6643E with IP address on WAN interface and indicated port number, for example: http://x.x.x.x:8080. Whereas you can get IP address from GATEWAY-BASIC-SETUP section.

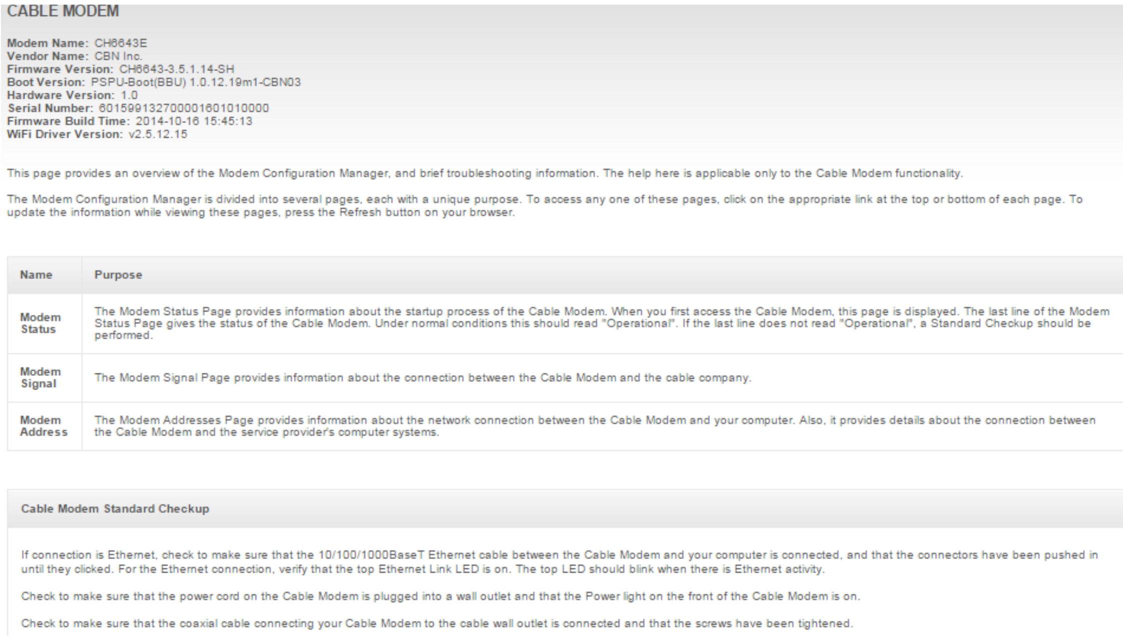
10.Help

Click any HELP submenu option to view the status information for that option.



HELP Cable Modem Section

This section provides some important and useful information about CH6643E, including modem name, firmware version, serial number and Wi-Fi driver version.



CABLE MODEM

Modem Name: CH6643E
Vendor Name: CBN Inc.
Firmware Version: CH6643-3.5.1.14-SH
Boot Version: PSPU-Boot(BBU) 1.0.12.19m1-CBN03
Hardware Version: 1.0
Serial Number: 601599132700001601010000
Firmware Build Time: 2014-10-16 15:45:13
WiFi Driver Version: v2.5.12.15

This page provides an overview of the Modem Configuration Manager, and brief troubleshooting information. The help here is applicable only to the Cable Modem functionality.

The Modem Configuration Manager is divided into several pages, each with a unique purpose. To access any one of these pages, click on the appropriate link at the top or bottom of each page. To update the information while viewing these pages, press the Refresh button on your browser.

Name	Purpose
Modem Status	The Modem Status Page provides information about the startup process of the Cable Modem. When you first access the Cable Modem, this page is displayed. The last line of the Modem Status Page gives the status of the Cable Modem. Under normal conditions this should read "Operational". If the last line does not read "Operational", a Standard Checkup should be performed.
Modem Signal	The Modem Signal Page provides information about the connection between the Cable Modem and the cable company.
Modem Address	The Modem Addresses Page provides information about the network connection between the Cable Modem and your computer. Also, it provides details about the connection between the Cable Modem and the service provider's computer systems.

Cable Modem Standard Checkup

If connection is Ethernet, check to make sure that the 10/100/1000BaseT Ethernet cable between the Cable Modem and your computer is connected, and that the connectors have been pushed in until they clicked. For the Ethernet connection, verify that the top Ethernet Link LED is on. The top LED should blink when there is Ethernet activity.

Check to make sure that the power cord on the Cable Modem is plugged into a wall outlet and that the Power light on the front of the Cable Modem is on.

Check to make sure that the coaxial cable connecting your Cable Modem to the cable wall outlet is connected and that the screws have been tightened.

11.Trouble Shooting

If the solutions listed here do not solve your problem, contact your service provider.

Before calling your service provider, try pressing the Reset button on the rear panel of the CH6643E. Please note, if you press the Reset button, you will lose all your custom configuration settings, including Firewall and Advanced settings. Your service provider may ask for the front panel LED status; see Front-Panel LEDs and Error Conditions.

Solutions

Table 1 – Troubleshooting Solutions

Problem	Possible Solution
Power light is off	Check that the CH6643E is properly plugged into the electrical outlet. Check that the electrical outlet is working. Press the **Power On/Off** button of CH6643E.
Cannot send or receive data	On the front panel, note the status of the LEDs and refer to Front-Panel LEDs and Error Conditions to identify the error. If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function. Check the coaxial cable at the CH6643E and wall outlet. Hand-tighten, if necessary. Check the IP address. Check that the Ethernet cable is properly connected to the CH6643E and the computer. If a device is connected via the Ethernet port, verify connectivity by checking the LINK LEDs on the rear panel.
Wireless client(s) cannot send or receive data	Perform the first four checks in "Cannot send or receive data." Check the Security Mode setting on the Wireless Security Section: • If you enabled WPA and configured a passphrase on the CH6643E, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check whether the wireless client supports WPA. • If you enabled WEP and configured a key on the CH6643E, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client's wireless adapter supports the type of WEP key configured on the CH6643E. • To temporarily eliminate the Security Mode as a potential issue, disable security. After resolving your problem, be sure to re-enable wireless security. • On the Wireless Access Control Section, be sure the MAC address for each affected wireless client is correctly listed.
Slow wireless transmission speed with WPA enabled	On the Wireless Primary Network Section, check whether the WPA Encryption type is TKIP. If all of your wireless clients support AES, change the WPA Encryption to AES.

Front-Panel LEDs and Error Conditions

The CH6643E front panel LEDs provides status information for the following error conditions:

Table 2 – Front-Panel LEDs and Error Conditions

LED	Status	if, During Startup:	if, During Normal Operation:
POWER	OFF	CH6643E is not properly plugged into the power outlet	The CH6643E is unplugged
RECEIVE	FLASHING	Downstream receive channel cannot be acquired	The downstream channel is lost
SEND	FLASHING	Upstream send channel cannot be acquired	The upstream channel is lost
ONLINE	FLASHING	IP registration is unsuccessful	The IP registration is lost

12. FCC Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

This device is restricted for indoor use.

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.