



let's make it *easy*

# U10C019/U10C020

## End User Guide

2/12/2009

Version 1.6

User's Guide

# Revision History

Issue	Date	Author/Prime	Description of changes
1.3	2005-09-05		
1.4	2008-07-22	David	Add new telnet commands
1.5	2008-08-13	John Yan	Revised the format. And enhance with VPN, DDNS configuration, merged U10C020 into this edition. Update Tool options page; Update user login screenshot; Remove Routing pages.
1.6	2009-02-11	Kyle Li	Revise to comply with new Ubee format

## CONTENTS

Revision History .....	1
1. Introduction.....	3
2. Before you begin.....	3
3. Installing the Modem Using Wireless .....	6
4. Installing the Modem Using the Ethernet Port.....	7
5. Wireless Cable Modem LEDs and Connectors.....	10
6. Web User Interface .....	11
6.1    MODEM.....	13
6.1.1    Information.....	13
6.1.2    Status .....	14
6.1.3    Downstream.....	15
6.1.4    Upstream .....	16
6.1.5    Upstream Burst.....	17
6.1.6    Operation Configuration.....	18
6.1.7    Event Log.....	19
6.2    Gateway .....	20
6.2.1    Information.....	21
6.2.2    Basic Setup .....	22
6.2.3    DHCP .....	23
6.2.4    DHCP static Lease .....	25
6.2.5    DDNS .....	26
6.2.6    Time .....	27
6.2.7    Advanced- Options .....	28
6.2.8    Advanced - MAC Filtering.....	28
6.2.9    Advanced - IP Filtering.....	29
6.2.10    Advanced - Port Filtering .....	30
6.2.11    Advanced - Forwarding.....	31
6.2.12    Advanced - Port Triggering .....	33
6.2.13    Advanced- Pass Through .....	35
6.2.14    Advanced- DMZ Host (Exposed Host).....	36
6.3    Wireless.....	37
6.3.1    Basic .....	37
6.3.2    Security .....	38

6.3.3	Access Control .....	41
6.3.4	Guest Network: Multiple SSID Support.....	43
6.4	VPN .....	44
6.4.1	VPN- Enable .....	45
6.4.2	VPN-Summary .....	45
6.4.3	VPN- Configure .....	46
6.4.4	VPN - L2TP / PPTP .....	53
6.4.5	VPN - Event Log.....	55
6.5	Parental Control.....	55
6.5.1	User Setup .....	55
6.5.2	Activation.....	58
6.5.3	TOD Filter .....	59
6.5.4	Event Log.....	61
6.6	Firewall.....	62
6.6.1	Content Filter .....	63
6.6.2	Event Log.....	65
6.6.3	Remote Log .....	66
6.7	Tools .....	66
6.7.1	Ping .....	66
6.7.2	Trace Route.....	67
6.7.3	Client List.....	68
6.7.4	Frequency Scanning Plan .....	69
6.7.5	Password.....	70
6.7.6	User Defaults.....	70

# 1. Introduction

Your new wireless cable modem provides high-speed wireless access to the Internet by using IEEE 802.11b/g wireless standard and an active Internet Connection through your cable service provider. This user guide describes how to set up and use the wireless cable modem. Before installing the wireless cable modem, you should read this user guide to ensure proper wireless cable modem operation. U10C019 is a wireless cable router, while U10C020 is a wired cable router that doesn't provide WiFi functionality. Other features are similar with U10C019.

## 2. Before you begin

### ***Understand the Wireless Cable Modem's Features***

- Your wireless cable modem has the following features to help you access and use the Internet:
- Wireless connectivity means that you can use your PC just about anywhere in your home.
- 802.11b/g compliance ensures interoperability with other 802.11b/g compliant devices
- Your wireless cable modem supports transmission rates of 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps.
- Two-way design allows the wireless cable modem to send and receive data over the cable television network.
- Cable bandwidth allows data rates of up to 38 megabits per second (Mbps)\*, which is faster than analog modems, integrated services digital network (ISDN), or asymmetric digital subscriber line (ADSL).
- Using your cable line means that the wireless cable modem is always on, always connected, and doesn't tie up your phone line.
- Plug-and-play operation through universal serial bus (USB) ensures easy setup and installation.

- Data Over Cable Service Interface Specification (DOCSIS<sup>1</sup>) compliance ensures interoperability with DOCSIS compliant cable operators.

*\*NOTE: Speeds may vary based on the following factors:*

- *Computer equipment including available RAM and processor speed*
- *Software applications utilizing your computer's resources*
- *Network traffic depending on the time of day*
- *Limitations set by your Cable Service Provider*

## **Contact Your Local Cable Operator**

Before installing your new wireless cable modem, you must contact your local cable service provider to activate your Internet account. Be sure to have the wireless cable modem's MAC address available, which can be found on the underside of the wireless cable modem.

## **Prepare Your Area for Wireless Cable Modem Installation**

Before installing your wireless cable modem, you should first prepare your area. To do this:

- 1) Locate your cable outlet and ensure that it is located within proper distance of your wireless cable modem and computer. Be sure not to bend the cable as this may strain the connector and cause damage.
- 2) Place wireless cable modem as high as possible. Allow sufficient airflow around the wireless cable modem to prevent overheating.
- 3) Place wireless cable modem and wireless clients in open areas or far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment.
- 4) Ensure that the temperature in the room where the wireless cable modem will be operating is between 0 and 40C (32 and 104F)
- 5) The wireless signal may be weaker after it has passed through metal, concrete, brick, walls, or floors. Also, make sure that the wireless cable modem and wireless adapters are positioned so that the signal will travel straight through a wall or ceiling for better reception. For example, a wall that is 1 foot thick, at a 45-degree angle appears to be almost 2 feet thick.

## ***Gather Supplied and Required Items***

You will use a variety of items to install your wireless cable modem. Some of the items are supplied with your wireless cable modem.

### ***Supplied***

Verify that these items were included in the cable modem's package:

- Wireless cable modem
- Power adapter
- USB cable (1.5m)
- Ethernet cable (1.8m)
- CD containing USB drivers

### ***Not Supplied***

Verify that these items are available before beginning the installation:

If using the wireless cable modem's USB port:

- A PC running Windows 98<sup>®</sup> Second Edition (SE), Windows Me, Windows 2000, or Windows XP. The cable modem's USB setup does not support the Macintosh operating system, Windows 98 First Edition, and NT.
- Windows 98 SE, Windows Me, Windows 2000, or Windows XP CD or disks.
- An active USB port on your PC.

If using the wireless cable modem's Ethernet port:

- A PC running Windows 95 (or later) operating system or a Macintosh computer running system 7.6 (or later) operating system
- An active Ethernet port on your PC or Macintosh

If using the wireless cable modem's Wireless feature:

- A PC running Windows 98 (or later) operating system or a Macintosh computer running system 7.6 (or later) operating system
- An active wireless client on your PC or Macintosh

Be sure to follow the instructions provided for the port that you want to use. Using the Wireless feature of your wireless cable modem is the simplest and quickest way to

connect your PC or MAC to the Internet. All you need is an 802.11b/g wireless client that is connected to your PC or MAC. Depending on your cable service provider, you may be able to connect multiple wireless clients to your wireless cable modem. Using the USB port allows you to install the wireless cable modem more quickly and easily than using the Ethernet port, because you do not have to install and configure a network interface card (NIC). USB, however, only enables you to connect one computer to the wireless cable modem. Using the Ethernet port allows you connect multiple computers to a wireless cable modem through the use of additional equipment, which is not included. Please contact your cable service provider for more information on using multiple computers.

## 3. Installing the Modem Using Wireless

This chapter explains the process for installing your wireless cable modem using the wireless feature. First you will install the hardware (wireless cable modem, wireless client (not included), coax cable (not included), and power adapter).

### ***Installing the Hardware***

This section explains how to connect the wireless cable modem to the computer, wall cable outlet, and electrical outlet. To install the hardware:

- Power off the computer
- Connect one end of the coaxial cable to the wireless cable modem's cable connector. Connect the other end of the coaxial cable to the cable wall outlet. Be sure not to bend or over tighten the cables as this may strain the connector and cause damage. If you plan to connect the wireless cable modem and television to the same wall outlet, you must use a cable line splitter (not included).
- Plug the wireless cable modem's power adapter into the wireless cable modem's power jack and into an electrical outlet or surge protector.
- Follow the installation and configuration instructions included with your wireless client.
- You are now ready to use your cable modem.

## ***Troubleshooting the Wireless Installation***

The *wlan* LED is not lit.

- Verify that your Wireless PC Card or Wireless USB client is properly connected to your computer.
- Try positioning the computer closer to the wireless cable modem. The wireless signal may be weaker after it has passed through metal, concrete, brick, walls, or floors. Make sure that the wireless cable modem and wireless adapters are positioned so that the signal will travel straight through a wall or ceiling for better reception. For example, a wall that is 1 foot thick, at a 45-degree angle appears to be almost 2 feet thick.
- Make sure PC's wireless client is connecting to right WLCM. Check the SSID of the WLCM and wireless client.
- If WEP (Wired Equivalent Privacy) is set, verify that the WEP key set in the modem matches the WEP key set in the wireless client

# 4. Installing the Modem Using the Ethernet Port

This chapter explains the process for installing your wireless cable modem using the Ethernet port. Using the Ethernet port allows to you connect multiple computers to a wireless cable modem through the use of additional equipment which is not included. Please contact your cable service provider for more information on using multiple computers.

You can use the wireless cable modem's Ethernet port if you have:

- A PC running Windows 95 (or later) operating system or a Macintosh computer running system 7.6 (or later) operating system
- An active Ethernet port on your PC

Before you begin, verify that your Network Interface Card (NIC) has been installed and configured for use with your wireless cable modem. The wireless cable

modem requires TCP/IP to be installed. Contact your cable service provider for assistance with installing and configuring TCP/IP. After installed the hardware, your computer can connect the wireless cable modem directly by using Network Interface Card. Unlike USB installation, there is no needed for software installation for the Ethernet connection.

## Installing the Hardware

This section explains how to connect the wireless cable modem to the computer, wall cable outlet, and electrical outlet.

To install the hardware:

- Power off the computer
- Connect one end of the coaxial cable to the wireless cable modem's cable connector. Connect the other end of the coaxial cable to the cable wall outlet. Be sure not to bend or over tighten the cables as this may strain the connector and cause damage. If you plan to connect the wireless cable modem and television to the same wall outlet, you must use a cable line splitter (not included).
- Connect one end of the Ethernet cable to the wireless cable modem's Ethernet port and the other end of the cable to the Ethernet port on the PC or network interface card (NIC).
- Plug the wireless cable modem's power adapter into the wireless cable modem's power jack and into a wall outlet or surge protector.
- If the **pwr**, **sync**, **ready**, and **ethernet** LEDs are solidly lit, the wireless cable modem is working properly.

## Troubleshooting the Ethernet Installation

### **None of the LEDs are on when I power on the Wireless LAN Cable Modem.**

Check the connection between the power adapter and the cable modem. Power off the Wireless LAN Cable Modem and wait for 5 seconds and power on the modem again. If the problem still exists, you may have a hardware problem.

### **The Ethernet 1 or 2 or 3 or 4 LED on my wireless cable modem is not lit.**

- Try restarting the computer so that it could re-establish a connection with the wireless cable modem.
- Check for a resource conflict (Windows users only). To do this:
  - 1) Right-click on the My Computer icon on your desktop and choose Properties.
  - 2) Click the Device Manager tab and look for a yellow exclamation point or red X over the NIC in the Network Adapters field. If you see either one, you may have an IRQ conflict. Refer to the manufacturer's documentation or your cable service provider for further assistance.
- Verify that TCP/IP is the default protocol for your network interface card (NIC)
- Power cycle the wireless cable modem by removing the power adapter from the electrical outlet and plugging it back in. Wait several minutes for the wireless cable modem to re-establish communications with your cable service provider.
- Your Ethernet cable may be damaged. Try another cable.

**All of the LEDs on the front of my modem look correct, but I cannot access the Internet.**

- If the **pwr**, **sync**, and **ready** LEDs are solidly lit, the wireless cable modem is working properly. Try restarting the computer so that it could re-establish a connection with the wireless cable modem.
- Power cycle the wireless cable modem by removing the power adapter from the electrical outlet and plugging it back in. Wait several minutes for the wireless cable modem to re-establish communications with your cable service provider.
- If your PC is connected to a hub or gateway, try connecting the PC directly into the wireless cable modem.
- If you are using a cable splitter, try removing the splitter and connect the wireless cable modem directly to the cable wall outlet. Wait several minutes for the wireless cable modem to re-establish communications with your cable service provider.
- Your Ethernet or coaxial cable may be damaged. Try using another cable.
- If none of these suggestions work, contact your cable service provider for further assistance.

# 5. Wireless Cable Modem LEDs and Connectors

This chapter describes the functions of the wireless cable modem's LEDs and connectors. When the **pwr**, **sync**, and **ready** LEDs are lit, the wireless cable modem is working properly. The **usb** or **enet 1, 2, 3, 4** LEDs should also be lit depending on what port is being used.

The following provides an overview of the LED indicator lights on the front of the wireless cable modem and what the LEDs mean.

---

## LEDs on the Front of the Modem



- **pwr:** Indicates that the wireless cable modem has successfully completed internal power-on tests.
- **usb:** Indicates connectivity between the USB port on the wireless cable modem and a PC's USB port.
- **sync:** Indicates the connection status between the wireless cable modem and the cable network. The LED is lit when the wireless cable modem has established a downstream channel with the cable service provider's Cable Modem Termination System (CMTS).
- **ready:** Indicates that the wireless cable modem has completed the ranging/registration process and is ready to send/receive data.
- **wlan:** Indicates that at least one wireless client is linked to the wireless cable modem.
- **Enet 1, 2, 3, 4:** Indicates connectivity between the Ethernet port on the wireless cable modem and the Ethernet port on a PC or Mac. This LED blinks when the wireless cable modem is transferring or receiving data over the Ethernet cable.

Installation problems with the wireless cable modem are commonly due to the cable network and its topography. LEDs on the front panel of the wireless cable modem reveal operational status and help you determine problem areas.

---

### **Connectors on the Back of the Modem**

This list of connectors describes where to connect the cables and power adapter when installing the wireless cable modem.

- **PWR:** This is where you plug the included power adapter. Remember to use only the power adapter that came with the wireless cable modem.
- **Ethernet 10/100 Port 1, 2, 3, 4:** This is where you plug the Ethernet cable. The other end connects to the Ethernet port on the PC or NIC
- **USB Port:** This is where you plug the included USB cable. The other end connects to the USB port on your PC.
- **Cable Connector:** This is where you connect the coaxial cable (not included) that leads to the cable splitter (not included) or the cable wall outlet.

## 6. Web User Interface

### *Accessing the Web User Interface*

This chapter describes how to access the wireless cable router via Web configuration interface. First, please connect your PC to the cable router's Ethernet port, via an Ethernet cable.

- Open the web browser and set the address to: <http://192.168.100.1> for local access or
- Open the web browser and set the address to: <http://Cable-RF-IP-address> for remote access or
- Open the web browser and set the address to: <http://Public-gateway-IP-address:64680> for remote access

<p><b>Login</b></p> <p>Factory default username/password is "user"</p>	<p><b>Cable Modem Information</b></p> <p>Cable Modem : DOCSIS 1.0/1.1/2.0 Compliant</p> <p>MAC Address : 00:D0:59:DE:AD:01</p> <p>Serial Number : 00d059dead01</p> <p>Boot Code Version : 2.1.7i</p> <p>Software Version : 5.100.1002</p> <p>Hardware Version : 4.24</p> <p>CA Key : Uninstalled</p>
--	--

1. Click Login. Enter **user** for User name and **user** for Password, and then click **OK**.



2. If the user enters an incorrect user name and/or password, the web user interface displays 401 Unauthorized.

\*\*\* User Name: **user** & Password: **user** only can access to MODEM, GATEWAY, WIRELESS, VPN, PARENTAL CONTROL, FIREWALL and TOOLS.

## Web User Interface Home Page

After login, user will see the CABLE MODEM page first. The layout is divided into 3 areas. Menu Bar, Menu Tree and Configure Area.

The screenshot shows a web user interface for Cable Modem configuration. At the top is a **Menu Bar** with links for **MODEM**, **GATEWAY**, **WIRELESS**, **VPN**, **PARENTAL CONTROL**, **FIREWALL**, and **TOOLS**. Below the menu bar is a **Menu Tree** on the left, listing options under **CABLE MODEM**: **Information**, **Status**, **Downstream**, **Upstream**, **Upstream Burst**, **Operation Config.**, and **Event Log**. The main content area is the **Configure Area**, which displays the selected **Information** option. It includes sub-sections for **Status**, **Downstream**, **Upstream**, **Upstream Burst**, **Operation Configuration**, and **Event Log**, each with a link to "Show Cable Modem [Section Name]".

Menu Bar includes top level menu, like GATEWAY, WIRELESS and VPN. Once user select the option in menu bar, Menu Tree will be changed correspondently. To change parameter settings, user needs to operate in Configure Area. Below chapter is to go through page by page, to ensure that you're clear about each feature and how to use it.

## 6.1 MODEM

User can select different options to view wireless cable modem's information and real time status. They include Information, Status, Downstream, Upstream, Upstream Burst, Operation Configuration, Event Log options.

### 6.1.1 Information

This page is to show Cable Modem Information.

**CABLE MODEM**

- [Information](#)
- [Status](#)
- [Downstream](#)
- [Upstream](#)
- [Upstream Burst](#)
- [Operation Config.](#)
- [Event Log](#)

**Cable Modem Information**

Cable Modem : DOCSIS 1.0/1.1/2.0 Compliant

MAC Address : 00:D0:59:DE:AD:01

Serial Number : 00d059dead01

Boot Code Version : 2.1.7i

Software Version : 5.100.1002

Hardware Version : 4.24

CA Key : Uninstalled

Label	Description
Cable Modem	Indicate the DOCSIS standard it's compliant with.
MAC address	Unique hardware address of cable modem.
Serial Number	Unique manufacture ID number of a product.
Boot Code Version	Software version of device driver.
Software version	Software
Hardware Version	An internal ID number to identify hardware design.
CA Key	This is required by BPI. Cable modem will install a CA Key that transferred from your service provider's server after cable modem is authenticated.

**6.1.2 Status**

This page is to show Cable Modem Status.

**CABLE MODEM**

- Information
- Status
- Downstream
- Upstream
- Upstream Burst
- Operation Config.
- Event Log

### Cable Modem Status

Item	Status	Comments
Acquire a Downstream Channel	567250000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Security	Disabled	Disabled

[Refresh](#)

Label	Description
Item	List the item to be showed here.
Status	Status of the item.
Comments	Additional information for this item.
Acquire a Downstream Channel	It shows a Downstream channel that cable modem is trying to lock to, and informs the progress.
Connectivity State	After physical layer's initialization, cable modem will be configured by a DHCP server. Once succeeds to get an IP, that means cable modem is online. In status column, it shows the progress. In comments Column, it tells the reason why cable modem's connectivity state is not ok.
Boot state	Shows the registration status.
Security	If BPI is enabled, status will show Enabled.

### 6.1.3 Downstream

This page is to Show Cable Modem Downstream.

**CABLE MODEM**

- Information
- Status
- Downstream
- Upstream
- Upstream Burst
- Operation Config.
- Event Log

### Cable Modem Downstream

Downstream Lock :	Locked
Downstream Channel Id :	0
Downstream Frequency :	231000000 Hz
Downstream Modulation :	QAM64
Downstream Symbol Rate :	6952 Ksym/sec
Downstream Interleave Depth :	taps12Increment17
Downstream Receive Power Level :	9.0 dBmV
Downstream SNR :	42.5 dB

Label	Description
Downstream lock	Display if the cable modem succeeded to lock to a downstream channel.
Downstream Channel ID	Display the channel ID.
Downstream Frequency	Display the channel frequency cable modem is scanning.
Downstream Modulation	Display the modulation method that's required for the downstream channel locked by cable modem. This is decided by service provider.
Downstream Symbol Rate	Display the symbol rate. Current cable modem downstream symbol rate  (QAM64 is 5056941 sym/sec, QAM256 is 5360537 sym/sec).
Downstream Interleave Depth	Current cable modem downstream Interleave depth (8/16/32/64/128/other).
Downstream Receive Power Level	Display the receiver power level after ranging process.
Downstream SNR	Display the SNR of this downstream channel.

## 6.1.4 Upstream

**CABLE MODEM**

- Information
- Status
- Downstream
- Upstream
- Upstream Burst
- Operation Config.
- Event Log

### Cable Modem Upstream

Upstream Lock :	Locked
Upstream Channel ID :	5
Upstream Frequency :	39984000 Hz
Upstream Modulation :	QAM16
Upstream Symbol Rate :	2560 Ksym/sec
Upstream transmit Power Level :	39.8 dBmV
Upstream Mini-Slot Size :	2

Label	Description
Upstream Lock	Current cable modem upstream lock status (Locked/Not locked).
Upstream Channel ID	Current cable modem upstream channel identify.
Upstream Frequency	Current cable modem upstream frequency (Hz).
Upstream Modulation	Current cable modem upstream modulation type. (QPSK/ QAM8 /QAM16/ QAM32/ QAM64/ QAM128/ QAM256).
Upstream Symbol Rate	Current cable modem upstream symbol rate (Ksym/sec)
Upstream transmit Power Level	Current cable modem upstream transmit power (dBmV)
Upstream Mini-Slot Size	Current cable modem upstream mini-slot.

### 6.1.5 Upstream Burst

**CABLE MODEM**

- Information
- Status
- Downstream
- Upstream
- Upstream Burst
- Operation Config.
- Event Log

### Cable Modem Upstream Burst

	Req (1)	Init Maint (3)	Per Maint (4)	Short Data (5)	Long Data (6)
	16QAM	16QAM	16QAM	16QAM	16QAM
Modulation Type	16QAM	16QAM	16QAM	16QAM	16QAM
Differential Encoding	Off	Off	Off	Off	Off
Preamble Length	128	256	256	72	160
Preamble Value Offset	384	256	256	424	352
FEC Error Correction (T)	0	5	5	5	10
FEC Codeword Information Bytes (k)	16	34	34	78	235
Scrambler Seed	338	338	338	338	338
Maximum Burst Size	0	0	0	15	138
Guard Time Size	8	48	48	8	8
Last Codeword Length	Fixed	Fixed	Fixed	Short	Short
Scrambler on/off	On	On	On	On	On

Label	Description
Modulation Type	QPSK/16QAM.
Differential Encoding	On/Off
Preamble Length	0-1024 (bits).
Preamble Value Offset	0-1022 (bits).
FEC Error Correction (T)	0 to 10 (0 implies no FEC. The number of codeword parity bytes is 2*T)
FEC Codeword Information Bytes (k)	Fixed: 16 to 253 (assuming FEC on). Shortened: 16 to 253 (assuming FEC on)
Scrambler Seed	15 bits (Not used if scrambler is off)
Maximum Burst Size	0-255 (mini-slots)
Guard Time Size	4-255 (symbols)
Last Codeword Length	Fixed/shortened
Scrambler on/off	On/Off

### 6.1.6 Operation Configuration

This page shows the running configuration of cable modem.

**CABLE MODEM**

- [Information](#)
- [Status](#)
- [Downstream](#)
- [Upstream](#)
- [Upstream Burst](#)
- [Operation Config.](#)
- [Event Log](#)

**Cable Modem Operation Configuration**

Network Access :	Allowed
Maximum Downstream Data Rate :	0
Maximum Upstream Data Rate :	0
Maximum Upstream Channel Burst :	0
Maximum Number of CPEs :	16
Modem Capability :	Concatenation Disabled, Fragametation Enabled, PHS Enabled

Label	Description
Network Access	Display the status of cable modem, denied means currently no connectivity is established. Deny the access to Internet. Allow means allow the access to Internet.
Maximum Downstream Data Rate	Display the maximum downstream data rate.
Maximum Upstream Data Rate	Display Maximum Upstream Data Rate
Maximum Upstream Channel Burst	Display Maximum Upstream Channel Burst
Maximum Number of CPEs	Shows the maximum CPE that can be connected at LAN side to access Internet at the same time.
Modem Capability	Displayed certain configuration, like PHS enabled.

**6.1.7 Event Log**

**CABLE MODEM**

- Information
- Status
- Downstream
- Upstream
- Upstream Burst
- Operation Config.
- Event Log

**Cable Modem Event Log**

First Time	Last Time	Priority	Description
Thu Apr 17 14:02:51 2008	Thu Apr 17 14:02:51 2008	Error (4)	Configuration File CVC Validation Failure
Time Not Established	Time Not Established	Critical (3)	No Ranging Response received - T3 time-out
Time Not Established	Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Time Not Established	Critical (3)	Resetting the cable modem due to console command

Refresh

Clear Log

Label	Description
First Time	Display the time of the event.
Last Time	Display the last time of the event.
Priority	Event log severity.
Description	Detail of the event log.
Refresh	Refresh the log record.
Clear Log	Clear all of the logs.

During daily operation and trouble shooting, log is very useful. For example, you can see “configuration file CVC validation Failure”, this indicates that cable modem failed to validate the CONFIG file downloaded from MSO’s TFTP server, maybe caused by error root key. Furthermore, event logs will be stored unless user clicks “clear log” button. Power cycle reboot will not clear event logs.

**6.2 GATEWAY**

Under gateway, user can configure basic parameters like WAN IP address, LAN IP address, DHCP and DDNS. Also, advanced setting like DMZ, MAC filtering and port forwarding are included.

## 6.2.1 Information

User can get an overview of IP address status.

### Basic Gateway Setup

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

### Gateway - Information

#### INTERNET SETTINGS

**Gateway MAC Address:** 00:d0:59:de:ad:03  
**Internet IP Address:** .....  
**Subnet Mask:**  
**Default Gateway:** 0.0.0.0  
**DNS:**  
**DHCP Remaining Time:** 0 days 00:00:00

Refresh

#### LOCAL SETTINGS

**Gateway IP Address:** 192.168.0.1  
**Subnet Mask:** 255.255.255.0  
**DHCP Server:** Enabled  
**NAT :** Enabled  
**Wireless Status :** Enabled  
**Operating Mode:** NAT mode  
**Private IP Range:** 192.168.0.10 through 192.168.0.15  
**Public IP DHCP Server Range:** 0.0.0.0 through 0.0.0.0  
**Public IP Total Range:** 0.0.0.0 through 0.0.0.0  
**System Up-Time:** 9 Minutes 5 Seconds

Label	Description
INTERNET SETTINGS	
Gateway MAC Address:	Display the MAC Address of Residential Gateway.
Internet IP Address:	Display the Internet IP address.
Subnet Mask:	Display the subnet mask of the Internet IP address.
Default Gateway:	Display the default gateway IP address.
DNS:	Display the DNS server IP address.
DHCP Remaining Time:	Display the remained DHCP lease time before expiration.
Refresh	Click to refresh the information.
LOCAL SETTINGS	
Gateway IP Address:	Display the local IP address of the LAN interface.

Subnet Mask:	Display the subnet mask value.
DHCP Server:	Display the status of DHCP sever feature.
NAT :	Display the status of NAT feature.
Wireless Status :	Display the status of wireless feature.
Operating Mode:	Display what mode the router is working on.
Private IP Range:	Display the private IP address assigned to DHCP client.
Public IP DHCP Server Range:	Display the Public IP DHCP Server Range.
Public IP Total Range:	Public IP DHCP Server Range.
System Up-Time:	Display the accumulated time since the last power cycle.

### 6.2.2 Basic Setup

This page allows configuration of the basic features of the Wireless Cable Modem related to your MSO's connection.

#### Basic Gateway Setup

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

#### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

#### Gateway - Basic Setup

##### Network Configuration

LAN IP Address:  .  .  .

MAC Address: **00:d0:59:de:ad:05**

WAN IP Address: ----.----.----.----

MAC Address: **00:d0:59:de:ad:03**

Duration: **D: -- H: -- M: -- S: --**

Expires: ----.----.----.----

WAN Connection Type:

Host Name:  (Required by some ISPs)

Domain Name:  (Required by some ISPs)

MTU Size:  (256-1500 octets, 0 = use default)

Label	Description
-------	-------------

LAN	
IP Address:	Define the local IP address, which will be the default gateway address for all of the LAN hosts.
MAC Address	Display the LAN interface's hardware address.
WAN	
IP Address:	Display the current WAN public address.
MAC Address:	Display the interface's hardware address.
Duration	Display the accumulated time since acquired WAN public IP address successfully.
Expires	Display the remained time duration before expirations.
Release WAN Lease	Click to release WAN public IP address.
Renew WAN Lease	Click to renew the WAN IP address.
Refresh	Click to refresh the status of this page.
WAN Connection Type	Select to define the WAN connection type, <ul style="list-style-type: none"> <li>- DHCP, determine the WAN interface to be a DHCP client, IP address will be assigned by ISP's DHCP server.</li> <li>- Static IP, need to manually define the IP address.</li> <li>- PPTP (DHCP), need to input the PPP username and password, and also, the PPTP server's IP address.</li> </ul>
Host Name	Filled with your host name for the router.
Domain Name	Filled with the domain for the router.
MTU Size	Define the Maximum Transmission Unit size, which defines the largest size of the packet or frame that a given physical interface can transfer. 256-1500
Apply	Click to save.

### 6.2.3 DHCP

This page allows configuration and displays status of the optional internal DHCP server for the LAN

**Basic Gateway Setup**

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - DHCP**

DHCP Server  Yes  No

Starting Address Set

Private Starting Address **192.168.0.10** (1~253) Number of CPEs

Public Starting Address **0.0.0.0** (1~254) Number of CPEs

Lease Time

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
001c2351abd4	192.168.000.010	255.255.255.000	D:00 H:01 M:00 S:00	-----:-- ----	<input checked="" type="radio"/>
001f3a28d780	192.168.000.011	255.255.255.000	D:00 H:01 M:00 S:00	-----:-- ----	<input checked="" type="radio"/>

Current System Time: -----:--

Label	Description
DHCP Server	Select to active or disable the DHCP feature.  If select No, all of the static DHCP rule will be eliminated.
Private Starting Address	Define the starting private IP address.
Public Starting Address	Define the starting public IP address.
Number of CPEs	Define the maximum number of CPEs.
Lease Time	Define the DHCP lease time duration.
Apply	Click to save.
DHCP Clients	Client list to show that all of the DHCP client currently connected to the wireless router, either via Ethernet link, or via wireless connection.
MAC Address	Display the MAC address.
IP Address	Display the IP address.
Subnet Mask	Display the subnet mask.
Duration	Display the accumulated time since client acquired the IP address.

Expires	Display the expiration time. If current IP address is reserved to a certain host statically, it will show "STATIC IP ADDRESS"
Select	Select to reserve the current private IP address to be assigned to this host statically. That means 192.168.0.10 will be reserved to host 001c2351abd4.
Force available	Click to active this rule.

### 6.2.4 DHCP static Lease

This page allows configuration of static-lease option for the internal DHCP server for the private LAN.

**Basic Gateway Setup**

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Gateway - DHCP Static Lease**

Note: If some IP addresses turn to red color, you should check the DHCP pools! Current DHCP Server IP Ranges' information

**Private Range:192.168.0.10 -- 192.168.0.15**

**Public DHCP Server Range:0.0.0.0 -- 0.0.0.0**

Index	MAC Address	IP Address	Enabled	Clear
1.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
2.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Index	Index number of the rule.
MAC Address	Filled in with the MAC address that you want to statically assign this reserved IP address to.
IP Address	Define the reserved IP address for a certain host.
Enabled	Click to activate this rule.
Clear	Select to delete the rule.

Apply	Click to save.
-------	----------------

## 6.2.5 DDNS

### Basic Gateway Setup

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

### Gateway - DDNS

DDNS Service:

User Name:

Password:

Host Name:

IP Address: **0.0.0.0**

Status: *DDNS service is not enabled.*

Label	Description
DDNS Service	Select the type of service that you are registered for from your Dynamic DNS service provider. <ul style="list-style-type: none"> <li>▪ www. DyDNS.org</li> <li>▪ www.no-ip.com</li> </ul>
UserName	Input your DDNS account username subscribed to the service provider
Password	Password of the account.
Host Name	Input the host name of your host
IP address	Display the current WAN side Public IP address.
Status	Display the DDNS status.
Apply	Click to save.
Refresh	Click to refresh the page.

## 6.2.6 Time

This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.

### Basic Gateway Setup

- Information
- Setup
- DHCP
- Static Lease
- DDNS
- Time

### Advanced Gateway Setup

- Options
- MAC Filtering

### Gateway - TIME

Enable SNTP  Yes  No

Current Time Thu Jan 01 00:01:06 1970

System Start Time Thu Jan 01 00:00:00 1970

Time Server 1

Time Server 2

Time Server 3

Timezone Offset Hours  Minutes

Label	Description
Enable SNTP	Click to enable SNTP feature.
Current Time	Display the system time currently.
System Start Time	Display the accumulated time since system was started.
Time Server 1	Define the Time server IP address or Domain name.
Time Server 2	Define the Time server IP address or Domain name.
Time Server 3	Define the Time server IP address or Domain name.
Time zone Offset	
Hours	Define the time zone to. '8' means GMT + 08, '-1' means GMT -01.
Minutes	Define the minute offset.
Apply	Click to save.
Reset Values	Click to reset values to factory default value.

## 6.2.7 Advanced- Options

<p><b>Basic Gateway Setup</b></p> <ul style="list-style-type: none"> <li>• Information</li> <li>• Setup</li> <li>• DHCP</li> <li>• Static Lease</li> <li>• DDNS</li> <li>• Time</li> <li><b>Advanced Gateway Setup</b></li> <li>• Options</li> <li>• MAC Filtering</li> <li>• IP Filtering</li> <li>• Port Filtering</li> </ul>	<p><b>Advanced Gateway - Options</b></p> <p>WAN Blocking <input type="checkbox"/> <i>Enable</i></p> <p>Ipssec PassThrough <input checked="" type="checkbox"/> <i>Enable</i></p> <p>PPTP PassThrough <input checked="" type="checkbox"/> <i>Enable</i></p> <p>Multicast Enable <input type="checkbox"/> <i>Enable</i></p> <p>UPnP Enable <input type="checkbox"/> <i>Enable</i></p> <p style="text-align: center;"><input type="button" value="Apply"/></p>
---	--

Label	Description
WAN Blocking	Select to block connection request initialized from Internet User.
Ipssec PassThrough	If Internet user initialized IPsec VPN request to the host located behind the router, NAT will make this attempt fail. Enable Pass Through is to force the router to redirect the IPsec request to local host.
PPTP PassThrough	If Internet user initialized PPTP VPN request to the host located behind the router, NAT will make this attempt fail. Enable Pass Through is to force the router to redirect the PPTP request to local host.
Multicast Enable	Multicast optimizes the bandwidth utilization compared with unicast. Especially, video stream application.
UPnP Enable	Select to activate UPnP. Be aware that anyone could use an UPnP application to open the web UI login screen without entering the router's IP address (although you must still enter the password to access the web UI).
Apply	Click to save.

## 6.2.8 Advanced - MAC Filtering

This page allows configuration of MAC address filters in order to block internet traffic to specific network devices on the LAN. You can regard this as black list, any host that its MAC address is among this MAC list will not be able to access Internet through the router.

#### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

#### Advanced Gateway - MAC Filtering

Index	MAC Address	Clear
1.	00 : aa : 12 : cd : 56 : ad	<input type="checkbox"/>
2.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
9.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
10.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>

View Additional Rules:

Label	Description
Index	Index number of the rule.
MAC Address	MAC address to block.
Clear	Select to delete the rule.
View Additional Rules:	Turn to view remained 10 rules. Totally, 20 rules are supported.
Apply	Click to save.

### 6.2.9 Advanced - IP Filtering

This page allows configuration of IP address filters in order to block internet traffic to specific network devices on the LAN.

### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

### Advanced Gateway - IP Filtering

IP Filtering		
Start Address	End Address	Enabled
192.168.0.15	192.168.0.18	<input checked="" type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Label	Description
Start Address	Fill in with start address.
End Address	Fill in with end address.
Enabled	Select to active the rule
Apply	Click to save.

### 6.2.10 Advanced - Port Filtering

This page allows configuration of port filters in order to block specific internet services to all devices on the LAN.

### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

### Advanced Gateway - Port Filtering

Port Filtering			
Start Port	End Port	Protocol	Enabled
5060	5060	Both	<input checked="" type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Label	Description
Start Port	Define the start port.
End Port	Define the end port.
Protocol	Define the protocol type.
Enabled	Select to active the rule.
Apply	Click to save.

### 6.2.11 Advanced - Forwarding

This page allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc, so they can be accessible from the public internet.

### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

### Advanced Gateway - Forwarding

Port Forwarding							
Index	Local IP	Internal Port	Public Interface IP	Ext Start Port	Ext End Port	Protocol	Enabled
1.	192.168.0. 10	21	69.10.22.129	21	22	Both	<input checked="" type="checkbox"/>
2.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
3.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
4.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
5.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
6.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
7.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
8.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
9.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>
10.	192.168.0. 0	0	0.0.0.0	0	0	Both	<input type="checkbox"/>

View Additional Rules: 1 to 10

Apply

Port Map

Label	Description
Index	Index number of the rule.
Local IP	Filled in with the IP address of
Internal Port	Filled in with the port number listened on server host located in LAN area.
Public Interface IP	Input the public IP address.
Ext Start Port	Define the port that published to Internet. Start port.
Ext End Port	Define the port that published to Internet. End port.
Protocol	Define the protocol type.
Enabled	Select to enable this rule.
Apply	Click to save.
Port Map	Click to show a list of common application and port.

#### Question:

What's the difference between "Internal Port" and "External Port"?

**Answer:**

Internal Port means which port the local server is listening to. External Port means which port the router is listening to. For example, local station John's running Telnet Daemon on port 64623, then internal port is 64623, external port is 23. Suppose Internet user initializes a Telnet connection request to this router's public IP address, router will recognize that this is a Telnet Connection request to a station. According to existing forwarding rule, router will first translate the packet's destination port to be 64623, and then forward this request to host John. If we designed "External port" only, then we'll have trouble to setup two FTP servers locally simultaneously, since there will be 2 FTP daemons running, and that's hard for router to figure out which connection request should be redirected to which FTP daemon.

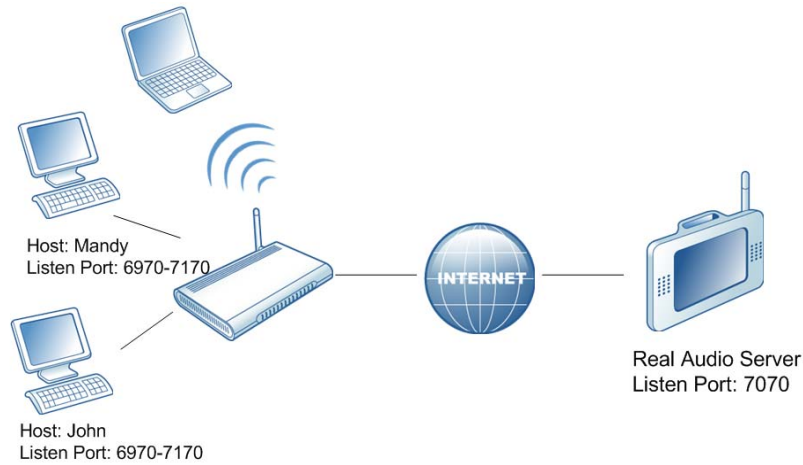
**6.2.12 Advanced - Port Triggering**

This page allows configuration of 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.

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service to the IP address of LAN side host. The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Here we define 2 kinds of ports, "Trigger Port" and "Target Port". Trigger port is defined as the service request with a specific destination port number sent from a LAN side host. Target Port is defined as the ports this specific application requires clients host to listen. So, server will return response to these ports.

Let's give an application scenario to get a clear concept.



### Suppose,

- 1) John requests a file from the Real Audio server (port 7070).
- 2) Port 7070 is a "trigger" port and causes the wireless router to record John's computer IP address. Ubee wireless router associates John's computer IP address with the "target" port range of 6970-7170.
- 3) The Real Audio server responds to a port number ranging between 6970-7170.
- 4) Ubee router forwards the traffic to John's computer IP address.
- 5) Only John can connect to the Real Audio server until the connection is closed or times out.

#### Advanced Gateway Setup

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

#### Advanced Gateway - Port Triggering

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Both	<input type="checkbox"/>

Label	Description
Trigger Range	The trigger port is a port (or a range of ports) that causes (or triggers) the router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Target Range	Target Range is a port (or a range of ports) that a server on the WAN uses when it response to service requests. The router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Protocol	Define the protocol type for this rule.
Enable	Click to active this rule.
Apply	Click to save.

### 6.2.13 Advanced- Pass Through

This page allows configuration of pass through table, the device in pass through table will be treated as bridge device.

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host

**Advanced Gateway - Pass Through**

Index	MAC Address	Clear
1.	00 : 13 : 04 : 00 : ac : c5	<input checked="" type="checkbox"/>
2.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
3.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
4.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
5.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
6.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
7.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>
8.	00 : 00 : 00 : 00 : 00 : 00	<input type="checkbox"/>

Label	Description
Index	Index number.
MAC address	Input the host's MAC address.
Clear	Select to delete this rule.
Apply	Click to save.

**6.2.14 Advanced- DMZ Host (Exposed Host)**

This page allows configuration of a specific network device to be exposed or visible directly to the WAN (public internet). This may be used when applications do not work with port triggers.

**Advanced Gateway Setup**

- Options
- MAC Filtering
- IP Filtering
- Port Filtering
- Forwarding
- Port Triggering
- Pass Through
- DMZ Host
- IP Mapping

**Advanced Gateway - DMZ Host (Exposed Host)**

DMZ Address

Label	Description
DMZ Address	Define the DMZ IP address.
Apply	Click to save.

## 6.3 WIRELESS

### 6.3.1 Basic

This page allows configuration of the Wireless Modem parameters the SSID and channel number. A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Note: U10C020 doesn't support wireless.

**Wireless 802.11b/g Basic**

Wireless MAC Address: **00:1E:4C:03:13:F8**

Network Name (SSID)

Broadcast SSID  Enable

Country

Channel:  Current : 1

Interface

Label	Description
Wireless MAC Address	Display MAC address of wireless router's wireless module.
Network Name (SSID)	The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the wireless router must have the same SSID.
Broadcast SSID	Click <b>Enable</b> to allow broadcast of SSID.
Country	When set to <b>USA</b> , Channel 1 to 11 is available.  If select worldwide, 13 channels are available.

Channel	Select a specific channel to deploy wireless network. This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Interface	When set to <b>enabled</b> , wireless clients can access to the network.
Apply	Click to save.
Restore Wireless Defaults	Click to restore the factory default setting for wireless module.

### 6.3.2 Security

This page allows configuration of the WEP keys and/or pass phrase.

#### Wireless Privacy

WPA	<input type="text" value="Disabled"/>	WiFi Protected Setup (WPS)	
WPA-PSK	<input type="text" value="Disabled"/>	WPS Config	<input type="text" value="Disable"/>
WPA2	<input type="text" value="Disabled"/>	Button Mode	<input type="text" value="SES"/>
WPA2-PSK	<input type="text" value="Disabled"/>	Device Name	<input type="text" value="AmbitAP"/>
WPA/WPA2 Encryption	<input type="text" value="Disabled"/>	STA PIN	<input type="text" value="size=8"/>
WPA Pre-Shared Key	<input type="password" value="....."/>	<input type="button" value="Apply"/>	
RADIUS Server	<input type="text" value="0.0.0.0"/>	WPS Method	<input type="text" value="Push Button"/>
RADIUS Port	<input type="text" value="1812"/>	<input type="button" value="Start WPS"/>	
RADIUS Key	<input type="password"/>	WPS Status:	
Group Key Rotation Interval	<input type="text" value="0"/>		
WPA/WPA2 Re-auth Interval	<input type="text" value="3600"/>		
WEP Encryption	<input type="text" value="Disabled"/>		
Shared Key Authentication	<input type="text" value="Optional"/>		
802.1x Authentication	<input type="text" value="Disabled"/>		
Network Key 1	<input type="password"/>		
Network Key 2	<input type="password"/>		
Network Key 3	<input type="password"/>		
Network Key 4	<input type="password"/>		
Current Network Key	<input type="text" value="1"/>		
PassPhrase	<input type="password"/>		
	<input type="button" value="Generate WEP Keys"/>		

Label	Description
WPA	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption
WPA-PSK	If you don't have an external RADIUS server you should use WPA-PSK (WPA Pre-Shared Key) that only requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.
WPA2	Advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, that is considered fully secure.
WPA2-PSK	If you don't have an external RADIUS server you should use WPA2-PSK (WPA Pre-Shared Key) that only requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.
WPA/WPA2 Encryption	Switch to enable and disable WPA/WPA2 encryption.
WPA Pre-Shared Key	The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials.
RADIUS Server	Input the IP address of RADIUS server
RADIUS Port	Enter RADIUS port number when WPA or 802. 1x network authentication is selected.
RADIUS Key	Enter RADIUS Key when WPA or 802. 1x network authentication is selected.
Group Key Rotation Interval	Allows the wireless router to generate best possible random group key and update all the key-management capable stations periodically.
WPA/WPA2 Re-auth Interval	Wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and

	all stations in a WLAN on a periodic basis. Setting of the WPA Group Key Update Timer is also supported in WPA-PSK mode.
WEP Encryption	If you don't have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key. Data Encryption can be set to WEP 128-bit, 64-bit, or Disable.
Shared Key Authentication	Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.
802.1x Authentication	Enable to user 802.1x to do authenticate wireless client.
Network Key 1	You can pre-define up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits) .
Network Key 2	As above
Network Key 3	As above
Network Key 4	As above
Current Network Key	You can select one of the four pre-defined keys as the current network key.
PassPhrase	You can set WEP encryption key by entering a word or group of printable characters in the Pass phrase box and click Generate WEP keys. These characters are case sensitive.
Generate WEP Keys	Force the wireless route to generate 4 WEP keys automatically.
Apply	Click to save the wireless configurations.
WiFi Protected Setup (WPS)	Configure WPS feature.
WPS Config	If choose to be Enable, then user can use external Registrar to configure this wireless router; otherwise, user has to login to wireless router WEB UI to configure the WPS security settings such as encryption mode and SSID, etc.

Button Mode	<p>Defines the mode of push button,</p> <ul style="list-style-type: none"> <li>▪ SES, technology developed by Broadcom and SES lets you configure the SSID and encryption keys on both the router and the client with the press of a button.</li> <li>▪ WPS, a protocol to simplify the process of configuring security on wireless networks, and so it was first named 'Wi-Fi Simple Config'.</li> </ul>
Device Name	To identify this wireless router in WPS network.
STA PIN	Personal Identification Number of your PC or game machine. When a WPS supported device tries to connect to this wireless router, user has to input its PIN into current WPS configure page's STA PIN field.
Apply	Click to make WPS configurations to take effect.
WPS Method	Select WPS mode to be deployed.
Start WPS	If selected push button mode, then user only needs to push the button on WPS supported host. Then, within 2 minutes, push this "WPS start" button to trigger the physical negotiation between them.
WPS Status:	Display the WPS status.

### 6.3.3 Access Control

This page allows configuration of the Access Control to the AP as well as status on the connected clients. Selects whether clients with the specified MAC address are allowed or restricted wireless access.

STATUS: Changes Accepted (Wireless Computer Added To Access List)

## Wireless Access Control

MAC Restrict Mode

MAC Addresses

Connected Clients	MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name
	00:1F:E1:78:C2:0F	1	-46	192.168.0.14	JohnYan

Label	Description
MAC Restrict Mode	Use to control wireless access control mechanism <ul style="list-style-type: none"> <li>▪ Disable, to turn off this feature, any wireless card can connect to this wireless router.</li> <li>▪ Allow, white list of the wireless client, their MAC address should be inputted here manually.</li> <li>▪ Deny, black list of the wireless client, their MAC address should be inputted here manually.</li> </ul>
MAC Addresses	Input the MAC address.
Apply	Click to save.
Connected Clients	List of current connected Wireless client.
MAC Address	MAC of the connected wireless client.
Age(s)	Duration since the wireless client connected to wireless router.
RSSI(dBm)	Received signal strength in a wireless environment
IP Addr	Display the IP address assigned to this wireless client.
Host Name	Host name of the wireless client.

### 6.3.4 Guess Network: Multiple SSID Support

Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The Ubee Wireless Cable Modem supports Multiple Service Set Identifier which allows you to use one access point to provide several BSSs simultaneously. You can then assign varying levels of privilege to different SSIDs and networks associated. Wireless stations can use different SSIDs to associate with the same AP.

- A maximum of four BSSs are allowed on one AP simultaneously. 1 for Admin access, 3 for Guest Networks
- You must use different WEP keys for different BSSs. If two stations have different SSIDs (they are in different BSSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).



#### Wireless 802.11b/g Guest Network

Guest Network:  ▼

Guest WiFi Security Settings	Guest LAN Settings
Guest Network: <input type="text" value="Disabled"/> ▼	DHCP Server: <input type="text" value="Disabled"/> ▼
Guest Network Name (SSID): <input type="text" value="GUEST_WLAN_0"/>	IP Address: <input type="text" value="192.168.1.1"/>
Closed Network: <input type="text" value="Disabled"/> ▼	Subnet Mask: <input type="text" value="255.255.255.0"/>
WPA: <input type="text" value="Disabled"/> ▼	Lease Pool Start: <input type="text" value="192.168.1.10"/>
WPA-PSK: <input type="text" value="Disabled"/> ▼	Lease Pool End: <input type="text" value="192.168.1.99"/>
WPA2: <input type="text" value="Disabled"/> ▼	Lease Time: <input type="text" value="86400"/>
WPA2-PSK: <input type="text" value="Disabled"/> ▼	<input type="button" value="Apply"/>
WPA/WPA2 Encryption: <input type="text" value="Disabled"/> ▼	<input type="button" value="Restore Defaults"/>
WPA Pre-Shared Key: <input type="text"/>	
RADIUS Server: <input type="text" value="0,0,0,0"/>	
RADIUS Port: <input type="text" value="1812"/>	
RADIUS Key: <input type="text"/>	

Label	Description
Guest Network	Display the three guest SSID supported by wireless router. Choices are

	<ul style="list-style-type: none"> <li>- GUEST_WLAN_0 (xx:xx:xx:xx:xx:xx)</li> <li>- GUEST_WLAN_1 (xx:xx:xx:xx:xx:xx)</li> <li>- GUEST_WLAN_0 (xx:xx:xx:xx:xx:xx)</li> </ul> <p>If enabled, MAC address of this BSSID will be displayed.</p>
Guest WiFi Security Settings	Wireless parameters are similar with the settings in Wireless-Security part before.
Guest Network	Enable or disable the
Guest Network Name (SSID)	Allow user to fill in with a new SSID name.
Closed Network	If select Enable, this will hide the SSID name. When nearby wireless client tries to scan the SSID, it will not discover this hidden SSID name, unless user manually add this SSID.
Guest LAN Settings	
DHCP Server	Allow user to deploy DHCP server for this guest SSID.
IP Address	This IP address will be the default gateway address for clients connected to this guest network.
Subnet Mask	Define the subnet mask value.
Lease Pool Start	Define the start IP address of this DHCP address pool.
Lease Pool End	Define the last IP address of this DHCP address pool.
Lease Time	Define the lease time for DHCP client. Before expiration, DHCP client will resend DHCP request. Max value is 86400 second.
Apply	Click to save.
Restore Defaults	Click to reset to factory default values for wireless part.

## 6.4 VPN

Under VPN feature, here provides IPsec VPN, L2TP VPN and PPTP VPN.

A **virtual private network (VPN)** is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the

Internet) instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

### 6.4.1 VPN- Enable

**VPN**

- [Enable](#)
- [Summary](#)
- [Configure](#)
- [L2TP / PPTP](#)
- [Event Log](#)

#### VPN - Enable Setup

**This page allows user to Enable or Disable VPN, and Cable Modem will reset after pressing Apply button.**

VPN Enable

VPN Disable

After enable or disable VPN feature, wireless router needs to reboot to take effect.

### 6.4.2 VPN-Summary

This page allows user to manage VPN tunnels with centralized view.

**VPN**

- [Enable](#)
- [Summary](#)
- [Configure](#)
- [L2TP / PPTP](#)
- [Event Log](#)

#### VPN - Summary

##### L2TP / PPTP

L2TP Server

PPTP Server

---

##### IPsec

IPsec Endpoint

#	Name	Status	Control	Configure
1	test	Connected	<input type="button" value="Connect"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Label	Description
L2TP Server	Wireless router integrated with L2TP/PPTP server inside, select Enable or Disable.
PPTP server	Wireless router integrated with L2TP/PPTP server inside,

	select Enable or Disable.
Configure	Click Configure to make the L2TP/PPTP setting to take effect.
IPSec Endpoint	Select to disable or enable IPSec VPN service.
#	ID of the IPSec VPN tunnel.
Name	Identical name of IPSec VPN tunnel
Status	Once an IPSec VPN is connected successfully, Status will turn to be connected. Otherwise, it shows Not Connected.
Control	User can manually trigger IPSec VPN connection request to the remote VPN gateway.
Configure	Click Edit to modify IPSec VPN parameters of this tunnel; Click Delete to delete this IPSec VPN tunnel.
Add New Tunnel	Click to quickly create a new IPSec VPN tunnel, and then to modify its parameters.

### 6.4.3 VPN- Configure

Internet protocol Security (IPSec) is a standard based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters wireless router and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between wireless router and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the wireless router and remote IPSec router can send data between computers on the local network and remote network.

Before IPSec VPN configuration, you will be involved with such terms like IPSec Algorithms, Authentication Header and ESP protocol.

- **IPSec Algorithms**

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

- **AH (Authentication Header) Protocol**

**AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

- **ESP (Encapsulating Security Payload) Protocol**

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated. An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

VPN

- Enable
- Summary
- Configure
- L2TP / PPTP
- Event Log

VPN - Configure

Tunnel

Name

Enabled

**Local endpoint settings**

Address group type

Subnet

Mask

Identity type

Identity

**Remote endpoint settings**

Address group type

Subnet

Mask

Identity type

Identity

Network address type

Remote Address

**IPsec settings**

Pre-shared key

Phase 1 DH group

Phase 1 encryption

Phase 1 authentication

Phase 1 SA lifetime  seconds

Phase 2 encryption

Phase 2 authentication

Phase 2 SA lifetime  seconds

Key management

IKE negotiation mode

Perfect forward secrecy (PFS)

Phase 2 DH group

Replay detection

NetBIOS broadcast forwarding

Dead peer detection

Label	Description
Tunnel	Select the specific VPN tunnel to configure.

Name	Input the naming for identifying.
Delete tunnel	This button will delete the selected VPN
Add New Tunnel	Once user inputted name in Name field, he can add this tunnel
Apply	Quickly select certain VPN tunnel, and enable or disable it, need to click apply.
Local endpoint Settings	Configure the local network that will be protected by IPSec VPN, located in your wireless router LAN side.
Address group type	Define the local address type, <ul style="list-style-type: none"> <li>- IP Subnet, to protect the whole subnet.</li> <li>- Single IP address, to protect a single PC</li> <li>- IP address range, to protect several PCs</li> </ul>
Subnet	Subnet scale.
Mask	Subnet mask value.
Identity Type	<p>Select different identity type to identify this wireless router by</p> <ul style="list-style-type: none"> <li>- WAN IP address</li> <li>- IP address</li> <li>- FQDN</li> <li>- Email address</li> </ul> <p>In Aggressive mode, VPN concentrator uses to identify incoming SAs by ID type and content since this identifying information is not encrypted, to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.</p> <p>In Main mode, the ID type and content are encrypted to provide identity protection. In this case VPN concentrator can only distinguish between up to 30 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Because you can select between five encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), two authentication algorithms (MD5 and SHA1) and three key groups (DH1 and DH2, DH5) when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming</p>

	SAs.
Identity	The value of corresponding to selected Identity type.
Remote endpoint settings	Define the local network that will be protected by IPSec VPN, located in peer wireless router LAN side.
Address group type	Define the local address type, <ul style="list-style-type: none"> <li>- IP Subnet, to protect the whole subnet.</li> <li>- Single IP address, to protect a single PC</li> <li>- IP address range, to protect several PCs</li> </ul>
Subnet	Subnet scale.
Mask	Subnet mask value.
Identity type	Select different identity type to identity this wireless router by <ul style="list-style-type: none"> <li>- WAN IP address</li> <li>- IP address</li> <li>- FQDN</li> <li>- Email address</li> </ul>
Identity	The value of corresponding to selected Identity type.
Network address type	Filled in with the IP address or Domain name of the peer IPSec VPN Gateway, you can select <ul style="list-style-type: none"> <li>- IP address, usually suitable for static public IP address.</li> <li>- Fully Qualified Domain Name (FQDN), usually suitable for dynamic public IP address.</li> </ul>
Remote address	Input IP address value when choose IP address in Network address type. Input FQDN value when selected FQDN in Network address type. This filed is used to identify specific remote IPSec VPN gateway which your wireless router will initiate IPSec VPN connection to.
IPSec settings	Configure the IPSec Protocol related parameters
Pre-shared Key	Type your pre-shared key in this field. A pre-shared key identifies a  communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.
Phase 1 DH group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are:

	<p><b>DH1</b> - use a 768-bit random number</p> <p><b>DH2</b> - use a 1024-bit random number</p> <p>DH5 – user a 1536-bit random number</p>
Phase 1 encryption	<p>Select which key size and encryption algorithm to use for data communications. Choices are:</p> <p><b>DES</b> - a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> - a 168-bit key with the DES encryption algorithm wireless router and the remote IPSec router must use the same algorithms and key , which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p> <p><b>AES</b> - Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. Here you can have the choice <b>AES-128, AES-192, AES-256</b></p>
Phase 1 authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are <b>SHA1</b> and <b>MD5</b>. <b>SHA1</b> is generally considered stronger than <b>MD5</b>, but it is also slower.</p> <p>MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.</p> <p>SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.</p>
Phase 1 SA lifetime	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 120 to 86400 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Phase 2 encryption	<p>Select which key size and encryption algorithm to use for</p>

	<p>data communications. Choices are:</p> <p><b>Null</b> – No data encryption in IPsec SA. Not suggested.</p> <p><b>DES</b> - a 56-bit key with the DES encryption algorithm</p> <p><b>3DES</b> - a 168-bit key with the DES encryption algorithm wireless router and the remote IPsec router must use the same algorithms and key , which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p> <p><b>AES</b> - Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES. Here you can have the choice <b>AES-128, AES-192, AES-256</b></p>
Phase 2 authentication	<p>Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are <b>Null, SHA1</b> and <b>MD5</b>. <b>SHA1</b> is generally considered stronger than <b>MD5</b>, but it is also slower.</p>
Phase 2 SA lifetime	<p>Define the length of time before an IPsec SA automatically renegotiates in this field. It may range from 120 to 86400 seconds.</p>
Show Advanced Settings	<p>Some advanced IPsec VPN configuration is hidden by default, usually you just keep it with no change.</p>
Key management	<p>Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.</p>
IKE negotiation mode	<p>Determines how the Security Association (SA) will be established for each connection through IKE negotiations.</p> <ul style="list-style-type: none"> <li>- Main Mode, which ensures the highest level of security when the communicating parties are negotiating authentication (phase 1).</li> <li>- Aggressive Mode, which is quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1).</li> </ul>
Perfect forward secrecy	<p>Perfect Forward Secret (PFS) is disabled (NONE) by default in phase 2 IPsec SA setup. This allows faster IPsec</p>

(PFS)	setup, but is not so secure. Select DH1, DH2 or DH5 to enable PFS.
Phase 2 DH group	After enable PFS, you need to choose DHx.
Replay detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
NetBIOS broadcast forwarding	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa. Select this check box to send NetBIOS packets through the VPN connection.
Dead peer detection	Force wireless router to detect if the remote IPSec gateway is available or not periodically.
Manual Encryption Key	If choose Manual in Key Management field, you need to input a Manual encryption key for encryption, 16 hexadecimal digits
Manual Authentication Key	Type a unique authentication key to be used by IPSec, 32 hexadecimal digits
Inbound SPI	Type a unique SPI (Security Parameter Index)
Outbound SPI	Type a unique SPI (Security Parameter Index)

#### 6.4.4 VPN - L2TP / PPTP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames, which is very similar to L2TP.

**VPN**

- Enable
- Summary
- Configure
- L2TP / PPTP
- Event Log

**VPN - L2TP / PPTP**

PPP Address Range

Start  .  .  .

End  .  .  .

PPP Security

MPPE Encryption

Users

Username

Password

Confirm Password

User List

#1 johnyan

L2TP Server

Preshared Phrase

Label	Description
PPP address Range	Select the specific VPN tunnel to configure.
Start/ End	Input the naming for identifying.
PPP Security – MPPE Encryption	Select to enable MPPE Encryption. It uses the RSA <a href="#">RC4</a> encryption algorithm.
Apply	Click to save.
Users	
Username	Manually input the L2TP/PPTP username
Password	Manually input the L2TP/PPTP password
Confirm Password	Double confirm with the password.
Add	Click to add.
User List	Display existing user list.
Remove	Click to delete a user.
L2TP Server	

Pre-shared Phrase	Define the pre-shared key.
Apply	Click to save.

### 6.4.5 VPN - Event Log

This page allows you to view the VPN Event Log.

Label	Description
Time	Local time mapping to a certain log event.
Description	Detail information of a log.
Refresh	Click to refresh current page to view new log event.
Clear	Click to clear all of the logs.

## 6.5 PARENTAL CONTROL

### 6.5.1 User Setup

This page allows configuration of users. 'White List Only' feature limits the user to visit only the sites specified in the Allowed Domain List of his/her content rule.

The Parental Control User Setup Page is the master page to which each individual user is linked to a specified time access rule, content filtering rule, and login password to get to the filtered content. Each specified user may also be enabled as a trusted user which means that person will have access to all Internet content regardless of filters that may be set up. This check box can be used as a simple override to grant a user full access but still having the ability to keep all of the previous filtering settings stored and available. Session duration timers can also be entered

to allow a finite amount of time that a user has Internet access via the rules entered once entering their password to get to the Internet for the first time. This allows access to the Internet for a defined user without having to enter a password every time a new web page is served to the client. Likewise, there is a password inactivity timer if there is no Internet access for the specified amount of time in minutes, requiring the user to re-login at expiration to continue using the Internet. These timed logins insure that a specific user is using the Internet gateway for access and logging/access can be provided appropriately. Any time a change is made on this page for a particular user, the Apply button at the bottom of the page needs to be pressed to activate and store the settings.

**Parental Control**

- User Setup
- Basic
- Tod Filter
- Event Log

**Parental Control - User Setup**

**User Configuration**

**User Settings**

2. john  Enable

Password

Re-Enter Password

Trusted User  Enable

Content Rule  White List Access Only

Time Access Rule

Session Duration  min

Inactivity time  min

**Trusted Computers**

Optionally, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer.

1. 00.13.48.08.88.88 ==> Default

2. 00.13.49.00.00.21 ==> john

Label	Description
User configuration	Input username to create a new user.
Add user	Click to direct add this user into local database even you haven't finished the configuration for this user.
User Settings	
Enable	Click to active this user account, and to modify current

	<p>selected user's profile.</p> <p>Unselect this checkbox, to disable this user account.</p>
Remove User	Click to delete the selected user.
Password	Input the password of this user. It's required when this user tries to access Internet via wireless router.
Re-Enter Password	Double confirm with the password.
Trusted User	Active the Enable checkbox to allow the selected user to be trusted user. That means he's now limited to timing and content when visiting Internet. But you can define the session duration period which will trigger wireless router to disable this privilege after expiration.
Content Rule	Select an existing content rule that defines what kind of website he can visit and what can't be visited.
White List Access Only	Suppose admin has created a content rule which defined black list and while list. Then admin can select "White List Access Only" checkbox to force to execute the policy to the selected user.
Time Access Rule	Select a defined time access rule to apply to the selected user.
Session Duration	This will trigger wireless router to disable this privilege after expiration.
Inactivity time	Define the time out value when user has no activity with his visiting to Internet.
Apply	Click to save.
Trusted Computers	Define the trusted host that will bypass the Parental Control Process.

Add	Input the trusted host's MAC address. And click to save.
Remove	Click to delete the selected MAC record.

## 6.5.2 Activation

This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Label	Description
Enable Parental Control	Enable the checkbox to activate the Parental Control feature.
Apply	Click to save.
Content Policy Configuration	Configure content policy configuration.

Add New Policy	Input rule name and click to create a new policy.
Content Policy List	Allow admin to select a certain policy rule.
Remove Policy	Click to delete the selected policy rule.
Keyword List	URL key word list that's used to be used.
Add Keyword	Click to insert a new keyword.
Remove Keyword	Click to delete an existing keyword.
Blocked Domain List	Domain list that's to be blocked.
Add Domain	Click to add a new domain.
Remove Domain	Click to delete an existing domain
Allowed Domain List	White list, which allows users to visit.
Add Allowed Domain	Click to insert new white list.
Remove Allowed Domain	Click to delete the selected URL list.

### 6.5.3 TOD Filter

This page allows configuration of time access policies to block all internet traffic to and from specific network devices based on time of day settings.

## Parental Control

- User Setup
- Basic
- Tod Filter
- Event Log

## Parental Control - Time Access Policy

### Time Access Policy Configuration

Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours"

### Time Access Policy List

1. weekend  Enabled

Days to Block

Everyday  Sunday  Monday  Tuesday  
 Wednesday  Thursday  Friday  Saturday

Time to Block

All day

Start:  (hour)  (min)

End:  (hour)  (min)

Label	Description
Add New Policy	Input policy name, and click Add new Policy button to create a new Time Policy rule.
Time Access Policy List	Allow admin to select time policy rule to enable or remove a selected rule.
Enable	Select the checkbox to active this time policy rule, unselect the checkbox to disable this rule.
Remove	Click to delete a selected rule.
Days to Block	Select the day that this time policy rule limited user to visit Internet.
Time to Block	Define the detailed time for this policy rule.
All Day	Select All Day to eliminate any chance for access within the day blocked.
Apply	Click to save.

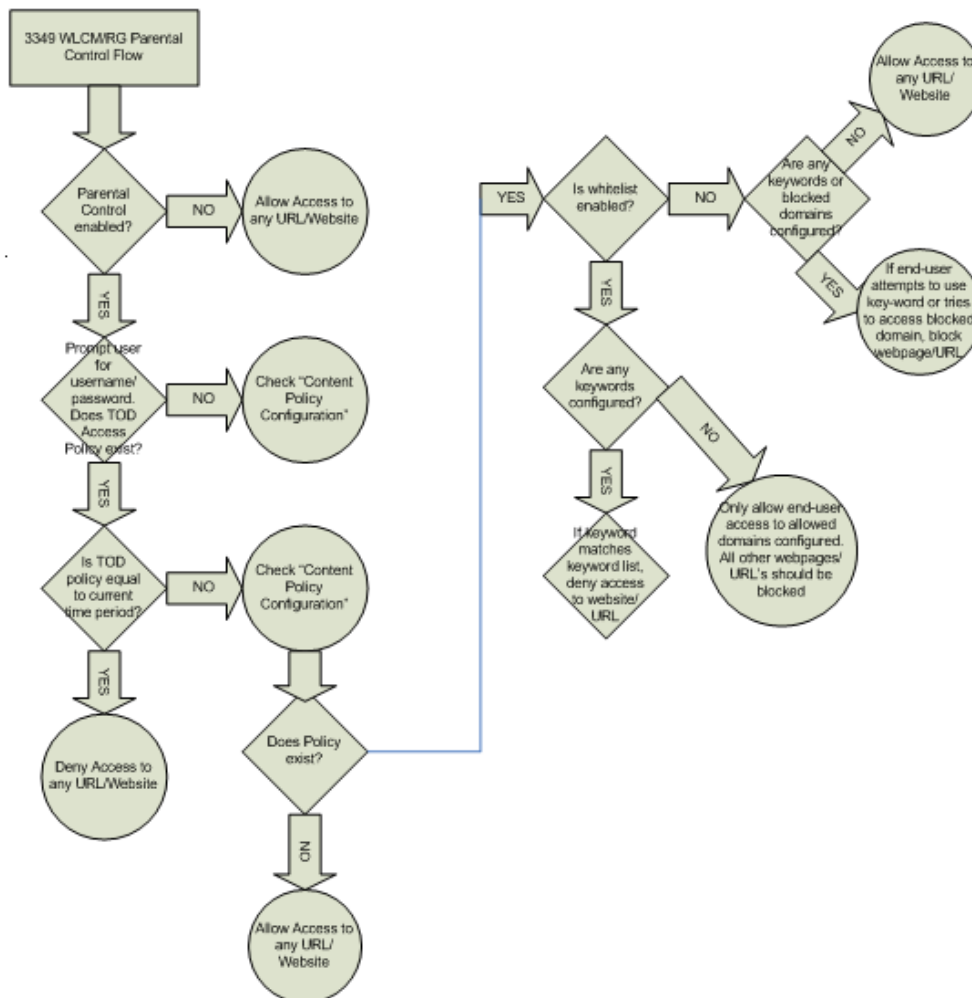
## 6.5.4 Event Log

This page displays Parental Control event log reporting.



Label	Description
Last Occurrence	Display the time when the last event occurred.
Action	Display what's done by parental control, drop or permit an access request.
Target	Display the destination IP address of a certain access request.
User	Display the user who triggered this event log.
Source	Display the source IP address of this event.

## NOTE: PARENTAL CONTROL FLOW



## 6.6 FIREWALL

Originally, the term firewall referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve all of the security problems. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

### 6.6.1 Content Filter

This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of "trusted computers" can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the Firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites.

**Firewall**

- Content Filter
- Event Log
- Remote Log

**Firewall - Content Filter**

**Content Filter Settings**

- Filter Proxy  Enable
- Filter Cookies  Enable
- Filter Java Applets  Enable
- Filter ActiveX  Enable
- Filter Popup Windows  Enable

**Firewall Settings**

- Block Fragmented IP Packets  Enable
- Port Scan Detection  Enable
- IP Flood Detection  Enable
- Firewall Protection  Enable
- Protection against incoming connection requests on routed subnet  Enable

Apply

Label	Description
<b>Content Filter Settings</b>	
Filter Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Filter Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.

Filter Java Applets	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Filter ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Filter Popup Windows	Filter those pop windows when visiting some website.
<b>Firewall Settings</b>	
Block Fragmented IP Packets	Enable the firewall to detect fragmented IP packet.
Port Scan Detection	Enable firewall to detect port scan attack.
IP Flood Detection	Enable firewall to detect IP flood attack.
Firewall Protection	Enable firewall function.
Protection against incoming connection requests on routed subnet	Enable firewall to protect all of the routed subnet connected to the wireless router.
Apply	Click to save the configuration.

**Note:**

- **Block Fragmented IP Packets**

"With this feature enabled, all packets are checked to determine if the packet contains a "fragment" flag. If the flag exists, the CM will discard the packet. This feature is used primarily to protect against any intruders/hackers from gaining access to the router or network." "Under certain conditions, this feature may cause communication issues with other devices on the network and should be disabled. For example, streaming media applications may fragment the packets depending on the encoding used for the video stream. Depending on the encoding used for the clip, some or a majority of the packets will become fragmented. For clips encoded at 300 Kbps, 66% of the packets are IP fragments, while below 100 Kbps there is no fragmentation.

## 6.6.2 Event Log

This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

Label	Description
Contact E-mail Address	Enter E-mail address for sending Firewall event log.
Email Address Password	The password of the E-mail you enter
SMTP Server Name	Enter SMTP Server Name for sending Firewall event log.
E-mail Alerts	If you enable ,the alert can appearance when have a new mail
Apply	Click to submit changes.
Description	Summary of this firewall event log.
Count	If a certain firewall event log repeated for several times, value in count will increase.
Last Occurrence	Display the time when the last of the firewall event occurred.
Target	Display the destination IP address of this access event.
Source	Display the source IP address of this access event.
E-mail log	Click to send current Firewall event log to e-mail address specified.

Clear log	Click to clear event log.
-----------	---------------------------

### 6.6.3 Remote Log

This page allows optional configuration of events to be sent to a local SysLog server.

Label	Description
Permitted Connections	Select to record all of the access attempts that are allowed by firewall.
Blocked Connections	Select to record all of the access attempts that are blocked by firewall.
Known Internet Attacks	Record event log for known attacks from Internet.
Product Configuration Events	Record into event log once device configuration is modified by user or admin.
SysLog server	Define the IP address of the Syslog server.
Apply	Click to make the configuration to take effect.

## 6.7 TOOLS

### 6.7.1 Ping

This page provides ping diagnostics to help with IP connectivity problems.

## Tools - Ping

### Ping Test Parameters

Ping Target :

Ping Size :  bytes (64 ~ 1518)

No. of Pings :  (1 ~ 5)

Ping Interval :  ms (100 ~ 10000)

Results
<pre> Pinging 192.168.0.10 ... No reply after 5000 ms... No reply after 5000 ms... No reply after 5000 ms... Pings sent: 3 (0 per second); Replies received: 0 (0 per second) Min time: 0 ms; Max time: 0 ms; Avg time: 0 ms; Total time: 17130 ms           </pre>
<input type="button" value="Refresh"/>
<p>To get an update of the results, you must select the REFRESH button above.</p>

Label	Description
Ping Target	Input the IP address user wants to pin to.
Ping Size	Define the packet size of ping operation.
No. of Pings	Define the amount of the batch ping operation.
Ping Interval	Define the interval between 2 ping operations.
Start Test	Click to start test
Abort Test	Click to stop test
Clear Results	Click to clear existing testing result.
Results	This area will display result.
Refresh	Click to refresh old logs.

## 6.7.2 Trace Route

This page provides trace route diagnostics to help with IP connectivity problems.

## Tools - Trace Route

### Tracert Test Parameters

Tracert Target :

MAX Hops :  Hops (1 ~ 50)

Time out :  ms (100 ~ 10000)

Results

To get an update of the results, you must select the REFRESH button above.

Label	Description
Tracert Target	Input the specific IP address user wants to trace route to it.
MAX Hops	Define the MAX hop.
Time out	Define the expiration time for this tracert operation.
Start Test	Click to start tracert test
Abort Test	Click to stop test
Clear Results	Click to clear existing testing result.
Results	This area will display tracert route operation result.
Refresh	Click to refresh old logs.

### 6.7.3 Client List

This page shows connected computer in client list.

## Tools - Client List

Host Name	IP Address	MAC Address	Interface
DJFQFB2X	192.168.0.10	00:1f:3a:28:b1:c7	WIRELESS
JohnYan	192.168.0.11	00:1c:23:51:ab:d4	ETHERNET

Label	Description
Host Name	Display the host name of the DHCP client.
IP address	Display the IP address assigned to this DHCP client.
MAC address	Display the MAC address.
Interface	Display the method via which the DHCP client is connected to wireless router.
Refresh	Click to refresh the client list.

## 6.7.4 Frequency Scanning Plan

### TOOLS

- [Ping](#)
- [Trace Route](#)
- [Client List](#)
- [Scanning Plan](#)
- [Password](#)
- [User Defaults](#)

### Frequency Scanning Plan

Lowest Center Frequency  Hz  
 Highest Center Frequency  Hz  
 Channel Spacing  Hz

Label	Description
Lowest Center Frequency	Display the lowest center frequency
Highest Center Frequency	Display the highest center frequency
Channel Spacing	Display spectrum width.  In US area, usually be 6000000Hz,  In EU area, usually be 8000000Hz.

Apply	Click to make the configuration to take effect.
-------	---

## 6.7.5 Password

This page allows configuration of password and username

Label	Description
User name	By default, there's one user account that has limited privilege, here to modify username for this account.
New Password	Input the value of new password
Confirm Password	Double confirm with the new password.

## 6.7.6 User Defaults

This page allows you to restore factory defaults to the system.

Label	Description
Restore Defaults	Select to make the wireless router to reset to factory default settings only for firewall and parental settings.

Reset The system	Select to do a power cycle reboot.
------------------	------------------------------------



U10C019/U10C020