

Samsung
Advanced Wireless Gateway
User Guide

TABLE OF CONTENTS

SAFETY INSTRUCTIONS	5
FCC Compliance	5
UL Compliance	6
INTRODUCTION	6
Purpose	6
Document Content and Organization	7
Conventions.....	7
Chapter 1. Advanced Wireless Gateway Overview	7
1.1 Introduction.....	8
1.2 Features.....	8
1.3 What's is in the box?	8
1.4 Front Panel.....	9
1.5 Back Panel	11
1.6 Bottom panel	11
1.7 Gateway for the Installation	12
Chapter 2. Installing the Advanced Wireless Gateway	13
2.1 Introduction.....	13
2.2 Connect the Wireless Gateway	13
2.3 Connect your wireless Note PC	14
2.3.1 How to connect your wireless Note PC.....	14
CHAPTER 3. Basic Gateway Configuration.....	17
3.1 Introduction.....	17
3.2 Using Web UI.....	17
3.2.1 Web UI Connection	17
3.2.2 Wireless Gateway Main Window.	18
3.2.3 Managing Operator Account	18
3.2.4 Managing the Gateway for the Wireless Network.....	18
CHAPTER 4. Gateway LED Status	22
4.1 Introduction.....	22
CHAPTER 5. Advanced Gateway Setup	24
5.1 Introduction.....	24

5.2 Parental control	24
5.3 Port Forwarding (virtual server)	25
5.4 port triggering	26
5.5 DMZ host	27
CHAPTER 6. Troubleshooting the Gateway	28
6.1 Introduction	28
6.2 Configuration TCP/IPv4 on Windows system (XP)	28
6.2 Reset/Restore the Gateway via the RESET button in Rear Panel	29

- . The basic settings are provided by the manufacturer and service provider.
- . The manual is intended to provide a basic guide for personal settings.

Document Content and Organization

This manual consists of ten Chapters, which are summarized as follow:

Chapter 1. This chapter describes the contents in the package and system requirements. It also provides an overview of the gateway's front, rear, and bottom panels.

Chapter 2. This chapter describes how to install the gateway.

Chapter 3. This chapter describes how to configure the gateway.

Chapter 4. This chapter describes how to understand the LEDs.

Chapter 5 – This chapter describes how to configure the gateway for advanced users.

Chapter 6 – This chapter provides troubleshooting information you can use in the unlikely event you encounter a problem with the gateway.

Conventions

The following paragraph contains special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



NOTE

Indicates additional information as a reference.

Chapter 1. Advanced Wireless Gateway Overview

1.1 Introduction

This chapter provides an overview of Samsung Advanced Wireless Gateway(AWG) features, indicators, and connectors to help you become familiar with the Advanced Wireless Gateway . This chapter also lists the accessories and equipment that are provided with the Advanced Wireless Gateway so you can verify that you received all of these items.

1.2 Features

This section provides a brief overview of the features of Samsung Gateway.

WAN connection features (DOCSIS 3.0/3.1)

- . 5 Gbps Downstream at 5 ~ 85 MHz frequency range.
- . 700+ Mbps Upstream at 5 ~ 85 MHz frequency range.

LAN connection features

- . MoCA 2.0 to interconnect your local MoCA devices via your coax network in home.
- . Four 10/100/1000BASE-T Ethernet ports for your local home network devices.
- . Wireless access point for your local home network devices via the integrated IEEE 802.11n 2.4 GHz and IEEE 802.11ac 5 GHz.
- . Firewall deters hackers and protects the home network from unauthorized access via Router Function.

Wi-Fi connection features

- . Dual Band Concurrent in mode 802.11a/b/g /n/ac
- . Wi-Fi 5GHz ac 4x4 mode (4Tx, 4Rx) with MU-MIMO
- . Wi-Fi 2.4GHz n 3x3 mode (3Tx, 3Rx) with MIMO

Fax/Telephony connection features

- . Two-line RJ-11 telephony ports for connecting to traditional telephones or fax machines

Design and Additional Function

- . Elegant, compact cube type design
- . LED status indicators on the front panel, providing an easy-to-understand display that indicates the operational status

Management

- . The Web UI allows you to configure your Gateway and network via your web browser.
- . Allows software upgrades by your service provider via TR-069 methods or CableModem

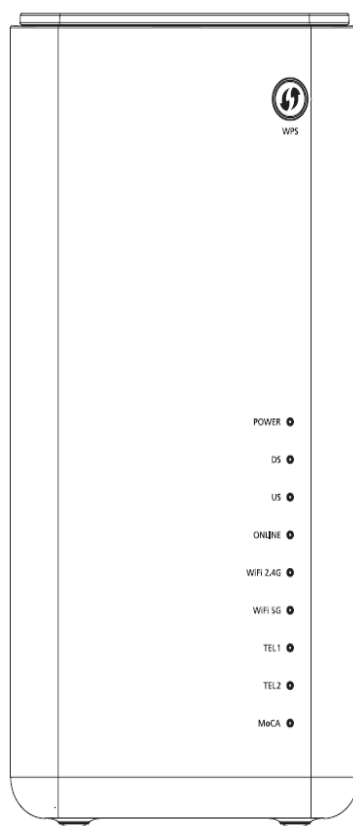
1.3 What's is in the box?

When you receive Samsung AWG, you should check the equipment and accessories to verify that each item is in the box and that each item is undamaged.

Items of the box can be changed by by your service provider.
Basically, the box contains the following items:

- . Advanced Wireless Gateway
- . Power Code
- . 35W Adpter for only Samsung Gateway

1.4 Front Panel



1. WPS (WIRELESS PROTECTED SETUP)—OFF (normal condition) Wireless Protected Setup is not active. Blinking indicates the button has been pressed and WPS is active so that a new wireless client can be added to the wireless network.

2. POWER—ON, power is applied to the Residential Gateway. OFF when power is off to the Residential Gateway.

3. DS—ON, the Gateway is exchanging data with the cable network. Blinking indicates the downstream scan is in progress.

4. US—ON, the Gateway is exchanging data with the cable network. Blinking indicates the upstream scan is in progress.

5. ONLINE—ON, the Gateway is registered on the network and fully operational. OFF indicates the Gateway has not registered on the network.

6. WiFi 2.4 G—ON, the wireless access point is operational. Blinking indicates that data is being transferred over the wireless connection. OFF indicates that the wireless access point is not enabled.

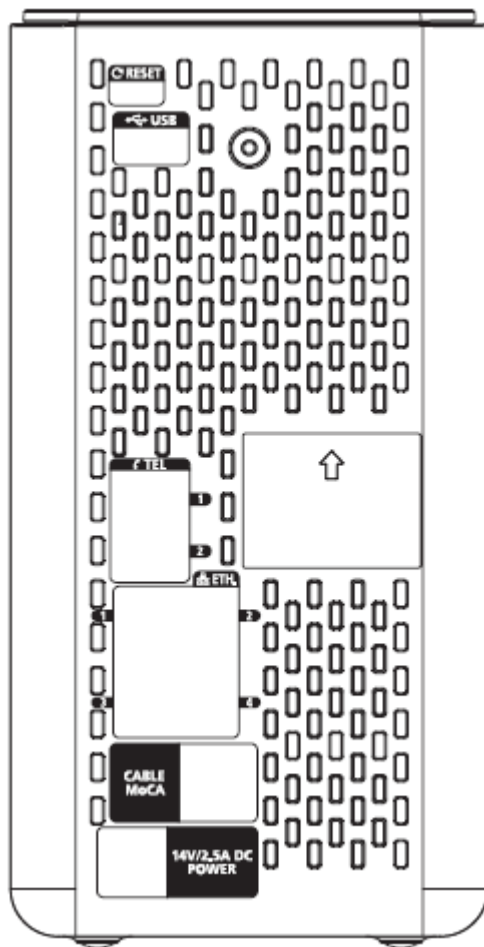
7. WiFi 5 G—ON, the wireless access point is operational. Blinking indicates that data is being transferred over the wireless connection. OFF indicates that the wireless access point is not enabled.

8. TEL1—ON indicates telephony service is enabled. Blinks when line 1 is in use. OFF indicates that phone service for TEL 1 is not enabled.

9. TEL2—ON indicates telephony service is enabled. Blinks when line 2 is in use. OFF indicates that phone service for TEL 2 is not enabled.

10. MoCA— ON, MoCA is operational. Blinking indicates that data is being transferred over the MoCA connection. OFF indicates that the MoCA is not enabled.

1.5 Back Panel



1. RESET—A momentary pressing (1-2 seconds) of this switch restarts the device. To press this switch, insert a thin object, such as a paper clip, into the RESET port; then press and hold the switch for more than ten seconds to reset all settings to their factory-settings and then restart the device.

2. USB —Connects the Residential Gateway to selected devices. For models that support USB, the default is one USB port.

3. TEL1 and TEL2—RJ-11 telephone ports for connecting telephones, fax machines, and/or an analog home alarm system.

4. ETHERNET—Four RJ-45 Ethernet ports allow connection to the Ethernet port on your PC or network device.

5. CABLE/MoCA—F-connector connects to your home coax network to provide Cable and MoCA service.

6. POWER—Connects the Gateway to the Samsung only Adpter with 35W.

1.6 Bottom panel

Product label (item A)

The label on the bottom of the Gateway contains information about your Gateway, like:

Device information

Wireless security settings

SAMSUNG**Samsung Electronics Co Ltd**
19 Chapin Rd., Building D, Pine Brook,
New Jersey, 07058MODEL : GX-MC990CL
Rating : 14V DC ---; 2.5ASamsung
FCC ID : A3LGXMC990CLAUDIO/VIDEO
APPARATUS
2A49
E221083

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

Manufactured : 2017.02



SN : 10Digits



MFG SN : 15Digits

SSID 1 Name(2.4Ghz) : MC990CL18C0-2.4G
SSID 2 Name(5Ghz) : MC990CL18C0-5G
Wi-Fi Password (2.4/5G) : GXMC9909018C0
WPS PIN : 99087612

SSID 1 NAME(2.4Ghz) is the network name of the 2.4 GHz access point and is of the following format:
MC990CLXXXX-2.4G (where X is an alphanumeric character).

SSID 2 NAME(5Ghz) is the network name for the 5 GHz access point and is of the following format:
MC990CLXXXX-5G (where X is an alphanumeric character).

Wi-Fi Password(2.4/5G) is the WPA2-PSK password for the 2.4/5 GHz access point and is of the
following format: GXMC990XXXXXX (where X is an alphanumeric character).

1.7 Gateway for the Installation

The ideal location for your Gateway is where it has access to adppter and other devices. Think about the layout of your home or office, and consult with your service provider to select the best location for your Gateway. Read this user guide thoroughly before you decide where to place your Gateway.

Consider these recommendations:

Choose a location close to your computer if you will also use the Gateway for high-speed Internet service.

Choose a location that is near an existing RF coaxial connection to eliminate the need for an additional RF coaxial outlet.

Choose a location that is relatively protected from accidental disturbance or harm, such as a closet, basement, or other protected area.

Choose a location so that there is plenty of room to guide the cables away from the Gateway without straining or crimping them.

Choose a location that allows adequate ventilation around the Gateway.

Choose a location for the Residential Gateway that is adjacent to your telephone equipment if you plan on connecting your phone directly to the Gateway.

Chapter 2. Installing the Advanced Wireless Gateway

2.1 Introduction

This chapter provides how to properly install the Advanced Wireless Gateway to your service provider's network and to connect the Advanced Wireless Gateway to your PC and your other IT devices.

2.2 Connect the Wireless Gateway

Connecting Coax Cable to your cable splitter and the Gateway

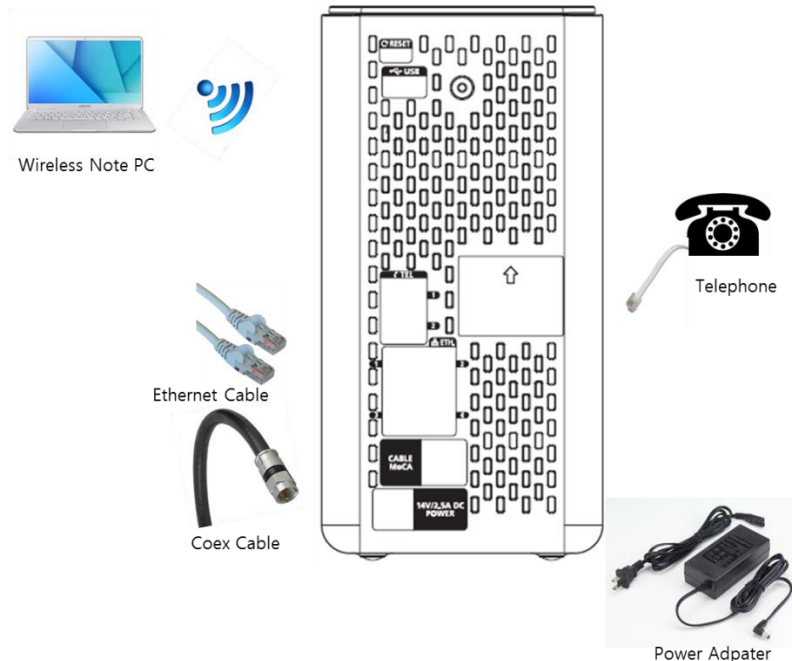
1. Choose an appropriate and safe location to install the Gateway.
2. Power off your PC and other IT device.
3. Connect the active RF coaxial cable from your service provider to the coax connector labeled CABLE/MoCA on the back of the Wireless Gateway.
4. If your Wireless Gateway supports telephone service , connect one end of a telephone jumper cable to a telephone outlet in your home. Then connect the other end of the jumper cable to the appropriate RJ-11 TEL1 or TEL2 port on the back of the Wireless Gateway.
5. Connect your PC to the Wireless Gateway using the Ethernet Connection or the Wireless Connection.
6. Connect the DC jack end of the Adapter into the DC plug on the back of the Gateway. Connect the power code to adapter and an electrical outlet.

The Wireless Gateway will perform an automatic search to locate and sign on to the broadband data network. This process may take up to 2-5 minutes. The Wireless Gateway will be ready for use when the Power, DS,US, and Online LEDs on the front panel of the Wireless Gateway stop blinking and remain on continuously.

- 7 . If your wireless devices uses wireless networking, the WiFi 2.4 G or WiFi 5 GHz LED on the Wireless Gateway should be on or blinking.

- 8 Finally, the installation is complete, and you can begin surfing the Internet sites.

An example of connection diagram is shown in the below figure.



2.3 Connect your wireless Note PC

The Gateway has two access points that allows you to connect wireless devices to your home network:

The 5 GHz (4x4) IEEE 802.11ac access point offers superior transfer rates, is less sensitive to interference and allows you to connect IEEE802.11a/n/ac wireless clients.

The 2.4 GHz (3x3) IEEE 802.11n access point allows you to connect IEEE802.11b/g/n wireless clients. Use this access point for wireless clients that don't support 5 GHz.

2.3.1 How to connect your wireless Note PC

Requirements

Your network device must be equipped with a wireless client.

Your network device must be configured to obtain an IP address automatically. This is the default setting.

Procedure

If you want to connect a computer using the wireless network, configure the wireless client on your computer with the wireless

settings printed on the Gateway's side or back panel label.

For the network name, two values are available:

Network Name 1 (SSID) is the network name of the 5 GHz access point and is of the following format: MC990CLXXXX-2.4G (where X is an alphanumeric character).

Network Name 2 (SSID) is the network name for the 5 GHz access point and is of the following format: MC990CLXXXX-5G (where X is an alphanumeric character).

The password is common for both access points.

To configure these settings on Windows 7.

Proceed as follows:

1 Click the wireless network icon in the notification area.

2 A list of available wireless networks appears.

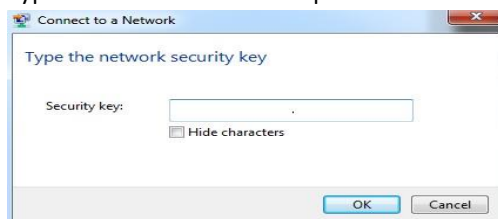


Double-click the Gateway access point.

The Gateway is listed with the MC990CLXXXX-2.4G and MC990CLXXXX-5G which is printed on the Gateway's bottom side.

3 Windows prompts you to enter the security key.

Type the **Password** which is printed on the Gateway's bottom panel label in the **Security key** and click **OK**.



4. And then, the wireless Note PC is connected to the Gateway



CHAPTER 3. Basic Gateway Configuration

3.1 Introduction

In this chapter, the basic gateway configuration using web and how to use Web UI is described.

3.2 Using Web UI

3.2.1 Web UI Connection

1. Open your web browser and browse to <http://192.168.0.1>, using a computer or device that is currently connected to you Gateway (either wired or wirelessly).
2. The Gateway prompts you to enter the username and password. Enter your user name (default: **admin**) and password (default:**admin**) and click **OK**.
Input the password of the Gateway that you got from your system default.
(Default ID and Passwd : admin/admin, support/support, user/user)



3.2.2 Wireless Gateway Main Window.

The Gateway Main window consists of menu bar, sub-menus, and detail windows of each menu.

SAMSUNG
Data Gateway

GX-MC990CL

Device Info

Board ID:	BCM93390SMWVG
Symmetric CPU Threads:	2
Build Timestamp:	20170207_1728
Software Version:	S-MC990CLDKUC-0010
Linux Version:	3.14.28-rgProd_6.1.2
Wireless Driver Version:	7.14.164.303 (r666427 WLTEST)
Uptime:	00 2H 4M 19S
SysTime:	1970-01-01T02:04:18-00:00

This information reflects the current status of your WAN connection.

WAN Hardware Address:	00:16:6B:FF:A4:0A
CM Hardware Address:	00:16:6b:ff:a4:08
LAN Hardware Address:	00:16:6B:FF:A4:0B

3.2.3 Managing Operator Account

After the first login, you go through the course of changing the password via Access Control Menu.

Configuration using Web UI

In the menu of **<Management>**, select **<Access Control>** and then select the **<Passwords>** menu in the sub-menus.

When you enter ID/PW values and click the **<Apply/Save>** button, the configuration is applied.

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

Apply/Save

3.2.4 Managing the Gateway for the Wireless Network

The Gateway supports 2 primary wireless network (2.4G/5G) and 6 multiple guest networks in each one primary wireless network.

Configuration Primary Wireless Network

Device Info
Advanced Setup
Wireless
5GHz
2.4GHz
Management
Network Topology
Spectrum Analyzer
WiFi Visualization
Cable Modem Docsis
MTA
Logout

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable Primary Network

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☐ Enable Wireless Multicast Forwarding (WMF)

☐ Enable DWDS

SSID:

BSSID:

Country:

Country Rev:

Max Clients:

Mode Required:

1. In the menu of **<Wireless>**, select Primary Wireless Network (**<5GHz-Basic>** or **<2.4GHz-Basic>**) to configure.
2. Check/Uncheck "Enable Primary Network" check box to turn ON or OFF primary wireless network.
3. Check "Hide Access Point" check box to block broadcasting and hide primary wireless network.
4. Enter new SSID to change primary wireless network's name in SSID field.
 - 32 characters maximum (letters, numbers and/or special characters)
5. Click **<Apply/Save>** button to apply and save the changed configuration.

Configuration Guest Wireless Network

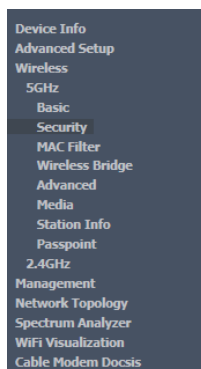
Device Info
Advanced Setup
Wireless
5GHz
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Media
Station Info
Passpoint
2.4GHz
Management
Network Topology
Spectrum Analyzer
WiFi Visualization
Cable Modem Docsis
MTA
Logout

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Enable DWDS	Max Clients	Mode Required	Guest Or LAN	BSSID
☐	MC990CL_GUEST_0_1	☐	☐	☐	☐	☐	50	None	LAN	N/A
☐	MC990CL_GUEST_0_2	☐	☐	☐	☐	☐	50	None	LAN	N/A
☐	MC990CL_GUEST_0_3	☐	☐	☐	☐	☐	50	None	LAN	N/A
☐	MC990CL_GUEST_0_4	☐	☐	☐	☐	☐	50	None	LAN	N/A
☐	MC990CL_GUEST_0_5	☐	☐	☐	☐	☐	50	None	LAN	N/A
☐	MC990CL_GUEST_0_6	☐	☐	☐	☐	☐	50	None	LAN	N/A

1. To enable guest network, check "Enabled" check boxes.
2. Enter new SSID to change guest wireless network's name in SSID field.
 - 32 characters maximum (letters, numbers and/or special characters)
3. Check "Hidden" check box to block broadcasting and hide guest wireless network.
5. Click **<Apply/Save>** button to apply and save the changed configuration.

Configuration Wireless Network Security – Manual Setup AP



Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

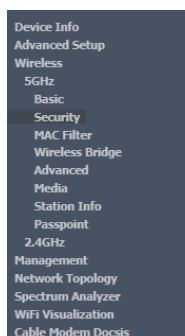
WPA Group Rekey Interval:

WPA/WAPI Encryption:

Protected Management Frame:

1. In the menu of **<Wireless>**, select Security Menu (**<5GHz-Security>** or **<2.4GHz-Security>**) to configure wireless networks' security settings.
2. Select one of the following Network Authentication:
 - A. Open : allows access to the wireless network without security key.
 - B. WPA2 : uses an authentication server to generate keys or certificates.
 - C. WPA2-PSK : use Pre-Shared key(PSK) for encryption.
 - D. Mixed WPA2/WPA : combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access with using an authentication server to generate keys or certificates.
 - E. Mixed WPA2/WPA-PSK : combination Wi-Fi Protected Access version 2 with Pre-Shared Key and Wi-Fi Protected Access with Pre-Shared Key.
3. WPA/WAPI passphrase : Enter wireless network's password.
4. WPA/WAPI Encryption :
 - A. AES (Advanced Encryption Standard) : enhanced encryption type to WPA2 over WPA.
 - B. TKIP+AES(Temporal Key Integrity Protocol and Advanced Encryption Standard) : TKIP and AES encryption types are capable to access wireless network.
5. Protected Management Frame : Select "Capable or Required" to protect management frames such as authentication, de-authentication, association, dissociation.
6. Click **<Apply/Save>** button to apply and save the changed configuration.

Configuration Wireless Network Security – WPS (WiFi Protected Setup) Setup



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually

OR

through WiFi Protected Setup(WPS)

Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

☒ Use STA PIN ☐ Use AP PIN

[Help](#)

Set Authorized Station MAC [Help](#)

1. In the menu of **<Wireless>**, select Security Menu (**<5GHz-Security>** or **<2.4GHz-Security>**) to configure wireless networks' WPS setup.
2. Select "Enabled" to Enable WPS.
 - A. For WPS-PIN configuration, choose "Use STA PIN" radio button and enter Client's PIN number. Press "Add Enrollee" button and start Client's WPS PIN.

- B. For WPS-PBC configuration, choose “Use STA PIN” radio button and empty both STA PIN and Authorized MAC. Press “Add Enrollee” button and start Client’s WPS PBC.

Configuration Wireless Network Channel/Bandwidth

Device Info

Advanced Setup

Wireless

5GHz

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Media

Station Info

Passpoint

2.4GHz

Management

Network Topology

Spectrum Analyzer

WiFi Visualization

Cable Modem Docsis

MTA

Logout

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply/Save" to configure the advanced wireless options.

Band:	5GHz	
Channel:	36/80	Current: 36
Auto Channel Timer(min)	15	
802.11n/EWOC:	Auto	
Bandwidth:	80MHz	Current: 80MHz
Control Sideband:	Lower	Current: N/A
802.11n Rate:	Auto	
802.11n Protection:	Auto	
RIFS Advertisement:	Auto	
OBSS Coexistence:	Enable	
54g™ Rate:	6 Mbps	
Multicast Rate:	Auto	

1. In the menu of **<Wireless>**, select Advanced Menu (**<5GHz-Advanced>** or **<2.4GHz-Advanced>**) to configure wireless networks’ radio configuration.
2. Select “Channel” and “Bandwidth” to improve wireless network interference and throughput performance.

CHAPTER 4. Gateway LED Status

4.1 Introduction

This chapter provides LED's status of front panel when the Advanced Wireless Gateway is power on, provisioning, normal status, and abnormal status.

Gateway LED indicates the various statuses of system. Each LED displays the following information:

POWER LED status is below table

POWER	LED State	Description
	ON	The Gateway is power on when the DC input supplied
	OFF	The Gateway is power off when the DC input don't supplied

CableMode start up LED sequence is table below.

CableModem	LED	Status	Description
	DS	ON	Downstream looking is in completed
		Blinking	Downstream looking is in progress
		OFF	The Gateway is power off
	US	ON	Upstream looking is in completed
		Blinking	Downstream looking is in progress
		OFF	The Gateway is power off
	ONLINE	ON	Downstream and Upstream looking are completed The connection is completed on internet
		Blinking	Downstream and Upstream looking are in progress
		OFF	The Gateway is power off

Wi-Fi connection LED sequence is table below.

Wi-Fi	LED	Status	Description
	WiFi 2.4G	ON	The Wi-Fi 2.4Ghz service is enabled
		Blinking	The data is being transferred in 2.4Ghz over the wireless connection
		OFF	The 2.4Ghz Wi-Fi service is disabled
	WiFi 5G	ON	The Wi-Fi 5Ghz service is enabled
		Blinking	The data is being transferred in 5Ghz

			over the wireless connection
		OFF	The 5Ghz Wi-Fi service is disabled

Telephony and MoCA connection LED sequence are table below.

	LED	Status	Description
Telephony	TEL1/TEL2	ON	The telephone or fax is not in use (on-hook)
		Blinking	The telephone or fax is in use (off-hook)
		OFF	The telephony service is disabled
MoCA	MoCA	ON	The MoCA service is enabled
		Blinking	The MoCA network has traffice
		OFF	The MoCA service is disabled

Ethernet connection LED sequence of rear panel are table below.

	LED	Status	Description
Ethernet	Orange	Blinking	Blinking while data exchanging
		OFF	No data exchanging
	Green	ON	Link connection display
		OFF	No link connection

CHAPTER 5. Advanced Gateway Setup

5.1 Introduction

This chapter describes the setup procedures for the security related setting such as parental control And port control for IP application. It includes blocking or open function, remote access, firewall function, and more

5.2 Parental control

Keep your children safe online with the parental control rules for Gateway

A max rules number is 64 entries.

The screenshot shows the Samsung Data Gateway web interface for the GX-MC990CL. The left sidebar contains a menu with options: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Parental Control (highlighted), Time Restriction, DNS, Passthrough MAC, Router Configuration, and Power Management. The main content area is titled 'Access Time Restriction Blacklist -- A maximum 64 entries can be configured.' Below this is a table with the following columns: RuleName, MAC Address, URL Keyword, Protocol, Start Port, End Port, Enabled, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Start (hh:mm in 24 hour format), Stop (hh:mm in 24 hour format), Edit, and Remove. A single rule is listed with RuleName 'Game', MAC Address '80:18:A7:90:18:C0', URL Keyword '*', Protocol '*', Start Port '*', End Port '*', Enabled 'Yes', and a blocking time from 09:00 to 23:59 on Saturdays. Below the table are 'Add' and 'Remove' buttons.

RuleName	MAC Address	URL Keyword	Protocol	Start Port	End Port	Enabled	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Start (hh:mm in 24 hour format)	Stop (hh:mm in 24 hour format)	Edit	Remove
Game	80:18:A7:90:18:C0	*	*	*	*	Yes	x						x	09:00	23:59	Edit	☐

The configuration windows is shown below. Click <Add> button for input values.

The screenshot shows the 'Access Time Restriction' configuration form in the Samsung Data Gateway web interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Access Time Restriction'. Below the title is a description: 'This page adds time of day restriction to a special LAN device connected to the Router. By default, it will block WAN access for any URLs on the LAN device. If only want to block specific URLs, enable Advanced filtering.' The form includes fields for 'Rule Name' (set to 'Game') and 'LAN Device MAC Address' (set to '80:18:A7:90:18:C0'). There is a checkbox for 'Enable Advanced filtering'. Below these is a table for 'Days of the week' with columns for Sunday through Saturday. The 'Click to select' row shows checkboxes for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, with Sunday and Saturday checked. Below the table are fields for 'Start Blocking Time' (09:00) and 'End Blocking Time' (23:59), both with '(hh:mm in 24 hour format)' labels. There is a dropdown for 'Enable this rule' set to 'Yes'. An 'Apply/Save' button is at the bottom right.

Days of the week	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Click to select	☒	☐	☐	☐	☐	☐	☒

Configuration using Web UI

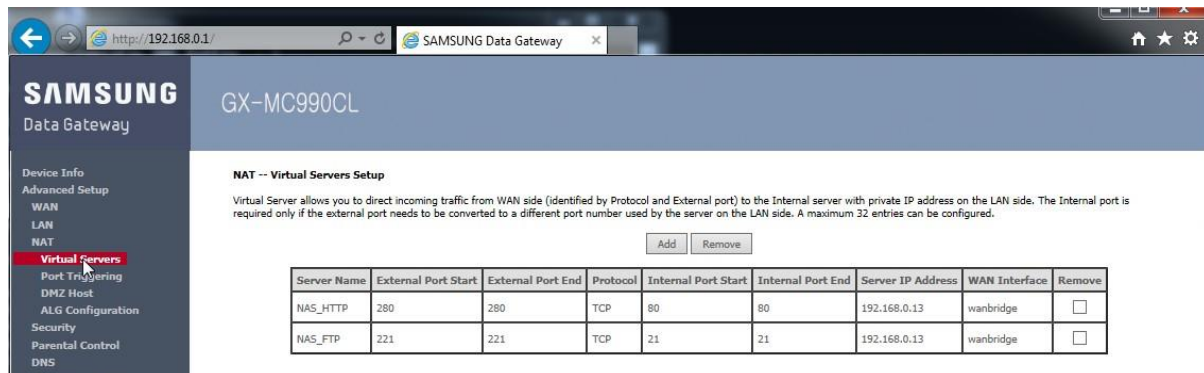
In the menu <Advanced Setup>, select <Parental Control>, select <Time Restriction> and then select the <Add> button .

Click Apply/Save after input Rule Name, MAC Address, days, and times, then user can configure the restricted service status.

5.3 Port Forwarding (virtual server)

Port forwarding opens certain ports on your home or small business network, usually blocked from access by your router, to the Internet. Opening specific ports can allow games, NAS servers, BitTorrent clients, and other applications to work through the usual security of your router that otherwise does not permit connections to these ports.

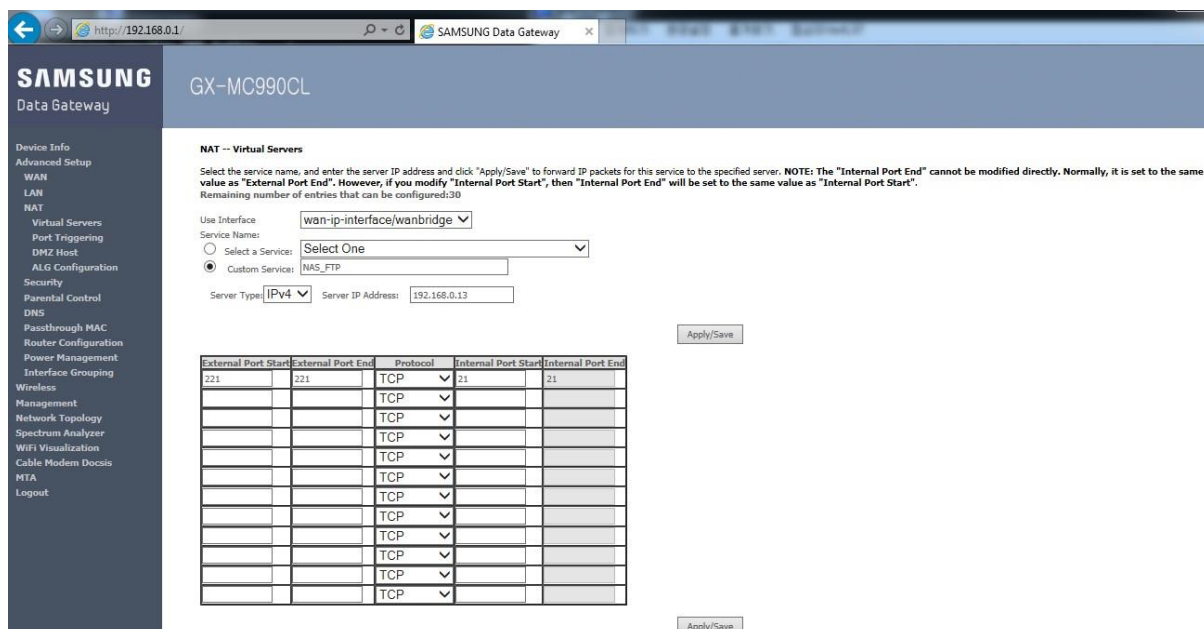
The port Forwarding has 32 entries.



Configuration using Web UI

In the menu of **<Advanced Setup>**, select **<NAT>** and then select the **<Virtual Servers>** menu in the sub-menus.

When you click the **<Add>** button in the Virtual Servers window, the servers creation window is displayed. When you enter a configuration value and click the **<Apply/Save>** button, the configuration is applied.



The Port Triggering is an advanced feature that can be used for gaming and other internet applications.

SAMSUNG

Data Gateway

GX-MC990CL

Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

ALG Configuration

Security

Parental Control

DNS

Passthrough MAC

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Add Remove

Application Name	Trigger				Open			WAN Interface	Remove		
	Protocol	Port Range		Protocol	Port Range						
		Start	End		Start	End					
battle	TCP	88	90	TCP	88	1023	wanbridge	☐			

In the menu of **<Advanced Setup>**, select **<NAT>** and then select the **<Port Triggering>** menu in the sub-menus.

Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Hosts

ALG Configuration

Security

Parental Control

DNS

Passthrough MAC

Router Configuration

Power Management

Interface Grouping

Wireless

Management

Network Topology

Spectrum Analyzer

WiFi Visualization

Cable Modem Docsis

MTA

Logout

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:31

Use Interface: wan-ip-interface/wanbridge

Application Name:

☐ Select an application: Select One

☒ Custom application: battle

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
88	90	TCP	88	1023	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

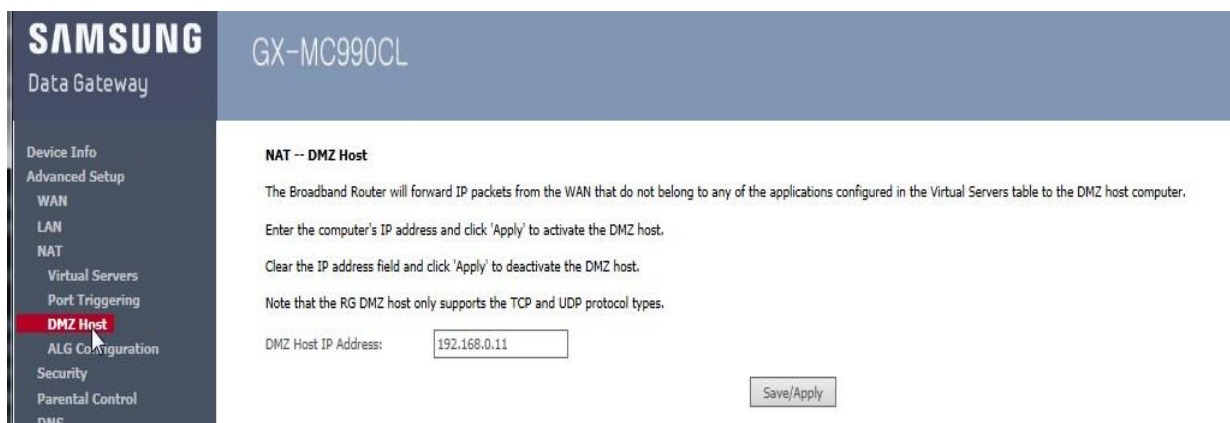
5.5 DMZ host

A DMZ (demilitarized zone) on a gateway refers to a DMZ Host. A gateway DMZ host is a host on the internal network that has all UDP and TCP ports open and exposed, except those ports otherwise forwarded. They are often used a simple method to forward all ports to another firewall/[NAT](#) device.

Configuration using Web UI

In the menu of **<Advanced Setup>**, select **<NAT>** and then select the **<DMZ Host>** menu in the sub-menus.

When you enter a configuration IP value and click the **<Apply/Save>** button, the configuration is applied.



The screenshot displays the Samsung Data Gateway web interface for the model GX-MC990CL. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Virtual Servers, Port Triggering, **DMZ Host** (highlighted in red), ALG Configuration, Security, Parental Control, and DNS. The main content area is titled "NAT -- DMZ Host" and contains the following text: "The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.", "Enter the computer's IP address and click 'Apply' to activate the DMZ host.", "Clear the IP address field and click 'Apply' to deactivate the DMZ host.", and "Note that the RG DMZ host only supports the TCP and UDP protocol types." Below this text, there is a label "DMZ Host IP Address:" followed by a text input field containing the value "192.168.0.11". A "Save/Apply" button is located at the bottom right of the configuration area.

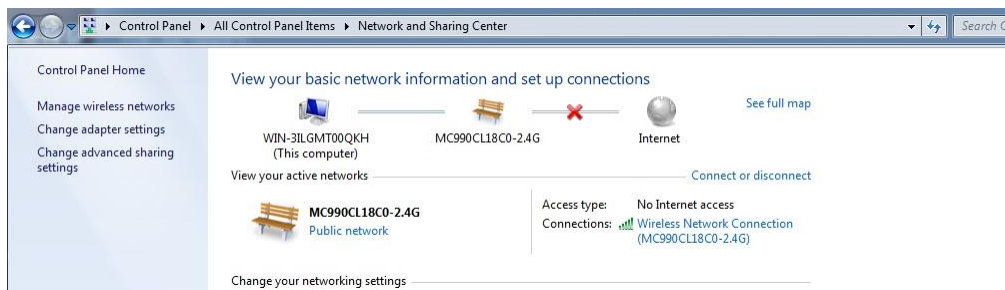
CHAPTER 6. Troubleshooting the Gateway

6.1 Introduction

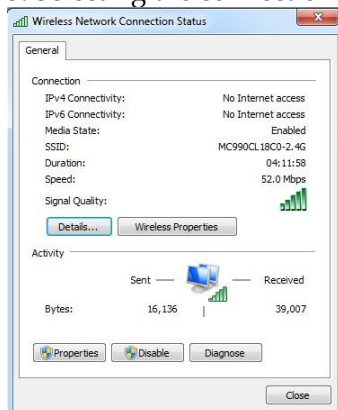
In this chapter, troubleshooting method are described.

6.2 Configuration TCP/IPv4 on Windows system (XP)

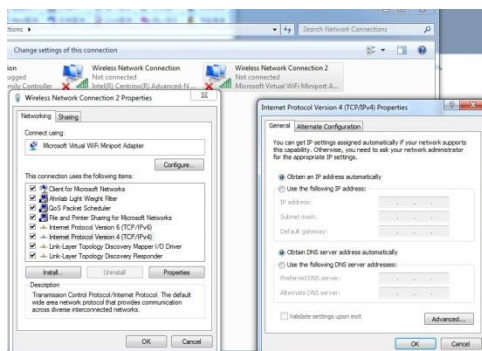
1. Open Network Connections by clicking the **Start** button, and then clicking **Control Panel**.
2. Selecting **Network and Sharing Center**, click **View network connections** as below.



3. Selecting the connection, you can see status as below.



4. Selecting the Properties, you can see networking protocol and then click **Internet Protocol Version 4 (TCP/IPv4)**



6.2 Reset/Restore the Gateway via the RESET button in Rear Panel

To reset the Gateway to factory defaults, you should press and hold the RESET button on the rear panel of Gateway for more five or ten seconds. You can also need to do this if a misconfigurations have locked out all access.

1 Make sure that the Gateway is turned on.

2 If you want to:

Reset the Gateway, use a pen or an unfolded paperclip to push the recessed Reset button on the back panel of the Gateway for approximately 5 seconds and then release it.

Restore the factory default settings of the Gateway, use a pen or an unfolded paperclip to push the recessed Reset button on the back panel of the Gateway for at least 15 seconds and then release it.

3 The Gateway can restart.

FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions :

- (1) This Device may not cause harmful interface, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

WARNING

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

"CAUTION : Exposure to Radio Frequency Radiation.

Antenna shall be mounted in such a manner to minimize the potential for human contact during normal operation. The antenna should not be contacted during operation to avoid the possibility of exceeding the FCC radio frequency exposure limit.

Information for OEM Integrator

This device is intended only for OEM integrators under the following conditions:

- 1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
- 2) The transmitter module may not be co-located with any other transmitter or antenna.

" CAUTION: Exposure to Radio Frequency Radiation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body. This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users."

Samsung

Advanced Wireless Gateway

User Guide

©2017 Samsung Electronics Co., Ltd.
All rights reserved.

Information in this manual is subject to change without notice.