

# AZTECH FG7009GR(AC)

Singtel - Gigabit Ethernet DUAL-BAND 2400 Mbps Wireless AC Residential Gateway

SINGAPORE | May 2015

**Aztech**



## CONTENTS

1. About the Product	Page 3
2. Recommended Setup	Page 7
3. Connecting to the Internet	Page 8
4. Wireless Connection	Page 9
5. How to do WPS pairing	Page 14
6. Wireless Clients	Page 15
7. How to enjoy Wireless AC	Page 16
8. Firewall Configuration	Page 17
9. Troubleshooting	
i. LED Troubleshooting	Page 44
ii. Wireless Troubleshooting	Page 49
iii. How to check existing FW version	Page 50
iv. How to Access Admin GUI	Page 51
10. FAQ	Page 52
11. Support Contact Info	Page 59

# about the product

## Hardware Features

### WAN Connection

- ¤ 1-Port **Gigabit Ethernet WAN** Port for ONT (FTTH) Connection

### LAN Connection

- ¤ 4-Port **Gigabit Ethernet LAN**
- ¤ Built-in Wireless a/b/g/n/ac Dual Band Access Point (2.4GHz and 5GHz)

### Others

- ¤ WPS – Wi-Fi Protected Setup button support
- ¤ LED Indicators for all interfaces and services

# about the product

## Firmware Features

- ¤ Out of the box pre-configuration to support Singtel TV and Singtel Broadband
- ¤ TR069 Compliant Residential Gateway (auto configuration, remote monitoring/troubleshooting, remote firmware upgrade etc.)
- ¤ Zero configuration Internet installation for FTTH
- ¤ Unique Wireless SSID and Wireless Key for each of the unit (default wireless credentials are printed on the casing label sticker)
- ¤ Dynamic LAN Port mapping for the IPTV – STB
- ¤ Port Forwarding and DMZ support, configurable from the user mode pages
- ¤ Standard support for Wireless Security / Encryption

# about the product

## Front Panel Indicators and Button

- ¤ Power
- ¤ Ethernet LAN Ports 1 to 4
- ¤ Wifi (2.4GHz and 5GHz)
- ¤ USB
- ¤ IPTV
- ¤ Broadband (Ethernet WAN)
- ¤ Internet
- ¤ WPS Indicator and button
- ¤ LED ON/OFF Indicator and button



# about the product

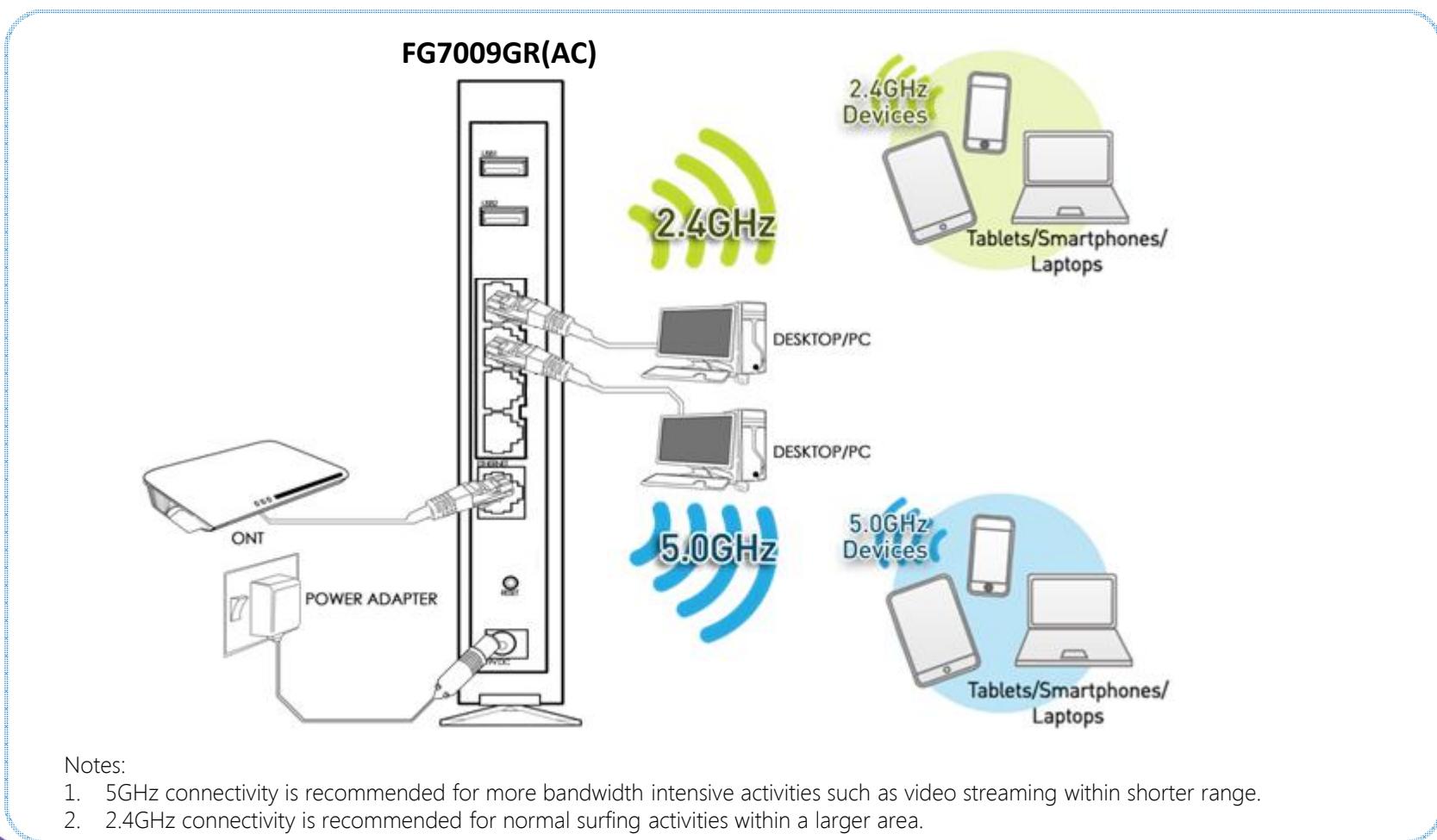
## Back Panel Ports and Button

- ¤ USB 1
- ¤ USB 2
- ¤ Ethernet LAN Ports 1 to 4
- ¤ Ethernet WAN Port
- ¤ Reset button
- ¤ Power Adapter Jack



# Recommended setup

## Recommended Hardware Setup (FTTH)



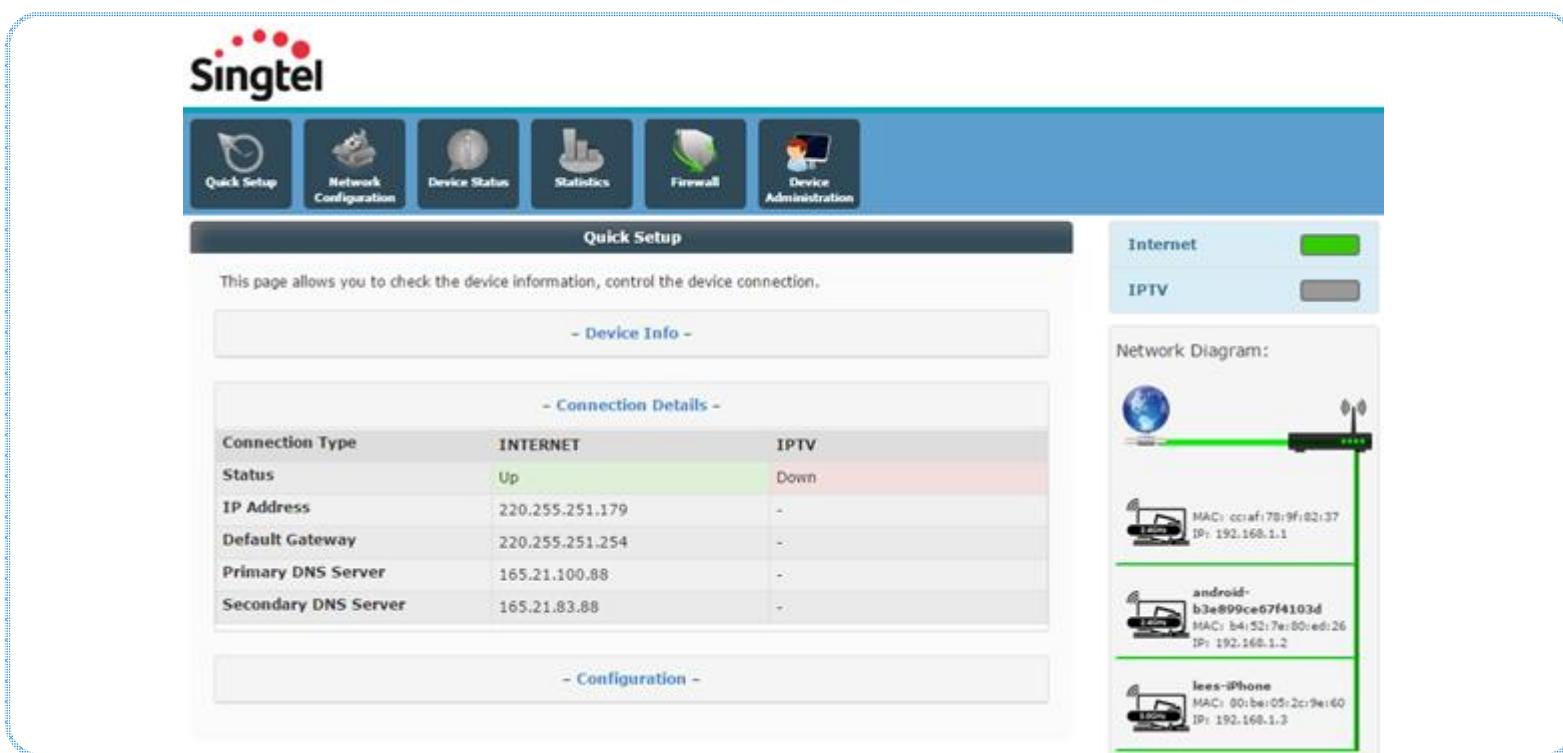
Notes:

1. 5GHz connectivity is recommended for more bandwidth intensive activities such as video streaming within shorter range.
2. 2.4GHz connectivity is recommended for normal surfing activities within a larger area.

# connecting to Singtel Broadband

## FTTH

To check the Internet connection for FTTH , go to <http://192.168.1.254>, scroll down to Connection Details



# wireless connection

## The Default Wireless Configuration

Each unit is preconfigured with a unique wireless network name and a unique password. The information on the default wireless can be found on the casing label sticker.



- ¤ The default wireless authentication is **Mixed WPA2/WPA-PSK**
- ¤ The wireless encryption is **TKIP + AES**
- ¤ Wireless channel is set to **Auto**
- ¤ The **WPS** is **enabled by default**.
- ¤ Both 2.4GHz and 5GHz SSIDs share the same network key by default.

# wireless connection

## Changing the Wireless Settings

Open your web-browser (e.g. Internet Explorer)

- go to <http://192.168.1.254>,
- hover your mouse over the Quick Setup, click on Wireless



- Note by default, it will go to 2.4GHz Wireless settings

# wireless connection

## Changing the Wireless Settings

- Note by default, it will go to 2.4GHz Wireless settings, *with 2.4 GHz button highlighted*

**Wireless Setup**

This page allows you to configure basic features for both the 2.4GHz and 5.0GHz wireless LAN interface.

Wireless Type	<b>2.4 GHz</b>	5.0 GHz
Enable Wireless	<b>Enabled</b>	
AP Mac Address	00:26:75:E3:AF:48	
Non-Broadcast SSID	Disabled	
SSID	SINGTEL-1234	
Channel	Auto	▼
Current	<b>1</b>	▼
Bandwidth	20/40MHz	▼
Current	<b>20MHz</b>	▼
Network Authentication	WPA2-PSK	
*****		
WPA Pre-Shared Key	<a href="#">Click here to display</a>	
WPA Group Rekey Interval	0	
WPA Encryption	AES	
OBSS Coexistence	Enable	
WPS		
Enable WPS	<b>Enabled</b>	
WPS AP PIN	12451791	

**Save/Apply**

# wireless connection

## Changing the Wireless Settings

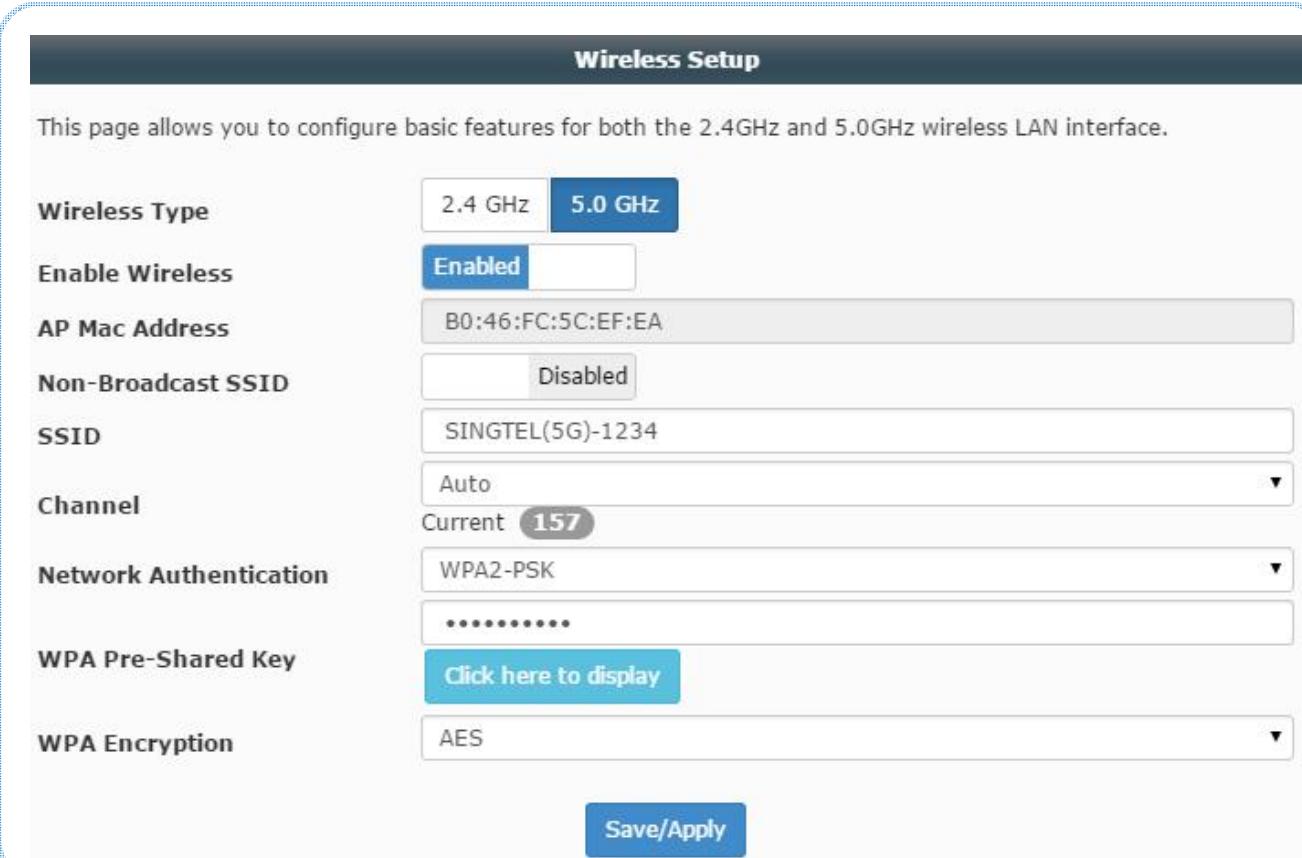
- To change 5 GHz Wireless settings, *click on 5.0 GHz button*

**Wireless Setup**

This page allows you to configure basic features for both the 2.4GHz and 5.0GHz wireless LAN interface.

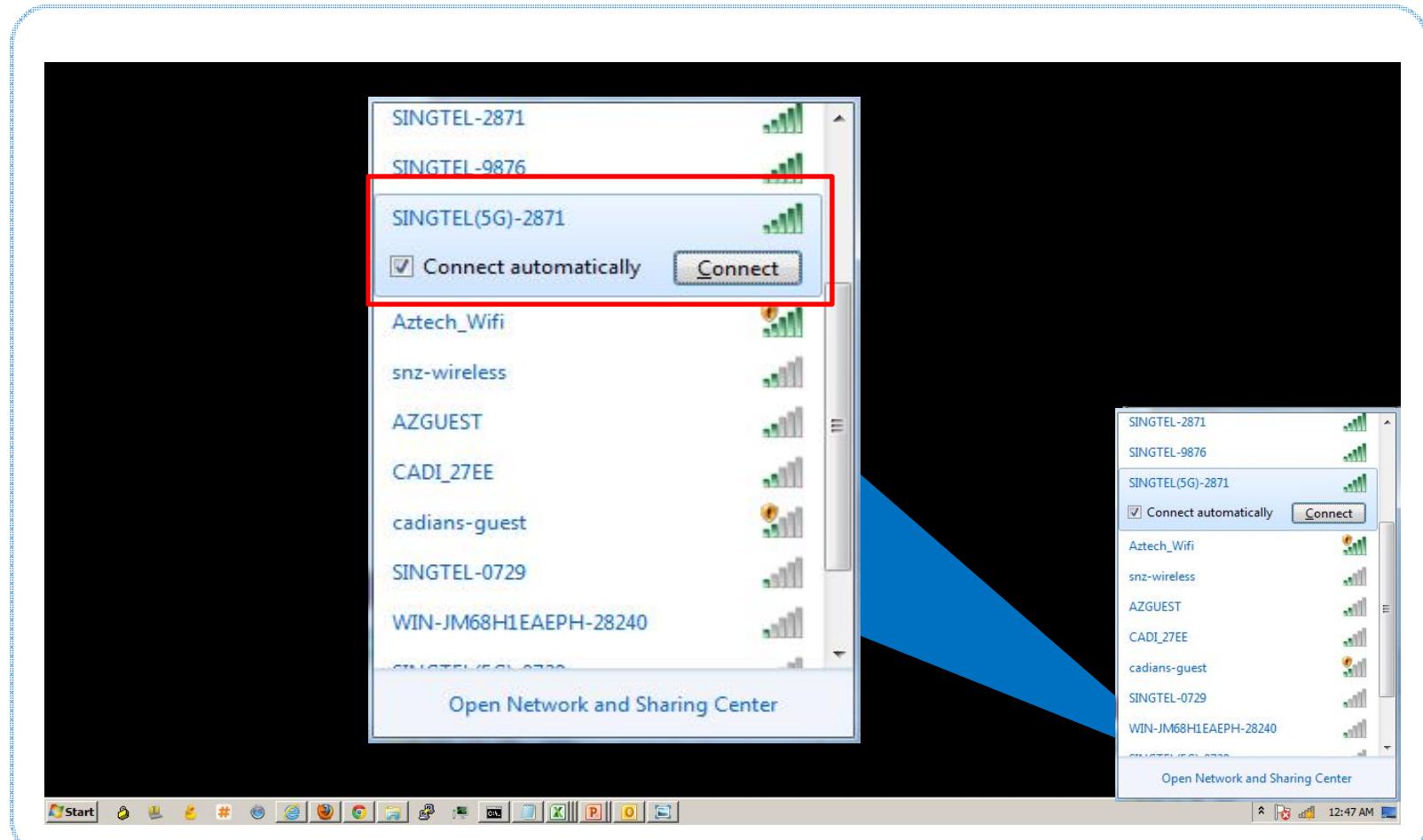
<b>Wireless Type</b>	<b>2.4 GHz</b> <b>5.0 GHz</b>
<b>Enable Wireless</b>	<b>Enabled</b>
<b>AP Mac Address</b>	B0:46:FC:5C:EF:EA
<b>Non-Broadcast SSID</b>	<b>Disabled</b>
<b>SSID</b>	SINGTEL(5G)-1234
<b>Channel</b>	Auto Current <b>157</b>
<b>Network Authentication</b>	WPA2-PSK
<b>WPA Pre-Shared Key</b>	***** <b>Click here to display</b>
<b>WPA Encryption</b>	AES

**Save/Apply**



# wireless connection

## Connecting to 2.4GHz and 5GHz Band



# wireless connection

## How to do WPS Pairing

Step 1. Press the WPS button on the RG once,

- upon pressed, WPS LED will start blinking green

Step 2. Press the WPS button on client device within 120 seconds from step 1 above.

- Once the connection is authenticated and established, WPS LED will be solid green, followed by OFF within the next few seconds.

# wireless clients

## Known wireless devices that supports 5GHz band

- iPhone 5
- iPhone 5S
- iPad 2
- iPad 3
- iPad 4
- iPad mini
- iPad Air
- HTC One
- HTC One S
- HTC One X
- Sony Xperia Z Ultra
- Sony Xperia Z1
- HTC Evo 4G LTE
- Samsung Galaxy S3
- Samsung Galaxy S4
- Samsung Galaxy Note 10.1
- Samsung Galaxy Tab 2 7.0 (GT-P3113)
- Samsung Galaxy Note 1
- Samsung Galaxy Note 2
- Samsung Galaxy Note 3
- Samsung Galaxy Note 8.0 with LTE
- Samsung Galaxy Note 10.1 2014 Edition (LTE)
- iPhone 6
- iPhone 6+
- Samsung Galaxy Note 4
- Samsung Galaxy S5
- Samsung Galaxy S6
- LG G Flex
- LG G Flex 2

Note: This list of devices that supports 5G does not necessarily support wireless AC.

## How to enjoy wireless AC

- Wireless Client: Wireless client need to be able to support wireless AC.
- List of wireless client adapters that support wireless AC:
  - Aztech WL592USB, WL593USB
  - Asus USB-AC53, USB-AC56, PCE-AC68
- List of mobile devices that supports wireless AC:
  - Sony Xperia Z1, Xperia Z Ultra
  - Samsung Galaxy Note 10.1 2014 Edition (LTE), Galaxy S4 with LTE (GT-I9505)
  - Samsung Galaxy Note 4 (LTE), Galaxy S5, Galaxy S6, iPhone 6, iPhone6+

### Notes:

1. This list of devices that supports wireless AC is not exhaustive.
2. Wireless performance is also dependant on the client
3. For end devices which do not support wireless AC, it can still connect to the RG using other wireless mode e.g. a/b/g/n but will not be able to achieve the wireless AC speed.

# firewall configuration

## Incoming and Outgoing Firewall Settings

The screenshot shows the 'Firewall' section of the device's configuration interface. A dropdown menu is open under the 'Firewall' tab, listing 'Outgoing IP Filtering', 'Incoming IP Filtering', 'Port Forwarding', 'Port Triggering', 'Dynamic DNS', 'DMZ Host', and 'Mac Filtering'. The 'Outgoing IP Filtering' option is highlighted.

**Outgoing IP Filtering**

**Internet** (Status: Up) **IPTV** (Status: Down)

**Network Diagram:**

```
graph LR; Internet[Internet] --- Router[Router]; Router --- WiFi1[WiFi Device 1: MAC cc:af:78:9f:82:37, IP 192.168.1.1]; Router --- WiFi2[WiFi Device 2: MAC b4:52:7e:80:ed:26, IP 192.168.1.2]; Router --- WiFi3[WiFi Device 3: MAC 80:be:05:2c:9e:60, IP 192.168.1.3];
```

**Connection Type**

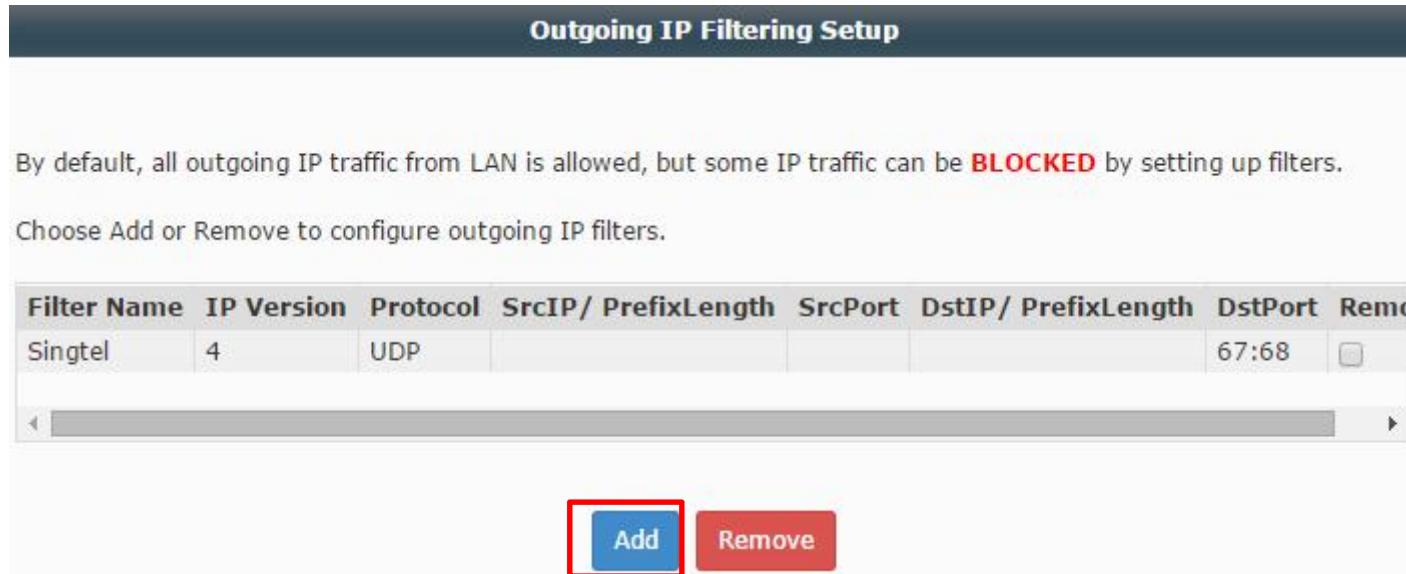
	INTERNET	IPTV
<b>Status</b>	Up	Down
<b>IP Address</b>	220.255.251.179	-
<b>Default Gateway</b>	220.255.251.254	-
<b>Primary DNS Server</b>	165.21.100.88	-
<b>Secondary DNS Server</b>	165.21.83.88	-

## How To Set IP Filtering (Outgoing)

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover mouse over Firewall Configuration, click on Outgoing IP Filtering link

Step 3. Click on Add button



The screenshot shows the 'Outgoing IP Filtering Setup' page. At the top, a message states: 'By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.' Below this, a sub-instruction says: 'Choose Add or Remove to configure outgoing IP filters.' A table lists a single filter entry: 'Singtel' (Filter Name), '4' (IP Version), 'UDP' (Protocol), and an empty row for 'SrcIP/ PrefixLength'. The 'DstIP/ PrefixLength' and 'DstPort' columns are also empty. The 'Removal' column shows '67:68' and an unchecked checkbox. At the bottom of the table are two buttons: 'Add' (highlighted with a red box) and 'Remove'.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Removal
Singtel	4	UDP					67:68 <input type="checkbox"/>

## How To Set IP Filtering (Outgoing)

Step 4. Fill in the fields required (Filter Name, Protocol, Source IP Address and its port number information as well as Destination IP Address and its port number information).

Step 4. Click on Apply/Save button.

**Add IP Filter -- Outgoing**

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:	<input type="text"/>
IP Version:	<input type="text" value="IPv4"/>
Protocol:	<input type="text"/>
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address[/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>

**Apply/Save**

## How To Set IP Filtering (Outgoing)

Step 5. The rule keyed in will be added in the list

*Note: There is a default SingTel rule created in the list, please do not remove.*

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Re
Singtel	4	UDP					67:68
Filter-Test-Out	4	TCP or UDP	192.168.1.99	8082	10.233.233.0	8082	<input type="checkbox"/>

[Add](#) [Remove](#)

## How To Set IP Filtering (Incoming)

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover mouse over Firewall Configuration, click on Incoming IP Filtering link

Step 3. Click on Add button

**Incoming IP Filtering Setup**

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	Ds

**Add** **Remove**

## How To Set IP Filtering (Incoming)

Step 4. Fill in the fields required (Filter Name, Protocol, Source IP Address and its port number information as well as Destination IP Address and its port number information).

Step 4. Click on Apply/Save button.

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:	<input type="text"/>
IP Version:	IPv4
Protocol:	<input type="text"/>
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address[/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**  
Select one or more WAN/LAN interfaces displayed below to apply this rule.

**Select All**

INTERNET/eth0.1  
 Management-ETH/eth0.3  
 br0/br0

**Apply/Save**

## How To Set IP Filtering (Incoming)

Step 5. The rule keyed in will be added in the list

**Incoming IP Filtering Setup**

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLen
Test	eth0.1,eth0.3,br0	4	TCP or UDP	233.233.233.9	8888	192.168.1.2

**Add** **Remove**

# firewall configuration

## Port Forwarding

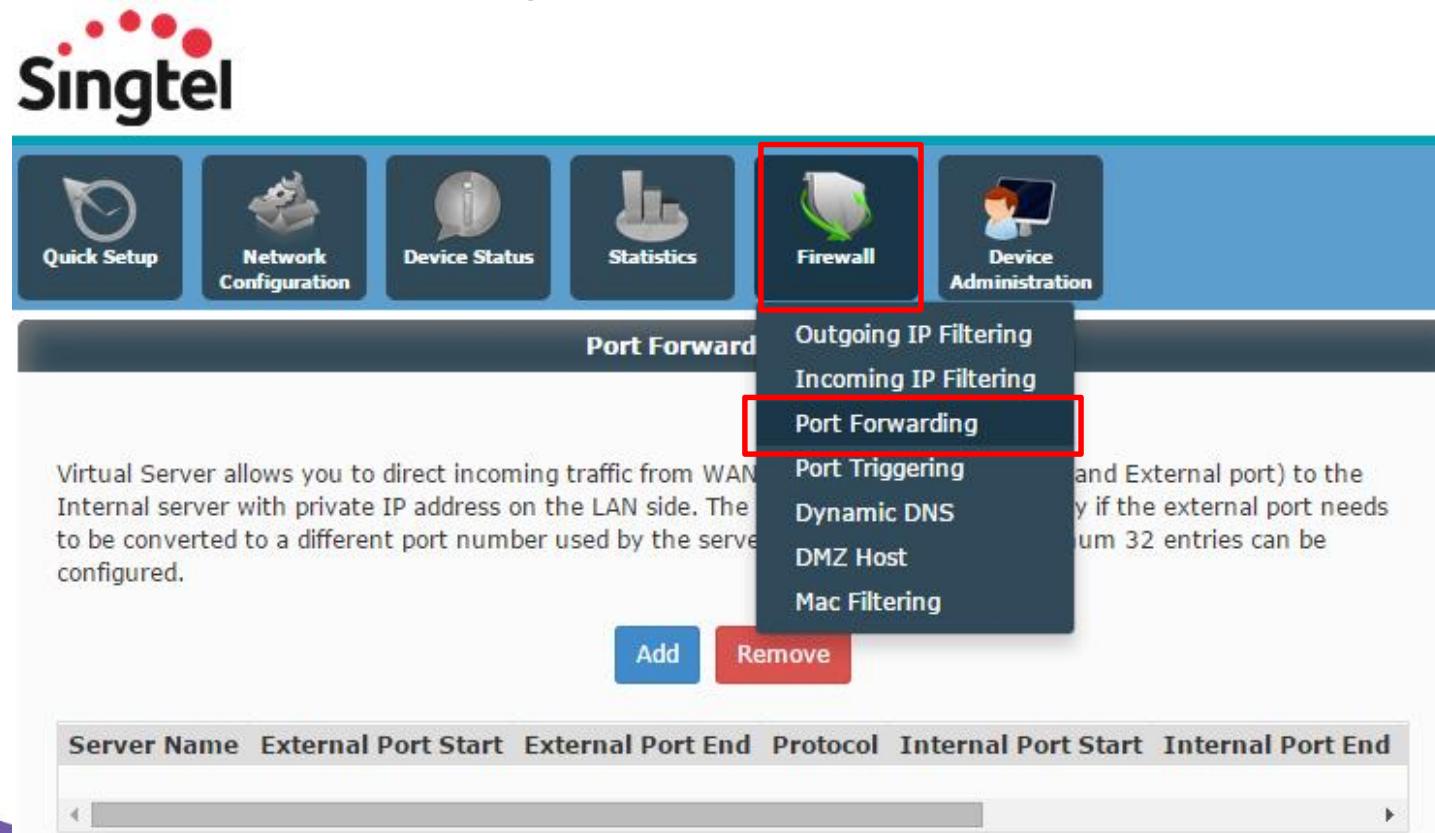
The screenshot shows the 'Port Forwarding Setup' page of the Singtel Residential Gateway. At the top, there is a navigation bar with icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall (which is highlighted in blue), and Device Administration. Below the navigation bar, the title 'Port Forwarding Setup' is displayed. A descriptive text block explains that Virtual Server allows directing incoming traffic from the WAN side to an Internal server with a private IP address on the LAN side. It mentions that the Internal port is required only if the external port needs to be converted to a different port number. A maximum of 32 entries can be configured. At the bottom of the page, there are 'Add' and 'Remove' buttons, and a table header with columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, and Internal Port End. A scroll bar is visible on the right side of the table area.

# How To Set Port Forwarding

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover over on Firewall

Step 3. Click on Port Forwarding Button



## How To Set Port Forwarding

Step 4. Check and confirm the IP Address of the device where the port forwarding rule will be pointed to. Fill in the filed Server IP Address field.

Step 5. Check Custom Server radio button and fill in the application name for easy reference.

Step 6. Fill in the respective port numbers to be forwarded to the server.

Step 7. Click on Apply/Save button.

# How To Set Port Forwarding

**Port Forwarding**

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.

NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured: **32**

Use Interface	INTERNET/eth0.1			
Service Name:	<input type="radio"/> Select a Service: Select One			
<input checked="" type="radio"/> Custom Service:	TestPortForwarding			
Server IP Address:	192.168.1.3			
<b>Apply/Save</b>				
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
88	99	TCP/UDP	88	99

# How To Set Port Forwarding

Step 8. Added rule will be shown

**Port Forwarding Setup**

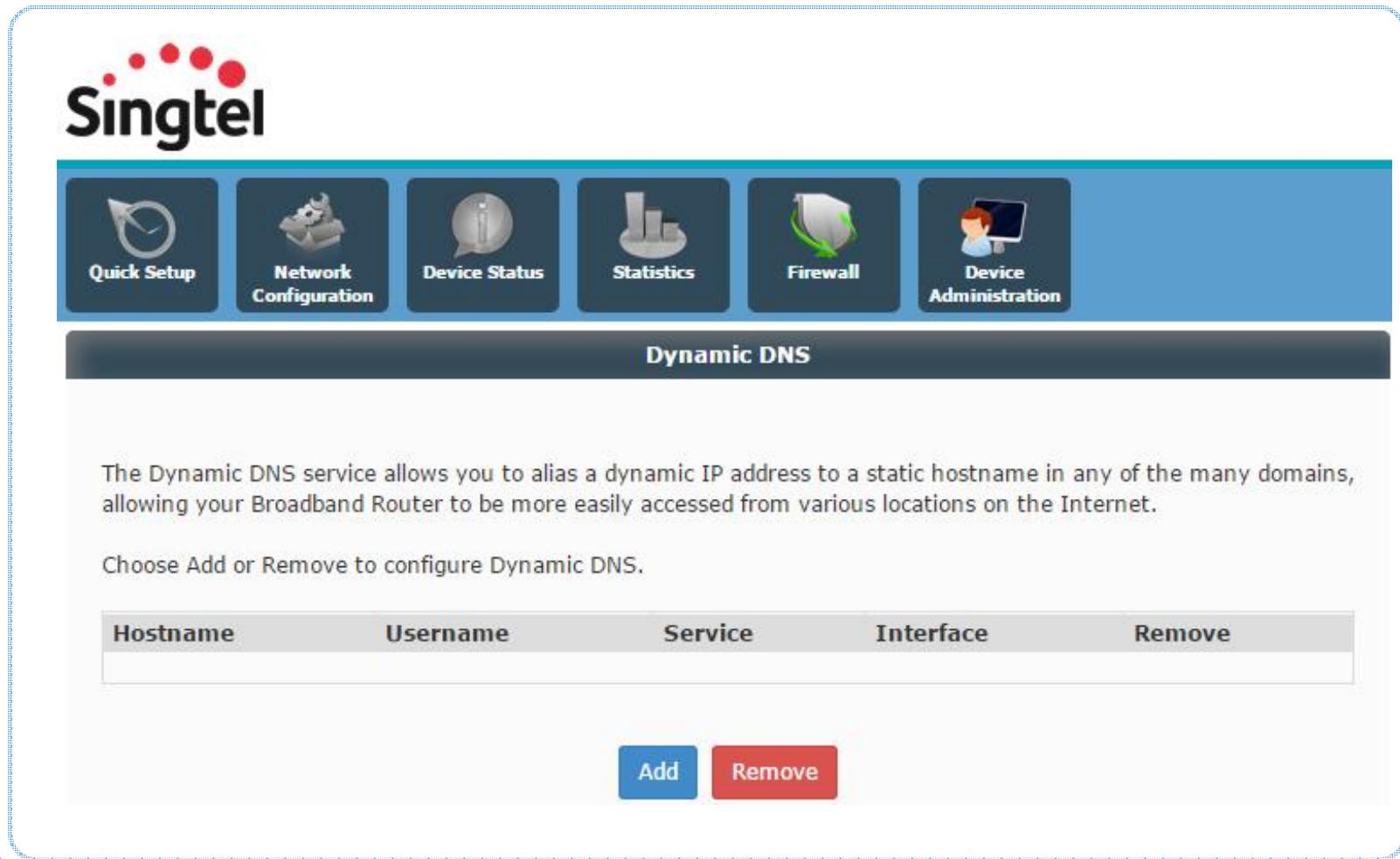
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

**Add** **Remove**

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
TestPortForwarding	88	99	TCP/UDP	88	99

# firewall configuration

## DDNS Settings



The screenshot shows the DDNS Settings page of a Singtel broadband router's web interface. The top navigation bar includes links for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. A prominent 'Dynamic DNS' button is located below the navigation bar. The main content area contains a table for managing Dynamic DNS entries, with columns for Hostname, Username, Service, Interface, and Remove. At the bottom of the table are 'Add' and 'Remove' buttons.

Hostname	Username	Service	Interface	Remove

**Add** **Remove**

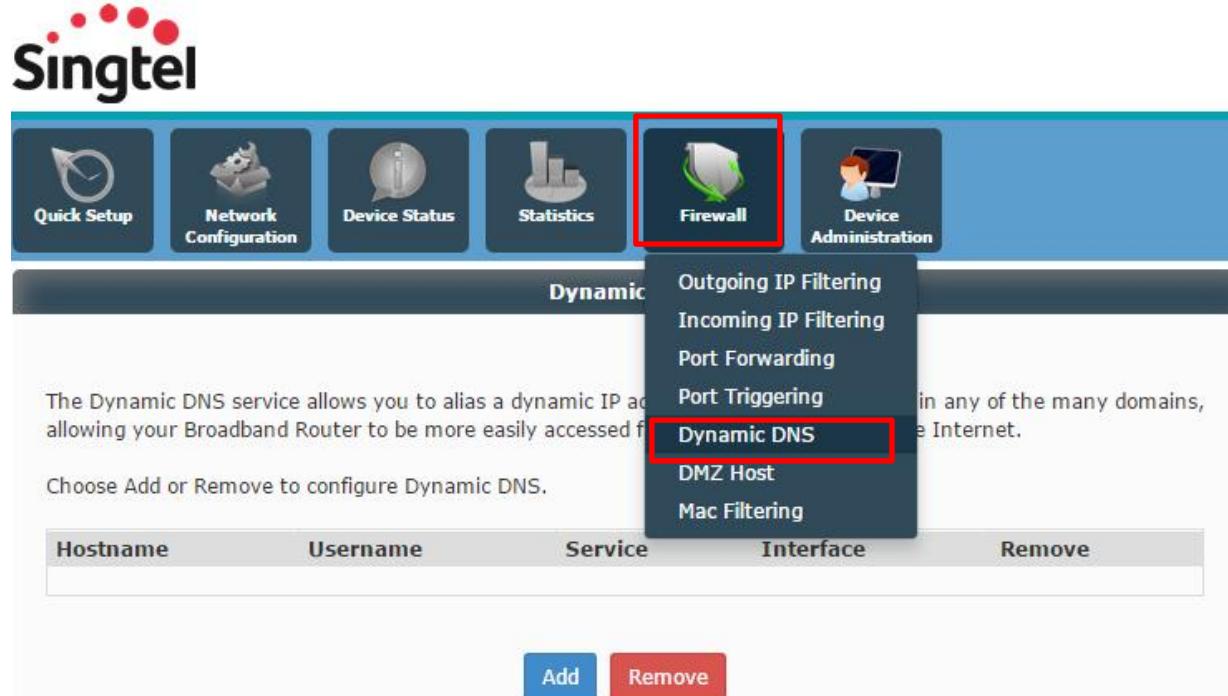
## How to Set DDNS

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover mouse over Firewall Button

Step 3. Click on Dynamic DNS button

Step 4. Click on Add button



## How to Set DDNS

- Step 5. Select the DDNS provider available (DDNS, TZO) from the drop down menu.
- Step 6. Fill in the Hostname field with the registered hostname to the DDNS provider.
- Step 7. Fill in the respective Username and Password fields accordingly.
- Step 8. Click on the Apply/Save button.

**Add Dynamic DNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text" value="MyHostName"/>
Interface	<input type="text" value="INTERNET/eth0.1"/>
<b>DynDNS Settings</b>	
Username	<input type="text" value="my-DDNS-Username"/>
Password	<input type="text" value="*****"/>
<b>Apply/Save</b>	

## How to Set DDNS

Step 9. Added Hostname will be shown

**Dynamic DNS**

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
MyHostName	my-DDNS-Username	dyndns	eth0.1	<input type="checkbox"/>

**Add** **Remove**

# firewall configuration

## MAC Filtering Settings

The screenshot shows the 'MAC Filtering Settings' page of the Singtel Residential Gateway. The top navigation bar includes 'Quick Setup', 'Network Configuration', 'Device Status', 'Statistics', 'Firewall' (selected), and 'Device Administration'. Below the navigation is a section titled 'Access Time Restriction' with a note: 'A maximum 16 entries can be configured.' A table allows for creating rules based on Rule name, MAC, and days of the week (Mon-Fri). Buttons for 'Add' and 'Remove' are at the bottom. To the right, a 'Network Diagram' shows a central router connected to three devices: 'android-b3e899ce67f4103d' (MAC: b4:52:7e:80:ed:26, IP: 192.168.1.1), 'HariantNB' (MAC: cc:af:78:9f:82:37, IP: 192.168.1.2), and 'android-6b03d4ebad340840' (MAC: 48:5a:3f:5e:06:4d, IP: 192.168.1.3). A status bar at the top right indicates 'Internet' is active (green bar) and 'IPTV' is inactive (grey bar).

Rule name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

**Add** **Remove**

Network Diagram:

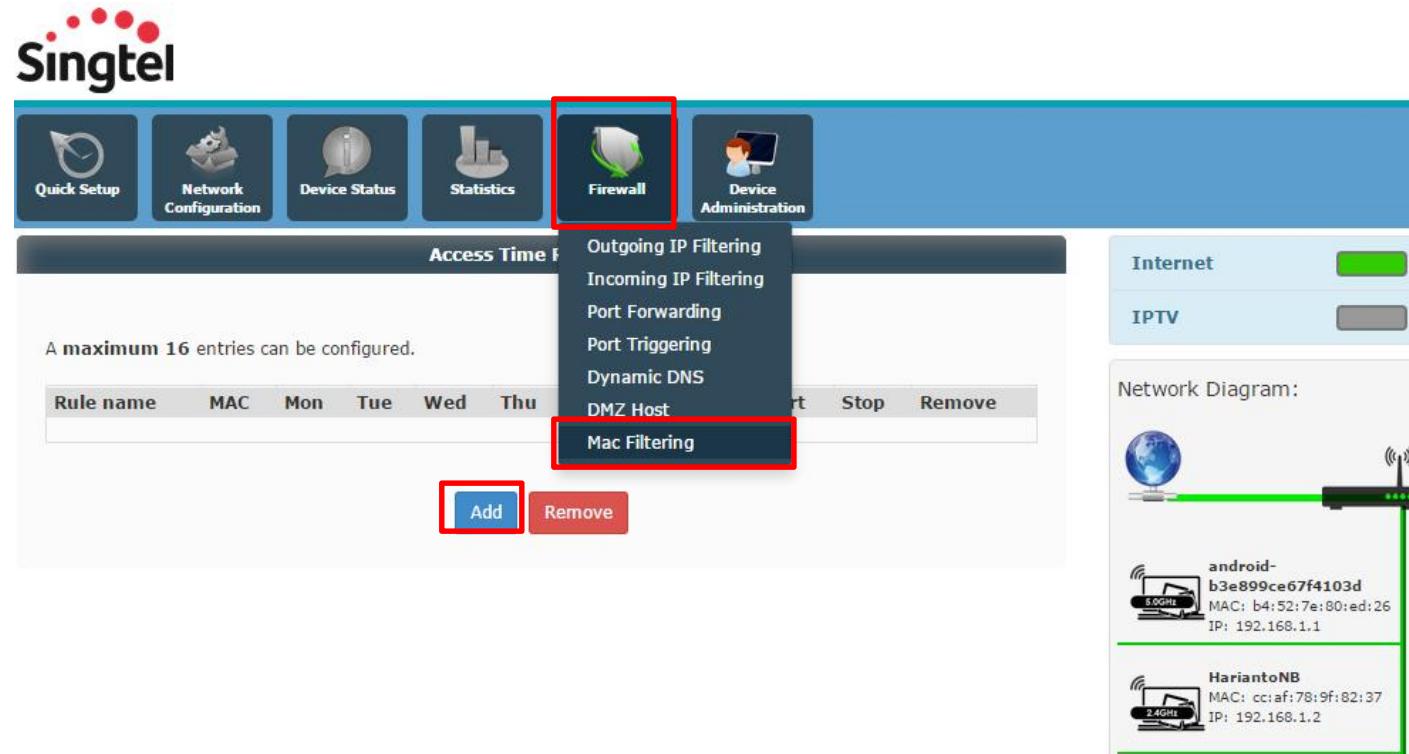
- android-b3e899ce67f4103d  
MAC: b4:52:7e:80:ed:26  
IP: 192.168.1.1
- HariantNB  
MAC: cc:af:78:9f:82:37  
IP: 192.168.1.2
- android-6b03d4ebad340840  
MAC: 48:5a:3f:5e:06:4d  
IP: 192.168.1.3

## How to Set Mac Filtering

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover over Firewall button

Step 3. Click on Mac Filtering , followed by Add button



## How to Set Mac Filtering

Step 4. Provide a Rule Name of which will let you identify whom you will be blocking.

Step 5. Tick on Other MAC Address radio button,

- A. If the device is already connected to the RG, you can copy and paste the MAC Address from the right hand side (at the Network Diagram)
- B. If the device is not yet connected to the RG, fill in the MAC Address value to be filtered in aa:bb:cc:dd:ee:ff format

Step 6. Check the day and fill in the 24-hr time format.

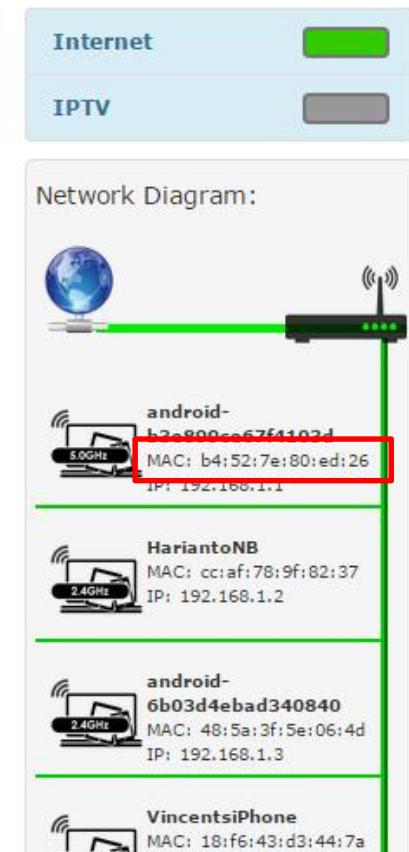
Step 7. Click on the Apply button.

# How to Set Mac Filtering

**Access Time Restriction**

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

Rule Name	<input type="text" value="Test"/>														
<input checked="" type="radio"/> Browser's MAC Address	<input type="text" value="cc:af:78:9f:82:37"/>														
<input type="radio"/> Other MAC Address (xx:xx:xx:xx:xx:xx)	<input type="text" value="b4:52:7e:80:ed:26"/>														
Days of the week Click to select	<table border="1"> <tr> <th>Mon</th> <th>Tue</th> <th>Wed</th> <th>Thu</th> <th>Fri</th> <th>Sat</th> <th>Sun</th> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table>	Mon	Tue	Wed	Thu	Fri	Sat	Sun	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mon	Tue	Wed	Thu	Fri	Sat	Sun									
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>									
Start Blocking Time (hh:mm)	<input type="text" value="00:00"/>														
End Blocking Time (hh:mm)	<input type="text" value="23:59"/>														
<input type="button" value="Apply/Save"/>															



# How to Set MAC Filtering

Step 8. Added filtered MAC Address will be shown

**Access Time Restriction**

A maximum 16 entries can be configured.

Rule name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Test	b4:52:7e:80:ed:26					x			0:0	23:59	<input type="checkbox"/>

**Add** **Remove**



# firewall configuration

## Port Triggering Settings

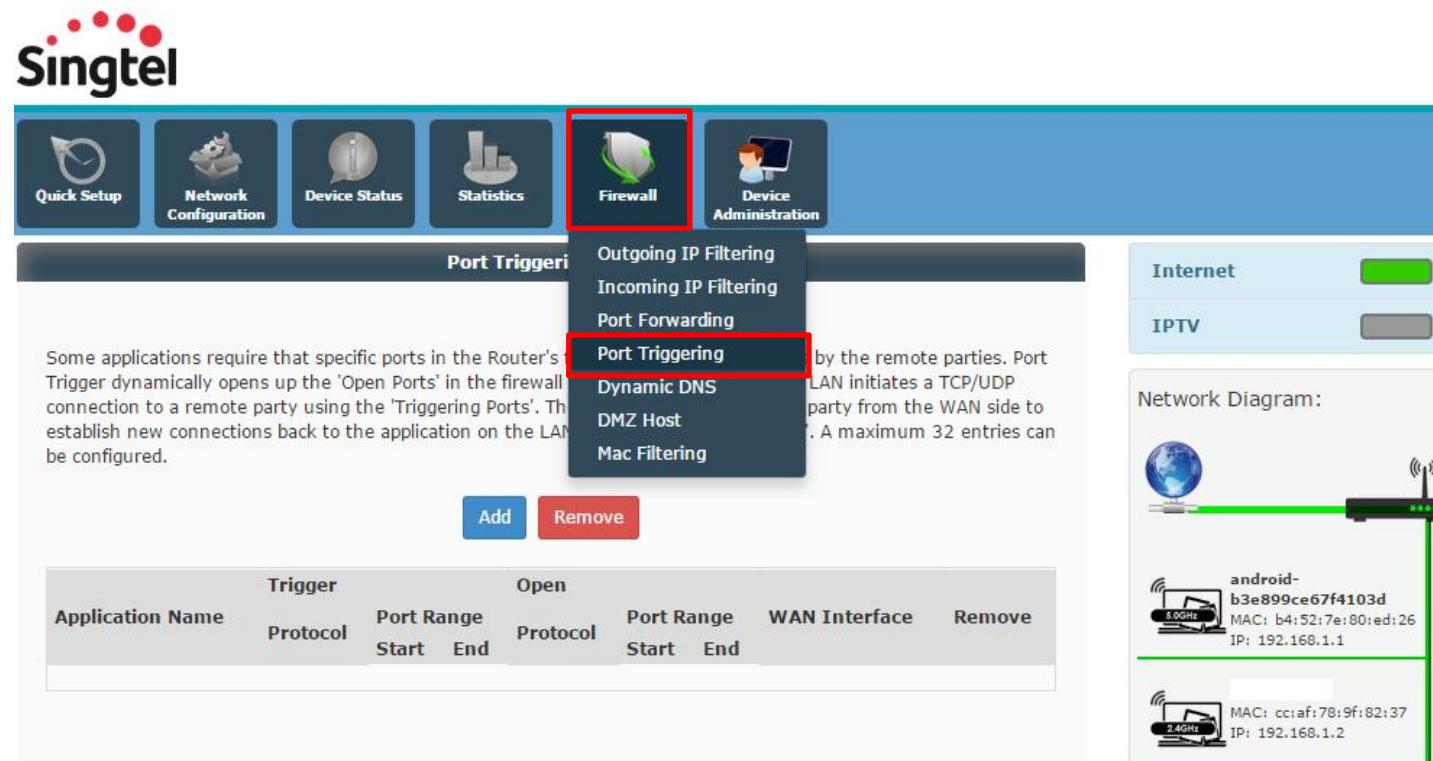
The screenshot shows the 'Port Triggering Setup' page of the Singtel router's web interface. The top navigation bar includes 'Quick Setup', 'Network Configuration', 'Device Status', 'Statistics', 'Firewall' (which is selected), and 'Device Administration'. The main content area is titled 'Port Triggering Setup' and contains a descriptive text about port triggering. Below the text is a table with two buttons: 'Add' (blue) and 'Remove' (red). The table columns are: Application Name, Trigger Protocol, Port Range Start, Port Range End, Open Protocol, Port Range Start, Port Range End, WAN Interface, and Remove. The table is currently empty. To the right of the table is a 'Network Diagram' showing a connection from the 'Internet' (green bar) through a router to two devices: 'android-b3e899ce67f4103d' (MAC: b4:52:7e:80:ed:26, IP: 192.168.1.1) and '2.4GHz' (MAC: cc:af:78:9f:82:37, IP: 192.168.1.2). Status indicators for 'Internet' (green) and 'IPTV' (grey) are also present.

# How To Set Port Triggering

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover over Firewall Button

Step 3. Click on Port Triggering, followed by Add button



# How To Set Port Triggering

Step 4. Check Custom Application radio button and fill in the application name for easy reference.

Step 5. Fill in the respective port numbers and protocol type and click Save/Apply button.

**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: **32**

Use Interface	INTERNET/eth0.1				
Application Name:	<input type="radio"/> Select an application: Select One				
<input checked="" type="radio"/> Custom application:	MyRule				
<b>Save/Apply</b>					
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
8881	8882	TCP	8883	8884	TCP
		TCP			TCP

# How To Set Port Triggering

Step 7. Created rule will be shown in the list

**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				
MyRule	TCP	8881	8882	TCP	8883	8884	eth0.1	<input type="checkbox"/>

# firewall configuration

## DMZ

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.

DMZ Host IP Address:

Save/Apply

Internet

IPTV

Network Diagram:

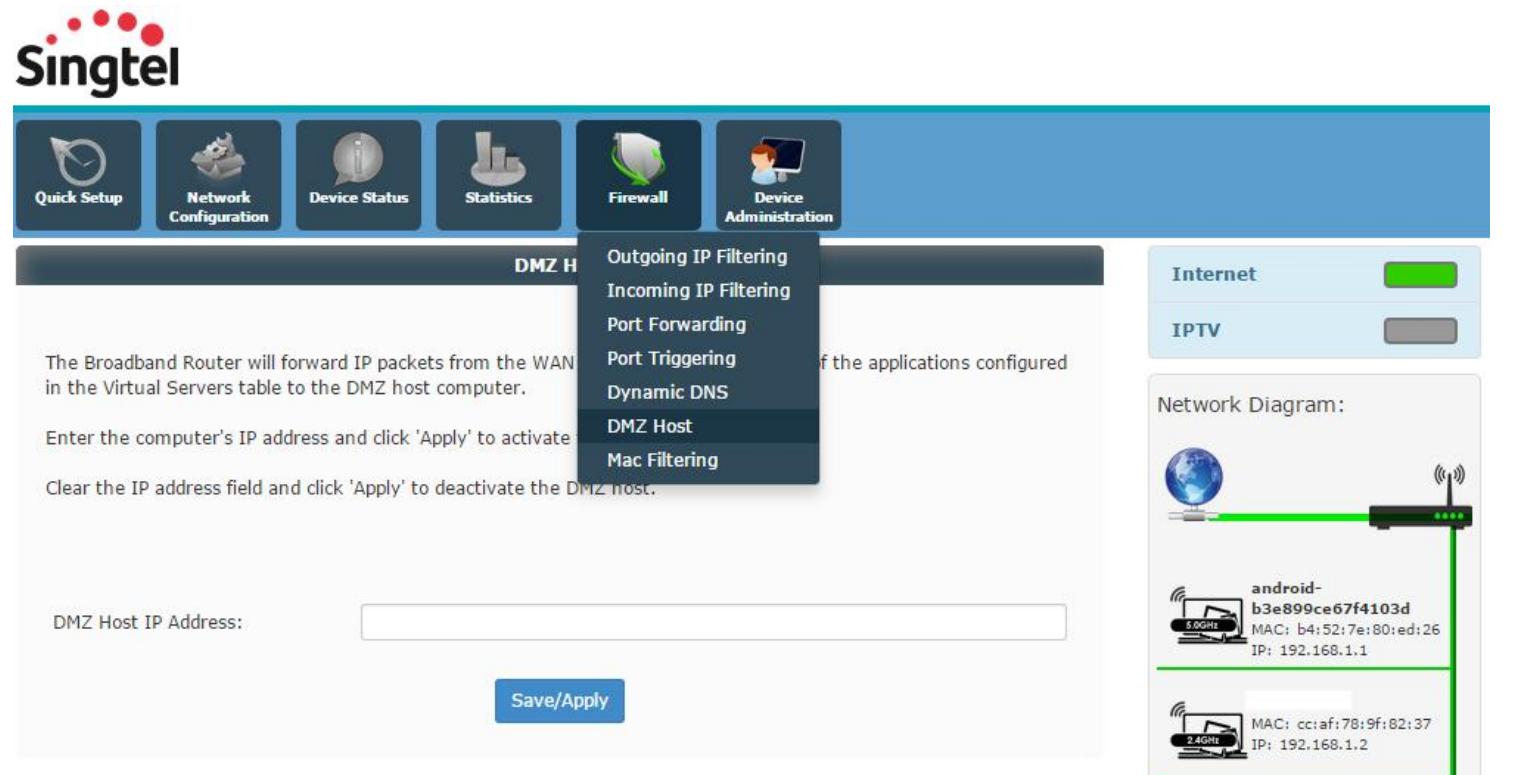
- android-  
b3e899ce67f4103d  
MAC: b4:52:7e:80:ed:26  
IP: 192.168.1.1
- MAC: cc:af:78:9f:82:37  
IP: 192.168.1.2

# How To Set DMZ

Step 1. Launch an internet browser and go to <http://192.168.1.254>

Step 2. Hover over Firewall

Step 3. Click on DMZ Host button



# How To Set DMZ

Step 4. Copy the IP Address value from list of clients connected, at Network Diagram.

Step 5. Paste on the DMZ Host IP Address field.

Step 6. Click on Save/Apply button



# troubleshooting

## LED Troubleshooting

### Power

- ¤ Steady Red – reset button is pressed
- ¤ Steady Red – unit is booting up or unit failed to boot
- ¤ Green – firmware is loaded to the RAM / unit has successfully booted up
- ¤ Off – no power or PSU faulty

### Ethernet LAN 1-4

- ¤ Blinking Green – indicates activity on the port
- ¤ Steady Green – Ethernet device is connected to the port
- ¤ Off – there is no Ethernet device plugged in to the port or the cable is faulty

# troubleshooting

## LED Troubleshooting

### Wireless - 5GHz

- ¤ Steady Green – wireless device(s) associated to the wireless AP
- ¤ Blinking Green – indicates wireless activity
- ¤ Off – no wireless device associated with the AP or AP is not activated

### Wireless - 2.4GHz

- ¤ Steady Green – wireless device(s) associated to the wireless AP
- ¤ Blinking Green – indicates wireless activity
- ¤ Off – no wireless device associated with the AP or AP is not activated

# troubleshooting

## LED Troubleshooting

### USB

- ¤ Steady Green – USB device is connected to the port
- ¤ Off – no device is connected

### IPTV

- ¤ Steady Green – IPTV service is working, STB is plugged in and streaming
- ¤ Steady Red – STB is not connected to the RG or  
STB in on DRA mode (if STB is connected to the RG) or  
STB is rebooting (if STB is connected to the RG) or  
IPTV service failed (if STB is connected to the RG) or  
no multicast streams coming (if STB is connected to the RG)
- ¤ Off – no service or service is down

# troubleshooting

## LED Troubleshooting

### Broadband on FTTH

- ¤ Steady Green – WAN ethernet port is connected to the ONT or an active ethernet device
- ¤ Off – No active connection to the WAN ethernet port

### Internet on FTTH

- ¤ Steady Green – connection is up and the interface is with an IP address
- ¤ Red – DNS resolution failed
- ¤ Off - no internet connection

# troubleshooting

## LED Troubleshooting

### WPS

- ¤ Steady Green – WPS is activated and a client is authenticated
- ¤ Blinking Green – WPS is ready to connect
- ¤ Off - WPS not activated

### LED ON/OFF

- ¤ Steady Green – function is active
- ¤ Off – function is not active

#### Notes:

- When this function is active, all other LEDs from POWER to INTERNET will be turned OFF.
- The LED for this function is intended to be slightly dimmer as compared to others.

# troubleshooting

## Wireless Troubleshooting

1. Always start with checking the wireless credentials, SSID and wireless security, if the wireless clients cannot connect to the AP
2. Place the RG vertically, on a flat surface, properly ventilated place, and away from:
  - ¤ Blockage such as artificial barriers
  - ¤ Electronic devices such as blue-tooth devices, microwave ovens and cordless telephones
  - ¤ Water containing equipment filled with water
3. Think of the possibility of wireless channel congestion
  - ¤ Please ensure wireless channel setting is set as "Auto" at all times. Should channel congestion is suspected, it is recommended to reboot the RG.
  - ¤ If the wireless channel is so congested, the wireless client may get an IP address but might not be able to, from time to time, surf the internet or use the wireless network resource

# troubleshooting

## Where to Check Firmware Version

Step 1. Launch an Internet Browser

Step 2. Fill in the Address bar <http://192.168.1.254> and enter

Step 3. Click on Device Info link, Firmware version information is located in the table



The screenshot shows a web-based interface for a Singtel device. At the top, there is a navigation bar with icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. Below the navigation bar, a dark bar displays the text "Quick Setup". The main content area contains a table titled "Device Info". The table includes the following data:

- Device Info -	
Model	FG7009GR(AC)
Board ID	963138REF_P402
Base MAC Address	00:26:75:E3:AF:47
Serial No	1598143500001
<b>Firmware Version</b>	339.6.2-001
Software Version	V4.16L.02A
Bootloader (CFE) Version	1.0.38-116.174

The "Firmware Version" row is highlighted with a red border.

admin gui

## Accessing the Admin GUI

<http://192.168.1.254/singtel>

Username: admin

Password: H3ll0t3ch

The screenshot shows the Admin GUI interface for the Singtel FG7009GR(AC) Residential Gateway. The top navigation bar includes links for Device Info, Statistics, Advanced Setup, Security, Parental Control, Wireless, Diagnostics, and Management. The main content area is titled 'Device Info Summary' and displays the following information:

Board ID:	963138REF_P402
Symmetric CPU Threads:	2
Build Timestamp:	150514_2043
Firmware Version:	339.6.2-001
Software Version:	V4.16L.02A
Bootloader (CFE) Version:	1.0.38-116.174
Wireless Driver Version:	7.14.89.14
Uptime:	16570D 7H 21M 10S

Below this, a note states: "This information reflects the current status of your WAN connection." A second table provides WAN connection details:

LAN IPv4 Address:	192.168.1.254
Default Gateway:	eth0.1
Primary DNS Server:	165.21.100.88
Secondary DNS Server:	165.21.83.88
Date/Time:	Fri May 15 15:21:10 2015

## Frequently Asked Questions

### CAN I USE BOTH 2.4GHz AND 5GHz BAND AT THE SAME TIME?

Both bands are enable by default. Please note that the same client can only connect to either one of the band available at any point of time.

### WHAT IS THE MAXIMUM NUMBER OF CLIENT IT CAN SUPPORT FOR WIRELESS?

30 for 2.4GHz band and 30 for 5GHz band.

### CAN I CONFIGURE MAC FILTERING ON FG7009GR(AC)?

Yes

## Frequently Asked Questions

HOW CAN I TELL IF MY WIRELESS CLIENT (i.e. the mobile / wireless device) SUPPORTS 5GHZ BAND?

- By doing wireless SSID scanning, if the client supports 5GHz band, you will be able to see the default 5GHz SSID, with prefix of SINGTEL(5G)-xxxx.

Please note that if the wireless client/adapter is able to see the 5GHz SSID, it does not necessarily mean that it is a Wireless AC client. There is a need to check against the hardware specifications if it really is a wireless AC client.

IS THIS FG7009GR(AC) VLAN TAG OR non VLAN TAG?

- The firmware loaded on FG7009GR(AC) is VLAN tagged

## Frequently Asked Questions

### WHAT IS LED ON/OFF FEATURE?

- LED On/Off feature allows end-users who prefers not to see a lot of lit-up LEDs able to turn OFF.

Please note:

- a. when this feature is active, its indicator will lit up and the rest of the LEDs will be OFF.
- b. for troubleshooting purpose, do pay attention if this feature is not active / active.

### WHAT IS THE EXPECTED AVERAGE WIRED AND WIRELESS AC PERFORMANCE?

- Over a 1Gbps plan, tested wired speed is average at 900Mbps;
- For wireless AC on the same 1Gbps plan, tested speed is average at 400Mbps.
- Do Note that result is subject to test environment and test equipment.

# Frequently Asked Questions

## RG COMPARISON

Main Features	Feature	Aztech DSL7002GRV(S) (Current)	Aztech FG7003GRV(AC) (Current)	Aztech FG7009GR(AC) (New)
Services Supported	ADSL	Yes	Not Available	Not Available
	FTTH	Yes	Yes	Yes
	Home Digital Line	Yes	Yes	Not Available
	Singtel TV	Yes	Yes	Yes
Operating Frequency	2.4 GHz	Yes	Yes	Yes
	5.0 GHz	Yes	Yes	Yes
Wireless Connection Mode		Wireless a/b/g/n	Wireless a/b/g/n/ac	Wireless a/b/g/n/ac
Wireless 5GHz Antenna (internal)		3	3	4
MAC Filtering		Not Supported	Yes <sup>1</sup>	Yes
WPS Push Button (2.4GHz only)		Yes <sup>1</sup>	Yes (enabled by default)	Yes (enabled by default for both 2.4GHz and 5GHz bands)
Gigabit Ethernet LAN		4	4	4
Voice Ports (FXS)		2	2	Not Available
USB Host Support		2 Disabled by default	2 Disabled by default	2 Disabled by default
DDNS		Not Supported	Yes <sup>1</sup>	Yes

Notes:

1. Firmware dependant

# Frequently Asked Questions

Graphical User Interface Look & Feel for previous RG:

First landing page from <http://192.168.1.254>

The screenshot shows the landing page of the Aztech FG7009GR(AC) Residential Gateway's web interface. The top navigation bar includes the SingTel logo, the Aztech logo with the tagline "Innovate to connect", and several menu icons: Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. Below the menu is a sub-navigation bar with "QuickSetup" and "Wireless" tabs, where "QuickSetup" is currently selected. A descriptive text block states: "This page allows you to check the device information, control the device connection." It lists two options: "Device Info" and "Internet Login Account Settings". A "Device Info" table is displayed, showing the following details:

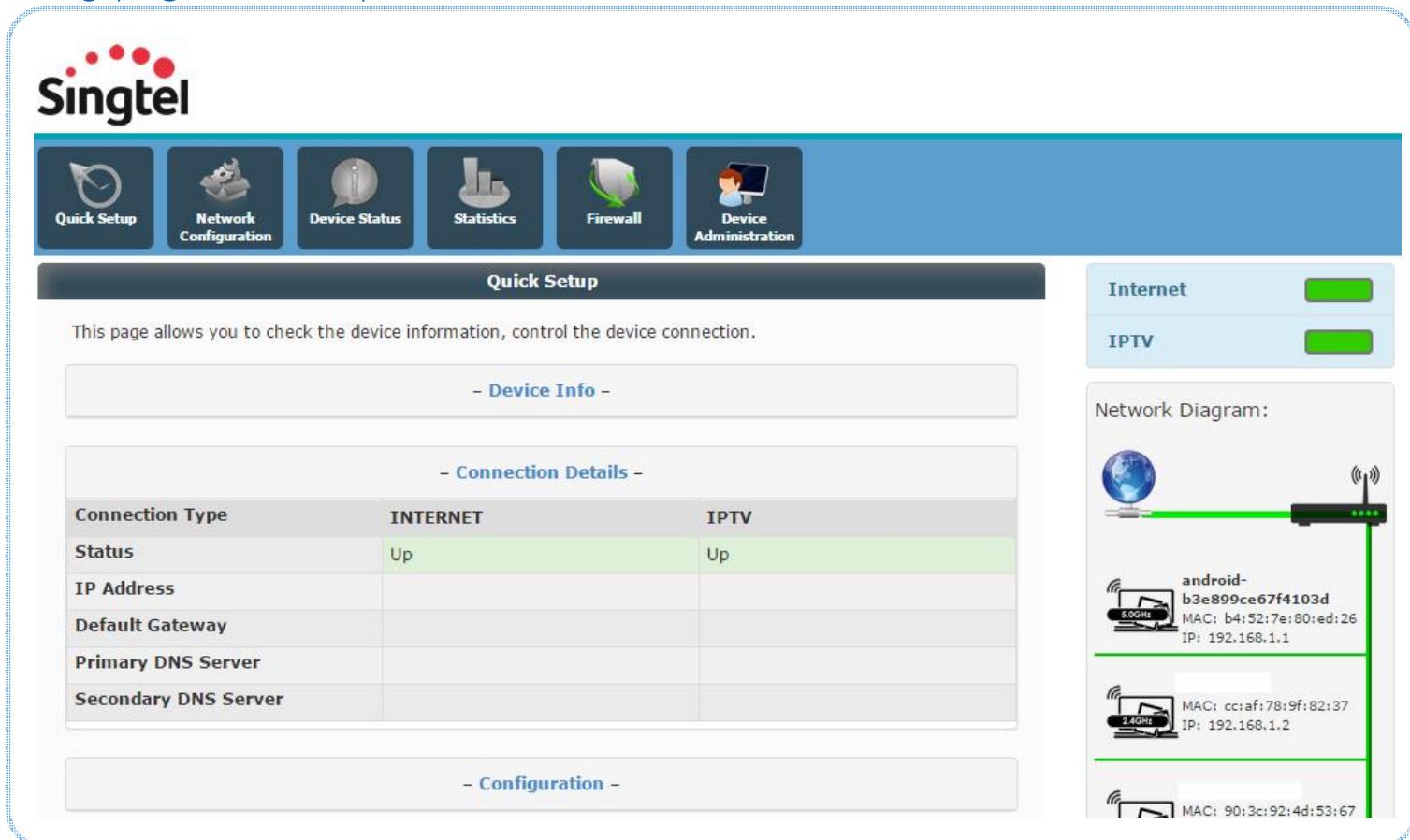
Model:	FG7003GRV(AC)
Board ID:	96362ADVN2xh
Base MAC Address:	00:26:75:C4:6E:AE
Serial No:	1596140801063
Firmware Version:	309.6.1
Software Version:	V4.12L.08
Bootloader (CFE) Version:	1.0.38-114.185

Below the table, there are sections for "Internet Connection", "Voice Connection", and "IPTV Connection".

# Frequently Asked Questions

Graphical User Interface Look & Feel for FG7009GR(AC):

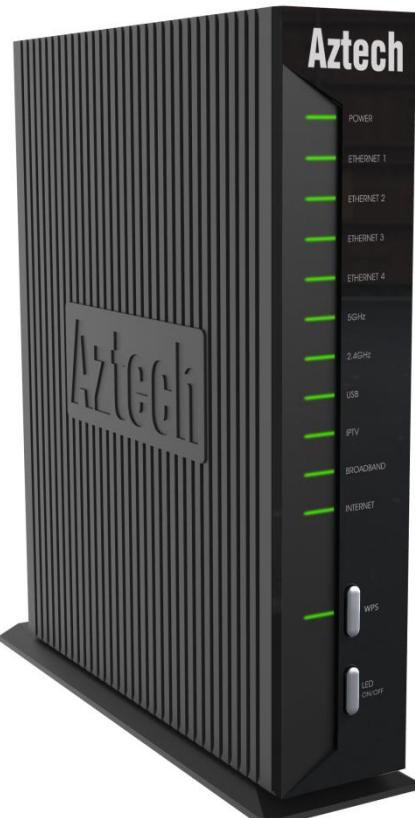
First landing page from <http://192.168.1.254>



# Frequently Asked Questions

How to Identify retail Aztech FG7008GR(AC) and Singtel FG7009GR(AC)

**Aztech FG7008GR(AC)**



**Singtel FG7009GR(AC)**



**Singtel FG7009GR(AC)**



# support contact info

Service Center Address:

31 Ubi Road 1 Aztech Building  
#01-05  
Singapore 408694

Hotline:

6594 2297

Email:

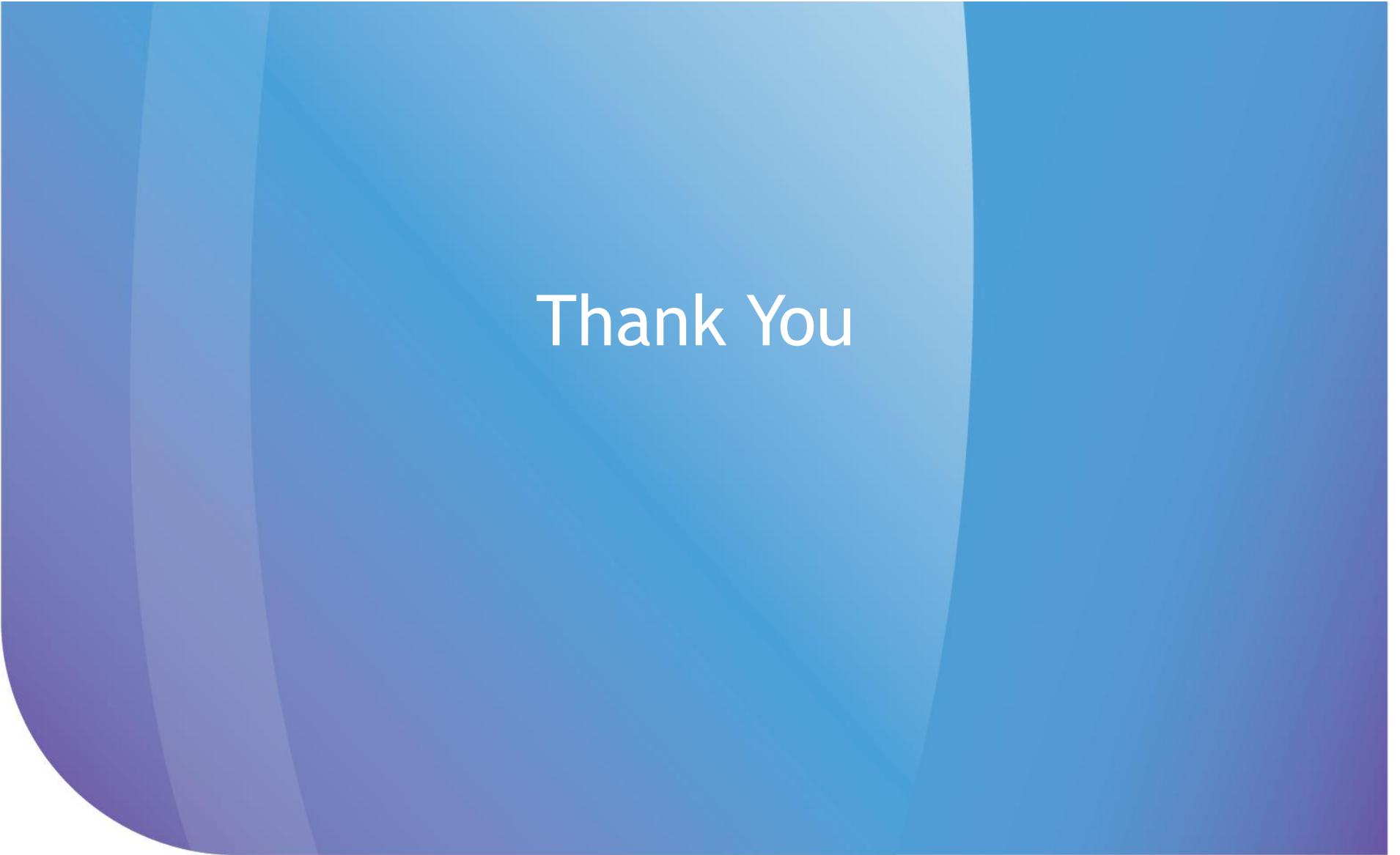
[support@aztech.com](mailto:support@aztech.com)

Operating Hours

Monday to Friday: 9:00 AM to 6:15 PM

Saturday: 9:00 AM to 1:00 PM

(Except Public Holidays)



A large, semi-transparent graphic in the background features a vertical gradient from dark blue on the left to light blue on the right. A curved, semi-transparent purple shape is positioned on the left side of the slide, starting from the bottom left and curving upwards and outwards towards the top left.

Thank You

**Aztech**