

AZTECH FG7009GR(AC)

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

SINGAPORE | May 2015

Aztech



C O N T E N T S

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

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

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

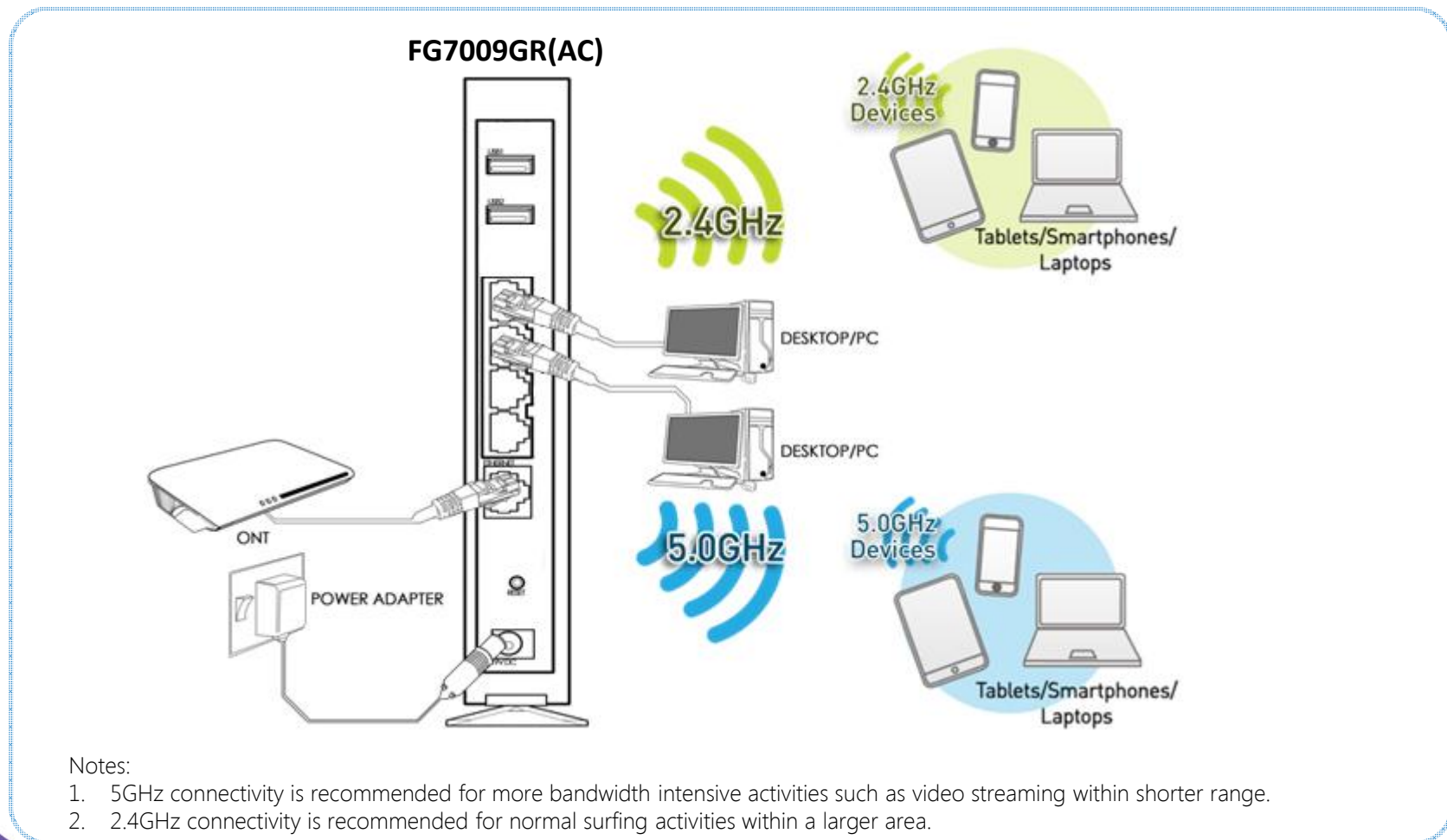
Back Panel Ports and Button

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



Recommended setup

Recommended Hardware Setup (FTTH)



connecting to Singtel Broadband

FTTH

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

The screenshot displays the Singtel Residential Gateway web interface. The top navigation bar includes links for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The main content area is titled 'Quick Setup' and contains a section for 'Connection Details'. This section includes a table with connection information for both Internet and IPTV services. To the right of the table, there is a 'Network Diagram' showing the gateway connected to various devices.

Connection Type	INTERNET	IPTV
Status	Up	Down
IP Address	220.255.251.179	-
Default Gateway	220.255.251.254	-
Primary DNS Server	165.21.100.88	-
Secondary DNS Server	165.21.83.88	-

Network Diagram:

- Internet (Green bar)
- LAN 1: MAC: cc:af:7b:9f:82:37, IP: 192.168.1.1
- android-b3e899ce67f4103d: MAC: b4:52:7e:80:ed:26, IP: 192.168.1.2
- lees-iphone: MAC: 80:be:05:2c:9e:60, IP: 192.168.1.3

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.

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

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

Save/Apply

Changing the Wireless Settings

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

Wireless Setup

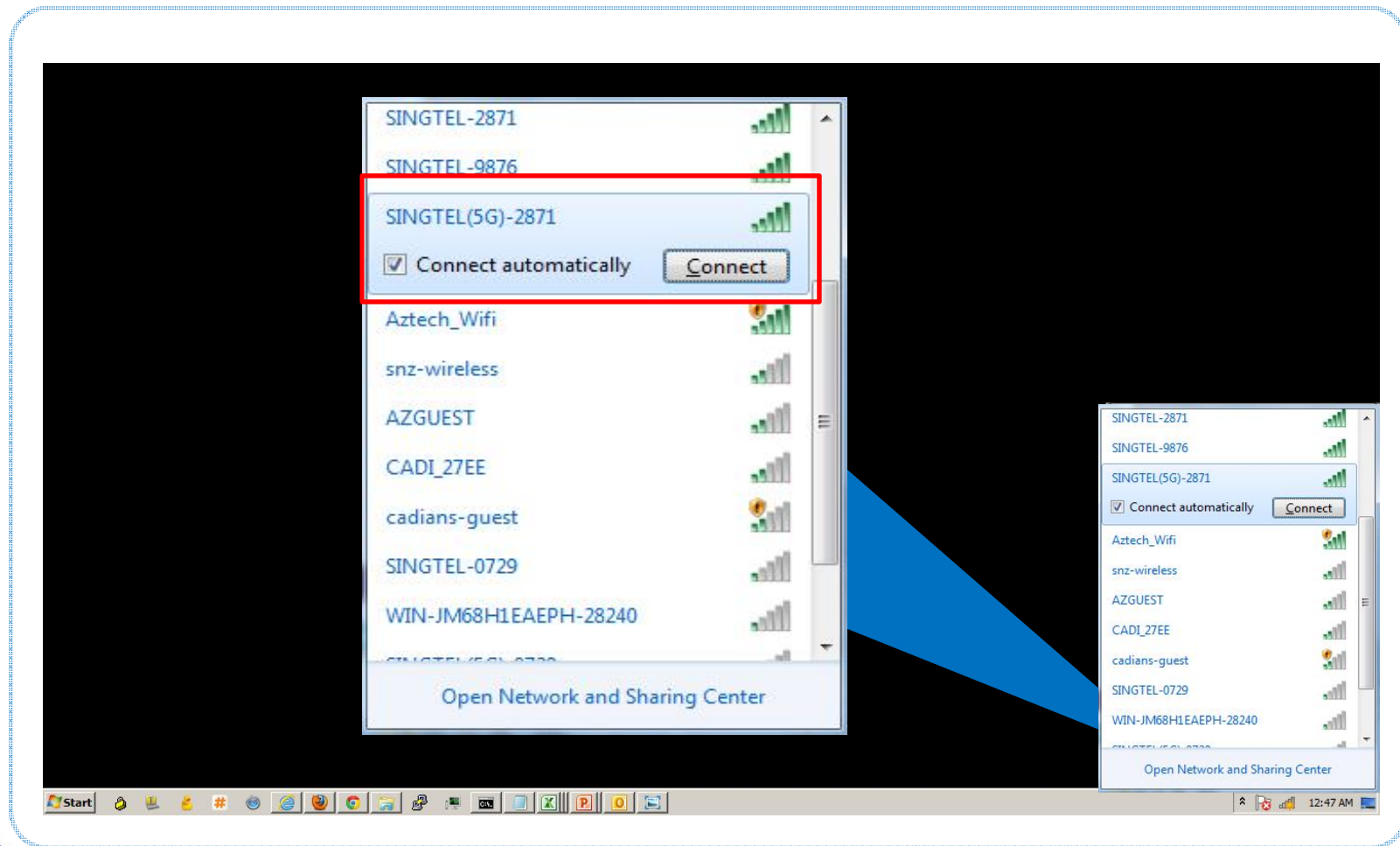
This page allows you to configure basic features for both the 2.4GHz and 5.0GHz wireless LAN interface.

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

Save/Apply

wireless connection

Connecting to 2.4GHz and 5GHz Band



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.

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 displays the Singtel web interface for the Aztech FG7009GR(AC) Residential Gateway. The top navigation bar includes icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The Firewall menu is expanded, showing options: Outgoing IP Filtering, Incoming IP Filtering, Port Forwarding, Port Triggering, Dynamic DNS, DMZ Host, and Mac Filtering.

Below the navigation bar, the 'Quick Setup' section is visible, with a description: 'This page allows you to check the device information, control...' and sections for '- Device Information -' and '- Connection Information -'.

The 'Connection Information' section contains a table with the following data:

Connection Type	INTERNET	IPTV
Status	Up	Down
IP Address	220.255.251.179	-
Default Gateway	220.255.251.254	-
Primary DNS Server	165.21.100.88	-
Secondary DNS Server	165.21.83.88	-

Below the table is a section for '- Configuration -'.

On the right side of the interface, there are status indicators for 'Internet' (green bar) and 'IPTV' (grey bar). Below these is a 'Network Diagram' showing a router connected to three devices: a laptop (MAC: cc:af:78:9f:82:37, IP: 192.168.1.1), an Android phone (MAC: b4:52:7e:80:ed:26, IP: 192.168.1.2), and an iPhone (MAC: 80:be:05:2c:9e:60, IP: 192.168.1.3).

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

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	Remove
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	<input type="checkbox"/>
Filter-Test-Out	4	TCP or UDP	192.168.1.99	8082	10.233.233.0	8082	<input type="checkbox"/>

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:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

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



Quick Setup Network Configuration Device Status Statistics Firewall Device Administration

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](#)

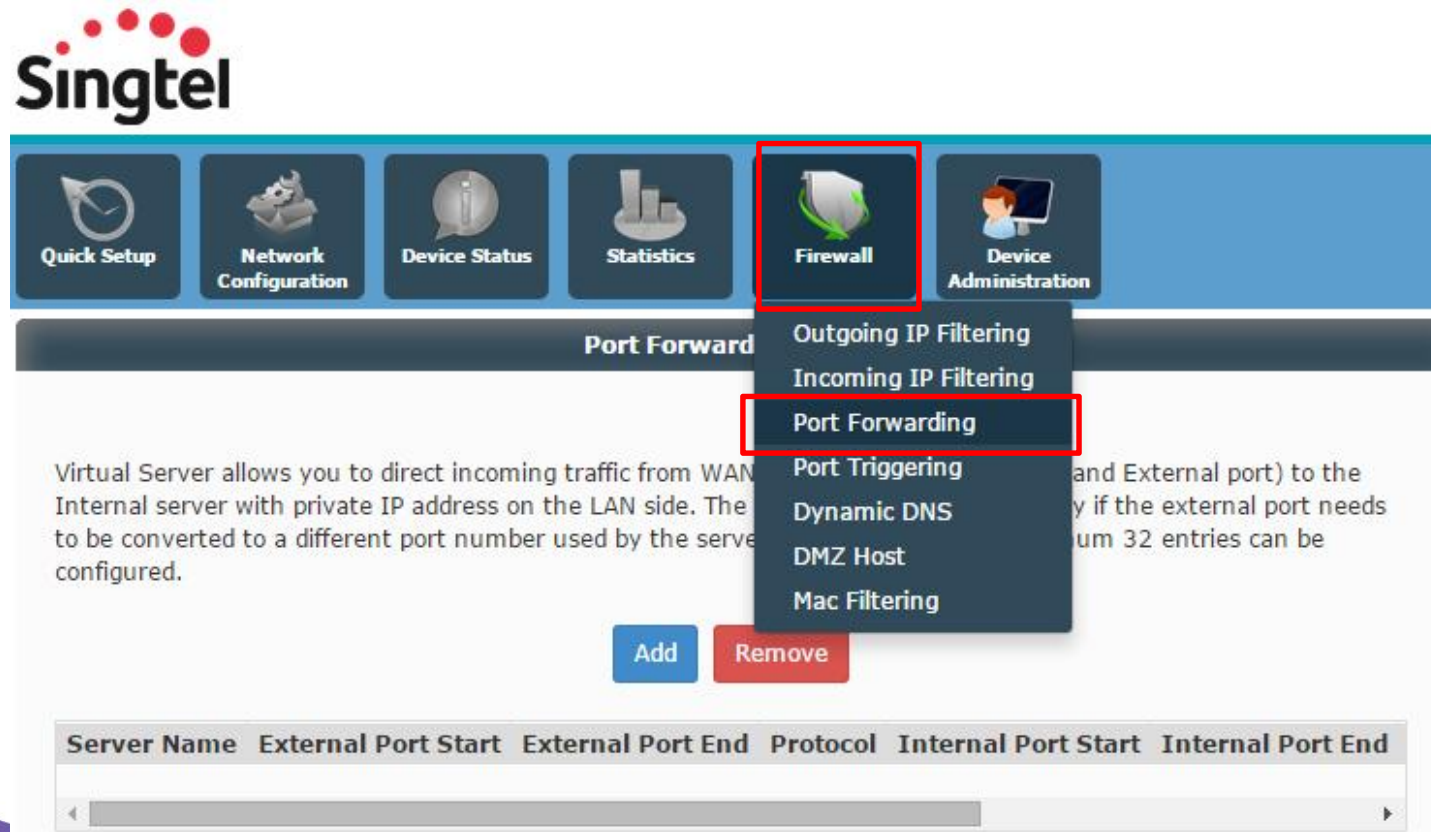
Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<div></div>					

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:

Service Name:

☐ Select a Service:

☒ Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="88"/>	<input type="text" value="99"/>	<input type="text" value="TCP/UDP"/>	<input type="text" value="88"/>	<input type="text" value="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





 Quick Setup

 Network Configuration

 Device Status

 Statistics

 Firewall

 Device Administration

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
----------	----------	---------	-----------	--------

Add

Remove

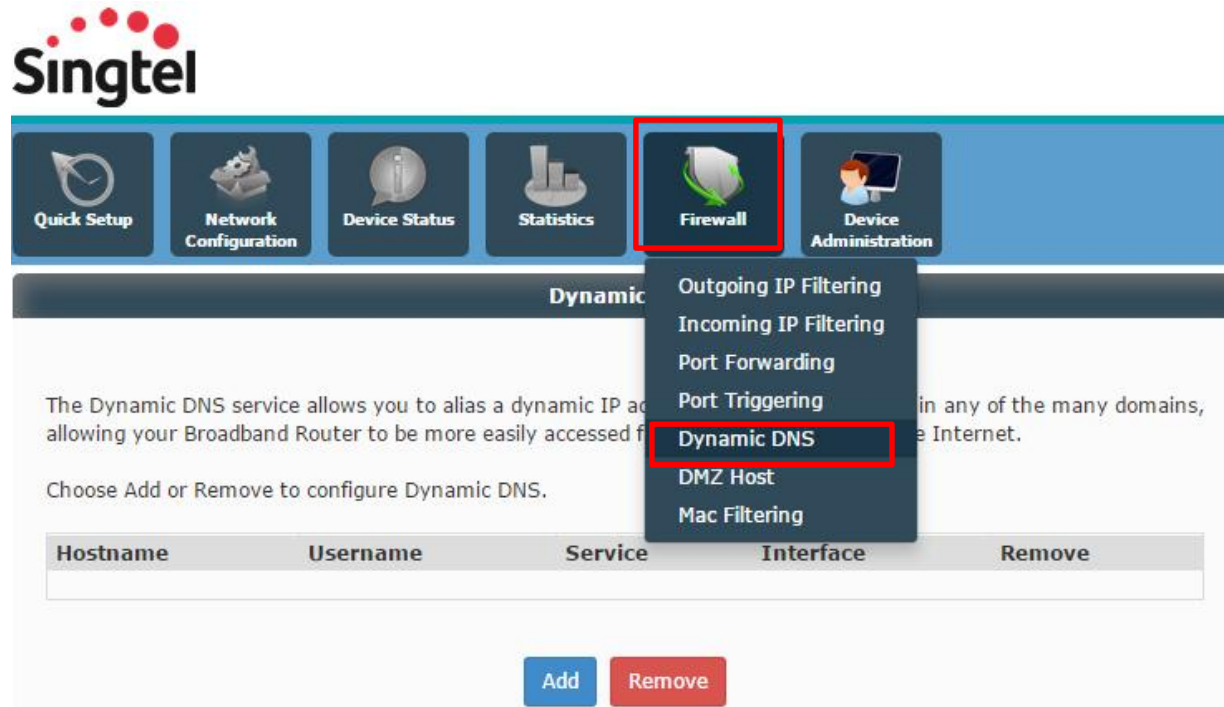
How to Set DDNS

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: DynDNS.org

Hostname: MyHostName

Interface: INTERNET/eth0.1

DynDNS Settings

Username: my-DDNS-Username

Password:

Apply/Save

How to Set DDNS

Step 9. Added Hostname will be shown

Dynamic DNS

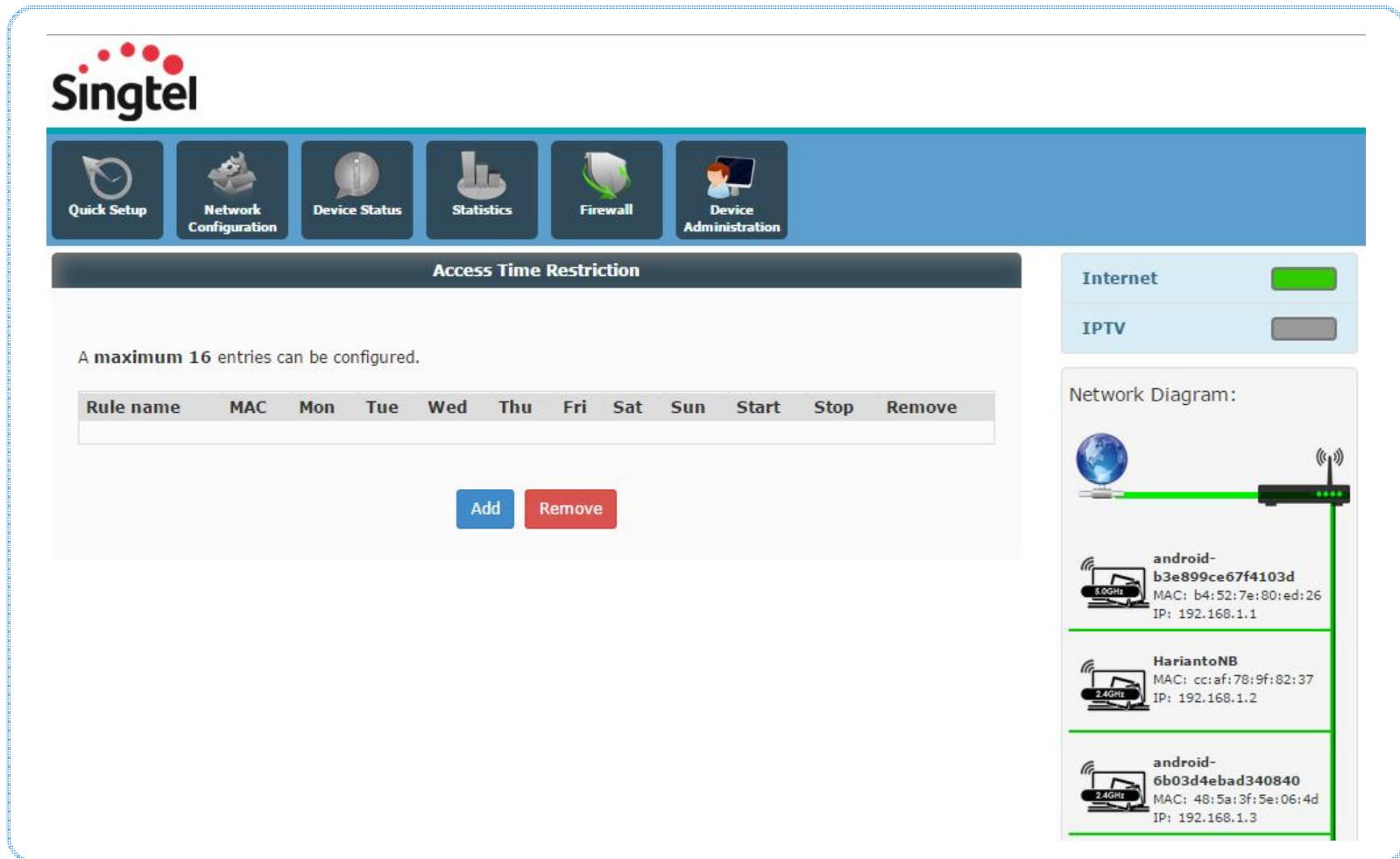
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

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

firewall configuration

MAC Filtering Settings



The image shows the Singtel web interface for MAC Filtering Settings. The interface includes a navigation bar with icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The main content area is titled "Access Time Restriction" and contains a table for configuring MAC filtering rules. A note states "A maximum 16 entries can be configured." The table has columns for Rule name, MAC, and days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun), along with Start, Stop, and Remove buttons. Below the table are "Add" and "Remove" buttons. On the right side, there are status indicators for Internet and IPTV, and a Network Diagram showing connected devices.

Singtel

Quick Setup Network Configuration Device Status Statistics Firewall Device Administration

Access Time Restriction

A maximum 16 entries can be configured.

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

Add Remove

Internet ☒ IPTV ☐

Network Diagram:

Diagram showing Internet connection and connected devices:

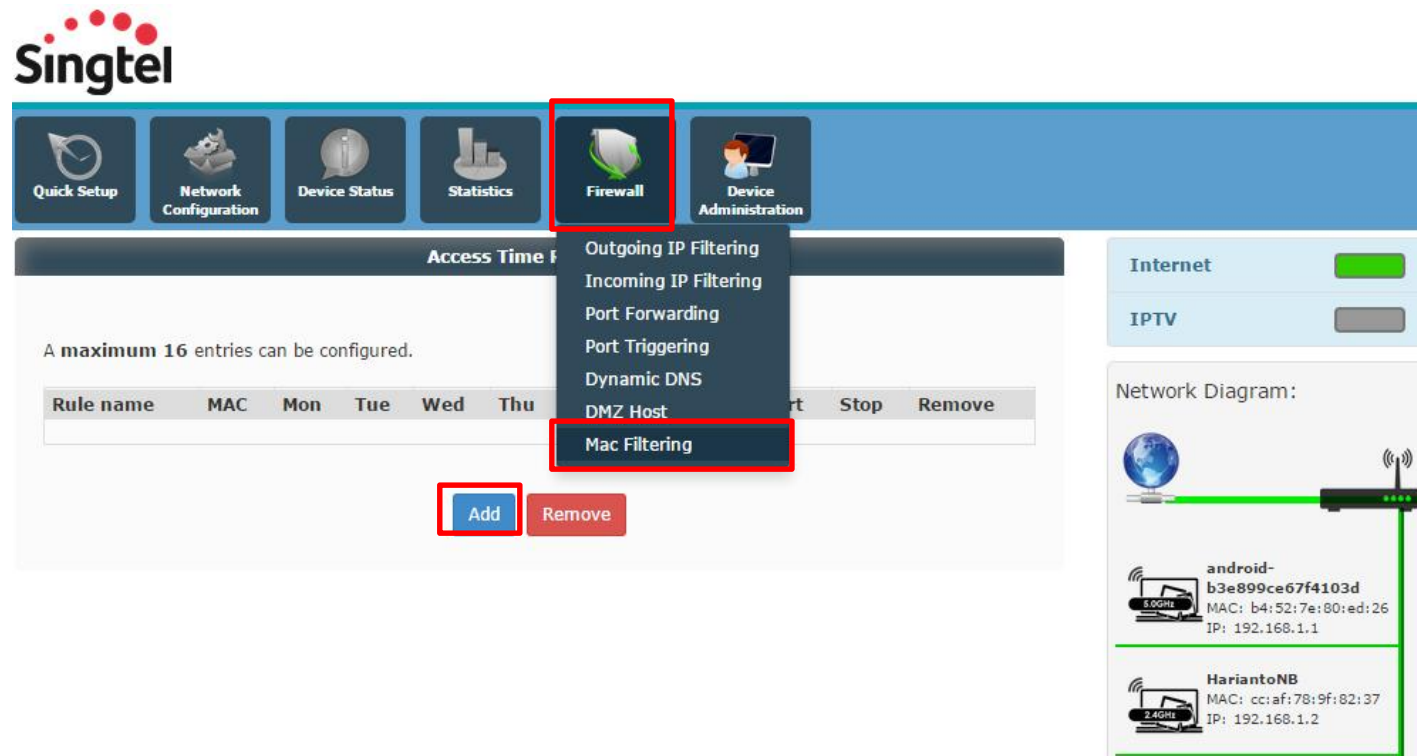
- android-b3e899ce67f4103d
MAC: b4:52:7e:80:ed:26
IP: 192.168.1.1
- HariantoNB
MAC: cc:af:78:9f:82:37
IP: 192.168.1.2
- android-6b03d4ebad340840
MAC: 48:5a:3f:5e:06:4d
IP: 192.168.1.3

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:

☐ Browser's MAC Address:

☒ Other MAC Address:

(xx:xx:xx:xx:xx:xx)

Days of the week: **Mon Tue Wed Thu Fri Sat Sun**

Click to select: ☐ ☐ ☐ ☐ ☒ ☐ ☐

Start Blocking Time (hh:mm):

End Blocking Time (hh:mm):



How to Set MAC Filtering

Step 8. Added filtered MAC Address will be shown

Access Time Restriction

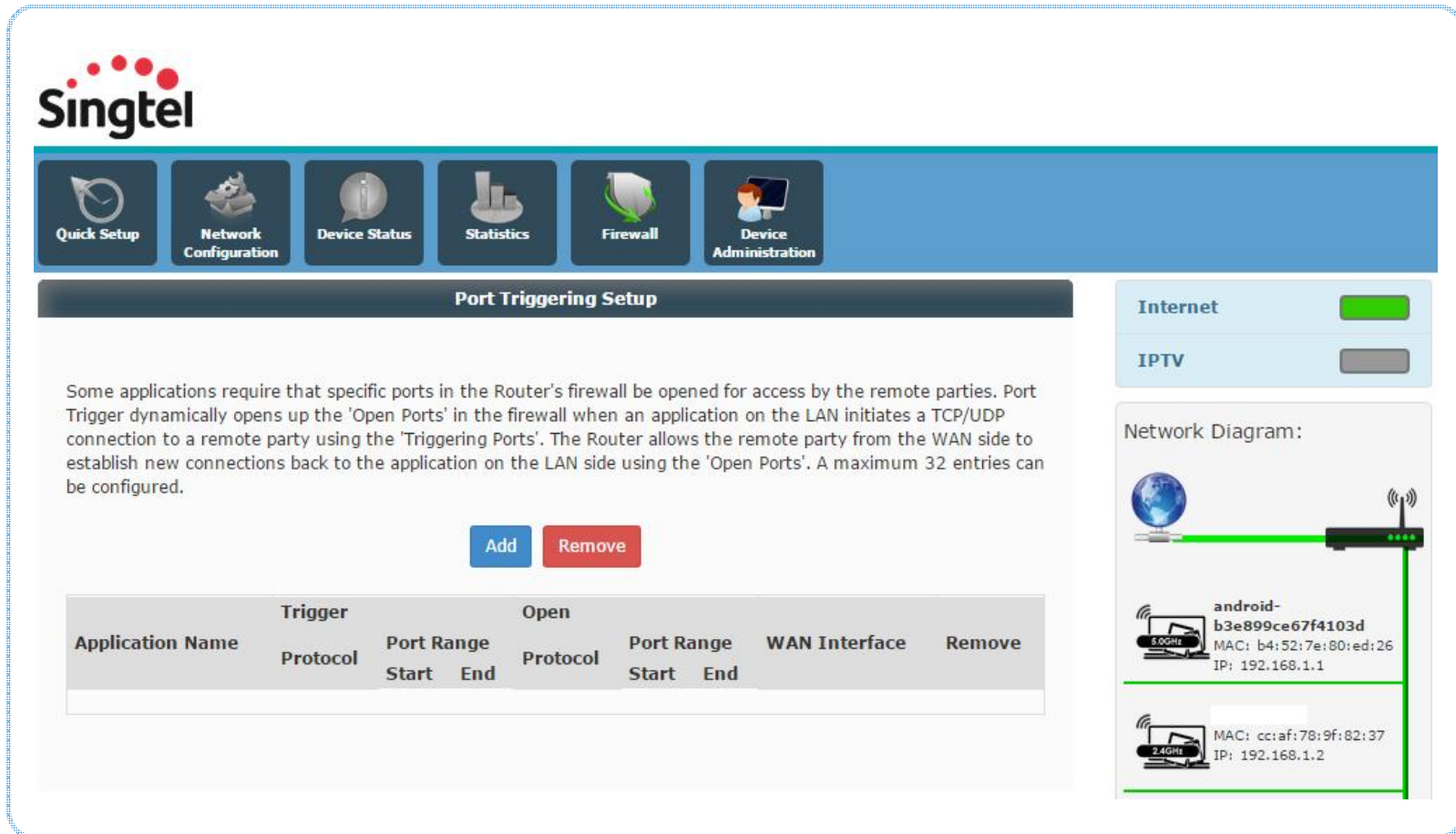
A **maximum 16** entries can be configured.

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"/>



firewall configuration

Port Triggering Settings



Singtel

Quick Setup | Network Configuration | Device Status | Statistics | Firewall | Device Administration

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.

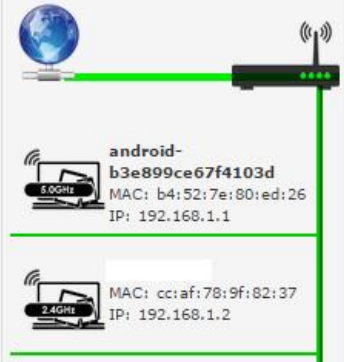
[Add](#) [Remove](#)

Application Name	Trigger		Open		WAN Interface	Remove
	Protocol	Port Range Start End	Protocol	Port Range Start End		

Internet ☒

IPTV ☐

Network Diagram:



android-b3e899ce67f4103d
MAC: b4:52:7e:80:ed:26
IP: 192.168.1.1

2.4GHz
MAC: cc:af:78:9f:82:37
IP: 192.168.1.2

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

The screenshot shows the Singtel web interface for the Aztech FG7009GR(AC) Residential Gateway. The top navigation bar includes icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall (highlighted with a red box), and Device Administration. A dropdown menu is open from the Firewall icon, showing options: Outgoing IP Filtering, Incoming IP Filtering, Port Forwarding, Port Triggering (highlighted with a red box), Dynamic DNS, DMZ Host, and Mac Filtering. Below the dropdown, the 'Port Triggering' section is visible, containing a description and an 'Add' button. To the right, there are status indicators for Internet and IPTV, and a Network Diagram showing the router connected to two wireless devices.

Port Triggering

Some applications require that specific ports in the Router's Firewall be opened by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall connection to a remote party using the 'Triggering Ports'. The router will then establish new connections back to the application on the LAN side. A maximum of 32 entries can be configured.

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

Application Name	Trigger		Open		WAN Interface	Remove
	Protocol	Port Range Start End	Protocol	Port Range Start End		

Network Diagram:

The diagram shows a router connected to two wireless devices:

- Device 1:** android-b3e899ce67f4103d, MAC: b4:52:7e:80:ed:26, IP: 192.168.1.1
- Device 2:** MAC: cc:af:78:9f:82:37, IP: 192.168.1.2

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:

Application Name:

☐ Select an application:

☒ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text" value="8881"/>	<input type="text" value="8882"/>	<input type="text" value="TCP"/>	<input type="text" value="8883"/>	<input type="text" value="8884"/>	<input type="text" value="TCP"/>
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="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.

AddRemove

Application Name	Trigger	Port Range		Open	Port Range		WAN Interface	Remove
	Protocol	Start	End	Protocol	Start	End		
MyRule	TCP	8881	8882	TCP	8883	8884	eth0.1	<input type="checkbox"/>

firewall configuration

DMZ

The screenshot displays the Singtel web interface for the Aztech FG7009GR(AC) Residential Gateway. The top navigation bar includes links for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The main content area is titled "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.

Below the text is a text input field labeled "DMZ Host IP Address:" and a "Save/Apply" button.

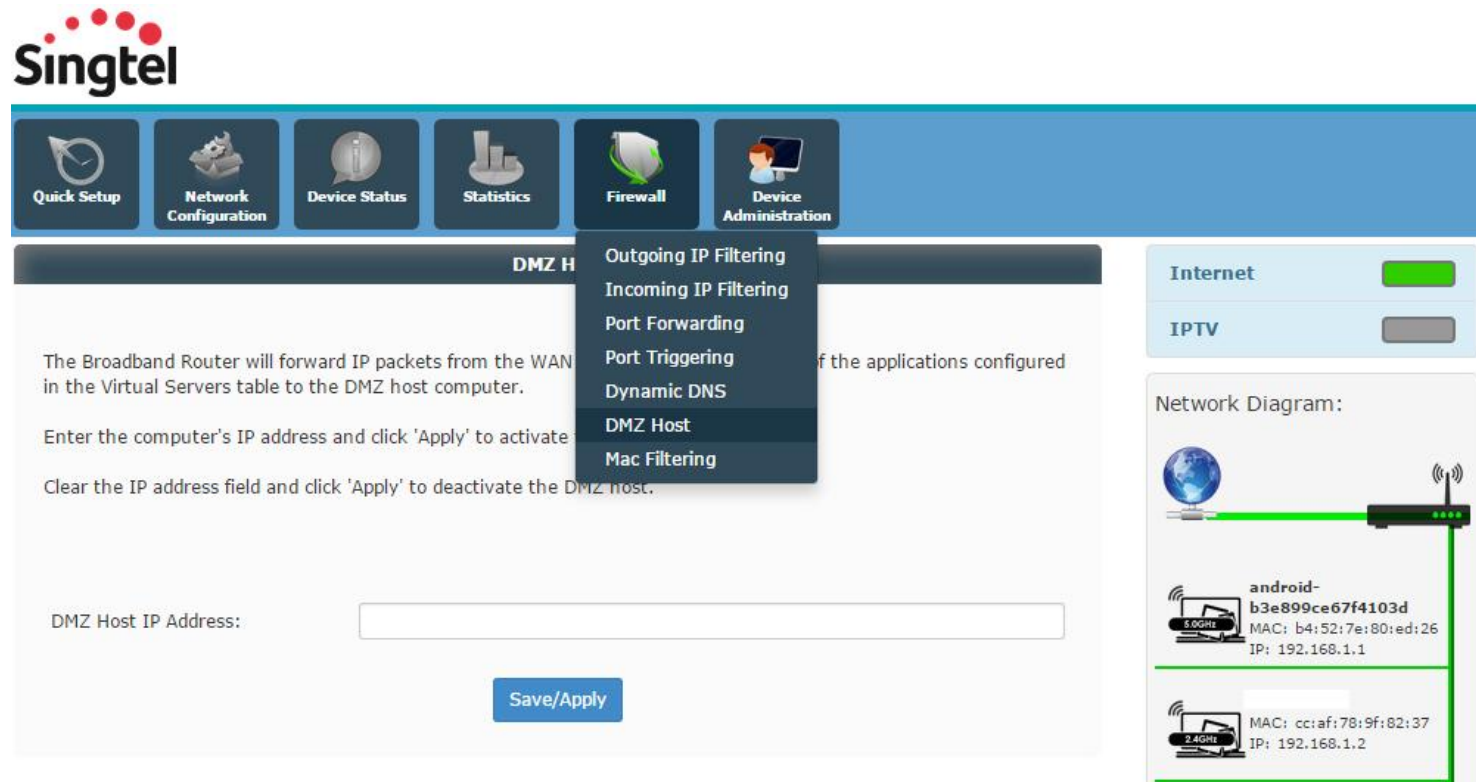
On the right side of the interface, there are status indicators for "Internet" (green bar) and "IPTV" (grey bar). Below these is a "Network Diagram:" showing a router connected to a 5.0GHz wireless device (android-b3e899ce67f4103d, MAC: b4:52:7e:80:ed:26, IP: 192.168.1.1) and a 2.4GHz wireless device (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

The screenshot shows the Singtel web interface for the Aztech FG7009GR(AC) Residential Gateway. The top navigation bar includes icons for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The main content area is titled "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.

Below this text, there is a form with the label "DMZ Host IP Address:" and a text input field containing the IP address "192.168.1.2". A red box highlights the input field. Below the input field is a blue button labeled "Save/Apply", which is also highlighted with a red box.

On the right side of the interface, there are two status indicators: "Internet" (green bar) and "IPTV" (grey bar). Below these is a "Network Diagram" section showing a router connected to a 5GHz wireless client (labeled "android-b3e899ce67f4103d" with MAC "b4:52:7e:80:ed:26" and IP "192.168.1.1") and a 2.4GHz wireless client (labeled "android-b3e899ce67f4103d" with MAC "b4:52:7e:80:ed:26" and IP "192.168.1.2"). The IP address "192.168.1.2" in the 2.4GHz client's details is highlighted with a red box.

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

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

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 is 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

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

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.

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

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 the Singtel web interface for the FG7009GR(AC) Residential Gateway. The top navigation bar includes links for Quick Setup, Network Configuration, Device Status, Statistics, Firewall, and Device Administration. The 'Quick Setup' section is active, displaying a message: 'This page allows you to check the device information, control the device connection.' Below this is a table titled '- Device Info -' containing the following information:

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

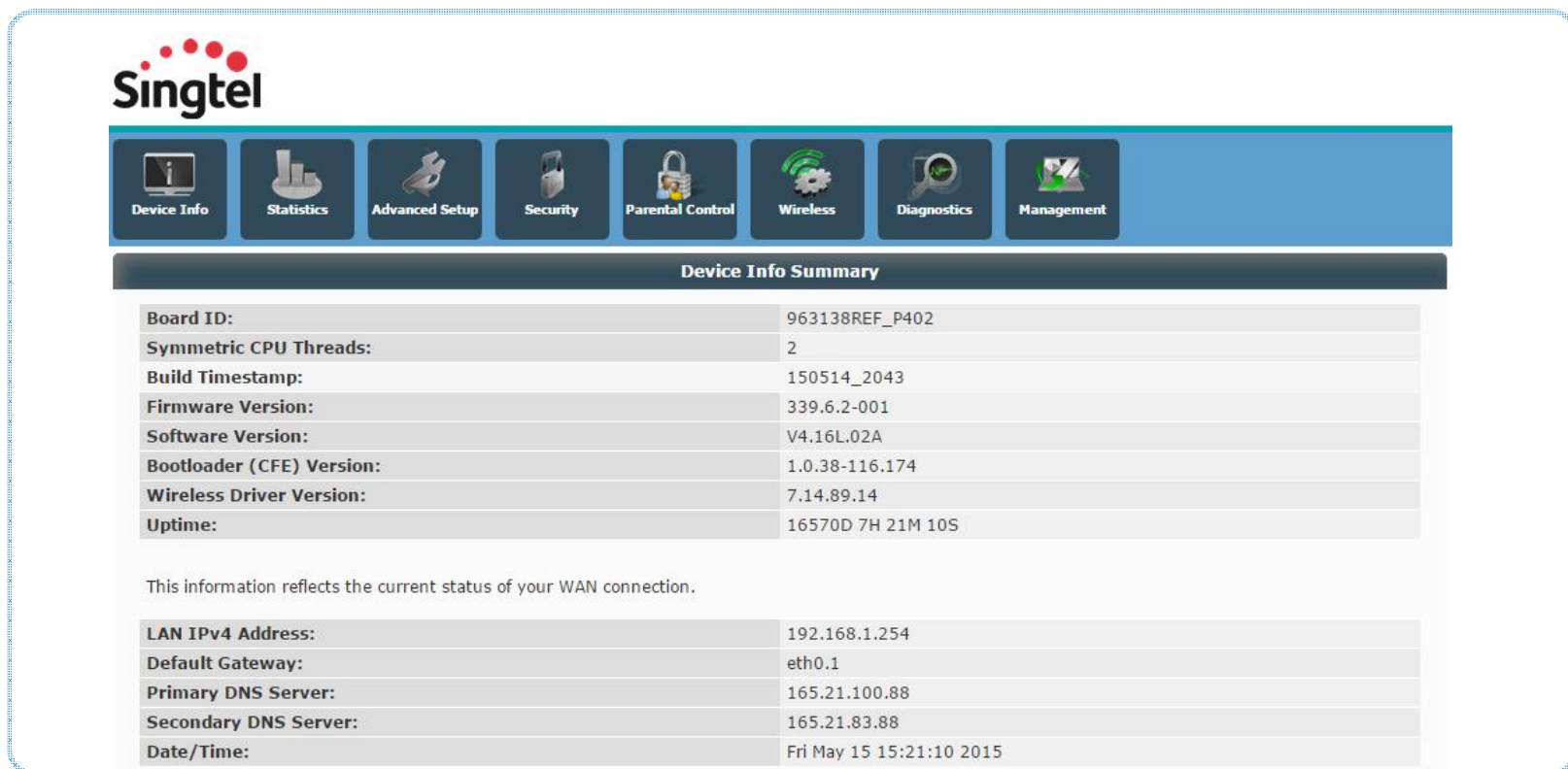
The 'Firmware Version' row is highlighted with a red border.

Accessing the Admin GUI

<http://192.168.1.254/singtel>

Username: admin

Password: H3ll0t3ch



The screenshot displays the Singtel Admin GUI. At the top is the Singtel logo. Below it is a navigation bar with icons and labels for Device Info, Statistics, Advanced Setup, Security, Parental Control, Wireless, Diagnostics, and Management. The main content area is titled "Device Info Summary" and contains two tables of system information.

Device Info Summary	
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

This information reflects the current status of your WAN connection.

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/adaptor 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 ¹	Yes
WPS Push Button (2.4GHz only)		Yes ¹	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 ¹	Yes

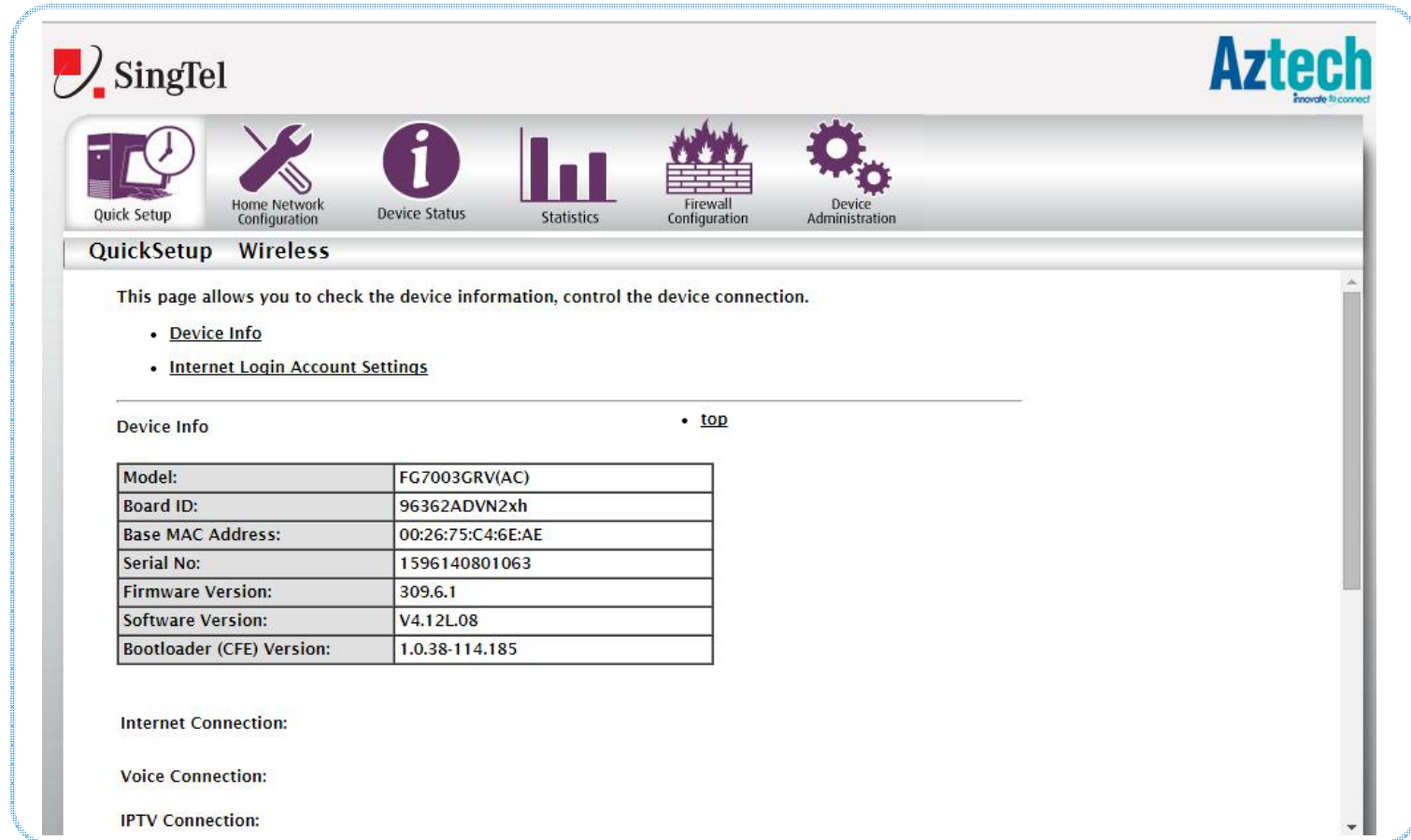
Notes:

1. Firmware dependant

Frequently Asked Questions

Graphical User Interface Look & Feel for previous RG:

First landing page from <http://192.168.1.254>



Frequently Asked Questions

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

First landing page from <http://192.168.1.254>

Singtel

Quick Setup | Network Configuration | Device Status | Statistics | Firewall | Device Administration

Quick Setup

This page allows you to check the device information, control the device connection.

– Device Info –

– Connection Details –

Connection Type	INTERNET	IPTV
Status	Up	Up
IP Address		
Default Gateway		
Primary DNS Server		
Secondary DNS Server		

– Configuration –

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

MAC: 90:3c:92:4d:53:67

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

Operating Hours

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

Saturday: 9:00 AM to 1:00 PM

(Except Public Holidays)

Thank You

Aztech