User Manual for HGB10R-02

Contents

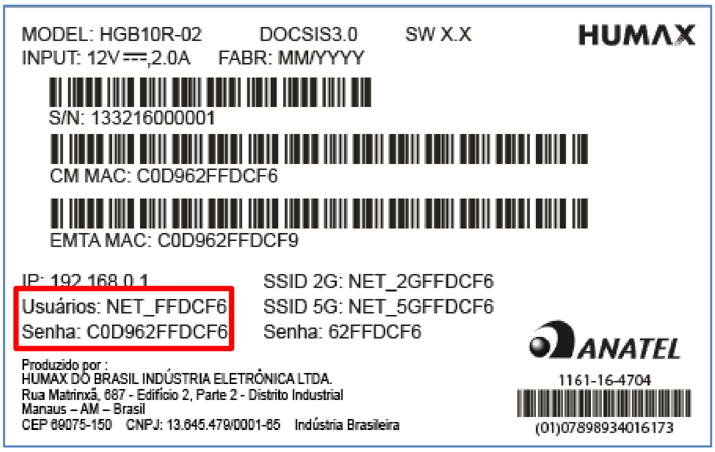
Access to WEB Page

To configure your cable modem, you have to access the configuration web page. The IP address of the residential gateway is 192.168.0.1. To configure the cable modem, follow the steps below:

1. Obtain an IP address from the built-in DHCP server for your PC to connect your product.

2. Open the web browser (Internet Explorer, Chrome, Mozilla, etc.) on your PC.

3. Enter ***http://192.168.0.1***, then the login page is displayed. The default username and password are located at the bottom of your product.



MODEL: HGB10R-02 DOCSIS3.0 SW X.X HUMAX
INPUT: 12V ⎓ 2.0A FABR: MM/YYYY

S/N: 133216000001

CM MAC: C0D962FFDCF6

EMTA MAC: C0D962FFDCF9

IP: 192.168.0.1
Usuários: NET_FFDCF6
Senha: C0D962FFDCF6

SSID 2G: NET_2GFFDCF6
SSID 5G: NET_5GFFDCF6
Senha: 62FFDCF6

Produzido por :
HUMAX DO BRASIL INDÚSTRIA ELETRÔNICA LTDA.
Rua Matrinxã, 687 - Edifício 2, Parte 2 - Distrito Industrial
Manaus – AM – Brasil
CEP 69075-150 CNPJ: 13.645.479/0001-65 Indústria Brasileira

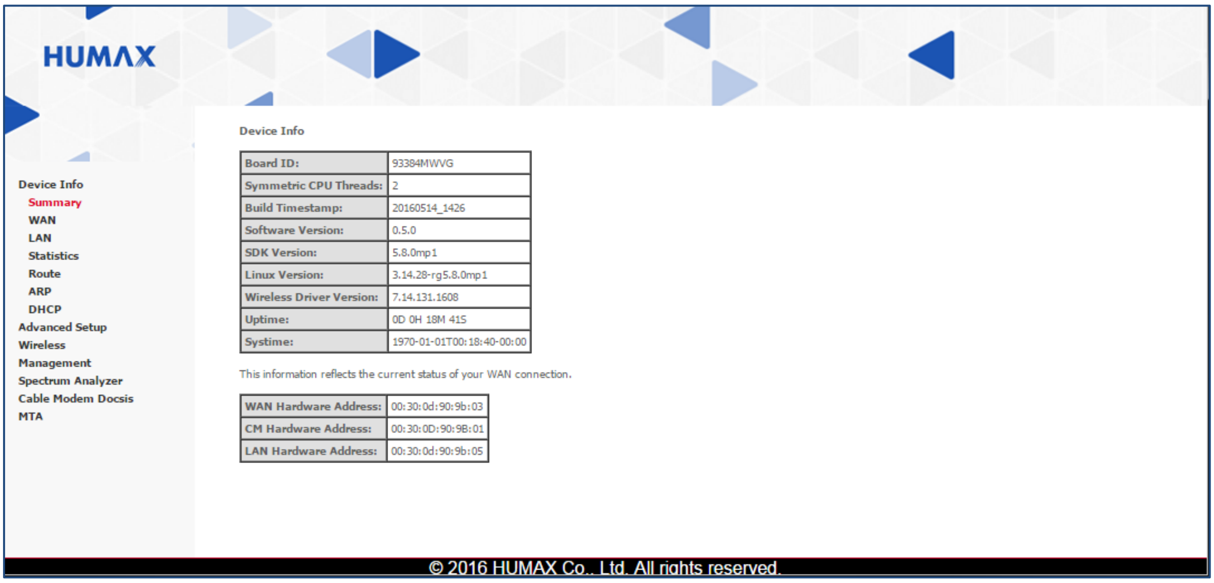
ANATEL
1161-16-4704
(01)07898934016173

You can have an easy access to the information about your product and the network connectivity, and see the current status of the product.

Basic Information

Device Info → Summary

You can see the basic information about your product and the network connectivity. In detail, you can check the hardware and software version, MAC address, IP address, serial number, system time on the product.



Device Info

Board ID:	93384MWVG
Symmetric CPU Threads:	2
Build Timestamp:	20160514_1426
Software Version:	0.5.0
SDK Version:	5.8.0mp1
Linux Version:	3.14.28-rg5.8.0mp1
Wireless Driver Version:	7.14.131.1608
Uptime:	0D 0H 18M 41S
Systime:	1970-01-01T00:18:40-00:00

This information reflects the current status of your WAN connection.

WAN Hardware Address:	00:30:0d:90:9b:03
CM Hardware Address:	00:30:0D:90:9B:01
LAN Hardware Address:	00:30:0d:90:9b:05

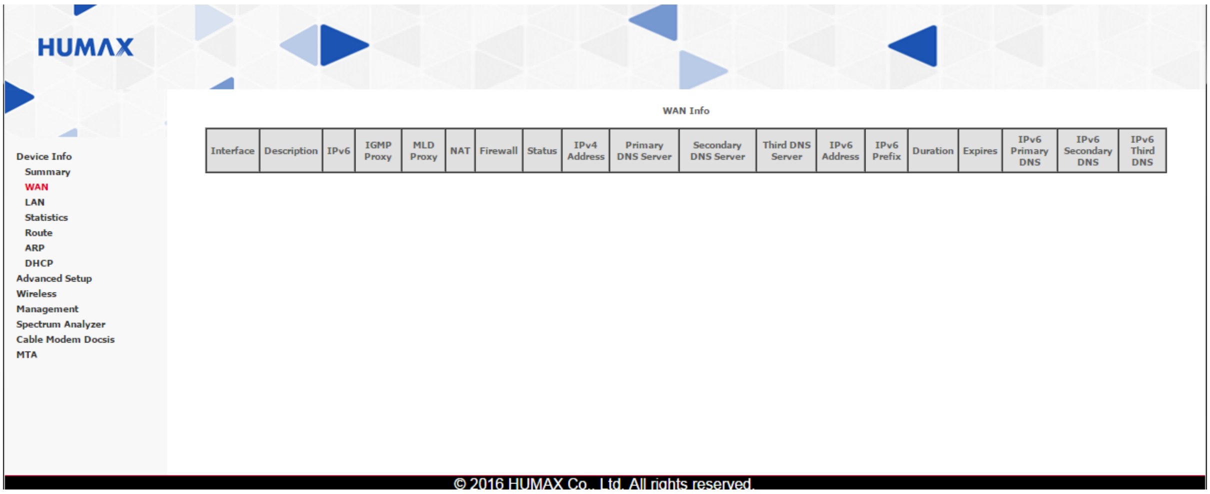
© 2016 HUMAX Co., Ltd. All rights reserved.

Note: The information on this page can be changed at any time by refreshing your web browser.

WAN Information

Device Info → WAN

You can see the information on the network connection between your Internet service provider and the product.



Device Info
Summary
WAN
LAN
Statistics
Route
ARP
DHCP
Advanced Setup
Wireless
Management
Spectrum Analyzer
Cable Modem Docsis
MTA

WAN Info

Interface	Description	IPv6	IGMP Proxy	MLD Proxy	NAT	Firewall	Status	IPv4 Address	Primary DNS Server	Secondary DNS Server	Third DNS Server	IPv6 Address	IPv6 Prefix	Duration	Expires	IPv6 Primary DNS	IPv6 Secondary DNS	IPv6 Third DNS

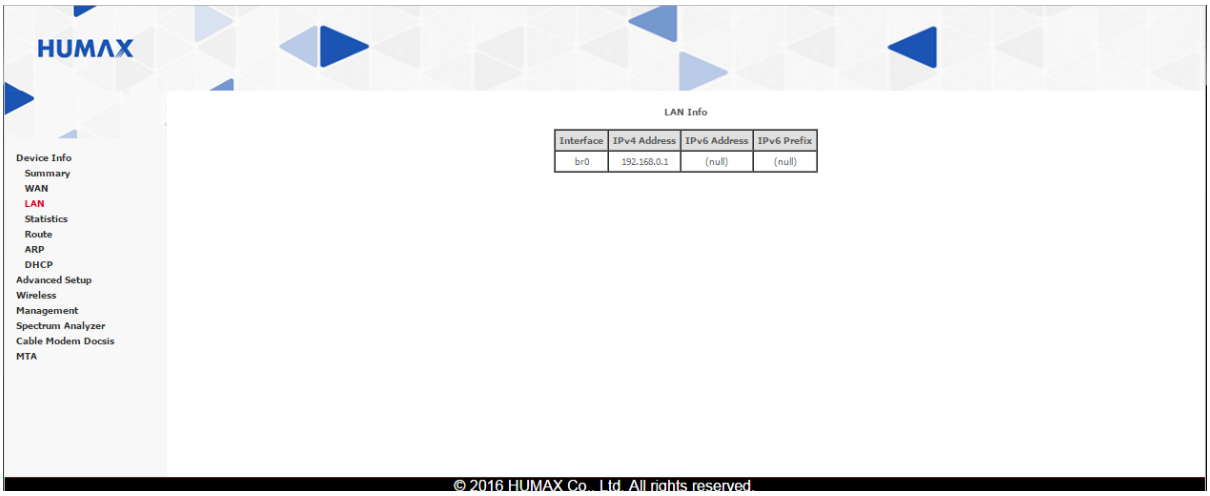
© 2016 HUMAX Co., Ltd. All rights reserved.

- **Interface** displays the WAN connection interfaces.
- **Description** displays the service description such as pppoe, ipor or br.
- **IPv6** displays if IPv6 is enabled or not.
- **IGMP Proxy** displays if Internet group management protocol (IGMP) is enabled or not.
- **MLD Proxy** displays if multicast listener discovery (MLD) is enabled or not.
- **NAT** displays if NAT is enabled or not.
- **Firewall** displays if the firewall is enabled or not.
- **Status** displays the status of WAN interface.
- **IPv4 Address** displays the obtained IPv4 address.
- **Primary DNS Server** displays the information on the primary DNS server.
- **Secondary DNS Server** displays the information on the secondary DNS server.
- **Third DNS Server** displays the information on the third DNS server.
- **IPv6 Address** displays the obtained IPv6 address.
- **IPv6 Prefix** displays the IPv6 prefix.
- **Duration** displays the lease time of WAN IP address.
- **Expires** displays the remaining time until WAN IP address expires.
- **IPv6 Primary DNS** displays the information on the primary IPv6 DNS server.
- **IPv6 Secondary DNS** displays the information on the secondary IPv6 DNS server.
- **IPv6 Third DNS** displays the information on the third IPv6 DNS server.

LAN Information

Device Info → LAN

You can see the information on the LAN connections such as the IP address or prefix of device connected to the product.



LAN Info

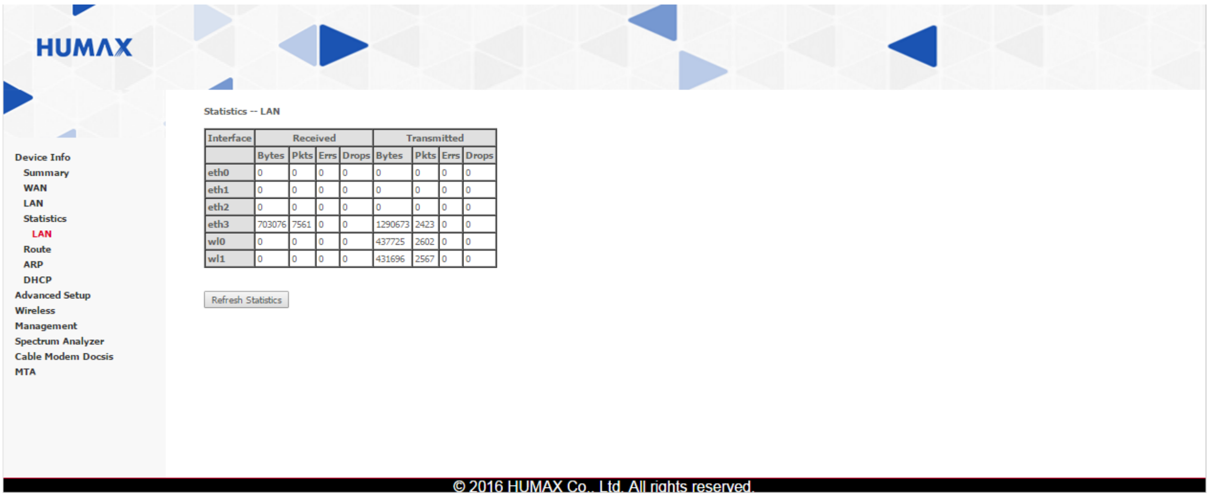
Interface	IPv4 Address	IPv6 Address	IPv6 Prefix
br0	192.168.0.1	(null)	(null)

- **Interface** displays the LAN connection interfaces.
- **IPv4 Address** displays the obtained IPv4 address.
- **IPv6 Address** displays the obtained IPv6 address.
- **IPv6 Prefix** displays the IPv6 prefix.

LAN Statistics

Device Info → Statistics → LAN

You can see the traffic statistics in transmitting or receiving data for byte or packet, and check the statistics of errors or drops occurring in transmitting or receiving data.



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	703076	7561	0	0	1290673	2423	0	0
wl0	0	0	0	0	437725	2602	0	0
wl1	0	0	0	0	431696	2567	0	0

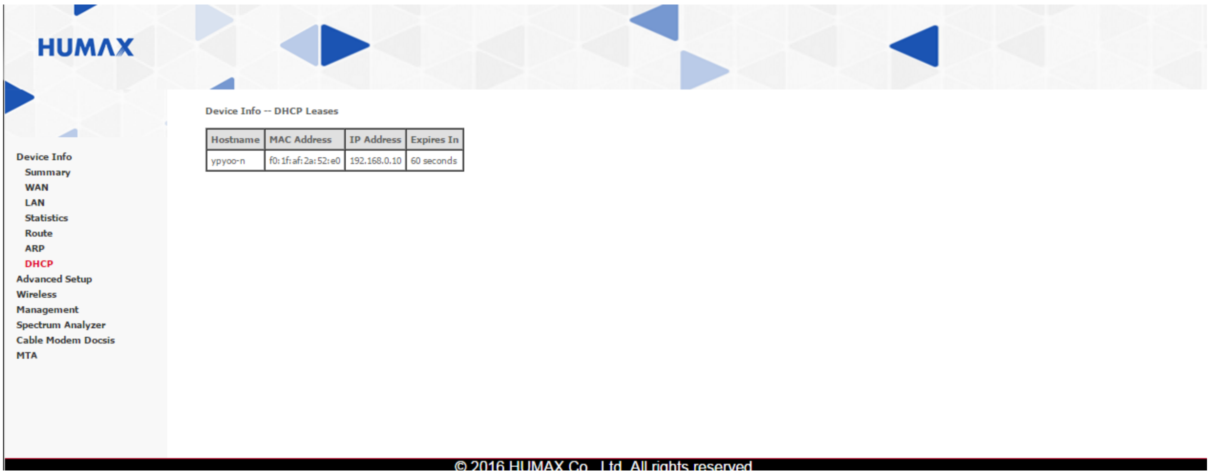
- **Interface** displays the LAN connection interfaces.
- **Bytes** displays the total quantity of packets in Bytes.
- **Pkts** displays the total quantity of packets.
- **Errs** displays the total quantity of error packets.
- **Drops** displays the total quantity of dropped packets.

Click **Refresh Statistics** to update the statistics.

DHCP Information

Device Info → DHCP

You can see the DHCP lease information of all devices having IP address assigned by DHCP server.
Note: The devices with a static IP address are not displayed.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
ypyoo-n	f0:1f:af:2a:52:e0	192.168.0.10	60 seconds

© 2016 HUMAX Co., Ltd. All rights reserved

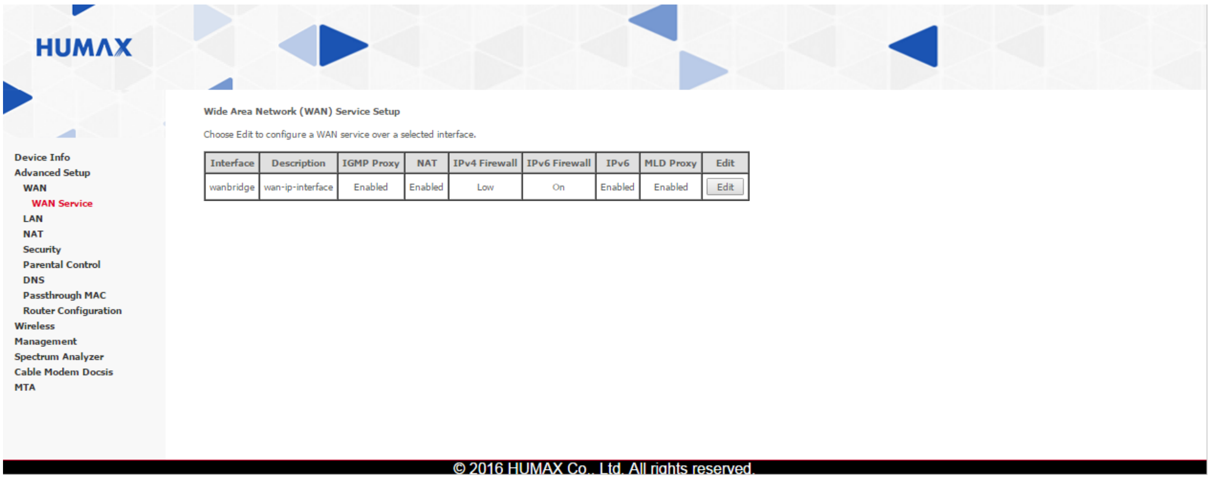
- **Hostname** displays the host name of connected network device.
- **MAC Address** displays the MAC address of connected network device.
- **IP Address** displays the IP address of connected network device.
- **Expires In** displays the remaining time until the DHCP lease expires for each network device.

Your product supports additional advanced features such as WAN service, IPv6 auto-configuration, network address translation (NAT), IP and MAC filtering, time restriction for child, DDNS, pass-through and mode change.

WAN Configuration

Advanced Setup → WAN → WAN Service

You can set the wide area network (WAN) IP. Enter the required information to configure the WAN service.



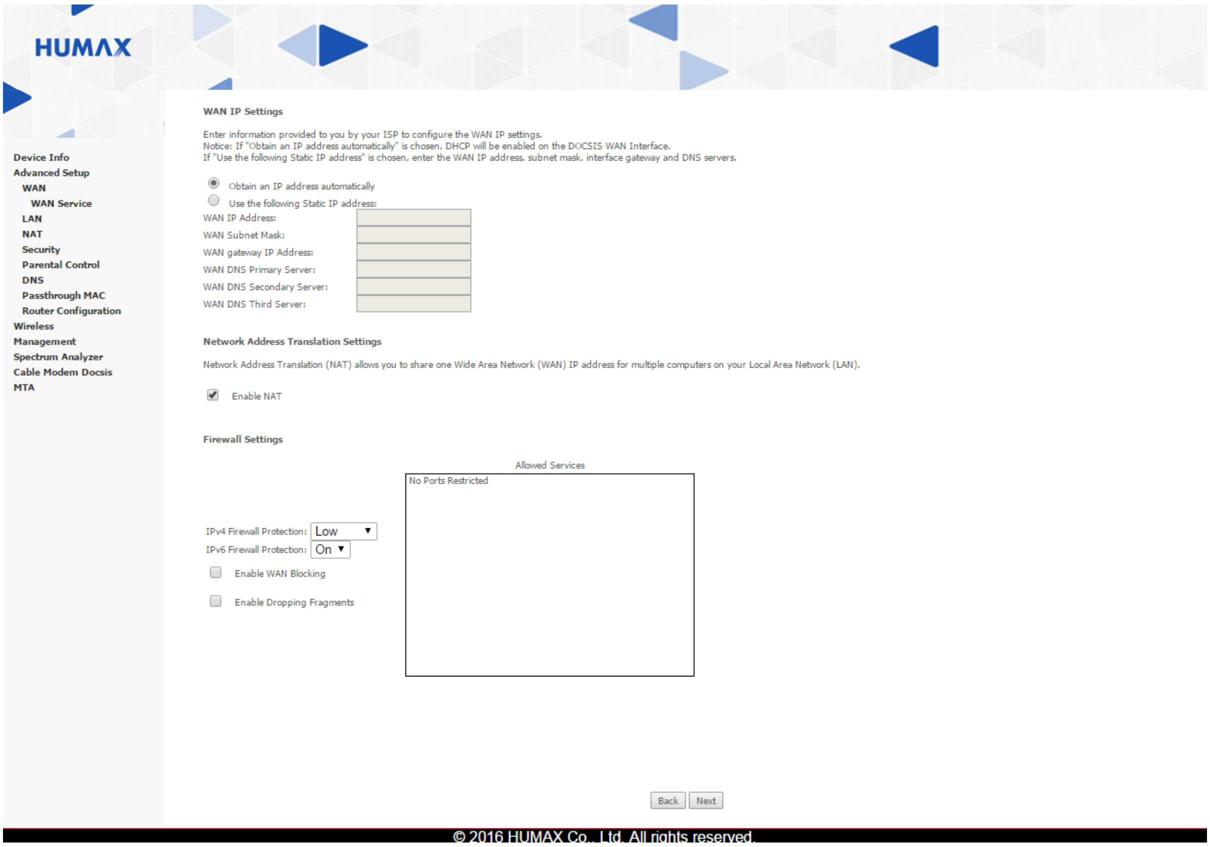
Wide Area Network (WAN) Service Setup

Choose Edit to configure a WAN service over a selected interface.

Interface	Description	IGMP Proxy	NAT	IPv4 Firewall	IPv6 Firewall	IPv6	MLD Proxy	Edit
wanbridge	wan-ip-interface	Enabled	Enabled	Low	On	Enabled	Enabled	Edit

- **Interface** displays the WAN connection interface.
- **Description** displays WAN service description.
- **IGMP Proxy** displays if the Internet group management protocol (IGMT) is enabled or not.
- **NAT** displays if NAT is enabled or not.
- **IPv4 Firewall** displays if the IPv4 firewall is enabled or not.
- **IPv6 Firewall** displays if the IPv6 firewall is enabled or not.
- **IPv6** displays if IPv6 is enabled or not.
- **MLD Proxy** displays if multicast listener discovery (MLD) is enabled or not.

Click **Edit** to configure a WAN service. Then, the following screen will appear.



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled on the DOCSIS WAN Interface.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask, interface gateway and DNS servers.

● Obtain an IP address automatically
○ Use the following Static IP address:

WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:
WAN DNS Primary Server:
WAN DNS Secondary Server:
WAN DNS Third Server:

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☑ Enable NAT

Firewall Settings

Allowed Services
No Ports Restricted

IPv4 Firewall Protection: Low
IPv6 Firewall Protection: On
□ Enable WAN Blocking
□ Enable Dropping Fragments

© 2016 HUMAX Co., Ltd. All rights reserved.

If **Obtain an IP address automatically** is selected, DHCP is currently enabled. To hardcode your network adapter, select **Use the following IP address** and enter the appropriate address.

- **WAN IP Address:** Enter the static WAN IPv4 address.
- **WAN Subnet Mask:** Enter the static subnet mask.
- **WAN gateway IP Address:** Enter the static gateway IP address.
- **WAN DNS Primary Server:** Enter the IP address of the primary WAN DNS server.
- **WAN DNS Secondary Server:** Enter the IP address of the secondary WAN DNS server.
- **WAN DNS Third Server:** Enter the IP address of the third WAN DNS server.

Check **Enable NAT** to activate the network address translation (NAT). Then, you can share a WAN IP address for multiple computers on your LAN.

In **Firewall Settings**, you can block or exclusively allow different types of data through the residential gateway from WAN to LAN.

- **IPv4 Firewall Protection**: Select the firewall protection option.
  Off
  Low does not block any services/ports, however it does protect against invalid packets and well known attacks.
  Medium may cause the firewall to drop a packet unless it is on a specific port of allowed services. The allowed services are listed on the same page.

High is similar to Medium, but allows access to even fewer services.
Disabled allows all traffic to pass.

- **IPv6 Firewall Protection**: Select **On** to set the IPv6 firewall protection.
- **Enable WAN Blocking**: Check to prevent all fragmented IP packets from passing through the firewall.
- **Enable Dropping Fragments**: Check to drop fragmented packet.
- **Allowed Services** displays allowed services. If no services are allowable, **No Ports Restricted** will appear.

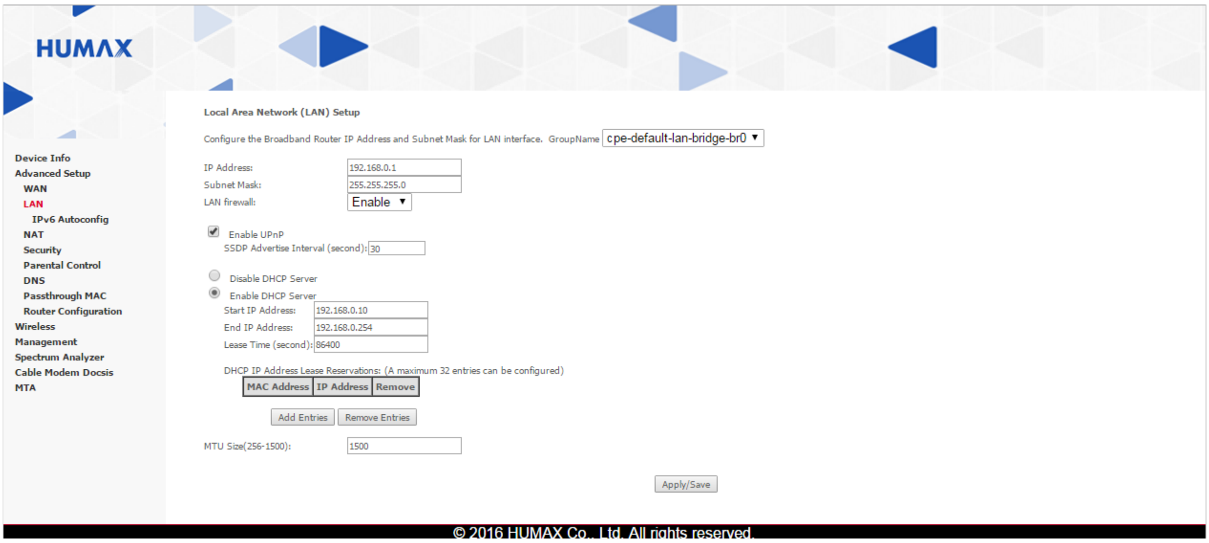
Click **Back** to cancel the settings and then go back to the previous screen.

Click **Next** to save your changes and then go to the next page.

LAN Configuration

Advanced Setup → LAN

You can configure the IP address of your product and the subnet mask for the LAN interface.



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName cpe-default-lan-bridge-br0

IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
LAN firewall: Enable

☑ Enable UPnP
SSDP Advertise Interval (second): 30

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.0.10
End IP Address: 192.168.0.254
Lease Time (second): 86400

DHCP IP Address Lease Reservations: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

MTU Size(256-1500): 1500

- **IP Address** Enter the IP address of your product. The default IP address is 192.168.0.1.

- **Subnet Mask** Enter the subnet mask of your product. The default subnet mask is 255.255.255.0.

- **LAN firewall** Select **Enable** to activate LAN firewall engine. Then, you can prevent any unauthorized access to your LAN.

- **Enable UPnP** Check to enable the UPnP agent in the product. If you are running a CPE application that requires UPnP, check this option.

SSDP Advertise Interval (second) Enter the advertise interval for simple service discovery protocol (SSDP). The default value is 30 seconds.

- **Disable DHCP Server** Select to inactivate the DHCP server on your LAN.

- **Enable DHCP Server** Select to run a network with the DHCP server running on your LAN.

Start IP Address Enter the first IP address to be assigned by the DHCP server to clients.

End IP Address Enter the last IP address to be assigned by the DHCP server to clients..

Lease Time (second) Enter the maximum lease time for IP address assignments. During the time, the IP address is valid.

Click **Add Entries** to make an additional lease reservation for DHCP IP address. You can add up to 32 entries.

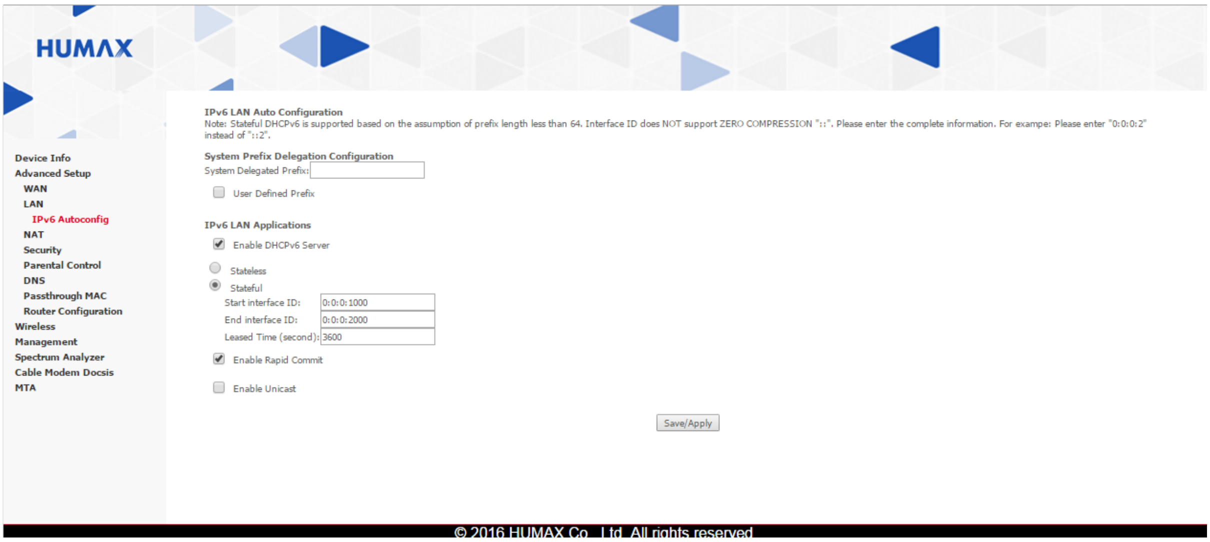
Click **Remove Entries** to remove the lease reservation for DHCP IP address.

- **MTU Size (256-1500)** Enter the maximum transmission units (MTU) for data transmission. The default MTU is 1500 octets.

Click **Apply/Save** to save your changes.

Advanced Setup → LAN → IPv6 Autoconfig

You can configure automatically IPv6 LAN interface.



IPv6 LAN Auto Configuration
Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".

System Prefix Delegation Configuration
System Delegated Prefix:

□ User Defined Prefix

IPv6 LAN Applications

☑ Enable DHCPv6 Server

○ Stateless
● Stateful
Start interface ID: 0:0:0:1000
End interface ID: 0:0:0:2000
Leased Time (second): 3600

☑ Enable Rapid Commit

□ Enable Unicast

© 2016 HUMAX Co., Ltd. All rights reserved

System Prefix Delegation Configuration

- **System Delegated Prefix** Displays the prefix provided from the system.

  Use Defined Prefix: Check to use the defined prefix.

IPv6 LAN Application

- **Enable DHCPv6 Server:** Check to turn on the DHCPv6 feature on the LAN.
- **Stateless:** Select to inherit IPV6 address assignments from the WAN IPV6 interface.
- **Stateful:** Select to configure IPv6 address using stateful DHCPv6.

  Start interface ID: Enter the first IPv6 addresses for DHCP to assign to LAN devices.

  End interface ID: Enter the last IPv6 addresses for DHCP to assign to LAN devices.

  Leased Time (second): Enter the time before a new IPv6 lease is requested by the LAN client.

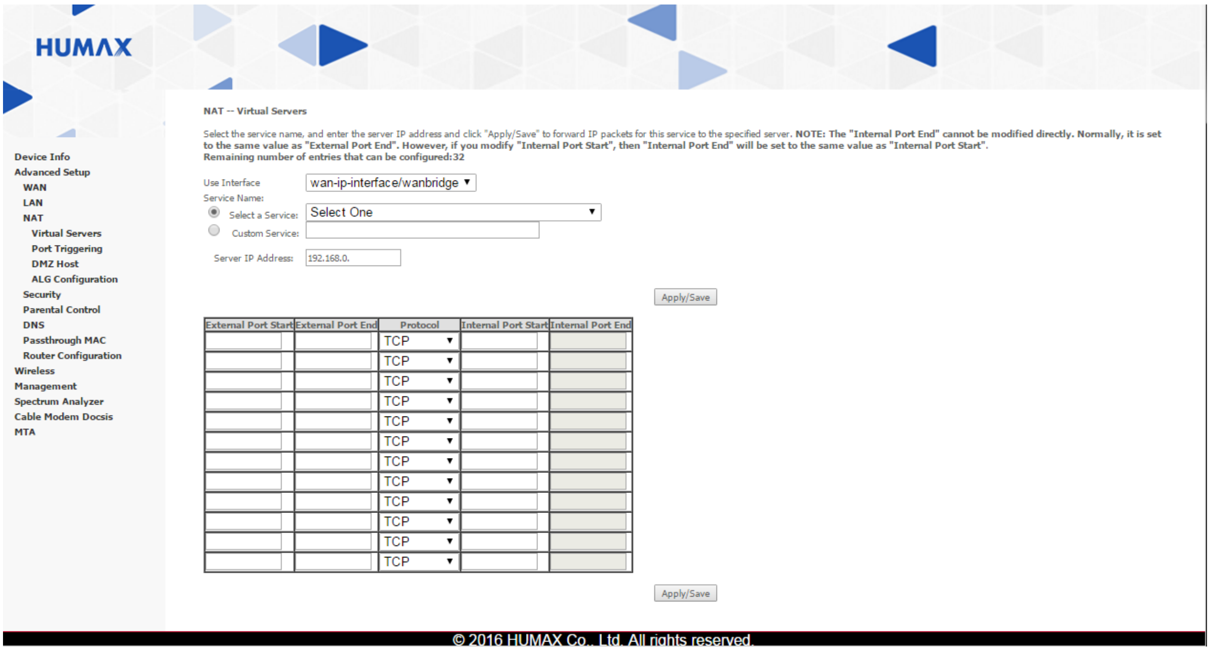
- **Enable Rapid Commit:** Check to get IPv6 addresses from a server.
- **Enable Unicast:** Check to enable IPv6 unicast packet forwarding.

Click **Save/Apply** to save your changes.

Network Address Translation (NAT)

Advanced Setup → NAT → Virtual Servers

Virtual Servers is a technique used to facilitate communications by external hosts with services provided within a private LAN. You can direct the incoming traffic from WAN side to the internal server with private IP address on the LAN side. You can add up to 32 entries.



NAT -- Virtual Servers

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: wan-ip-interface/wanbridge

Service Name:
● Select a Service: Select One
○ Custom Service:

Server IP Address: 192.168.0.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

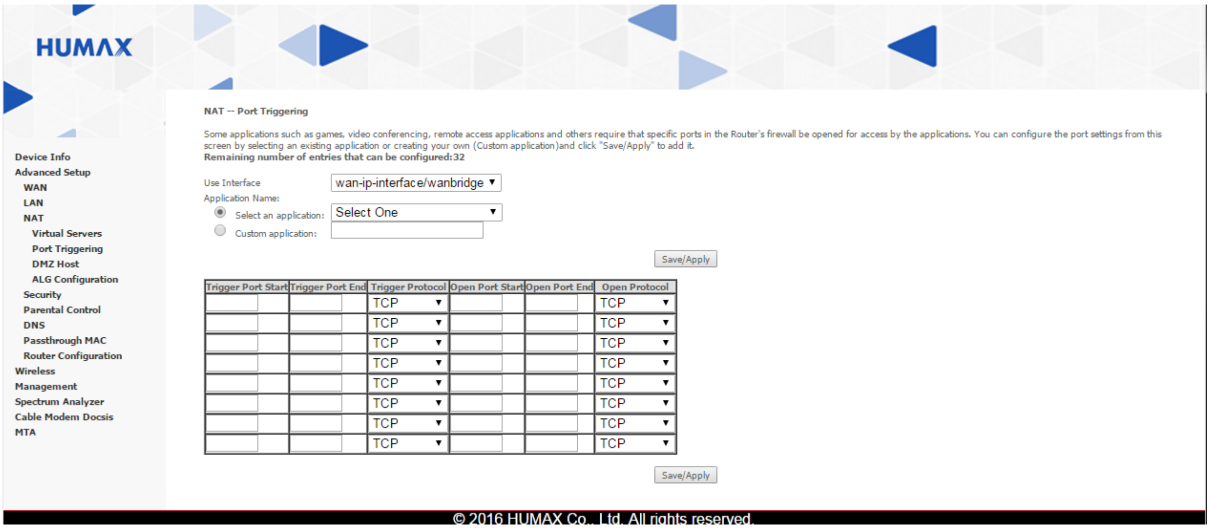
- **Use Interface** Select the WAN interface to apply the network address translation (NAT) rule.
- **Service Name** You can select a service name from the list or manually enter a unique name for the application.
- **Server IP Address** Enter the IP address of the LAN client in which the service has been hosted.

Click **Apply/Save** to save your changes.

- **External Port Start** Enter the first port number of external port.
- **External Port End** Enter the last port number of external port.
- **Protocol** Select a protocol among transmission control protocol (TCP), user data gram protocol (UDP) or TCP/UDP.
- **Internal Port Start** Enter the first port number of internal port.
- **Internal Port End** Enter the last port number of internal port.

Advanced Setup → NAT → Port Triggering

Port triggering is a configuration option on a NAT-enabled router that allows a host machine to dynamically and automatically forward a specific port back to itself. You can configure your product to allow the remote party from the WAN side to establish new connections back to the application on the LAN side using the Open Ports.



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:32

Use Interface: wan-ip-interface/wanbridge

Application Name:

● Select an application: Select One

○ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

© 2016 HUMAX Co., Ltd. All rights reserved.

- **Use Interface:** Select the interface to apply the port triggering rule.

- **Select an Application:** Select an application from the list to commonly require a port triggering entry.

- **Custom Application:** Enter a unique name or comments for the application.

Click **Save/Apply** to save your changes.

- **Trigger Port Start:** Enter the first port number of an outgoing trigger port.

- **Trigger Port End** Enter the last port number of an outgoing trigger port.

- **Trigger Protocol:** Select the protocol among TCP/UDP, TCP, UDP.

- **Open Port Start:** Enter the first port number of an incoming port.

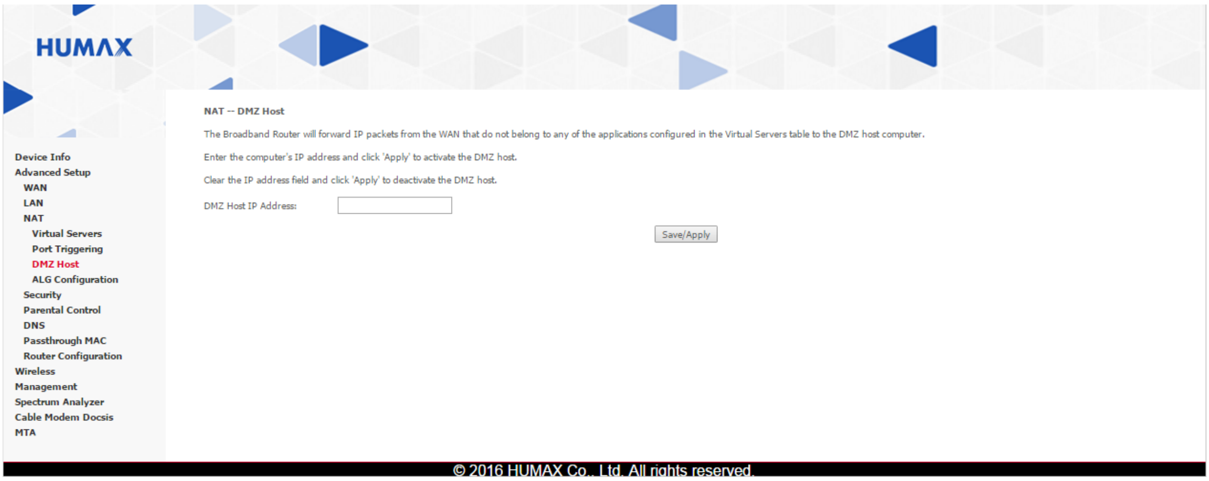
- **Open Port End:** Enter the last port number of an incoming port.

- **Open Protocol:** Select the protocol among TCP/UDP, TCP, UDP.

Click **Save/Apply** to save your changes.

Advanced Setup → NAT → DMZ Host

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. If it is desired to route all internet traffic with no filtering or security to a specific LAN device, add the IP address of that device to this field.



NAT -- DMZ Host

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:

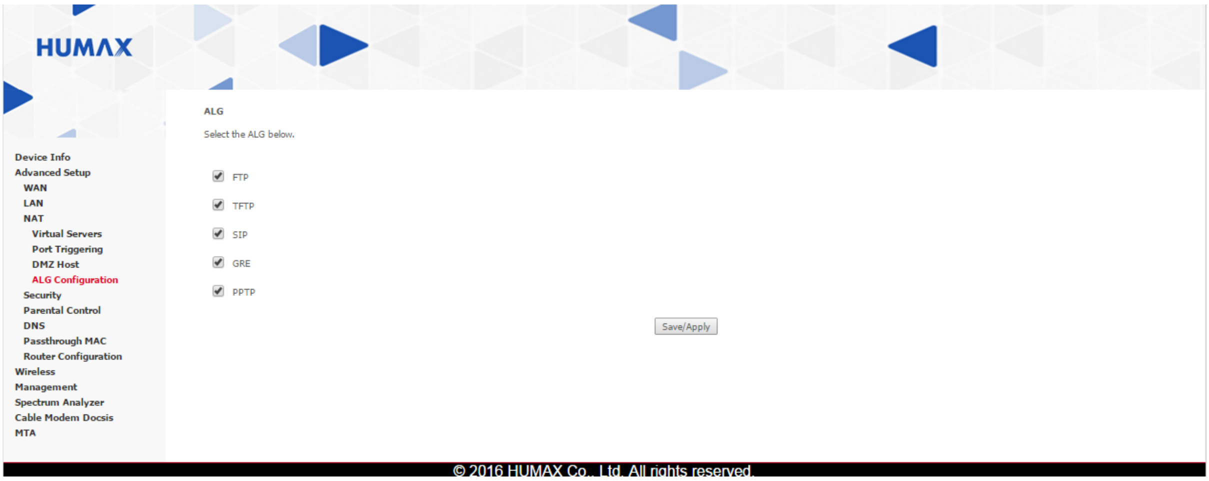
- **DMZ Host IP Address**: Enter the IP address of the network device that you want to have unrestricted Internet communication.

Click **Save/Apply** to save your changes.

Advanced Setup → NAT → ALG Configuration

Network address translation (NAT)

You can enable or disable application level gateway (ALGs). Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.



ALG

Select the ALG below.

☑ FTP

☑ TFTP

☑ SIP

☑ GRE

☑ PPTP

- **FTP** allows FTP client and server to communicate across NAT.

- **TFTP** allows TFTP client and server to communicate across NAT.

- **SIP** allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off

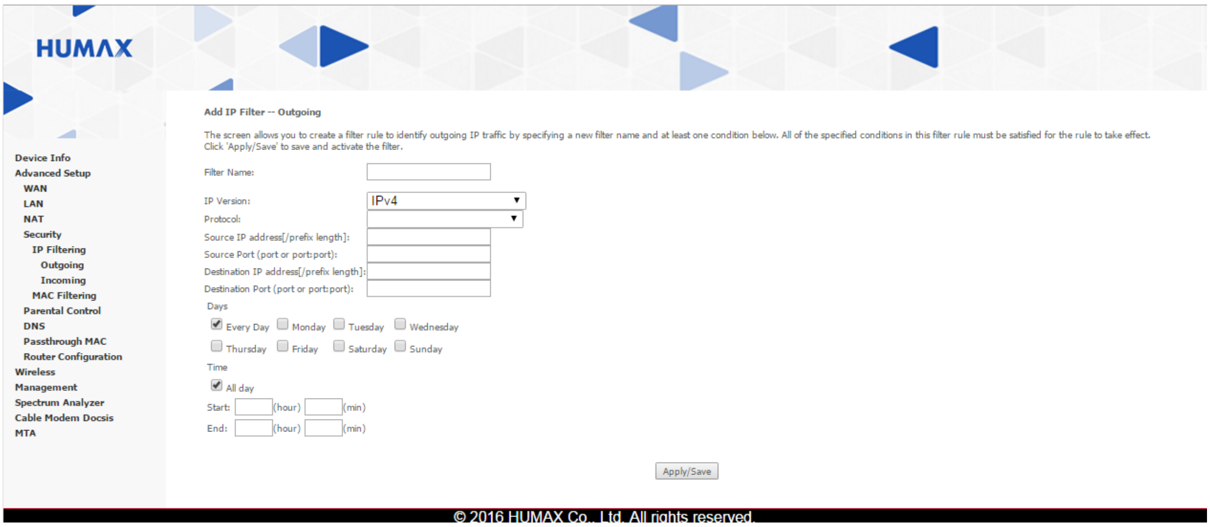
- **GRE** allows GRE client and server to communicate across NAT.

- **PPTP** allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to Advanced→Virtual Server).

Security Setup

Advanced Setup → Security → IP Filtering → Outgoing

You can configure a filtering rule to control outgoing traffic so that your product prevents local PCs from getting access to the WAN.



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:

IP Version: IPv4 ▾

Protocol: ▾

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Days

☑ Every Day ☐ Monday ☐ Tuesday ☐ Wednesday

☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Time

☑ All day

Start: (hour) (min)

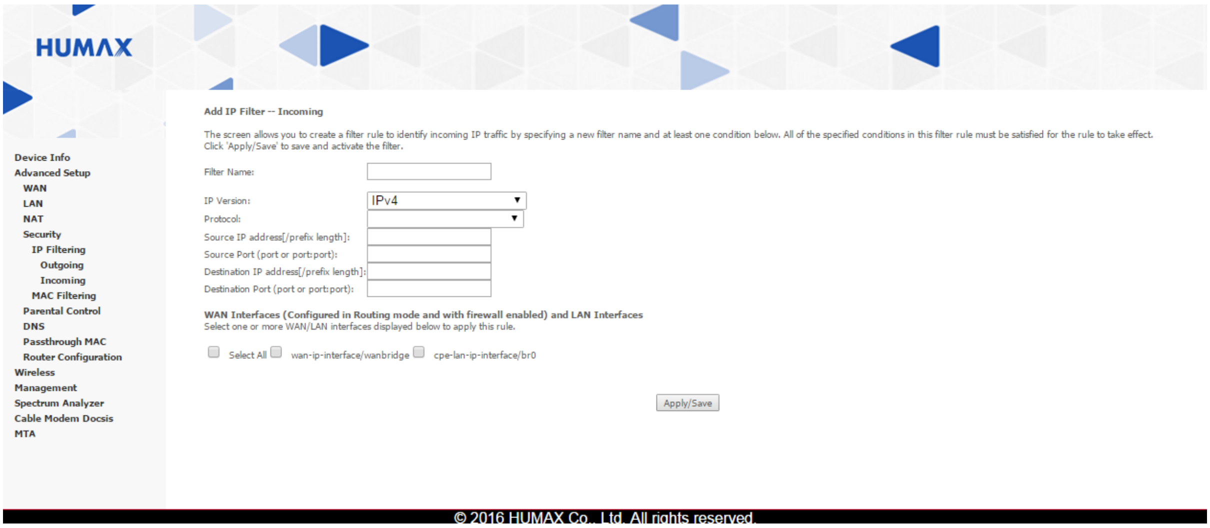
End: (hour) (min)

- **Filter Name**: Enter a filtering name.
- **IP Version**: Select an IP version. The default version is IPv4.
- **Protocol**: Select a protocol profile for your filtering rule. TCP/UDP is most commonly used.
- **Source IP address**: Enter the source IP address of a LAN side host to control outgoing traffic.
- **Source Port (port or port:port):** Enter the source port number of a LAN side host to block.
- **Destination IP address**: Enter the destination IP address of a LAN side host.
- **Destination Port (port or port:port)**: Enter the destination host port of a LAN side host
- **Days/Time:** Set the time for the IP filtering rule to be enabled.

Click **Apply/Save** to save your changes.

Advanced Setup → Security → IP Filtering → Incoming

You can configure a filtering rule to control incoming traffic. Your product is set to block all of incoming traffics, but you can set a filtering rule to transfer a specific incoming traffic.



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:	IPv4
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 □ wan-ip-interface/wanbridge □ cpe-lan-ip-interface/br0

© 2016 HUMAX Co., Ltd. All rights reserved.

- **Filter Name**: Enter a filtering name.
- **IP Version**: Select an IP version. The default version is IPv4.
- **Protocol**: Select a protocol profile for your filtering rule. TCP/UDP is most commonly used.
- **Source IP address[/prefix length]**: Enter the source IP address of a LAN side host to control incoming traffic.
- **Source Port (port or port:port):** Enter the source port number of a LAN side host to block.
- **Destination IP address[/prefix length]**: Enter the destination IP address of a LAN side host.
- **Destination Port (port or port:port)**: Enter the destination host port of a LAN side host.

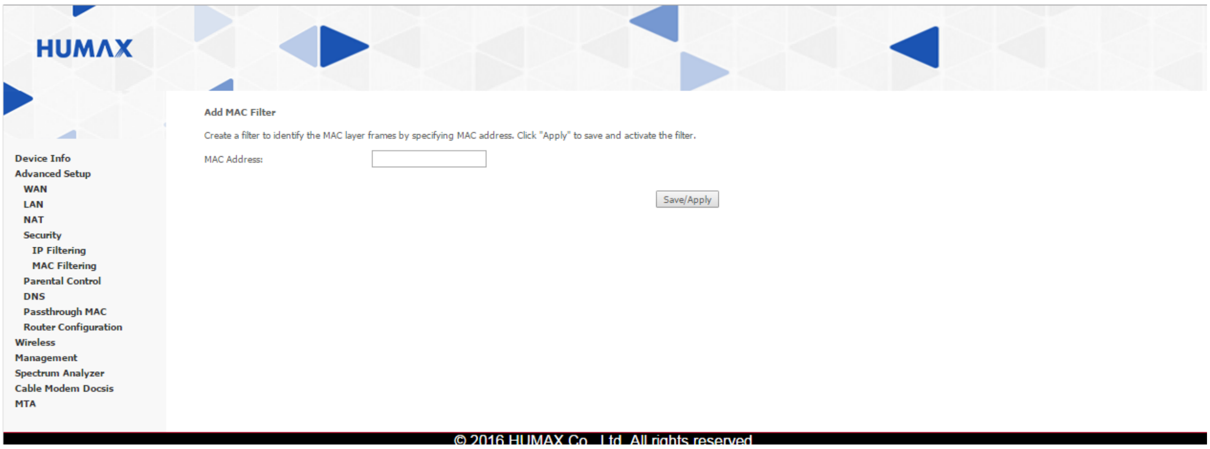
Select WAN/LAN interfaces to apply the filtering rules. Check one or more options from **Select All**, **wan-ip-interface/wanbridge** and **cpe-lan-ip-interface/br0**.

Click **Apply/Save** to save your changes.

Advanced Setup → Security → MAC Filtering

You can prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC address.

This is useful in that the MAC address of a specific NIC card never changes, unlike its IP address which can be assigned via DHCP server or hardcoded to various addresses over time.



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying MAC address. Click "Apply" to save and activate the filter.

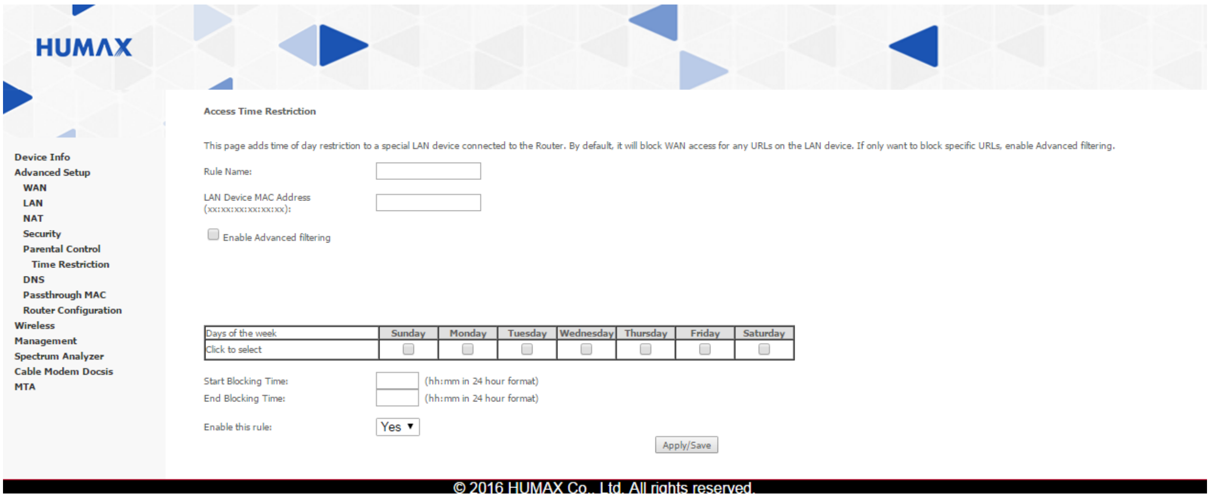
MAC Address:

Enter the MAC address to block the wireless client to access your PC.

Parental Control

Advanced Setup → Parental Control → Time Restriction

You can restrict Internet access on a LAN host by LAN host basis. The time restriction features are set on each MAC address for individual LAN hosts.



Access Time Restriction

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.

Rule Name:

LAN Device MAC Address (xx:xx:xx:xx:xx:xx):

□ Enable Advanced filtering

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

Start Blocking Time: (hh:mm in 24 hour format)
End Blocking Time: (hh:mm in 24 hour format)

Enable this rule: Yes ▾

© 2016 HUMAX Co., Ltd. All rights reserved.

- **Rule Name:** Enter a unique name for this restriction.

- **LAN Device MAC Address:** Enter the MAC address of your client network device to restrict access to the Internet.

- **Enable Advanced filtering:** Check to set more specific options. The following menus will be shown.

  Blocked URL keyword: Enter a keyword to always block a web site with a certain word.
  Protocol: Select a protocol from **TCP, UDP** or **BOTH.**
  Start Port/End Port: Enter the port range to restrict access to the Internet.

- **Days of the week:** Check the days and enter the time to restrict access to the Internet.
- **Start Blocking Time/End Blocking Time:** Enter the time range to restrict the LAN device from access to the Internet.

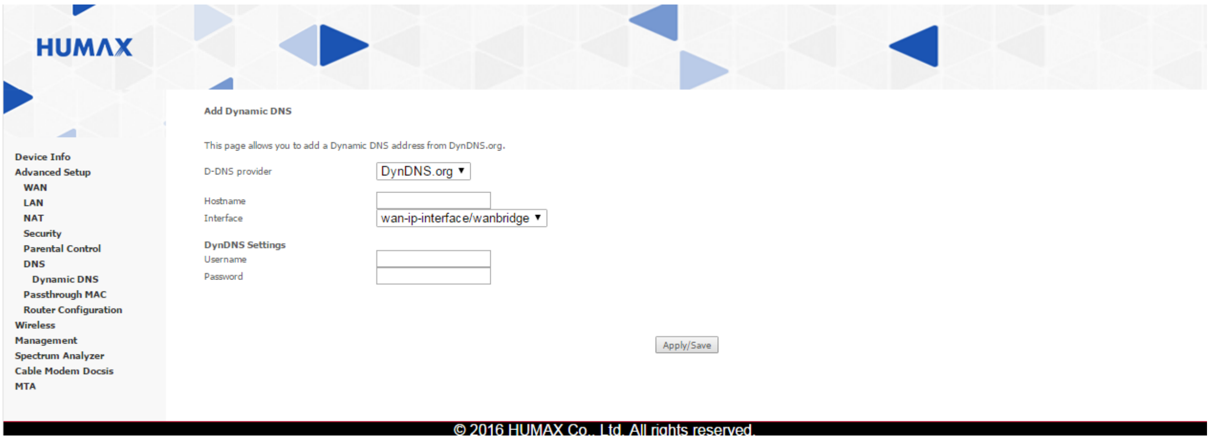
- **Enable this rule:** Select **Yes** to activate the restriction rule.

Click **Apply/Save** to save your changes.

DNS Setup

Advanced Setup → DNS → Dynamic DNS

Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, predefined host name so that the host can be easily contacted by other hosts on the Internet even if its IP address changes. Your product supports a dynamic DNS client compatible with the Dynamic DNS service.



Add Dynamic DNS

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

D-DNS provider: DynDNS.org ▾

Hostname:

Interface: wan-ip-interface/wanbridge ▾

DynDNS Settings

Username:

Password:

© 2016 HUMAX Co., Ltd. All rights reserved.

How to activate DDNS client

1. Go *http://www.dyndns.com* or *http://www.noip.com* and create an account for the Dynamic DNS service.

- Log into DynDNS with username and password.
- Go to My Account > My Services > Add Host Services.
- Type in the host name for your server and select dynamic DNS domain to assign your host.
- Check the retry interval at which the residential gateway tries repeatedly to contact the domain name server.
- Check your host's current IP address. This is the WAN IP address that has been assigned to your router during provisioning.

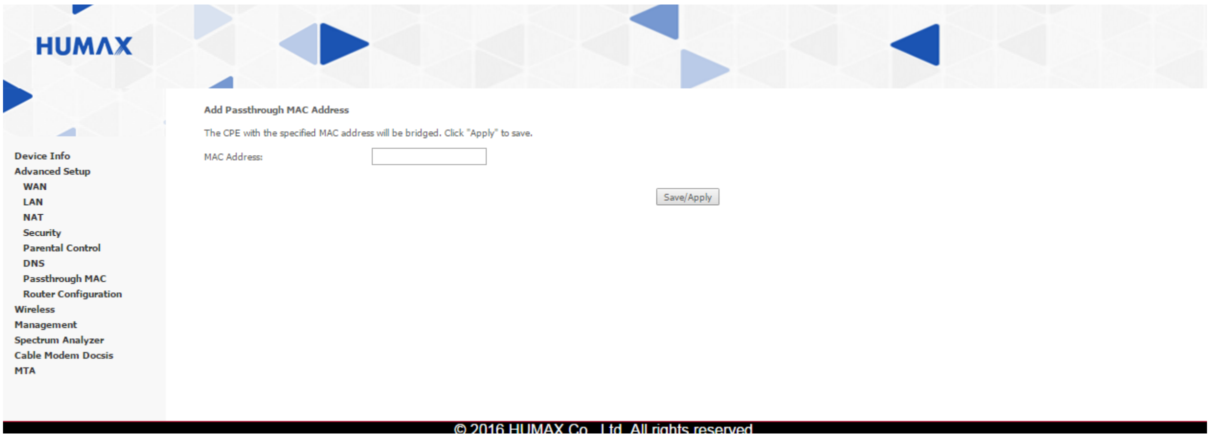
2. On this Dynamic DNS page, select **DynDNS.org** from the D-DNS provider to enable the service, enter your account information, and click **Apply/Save**.

3. The DDNS client will notify the DDNS service whenever the WAN IP address changes so that your chosen host name will be resolved properly by inquiring hosts.

Passthrough MAC

Advanced Setup → Passthrough MAC

You can add or edit the passthrough MAC address.



Add Passthrough MAC Address

The CPE with the specified MAC address will be bridged. Click "Apply" to save.

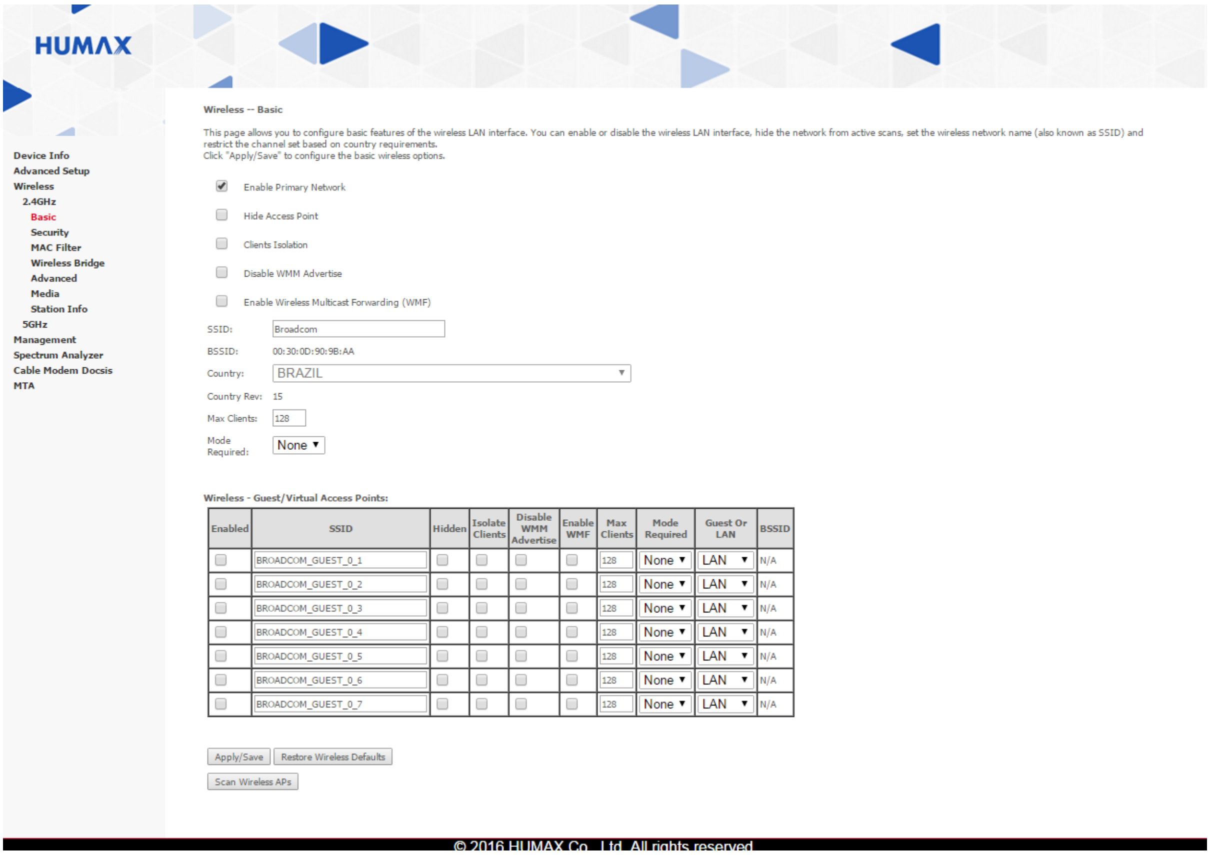
MAC Address:

Enter the MAC address to get a public IP address.

Basic Setup

Wireless → 2.4GHz → Basic

You can configure basic features of the Wi-Fi LAN interface. You can enable or disable the Wi-Fi LAN interface, hide the network from active scans, set the Wi-Fi network name (also known as SSID) and restrict the channel set based on country requirements.



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)

SSID: Broadcom

BSSID: 00:30:0D:90:9B:AA

Country: BRAZIL

Country Rev: 15

Max Clients: 128

Mode Required: None

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	Mode Required	Guest Or LAN	BSSID
□	BROADCOM_GUEST_0_1	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_2	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_3	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_4	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_5	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_6	□	□	□	□	128	None	LAN	N/A
□	BROADCOM_GUEST_0_7	□	□	□	□	128	None	LAN	N/A

© 2016 HUMAX Co., Ltd. All rights reserved

- **Enable Primary Network:** Check to enable the gateway's Wi-Fi radio.
- **Hide Access Point:** Check to hide Access Point SSID.
- **Client Isolation:** Check to prevent LAN client devices from communicating with one another on the wireless network.
- **Disable WMM Advertise:** Check to stop the wireless from advertising Wireless Multimedia (WMM) functionality. WMM provides basic Quality of Service (QOS) for applications.
- **Enable Wireless Multicast Forwarding**: Check to enable Wireless Multicast Forwarding (WMF). Forwards multicast traffic across wireless clients when enabled.
- **SSID:** Enter the Wi-Fi Service Set Identifier (SSID) here.
- **BSSID:** Enter the basic service set identification (BSSID). Provides the MAC address assigned to the wireless router.
- **Country**: Displays the country where the product is deployed.
- **Country Rev**: Displays the revision version.
- **Max Clients**: Enter the maximum number of clients that can access the router wirelessly.

- **More Required**: Select an option to allow access from wireless network devices.
- **Wireless-Guest/Virtual Access Points**

Enabled: Check to enable a virtual wireless access point for guest access.

SSID: Enter your desired wireless Service Set Identifier (SSID) here.

Hidden: Check this option to hide the SSID from being broadcasted publicly.

Isolate Clients: Check to prevent client PC's from communicating with one another.

Disable WMM Advertise: Check to stop the wireless from advertising Wireless Multimedia (WMM) functionality.

Enable WMF: Check to enable Wireless Multicast Forwarding (WMF).

Max Clients: Enter the maximum number of clients that can access the router wirelessly.

Mode Required: Select an option to allow access from wireless network devices.

Guest Or LAN: Select an option to isolate WLAN for host and guest.

BSSID: Enter the basic service set identification (BSSID). Provides the MAC address assigned to the wireless router.

Click **Apply/Save** to save your changes.

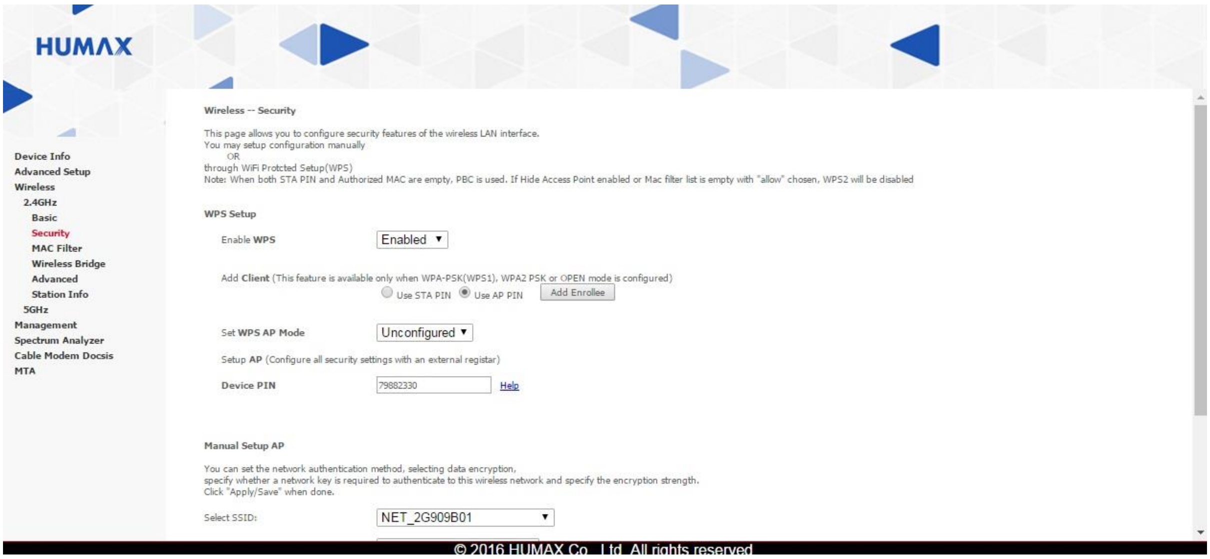
Click **Restore Wireless Defaults** to clear all settings and reset them to the default values

Click **Scan Wireless Aps** to force the modem access point to scan for other AP's within receive range.

Security Setup

Wireless → 2.4GHz → Security

You can configure the security features on your wireless LAN interface.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted 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: Enabled ▾

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)
○ Use STA PIN ● Use AP PIN [Add Enrollee]

Set WPS AP Mode: Unconfigured ▾

Setup AP (Configure all security settings with an external registar)

Device PIN: 79882330 Help

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: NET_2G909B01 ▾

© 2016 HUMAX Co., Ltd. All rights reserved

WPS Setup

- **Enable WPS:** Select **Enabled** to use Wi-Fi protected setup.
- **Use STA PIN/Use AP PIN:** Select how the WPS PIN is generated.
- **Set Authorized Station MAC:** Enter the MAC address of the client device.
- **Set WPS AP Mode:** Select **Configured** to assign an address.
- **Device PIN:** Displays the device pin generated by AP.

Manual Setup AP

- **Select SSID:** Select an SSID to apply the security configuration.
- **Network Authentication:** Select the security type.

WPA2: An advanced form of WPA that is more secure. This is the Enterprise mode of WPA2 which requires the use of a RADIUS server. WPA2 and WPA may be used at the same time to provide backward compatibility with devices that do not support WPA2.

WPA2PSK: The Pre-Shared Key mode of WPA2, also known as WPA2 Personal. WPA2 and WPA2-PSK cannot be used at the same time. WPA2-PSK and WPA-PSK may be used at the same time to provide backward compatibility with devices that do not support WPA2.

Mixed WPA2/WPA: WPA and WPA2 mixed mode operation permits the coexistence of WPA and WPA2 clients on a common SSID. During WPA and WPA2 mixed mode, the Access Point (AP) advertises the encryption ciphers (TKIP, CCMP, other) that are available for use. The client selects the encryption cipher it would like to use and the selected encryption cipher is used for encryption between the client and AP once it is selected by the client.

WPAPSK: The Pre-Shared Key mode of the WPA algorithm which does not require use of a

RADIUS server. This is also known as WPA Personal. WPA and WPA-PSK cannot be used at the same time.

WPAPSK/WPA2PSK: The Pre-Shared Key mode of the WPA algorithm which does not require use of a RADIUS server. This is also known as WPA Personal. WPA and WPA-PSK cannot be used at the same time.

The Pre-Shared Key mode of WPA2, also known as WPA2 Personal.

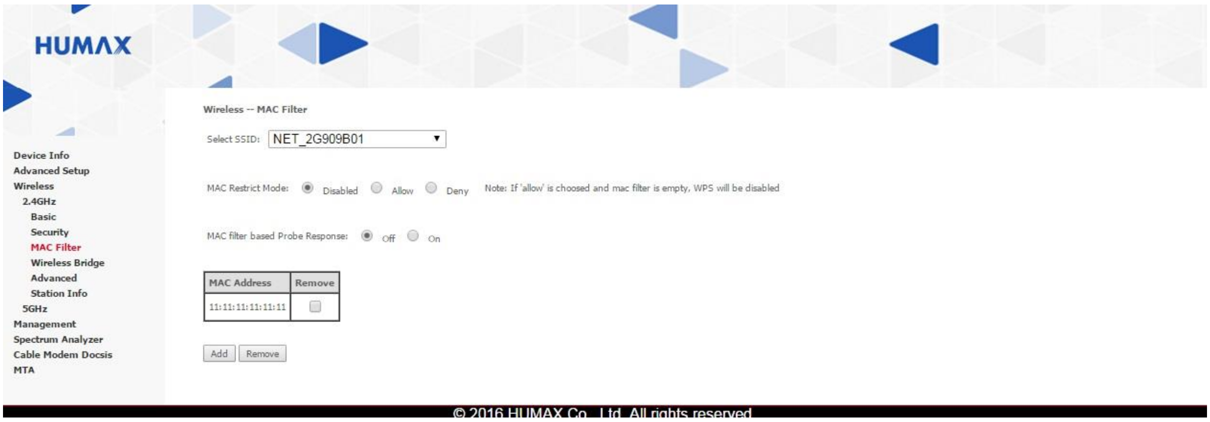
WPA2 and WPA2-PSK cannot be used at the same time. WPA2-PSK and WPA-PSK may be used at the same time to provide backward compatibility with devices that do not support WPA2.

- **Encryption Type**: Set the encryption mode when using any of the WPA authentication schemes.

MAC Filtering

Wireless → 2.4GHz → MAC Filter

You can add or edit MAC address to allow client devices on your Wi-Fi network.



Wireless -- MAC Filter

Select SSID: NET_2G909B01 ▾

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC filter based Probe Response: ● Off ○ On

MAC Address	Remove
11:11:11:11:11:11	□

© 2016 HUMAX Co., Ltd. All rights reserved

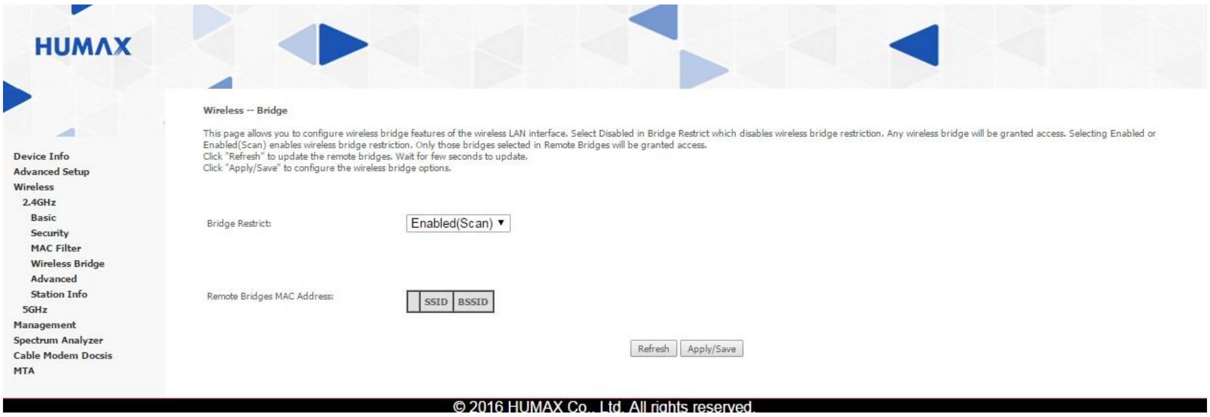
- **Select SSID**: Select an SSID to apply the MAC filtering rule.
- **MAC Restrict Mode**: Select a restriction mode.
  Disabled: Turns off MAC filtering.
  Allow: Permits access to a specified MAC address.
  Deny: Rejects access to a specified MAC address.
- **MAC filter based Probe Response**

Click **Add** to add a MAC address to the filtering list and them **Apply/Save** to save your changes. Click **Remove** to remove the client device from the list.

Wireless Bridge

Wireless → 2.4GHz → Wireless Bridge

You can configure the wireless bridge features of the wireless LAN interface.



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

Bridge Restrict: Enabled(Scan)

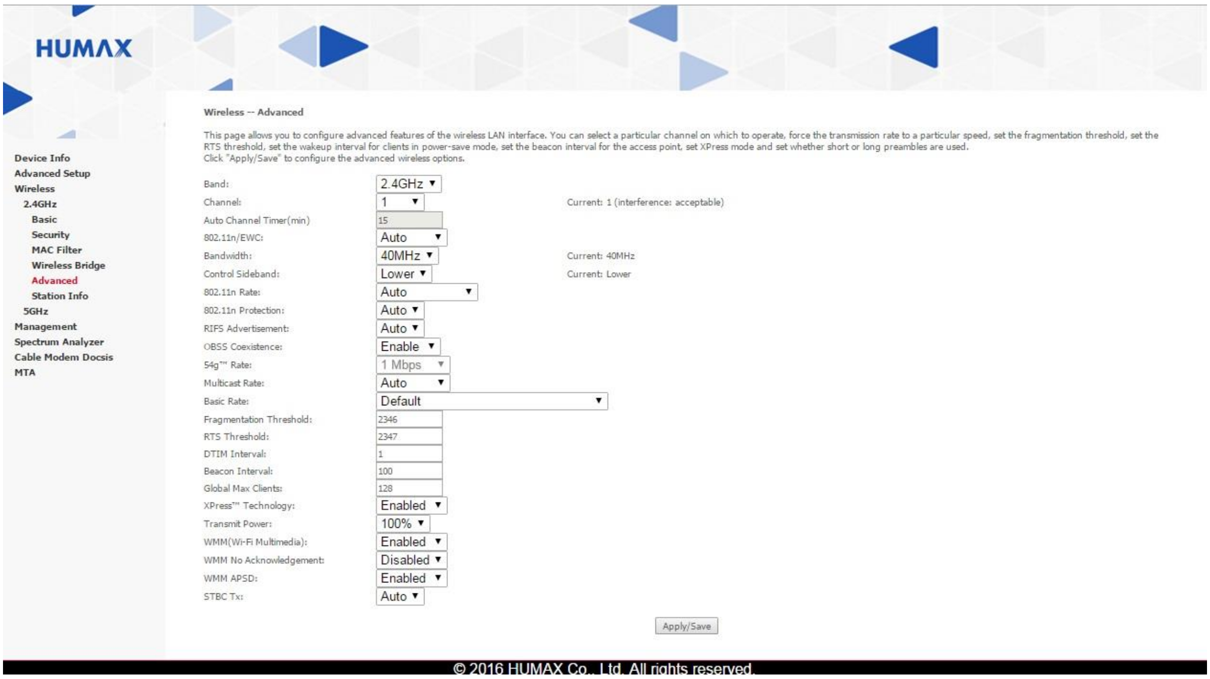
Remote Bridges MAC Address:

- **Bridge Restrict:** Select an option to turn the wireless bridge restriction on or off.
  Disabled: Allows all of the wireless bridges on the same network to communicate with each other.
  Enabled/Enabled (Scan): Turns on the wireless bridge restriction. Only those bridges selected in the remote bridges list will be allowed.
  Click **Refresh** to update the station list when the bridge restriction is enabled.
- **Remote Bridge MAC Address:** Enter a MAC address of the remote bridges. You can enter up to 4 bridges.

Advanced Setup

Wireless → 2.4GHz → Advanced

You can configure advanced features of the wireless LAN interface.



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:	2.4GHz	
Channel:	1	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	15	
802.11n/EWC:	Auto	
Bandwidth:	40MHz	Current: 40MHz
Control Sideband:	Lower	Current: Lower
802.11n Rate:	Auto	
802.11n Protection:	Auto	
RIFS Advertisement:	Auto	
OBSS Coexistence:	Enable	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	128	
XPress™ Technology:	Enabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	
STBC Tx:	Auto	

© 2016 HUMAX Co., Ltd. All rights reserved.

- **Band:** The frequency band is set to 2.4 GHz for compatibility with IEEE 802.11x standards.
- **Channel**: Select the Wi-Fi channel from 1 to 9 or Auto.
- **Auto Channel Timer(min)**: Set the frequency with which the gateway scans channels for interference. If a threshold of inference is detected, a new channel will be selected automatically from 0 to 65535 minutes.
- **802.11n/EWC**: Select **Auto** to activate IEEE 802.11n, or **Disabled** to inactivate.
- **Bandwidth**: Select the bandwidth from 20MHz or 40MHz.
- **Control Sideband**: Select the appropriate sideband to minimize RF interference from adjacent channels and maximize the throughput. This option is available only in 40MHz mode.
- **802.11n Rate:** Select the physical transmission rate.
- **802.11n Protection**: Select **Auto** to maximize the security. Select **Off** to maximize the throughput.
- **RIFS Advertisement**: Select **Auto** to enable RIFS advertisement, or **Off** to disable it. This function improves performance by reducing the amount of dead time required between OFDM transmission.
- **OBSS Coexistence**: Select **Enable** to prevent overlapping in 20 MHz and 40MHz frequencies. OBSS coexistence refers to the ability of the AP to support 20 MHz devices within 40 MHz channels. It also allows the AP to better deal with nearby 20 MHz devices that are interfering with part of its 40 MHz channel.
- **54g™ Rate:** Select a fixed data rate from the list. This feature is activated only when **802.11n Rate** is set to **54g Rate**.

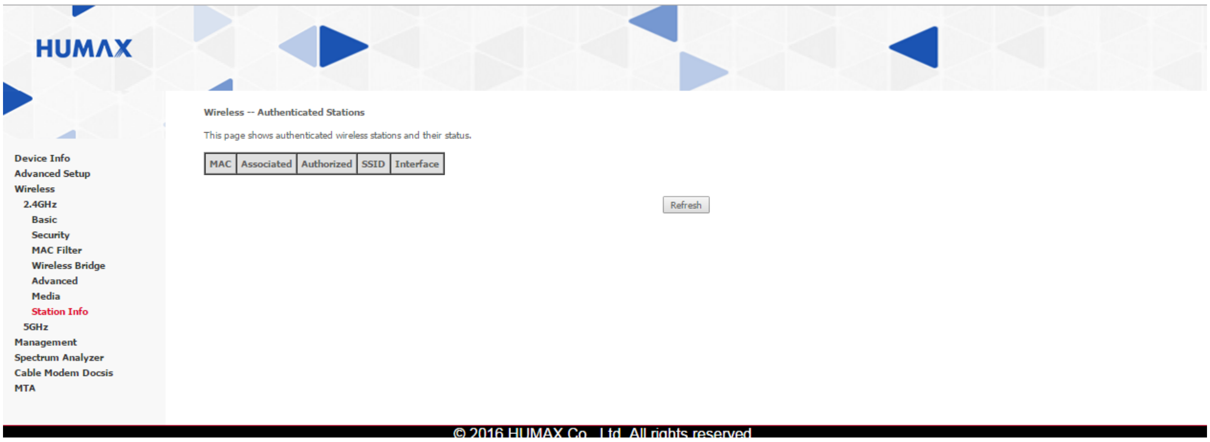
- **Multicast Rate:** Select a packet transmission rate for multicast.
- **Basic Rate:** Select a basic transmission rate.
- **Fragmentation Threshold:** Enter a fragmentation threshold. Packets exceeding this threshold are fragmented into packets no larger than the threshold before packet transmission.
- **RTS Threshold** Enter the request to send (RTS) packet size. Packets exceeding this threshold cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission. The threshold is off when using the default setting of 2347.
- **DTIM Interval:** Enter the wakeup interval for clients in power saving mode. When a client is running in power saving mode, lower values provide higher performance but result in decreased client battery life, while higher values provide lower performance but result in increased client battery life.
- **Beacon Interval:** Enter the time interval between beacon transmissions to synchronize wireless network.
- **Global Max Clients**: Enter the maximum number of client devices that are connectable to the router.
- **XPress™ Technology:** Select **Enabled** to use XPress™ Technology which specifies block frame acknowledgement for 802.11g frames. This feature may improve throughput but cause problems.
- **Transmit Power:** Select the transmission power from the list.
- **WMM (Wi-Fi Multimedia)**: Select **Enabled** to allow multimedia services such as audio, video and voice to get higher priority.
- **WMM No Acknowledgement:** Select **Enabled** to activate this function. WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.
- **WMM APSD:** Select **Enabled** to use automatic power save delivery (APSD) to save power consumption. This feature is activated only when **WMM** is set to **Disabled**.
- **STBC Tx:** Set the STBC state to **Auto**, **On** or **Off.** STBC refers to the space-time block code transmitter to transmit multiple copies of a data stream.

Click **Apply/Save** to save your changes.

Station Information

Wireless → 2.4GHz → Station Info

You can see the authenticated wireless stations and their status.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

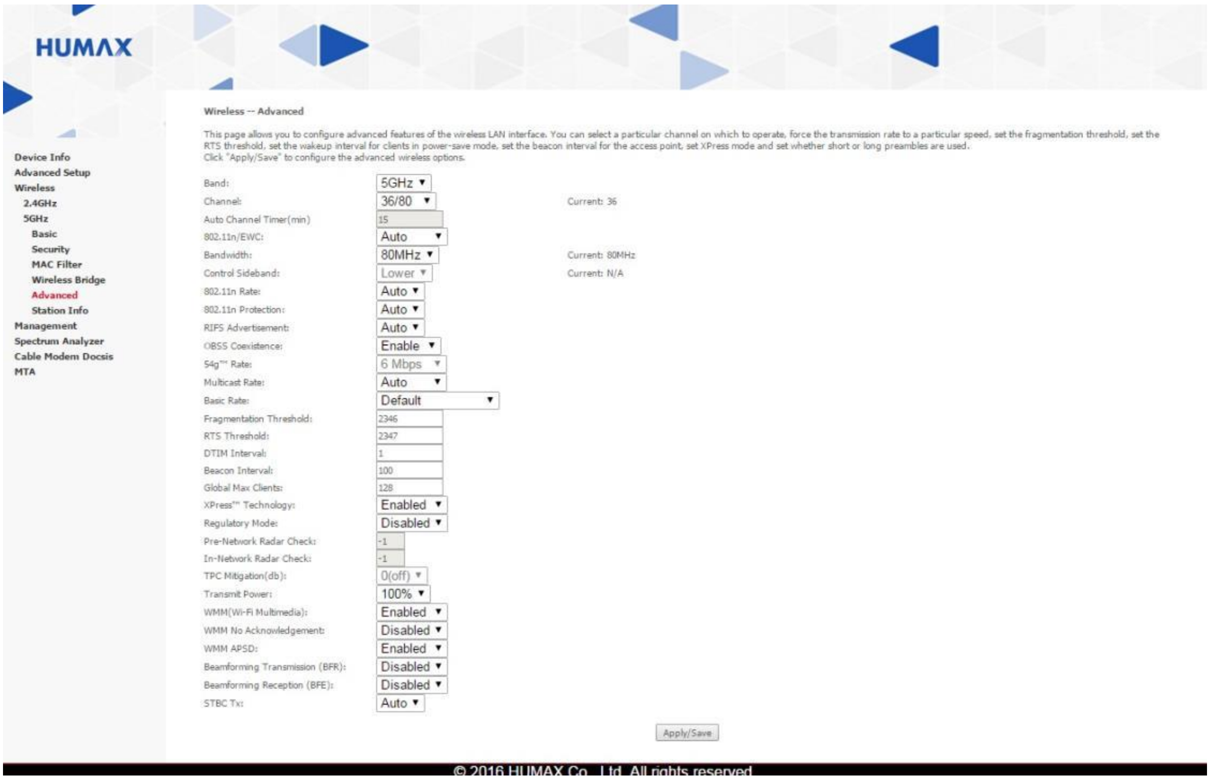
© 2016 HUMAX Co., Ltd. All rights reserved

5GHz Setup

Wireless → 5GHz

You can configure various features of the wireless network on 5GHz in the same manner as on 2.4GHz. You can refer to the wireless network settings on 2.4GHz, so detailed explanation will be omitted.

Wireless → 5GHz → Advanced



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/EWC:	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	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	128	
XPress™ Technology:	Enabled	
Regulatory Mode:	Disabled	
Pre-Network Radar Check:	-1	
In-Network Radar Check:	-1	
TPC Mitigation(db):	0(off)	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	
Beamforming Transmission (BFR):	Disabled	
Beamforming Reception (BFE):	Disabled	
STBC Tx:	Auto	

© 2016 HUMAX Co., Ltd. All rights reserved

- **Band:** The frequency band is set to 5GHz for compatibility with IEEE 802.11x standards.

- **Channel**: Select the Wi-Fi channel from the list.

- **Bandwidth**: Select the bandwidth from 20MHz, 40MHz or 80MHz.

- **Control Sideband**: Select the appropriate sideband to minimize RF interference from adjacent channels and maximize the throughput. This option is available only in 40MHz mode.

- **Basic Rate:** Select a basic transmission rate.

- **Regulatory Mode:** Select either 802.11d or 802.11h modes of operation.

  802.11d allows stations to operate in any country without reconfiguration.

  802.11h allows below three options to be activated and the country code information to be broadcast in the beacons.

These are amendments to the 802.11 specifications for solving interference issues with other transmission systems such as satellite or radar, and also transmission requirements in different parts of the world.

- **Pre-Network Radar Check:** Enter the number of seconds to check for radar on a channel before establishing a network.

- **In-Network Radar Check:** Enter the number of seconds to check for radar when switching to a new channel after a network has been established.

- **TPC Mitigation(db):** Select the transmit power control (TPC) mitigation to automatically reduce the transmission power when other networks are within the range.

- **Beamforming Transmission (BFR):**

- **Beamforming Reception (BFE):**

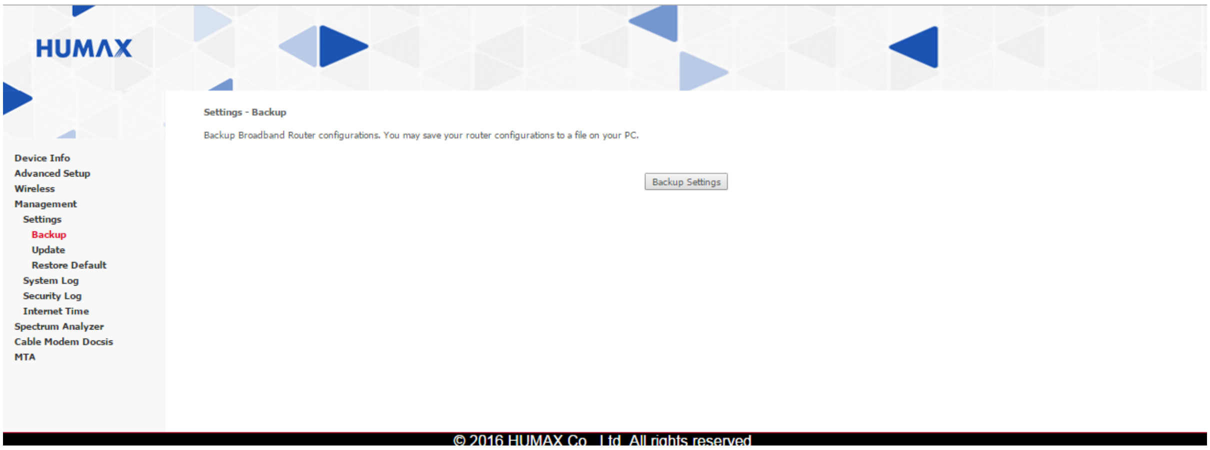
- **STBC Tx**: Select **On** to set the space-time block codes (STBCs) for the transmitting antenna.

Click **Apply/Save** to save your changes.

Backup

Management → Settings → Backup

You can save the current broadband router configuration settings to your local PC. You can then later restore these settings if you need restore a particular configuration, or to recover from changes you may have made.



Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

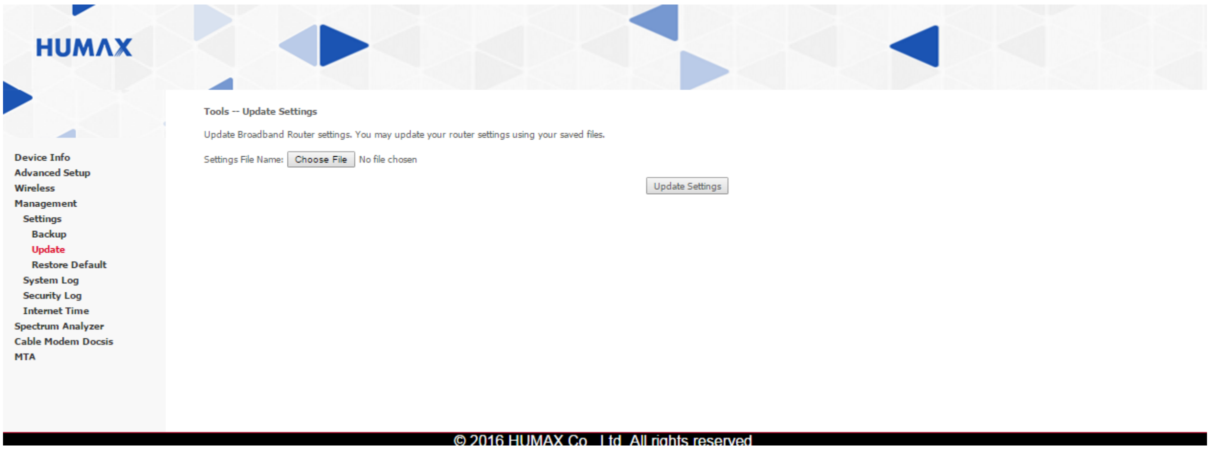
© 2016 HUMAX Co., Ltd. All rights reserved

Click **BackupSettings** to save the current configuration.

Update

Management → Settings → Update

You can restore previously backed-up router settings from your local PC.



Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: Choose File No file chosen

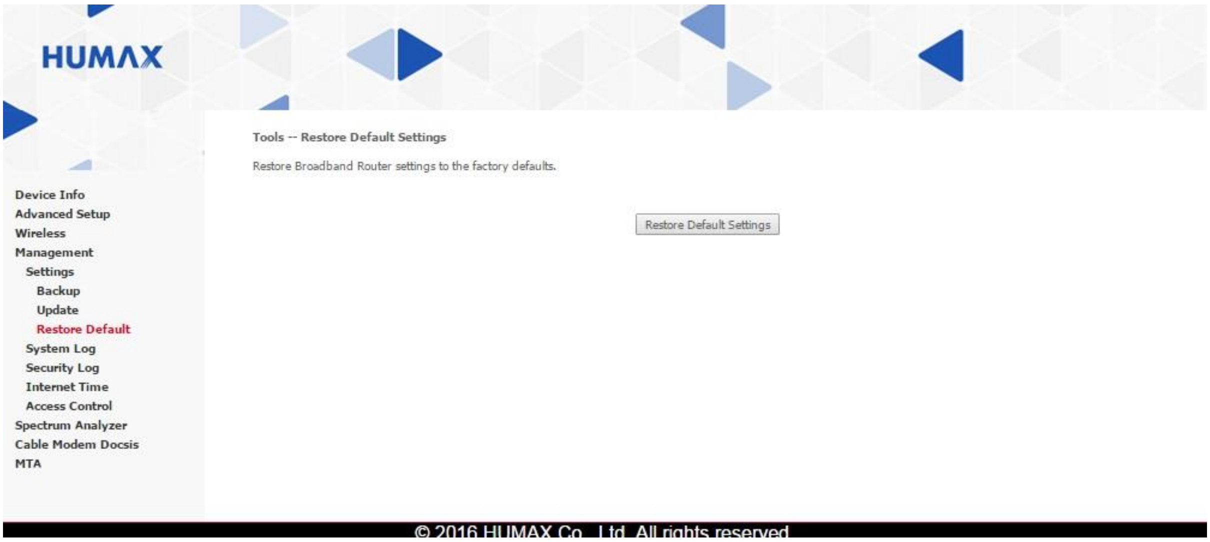
Click **Choose File** and browse the file explorer on your PC to upload a file.

Note: Once a file upload is complete, the broadband router will restart. This process may take about 2 minutes.

Restore Default

Management → Settings → Restore Default

You can restore the broadband router to the factory default settings.



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

© 2016 HUMAX Co., Ltd. All rights reserved.

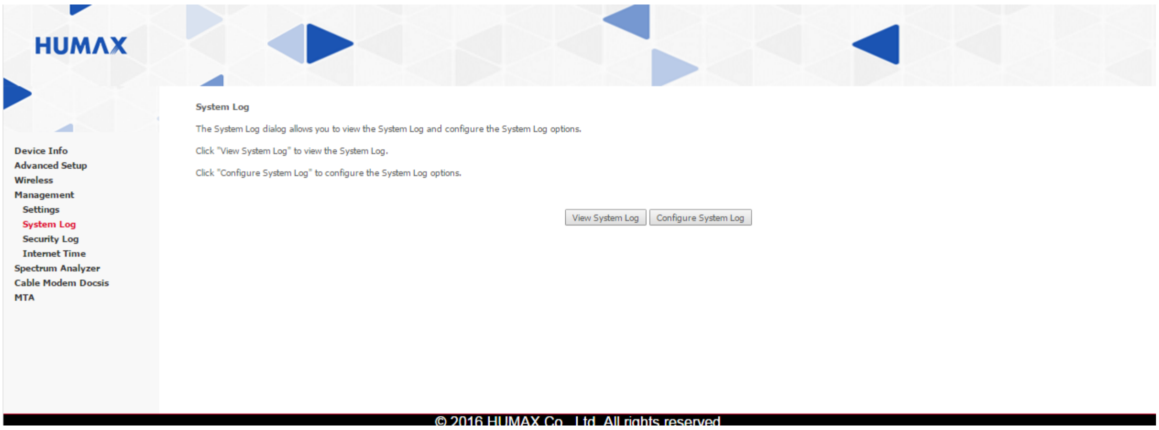
Click **Restore Default Settings** to reset the router to the factory default settings.

Warning: Once you restore the factory defaults, all user configured data will be reset.

System Log

Management → System Log

You can see a history of error conditions and other events encountered by your gateway.



System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

© 2016 HUMAX Co., Ltd. All rights reserved.

Click **View System Log** to see the system log.

Setting logging options

Click **Configure System Log** to edit the system log.

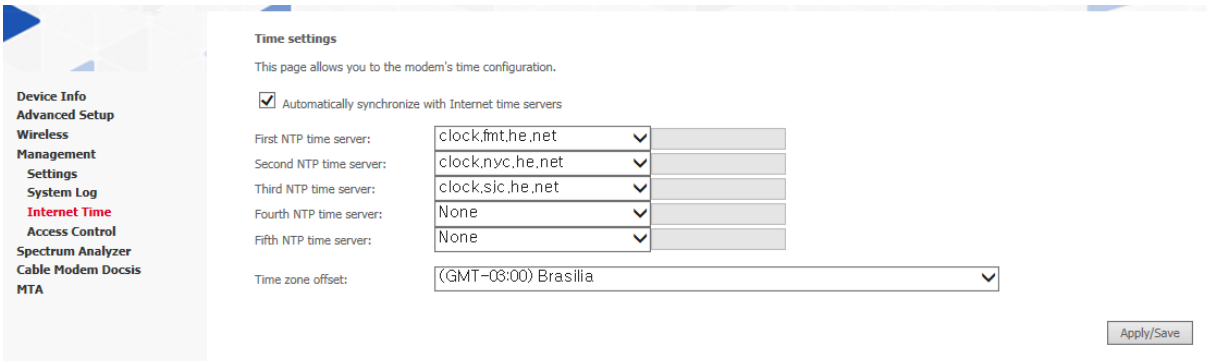
- **Log:** Select **Enable** to turn logging off or on.
- **Log Level:** Select an error option from the list. The options are listed in order from least to most verbose.
- **Display Level:** Select an error option from the list. The options are listed in order from least to most verbose.
- **Mode:** Select **Remote** to send log events to the specified IP address and UDP port of the remote syslog server, or **Local** to record events in the gateway's local memory. In **Remote** mode, you can enter the server IP address and UDP port.

Click **Apply/Save** to save your changes.

Time Setup

Management → Internet Time

You can set the time to synchronize the clock I your router with reliable external clocking servers.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: clock.fmt.he.net

Second NTP time server: clock.nyc.he.net

Third NTP time server: clock.sjc.he.net

Fourth NTP time server: None

Fifth NTP time server: None

Time zone offset: (GMT-03:00) Brasilia

Automatically synchronize with Internet time servers: Check to enable the network time protocol.

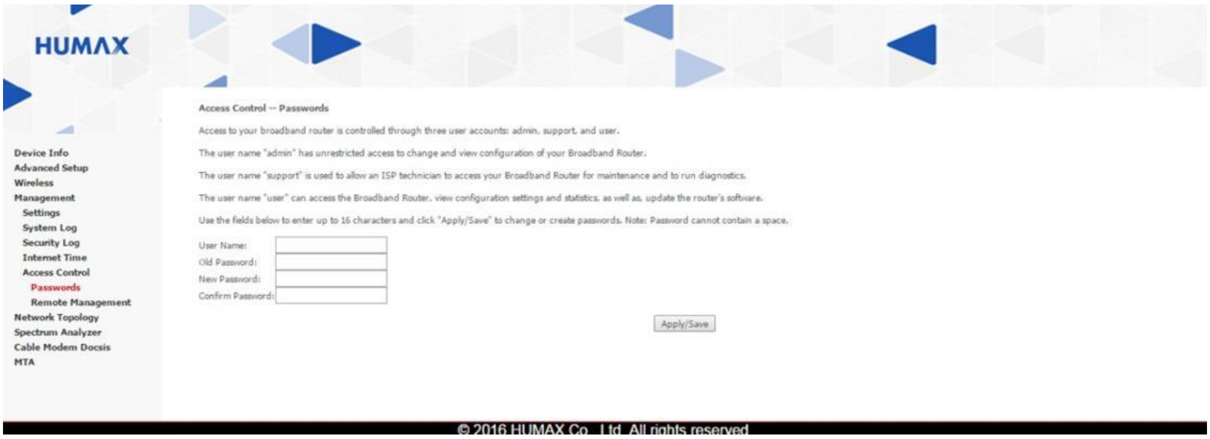
- **First to Fifth NTP time server:** Select or enter your own NTP servers.
- **Time zone offset:** Select the time zone to automatically synchronize the system clock using a network time protocol (NTP) server.

Click **Apply/Save** to save your changes.

Password Change

Management → Access Control → Passwords

You can set or change your password to prevent unauthorized access to the configuration page.



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 "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

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:

© 2016 HUMAX Co., Ltd. All rights reserved

- **User Name**: Enter a username.
- **Old Password**: Enter the current password.
- **New Password**: Enter a new password to be changed.
- **Confirm Password**: Enter the new password again.

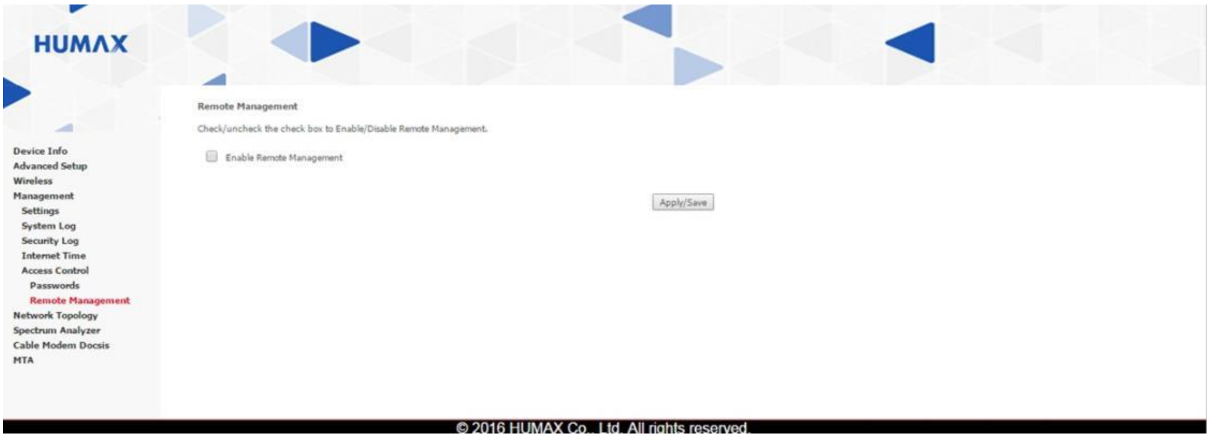
Note: The default username and password are located at the bottom of your product.

Click **Apply/Save** to save your changes.

Remote Management

Management → Access Control → Remote Management

You can allow a user on the Internet to remotely manage your router.



Remote Management

Check/uncheck the check box to Enable/Disable Remote Management.

□ Enable Remote Management

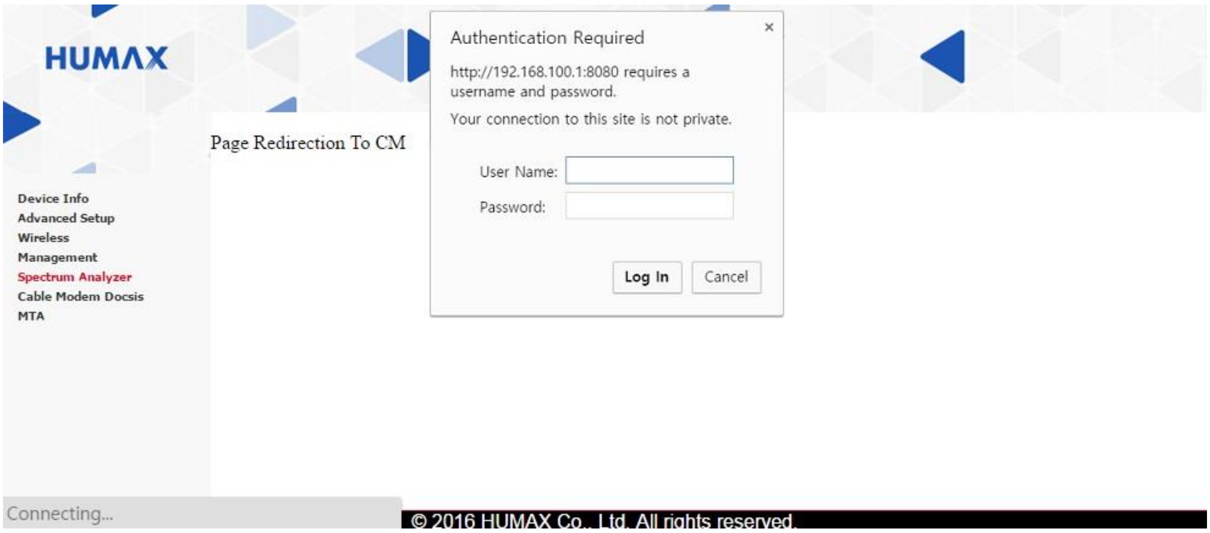
© 2016 HUMAX Co., Ltd. All rights reserved.

Enable Remote Management: Check to allow remote management. To access your router remotely from a web browser, enter the *WAN IP address:8080*.

Spectrum Analyzer

Spectrum Analyzer

You can see the magnitude of an input signal versus frequency within the full frequency range of your router.



Authentication Required

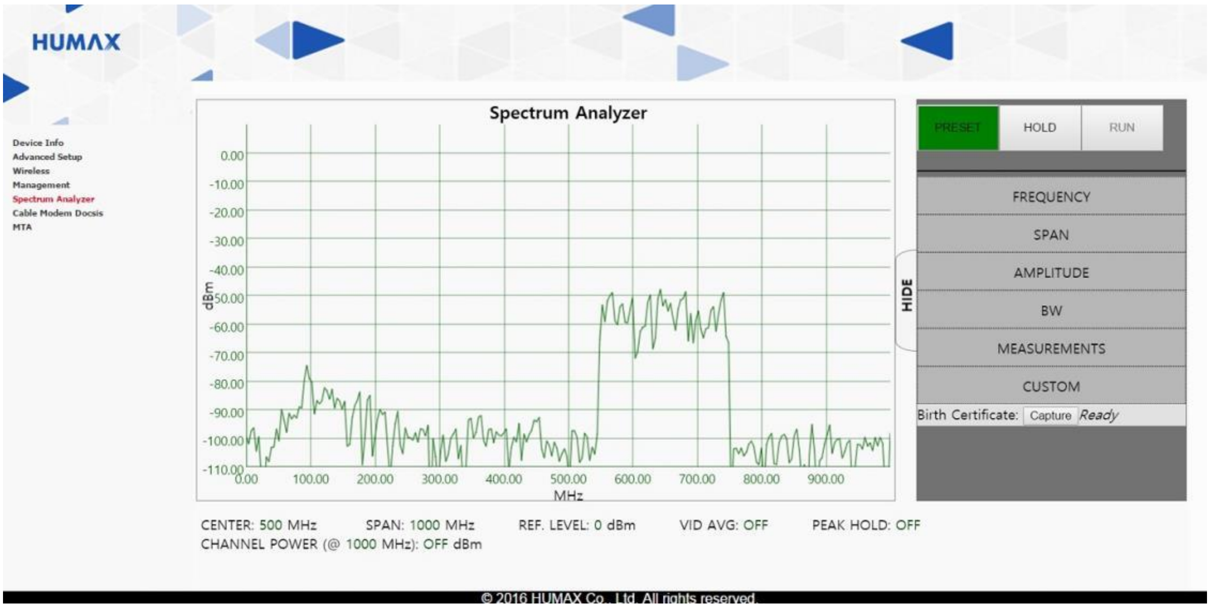
http://192.168.100.1:8080 requires a username and password.

Your connection to this site is not private.

User Name:

Password:

Enter the user name and password to log in, then the spectrum analyzer will appear.



CENTER: 500 MHz SPAN: 1000 MHz REF. LEVEL: 0 dBm VID AVG: OFF PEAK HOLD: OFF

CHANNEL POWER (@ 1000 MHz): OFF dBm

Click **PRESET**, **HOLD** or **RUN** to set the spectrum monitoring. **PRESET** restores to the default settings, **HOLD** pauses spectrum monitoring and **RUN** starts spectrum monitoring.

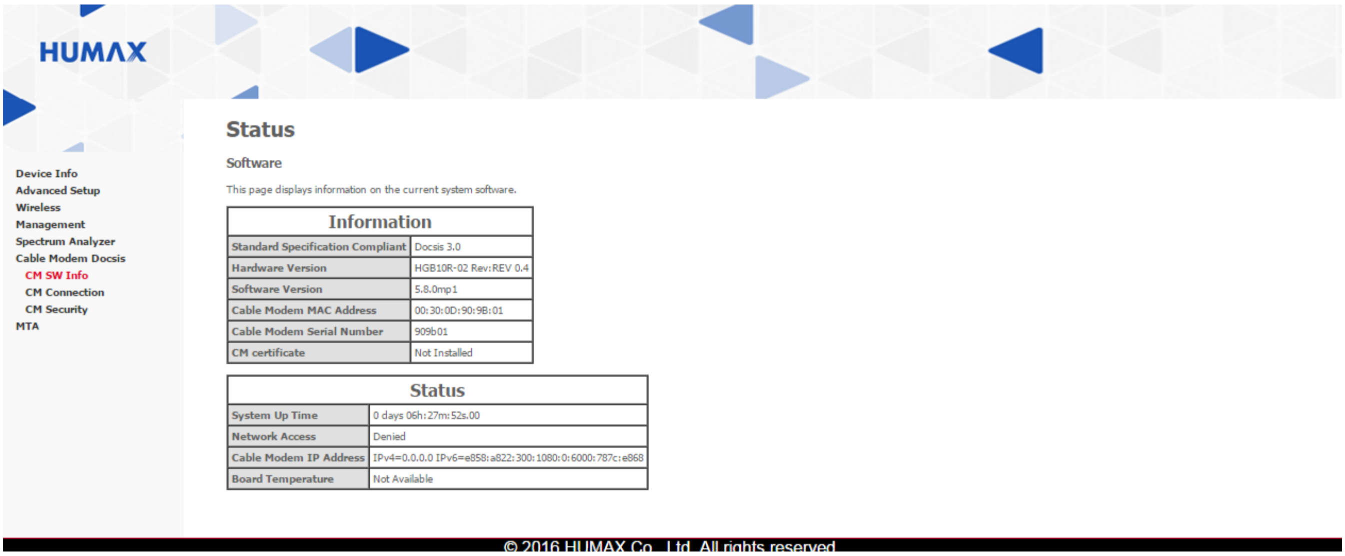
- **FREQUENCY:** Enter the frequency and click **MHz** to apply.
- **SPAN:** Enter the frequency span from the center frequency and click **MHz** to apply.
- **AMPLITUDE:** Enter the amplitude and click **dBm** to apply.

- **BW:** Select an option to display bandwidth. **Vid Avg** displays the average value and **Peak Hold** displays the maximum peak value.
- **MEASUREMENTS:** Select an option to display the channel power or not.

Cable Modem Software Information

Cable Modem Docsis → CM SW Info

You can see the information on the current system.



Status

Software

This page displays information on the current system software.

Information	
Standard Specification Compliant	Docsis 3.0
Hardware Version	HGB10R-02 Rev:REV 0.4
Software Version	5.8.0mp1
Cable Modem MAC Address	00:30:0D:90:9B:01
Cable Modem Serial Number	909b01
CM certificate	Not Installed

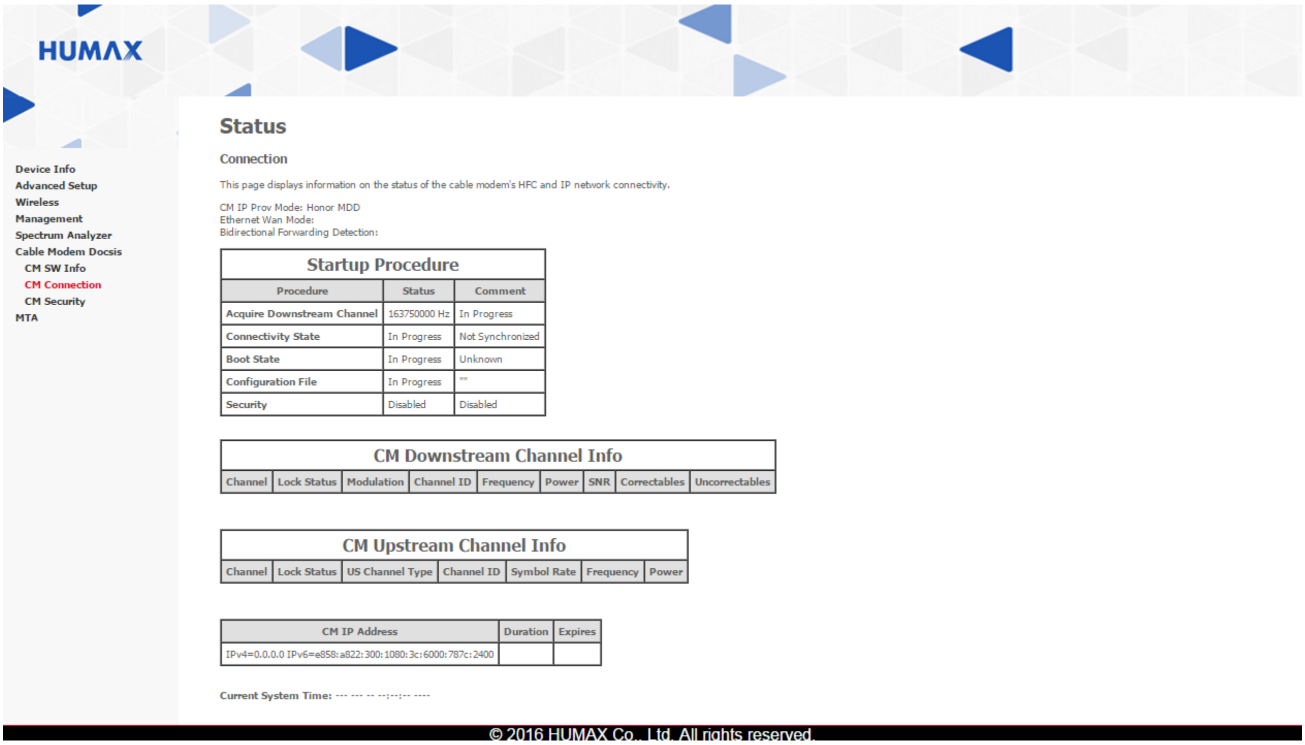
Status	
System Up Time	0 days 06h:27m:52s.00
Network Access	Denied
Cable Modem IP Address	IPv4=0.0.0.0 IPv6=e858:a822:300:1080:0:6000:787c:e868
Board Temperature	Not Available

© 2016 HUMAX Co., Ltd. All rights reserved.

Cable Modem Connection

Cable Modem Docsis → CM Connection

You can see the status information on the current network connectivity.



Status

Connection

This page displays information on the status of the cable modem's HFC and IP network connectivity.

CM IP Prov Mode: Honor MDD
Ethernet Wan Mode:
Bidirectional Forwarding Detection:

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	163750000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File	In Progress	""
Security	Disabled	Disabled

CM Downstream Channel Info

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables

CM Upstream Channel Info

Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power

CM IP Address	Duration	Expires
IPv4=0.0.0.0 IPv6=e858:a822:300:1080:3c:6000:787c:2400		

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

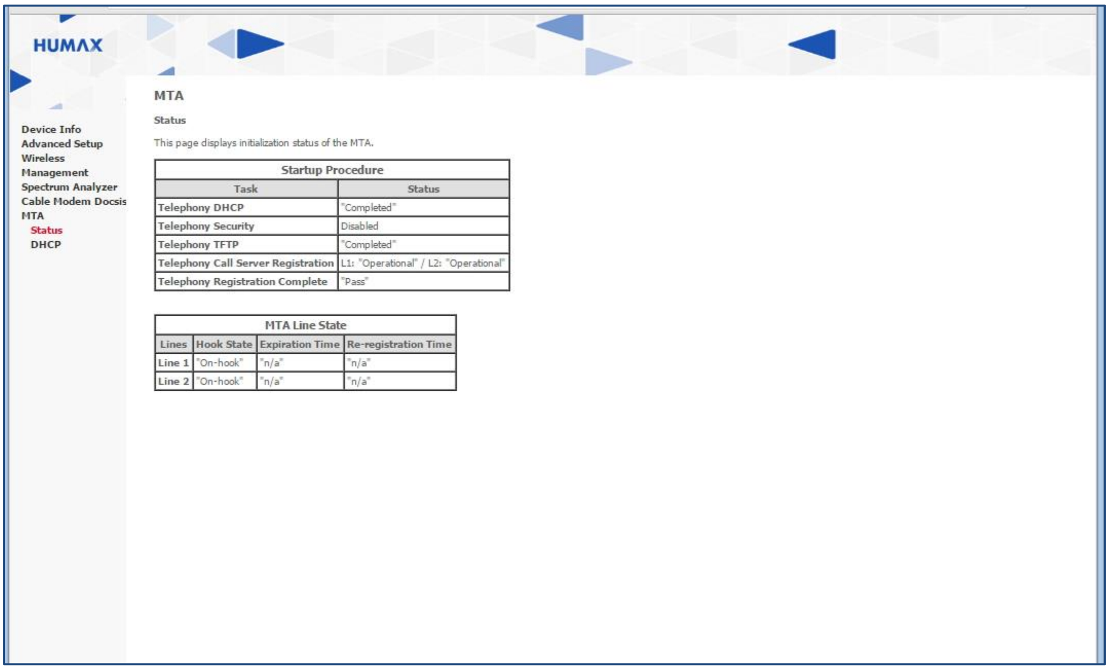
© 2016 HUMAX Co., Ltd. All rights reserved.

The Multimedia Terminal Adapter (MTA) in the router provides digital voice-over-IP (VoIP) services. You can make telephone calls over the Internet. Basic telephone functions, such as call waiting, three-way calling, voice mail and fax transmissions, are supported with this connection on the router. You can click any MTA submenus to view the status information for that option.

MTA Status

MTA → Status

You can see the current status of the embedded MTA. This page displays Registration/Provisioning and line states.



MTA

Status

This page displays initialization status of the MTA.

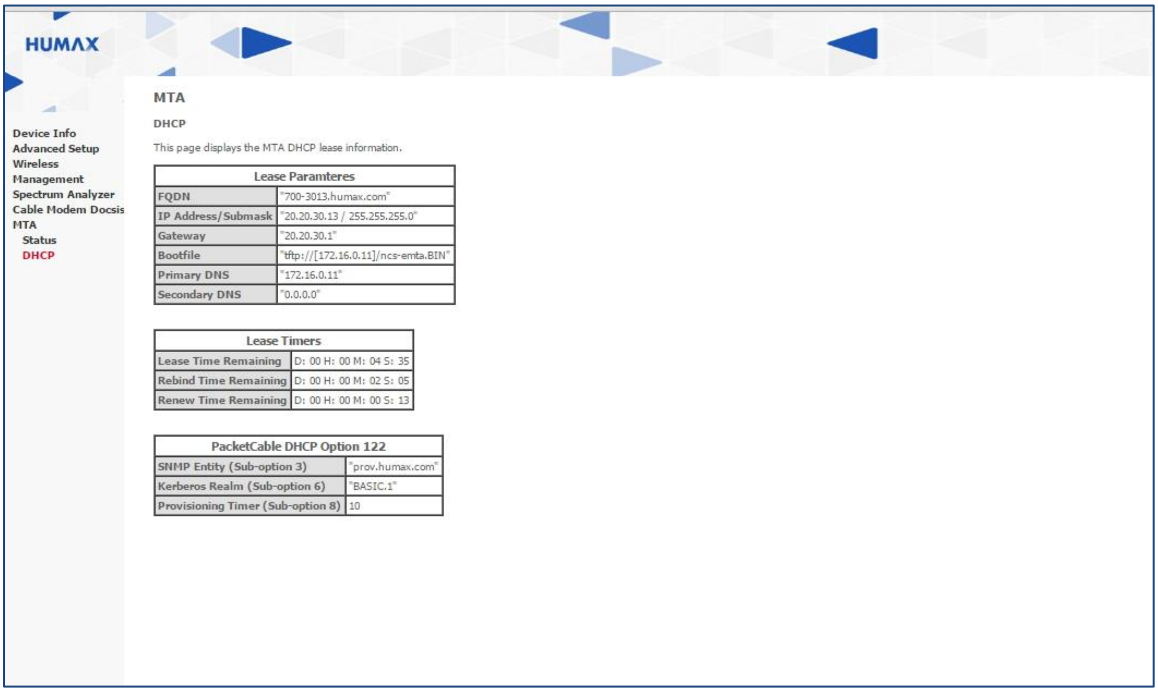
Startup Procedure	
Task	Status
Telephony DHCP	"Completed"
Telephony Security	Disabled
Telephony TFTP	"Completed"
Telephony Call Server Registration	L1: "Operational" / L2: "Operational"
Telephony Registration Complete	"Pass"

MTA Line State			
Lines	Hook State	Expiration Time	Re-registration Time
Line 1	"On-hook"	"n/a"	"n/a"
Line 2	"On-hook"	"n/a"	"n/a"

MTA DHCP Information

MTA → DHCP

You can see the MTA DHCP lease information.



MTA

DHCP

This page displays the MTA DHCP lease information.

Lease Paramteres	
FQDN	"700-3013.humax.com"
IP Address/Submask	"20.20.30.13 / 255.255.255.0"
Gateway	"20.20.30.1"
Bootfile	"tftp://[172.16.0.11]/ncs-emta.BIN"
Primary DNS	"172.16.0.11"
Secondary DNS	"0.0.0.0"

Lease Timers	
Lease Time Remaining	D: 00 H: 00 M: 04 S: 35
Rebind Time Remaining	D: 00 H: 00 M: 02 S: 05
Renew Time Remaining	D: 00 H: 00 M: 00 S: 13

PacketCable DHCP Option 122	
SNMP Entity (Sub-option 3)	"prov.humax.com"
Kerberos Realm (Sub-option 6)	"BASIC.1"
Provisioning Timer (Sub-option 8)	10

Specification

Size (W x D x H)	220 x 193.5 x 55 (mm)
Weight	760g
Input Voltage	12V
Power Consumption	24W
Operating Temperature	5° to 45°C

Note: The specifications are subject to change without notice.

Glossary

Glossary

access point A device that provides WLAN connectivity to wireless clients (stations).

adaptor A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A wireless adapter connects a computer to the WLAN.

ASCII The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.

authentication A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.

authorization Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.

bandwidth The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.

bridge An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side.

broadcast Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing.

cable modem A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to “cable modem” in this documentation refer to DOCSIS or Euro-DOCSIS cable modems only.

client In a client/server architecture, a client is a computer that requests files or services, such as file transfer, remote login, or printing from the server. Also called a CPE. On a WLAN, a client is any host that can communicate with the access point. A wireless client is also called a “station.”

CMTS A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connect IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.

coaxial cable A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided (coax) wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.

CPE Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber’s location. CPE can be provided by the subscriber or the Internet Service provider. Also called a client.

DHCP A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses.

A DHCP server at the cable system headend assigns a public IP address to the residential gateway and optionally to clients on the residential gateway LAN. The residential gateway contains a built-in DHCP server that assigns private IP addresses to clients.

DMZ A "de-militarized zone" is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries, such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.

DNS The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names, such as Internetname.com, to IP addresses, such as 192.169.9.1. When you access the worldwide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain names to IP address matches.

DOCSIS Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.

downstream In a cable data network, the direction of data received by the computer from the Internet.

dynamic IP address An IP address that is temporarily leased to a host by a DHCP server. The opposite of static IP address.

encrypt To encode data.

endpoint A VPN endpoint terminates the VPN at the router so that computers on the residential gateway LAN do not need VPN client software to tunnel through the Internet to the VPN server.

Ethernet The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. "Base" means "baseband technology" and "T" means "twisted pair cable." Each Ethernet port has a physical address called the MAC address.

Euro-DOCSIS A ComLabs standard that is DOCSIS adapted for use in Europe.

event A message generated by a device to inform an operator or the network management system that something has occurred.

firewall A security software system on the residential gateway that enforces an access control policy between the Internet and the residential gateway LAN

frame A unit of data transmitted between network nodes that contain addressing and protocol control data. Some control frames contain no data.

frequency Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz gateway A device that enables communication between networks using different protocols. See also router.

gateway IP address The address of the default gateway router on the Internet.

hexadecimal A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.

host In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that, when combined with the network number, forms its IP address. Host also can mean: • A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals • A company that provides this service • In IBM environments, a mainframe computer On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.

Hz Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

ICMP Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.

IEEE The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.

IEEE 802.11b IEEE wireless network standards

IEEE 802.11g

IEEE 802.3 See Ethernet.

IP Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

IP address A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts: • A network address assigned by IANA • The residential gateway network administrator assigns a host address to each host connected to the residential gateway, automatically using its DHCP server as a static IP address. For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format, the IP address appears as “network.network.network.host.” If you enable the residential gateway DHCP client on the Basic DHCP Page, the Internet Service provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.

IPSec The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.

IKE Internet Key Exchange

ISP Internet Service Provider

LAN A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.

MAC address The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device.

MHz Megahertz — one million cycles per second. A measure of radio frequency

Multicast A data transmission sent from one sender to multiple receivers.

NAT Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic.

network Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.

NIC A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.

Packet The unit of data that is routed between the sender and destination on the Internet or other packetswitched network. When data, such as an Email message, is sent over the Internet, the sender's IP divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets.

pass-through A pass-through client on the residential gateway LAN obtains its public IP address from the Internet Service provider's DHCP server.

PING A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for Packet InterNet Groper.

port On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices. In TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved.

port triggering A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.

PPTP Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.

protocol A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.

provisioning The process of auto discovery or manually configuring a cable modem on the CMTS.

QoS Quality of service describes the priority, delay, throughput, and bandwidth of a connection.

RF Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.

router On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a gateway between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them. A router is often included as part of a network switch. A router can also be implemented as software on a computer.

routing table A table listing available routes that is used by a router to determine the best route for a packet.

RTS request to send

server In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.

Service provider A company providing data or telephone services to Subscribers

SMTP Simple Mail Transfer Protocol is a standard Internet protocol for transferring Email communications.

splitter A device that divides the signal from an input cable between two or more cables.

SSID The Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple WLANs in the same area. All clients on a WLAN must have the same SSID as the access point.

static IP address An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address station IEEE 802.11b term for wireless client subscriber A home or office user who accesses television, data or other services from an Internet Service provider.

subnet mask A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.

SYSLOG A de-facto UNIX standard for logging system events.

TCP Transmission Control Protocol on OSI transport layer four provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.

TCP/IP Transmission Control Protocol/Internet Protocol suite. It provides standards and rules for data communication between networks on the Internet. It is the worldwide Internetworking standard and basic communications protocol of the Internet.

TFTP Trivial File Transfer Protocol is a very simple protocol used to transfer files.

TKIP Temporal Key Integrity Protocol

tunnel To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits on the network. VPNs rely on tunneling to create a secure network.

Tunneling requires the following protocol types:

- A carrier protocol, such as TCP, used by the network that the data travels over

• An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data

• A passenger protocol, such as IP, for the original data two-way A cable system that can transmit signals in both directions to and from the headend and the subscriber UDP User Datagram Protocol

unicast A point-to-point data transmission sent from one sender to one receiver. This is the normal way you access websites.

upstream In a cable data network, upstream describes the direction of data sent from the subscriber's computer through the cable modem to the CMTS and the Internet.

VoIP Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.

VPN A virtual private network is a private network that uses "virtual"connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection, usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.

WAN A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.

WEP Wired Equivalent Privacy encryption protects the privacy of data transmitted over a WLAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b. Because WEP can be difficult to use and does not provide very strong encryption.

WiFi Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.

WLAN wireless LAN

WPA Wi-Fi Protected Access (WPA) encryption, as described on the Wi-Fi Alliance web page: http://www.wifialliance.org. It is a far more robust form of encryption than WEP.