Leading Provider
of 3C Total Solutions

Standalone Media Terminal Adapter
(SMTA)

User Manual

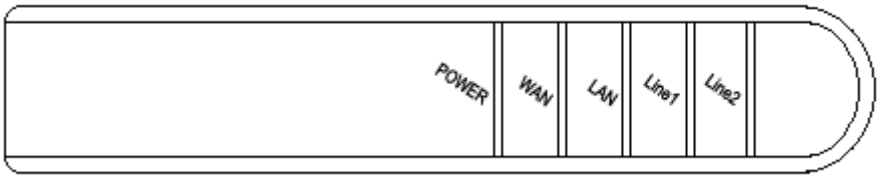
Version 1.0

TABLE OF CONTENTS

1. General Information

The ASUS Standalone Media Terminal Adapter (SMTA) is a voice-over-IP (VoIP) gateway with 10/100 Ethernet, router and firewall all in one compact hardware and firmware platform.

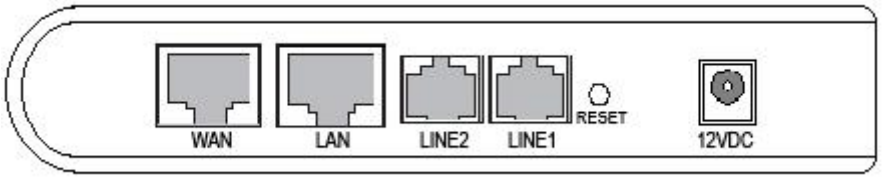
1.1 SMTA Front Panel



LED	Description	
Power	ON	SMTA is powered
	OFF	SMTA is not powered
WAN	ON	WAN port is connected to a device, such as a cable modem
	OFF	No connection
LAN	ON	PC is connected to LAN port
	OFF	No connection
	Blinking	SMTA is sending / receiving data via LAN
Line1	ON	Line1 is off-hook
	OFF	Line1 is on-hook
Line2	ON	Line2 is off-hook
	OFF	Line2 is on-hook

1.2 SMTA Back Panel

Your SMTA provides two Ethernet interfaces (WAN and LAN) as well as two voice interfaces that allow you to connect directly to telephones, fax machines, etc.



Port	Description
WAN	**WAN FastEthernet Port,** RJ-45 connects the unit to an Ethernet WAN device such as a cable modem or ADSL router.
LAN	**LAN FastEthernet Port,** RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
LINE2	RJ-11 telephone ports connect telephone wiring to telephones or fax machines.
LINE1	
RESET	• **Short Reset**–resets device with current startup configuration. Press and hold the reset button for 1 second and then release. • **Long Reset**–resets device to factory default configuration. Press the reset button for 6 seconds or more and then release.
POWER	Connects to a 12VDC AC power adapter.

2. SMTA Installation

2.1 Safety Instructions

! Before installation, it is important that you read the following.

- Place your SMTA on a flat surface close to the cables in a location with sufficient ventilation.
- To prevent overheating, do not obstruct the ventilation openings of this equipment.
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.
- Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.
- Do not open the cover of this equipment. Opening the cover will void any warranties on the equipment.
- Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

2.2 Installing the SMTA

Connect all the cables from the SMTA to the appropriate outlet.

The SMTA comes with two *line* ports. Install the cables as follows–

1. Connect an RJ-11 cable between the port labeled **LINE1** on the SMTA and the telephone or fax machine.
2. If you will be using the second port, connect another RJ-11 connector between the port labeled **LINE2** on the SMTA and the second telephone or fax machine.

The SMTA also has two 10/100Base-T auto MDI/MDIX ports for LAN and WAN. Any of the ports can be connected to a host or hub/switch with an RJ-45 cable. Install the cables as follows–

1. Connect the **WAN** port to the subscriber port of your DSL or cable.
2. Connect the **LAN** port to the Ethernet port of your network device (PC, notebook, switches, etc.).

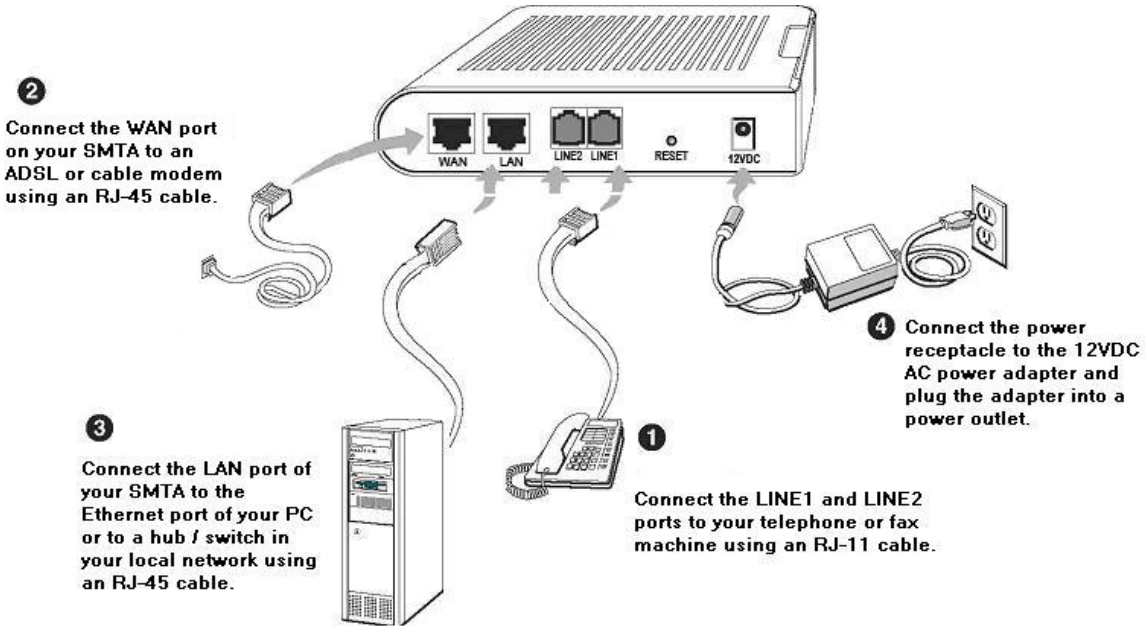
Lastly, connect the power supply to your SMTA.

1. Insert the barrel-type connector end of the AC power adapter into the 12VDC port.

   NOTE: *The AC power adapter will automatically adjust to accept an input voltage from 100 to 240VAC (50/60 Hz).*

2. Plug the AC power adapter into an appropriate power outlet.

The below diagram illustrates the connections for your SMTA.



3. Quick Start

This section contains instructions that will allow you to quickly configure and run the Standalone Media Terminal Adapter (SMTA) so your PC can access the public Internet using your chosen Internet Service Provider (ISP).

3.1 Required Information

To configure the SMTA, you will need the following information, typically provided by your ISP:

1. If your ISP does NOT use DHCP (dynamically assigned IP addresses), you will need the following:
    - The static IP address or PPPoE account assigned to your PC by your ISP
    - The subnet mask used by your ISP
    - The IP address of the default gateway
    - The IP addresses of the primary and secondary DNS servers

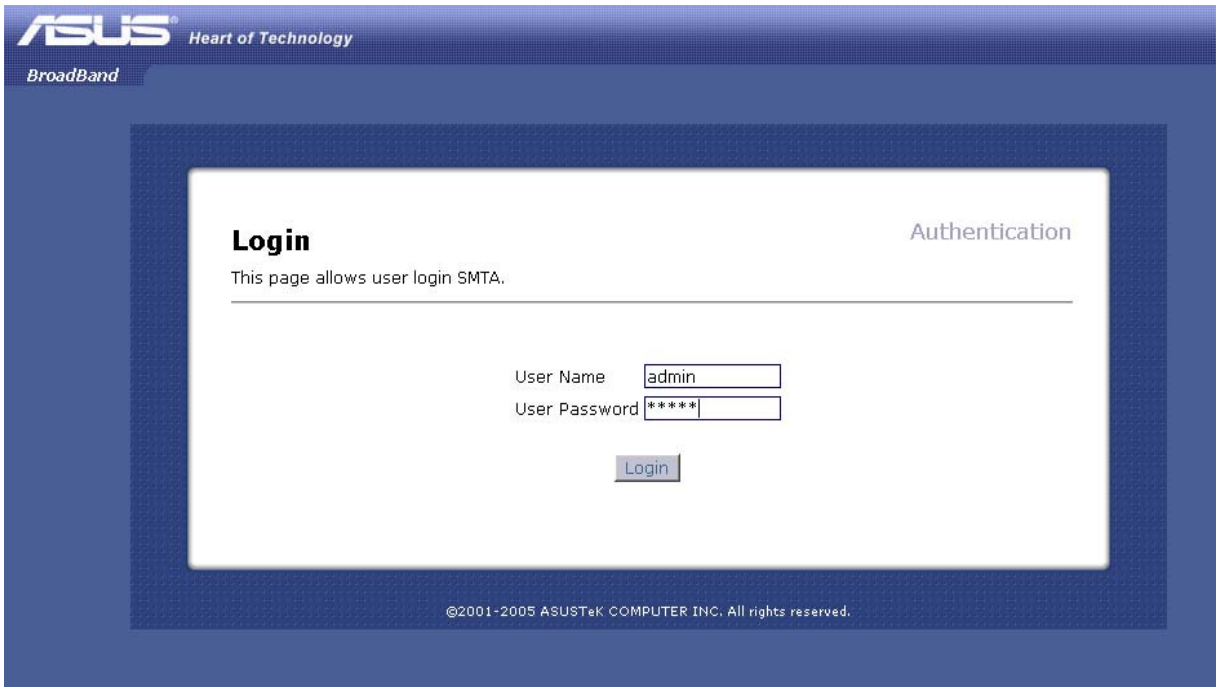
2. Some ISPs MAY require the following information:
    - The MAC address of the PC that is registered with your ISP
    - The host name of the PC that is registered with your ISP
    - The domain name used by your ISP

3.2 Accessing the SMTA

The default **IP address of the SMTA is 192.168.15.1**. To access the configuration web pages, follow the below steps:

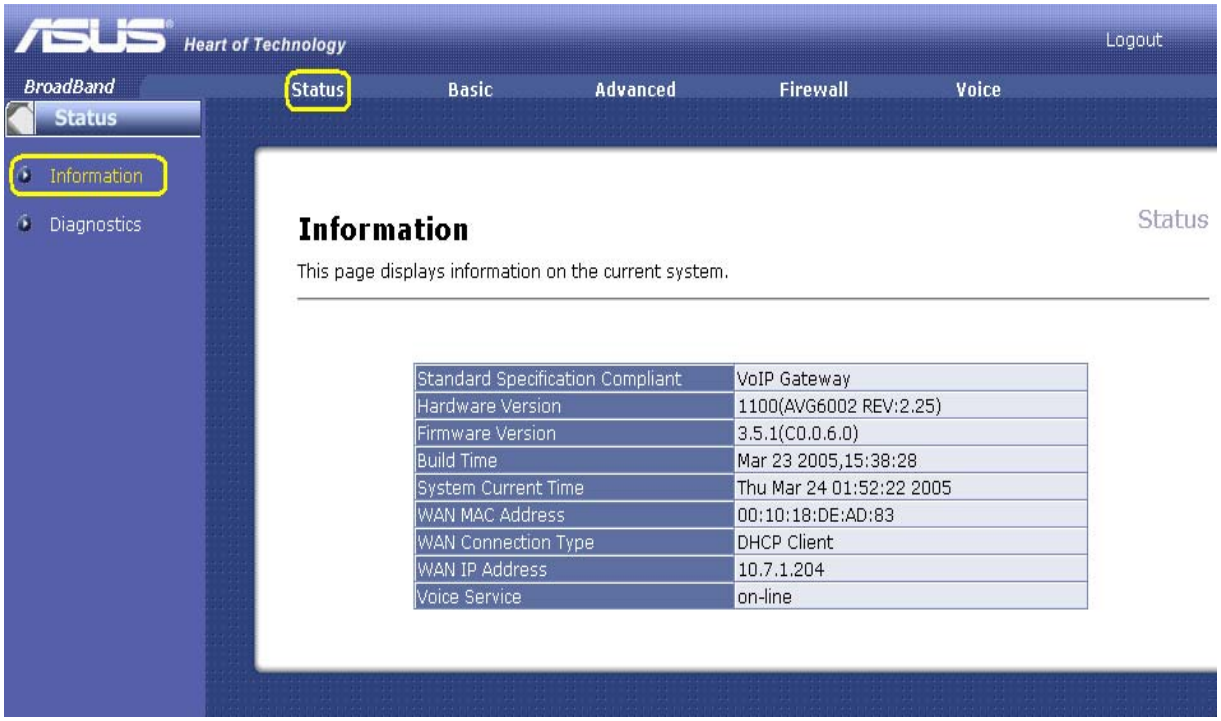
1. Obtain an IP address from the built-in DHCP server for the PC you are using to connect the SMTA
2. Launch your web browser (Internet Explorer or Netscape)
3. Enter the URL http://192.168.15.1 in the address bar

An authentication window like the one below will be displayed after you connect to the user interface. To log in, enter either “admin” or “user” in both the user name and user password fields. Then click on the **Login** button. Using the “admin” login will give you certain accesses that are not available when using the “user” user name and password combination.



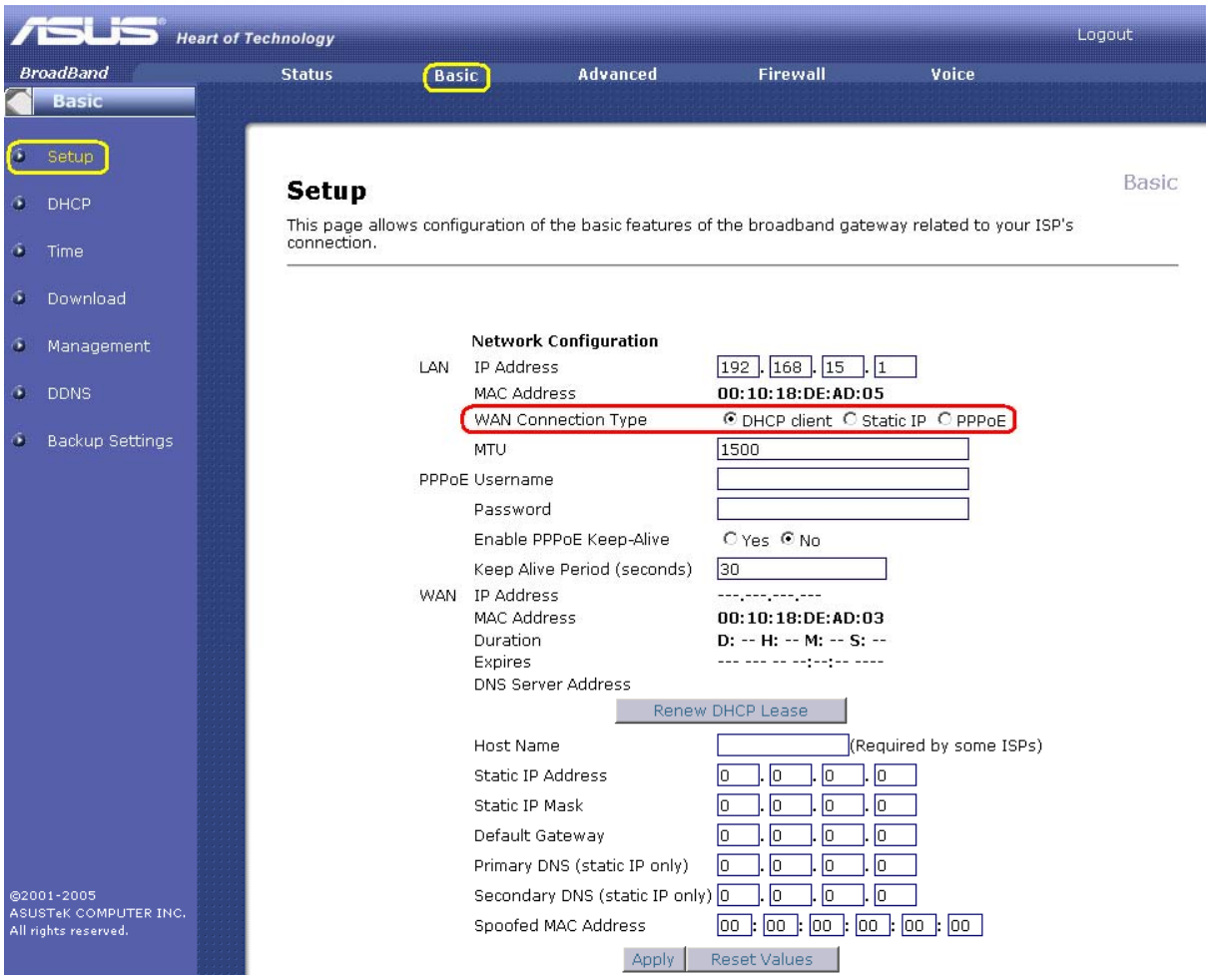
3.3 Basic Setup

After logging in, a status page with information on the current system will be displayed.



3.4 Setup

The Setup page allows you to configure WAN settings (only the LAN IP Address shows LAN-related information). A WAN connection type must be selected based on the connection that your ISP uses. As seen in the illustration below, you will need to select from either DHCP client, static IP, or PPPoE from the list of WAN connection types.



3.4.1 If Using DHCP Client WAN Connection Type

If your ISP uses DHCP, just click on the DHCP radio button and click on the **Apply** button. If you already configured your WAN connection type to DHCP client and you just want to renew your DHCP lease, then click on the **Renew DHCP Lease** button.

3.4.2 If Using a Static IP WAN Connection Type

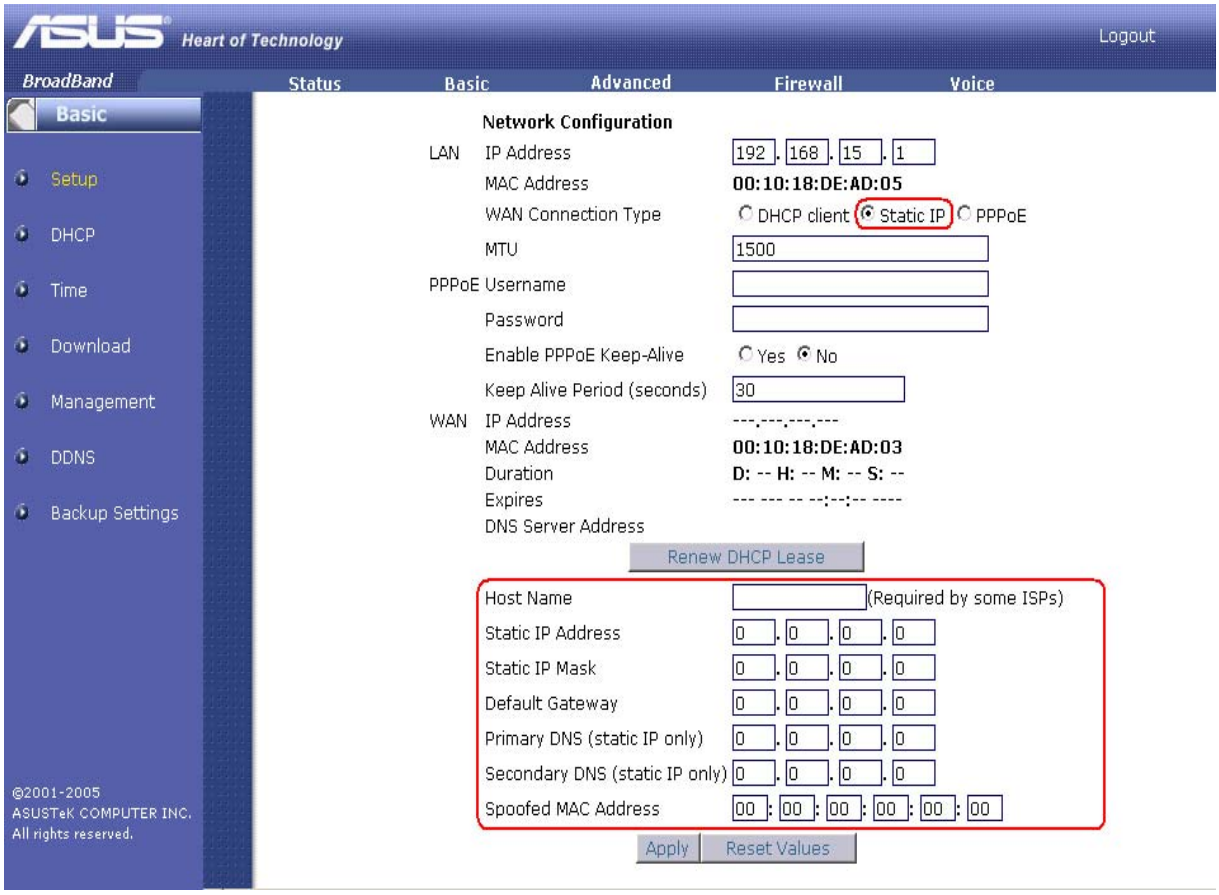
If your ISP uses static IP connection, then you will only need to update the boxed section as illustrated below.

- **Host Name**–optional, required by some ISPs
- **Static IP Address**
- **Static IP Mask**
- **Default Gateway**
- **Primary DNS**
- **Secondary DNS**

Enter the information as indicated in Section 1.1 Required Information.

- **Spoofed MAC Address**–enter a unicast MAC address in this field. Your ISP may require this to be your PC's MAC address. If not, you can simply supply the WAN side MAC address of the router as your CPE and leave the spoofed MAC address entry set to all 0's since there will be no spoofing required.

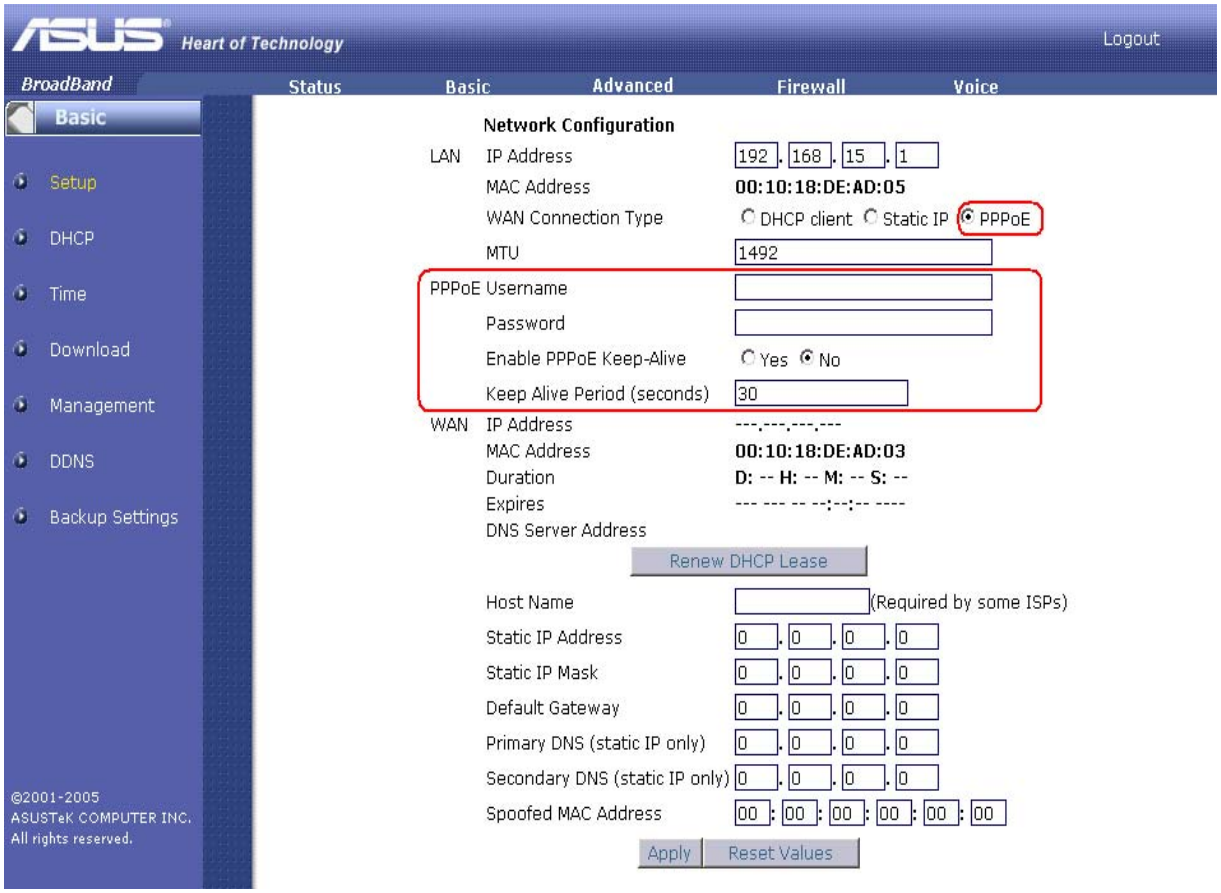
Upon completion of these fields, click on the **Apply** button to reset the SMTA to your settings.



3.4.3 If using a PPPoE Connection Type

If your ISP uses a PPPoE connection, you will only need to update the fields as indicated in the box below.

1. Enter PPPoE username and password.
2. Select 'yes' if you want to enable the PPPoE KeepAlive function.
3. If you select 'yes', then enter the KeepAlive Period in seconds.
4. When finished, click on the **Apply** button at the bottom of the screen.



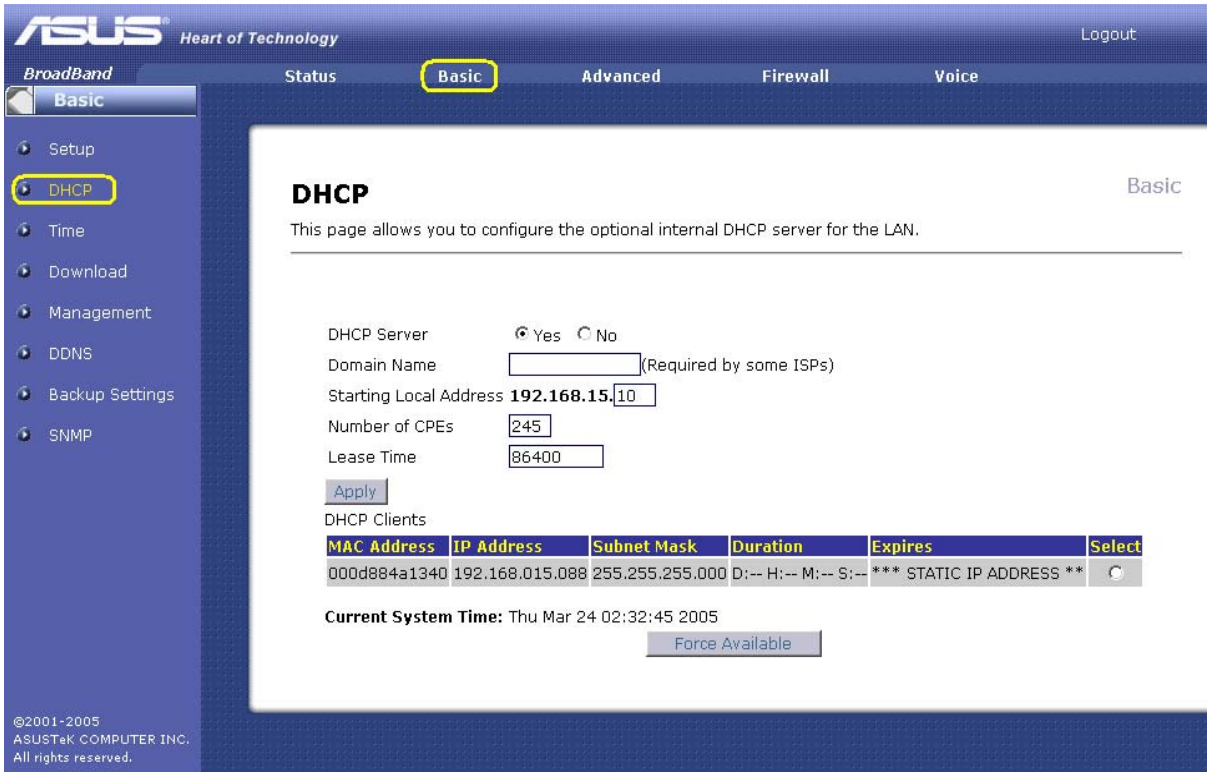
At this point, the SMTA is configured for basic use using the suitable settings. Before you can access the Internet, the following must be done.

1. Power up the SMTA and wait for it to register with the ISP and obtain an Internet-routable IP address.
2. Obtain an IP lease from the internal DHCP server for each PC attached to the LAN side of the SMTA.

NOTE: *Communication on the LAN will work regardless of whether the WAN connection is up. However, you will not be able to access the Internet until the WAN connection is enabled and has an IP address.*

3.5 Configure the DHCP Server

The configuration of the DHCP server can also be modified. This can be done from the DHCP page in the Basic menu as shown below.

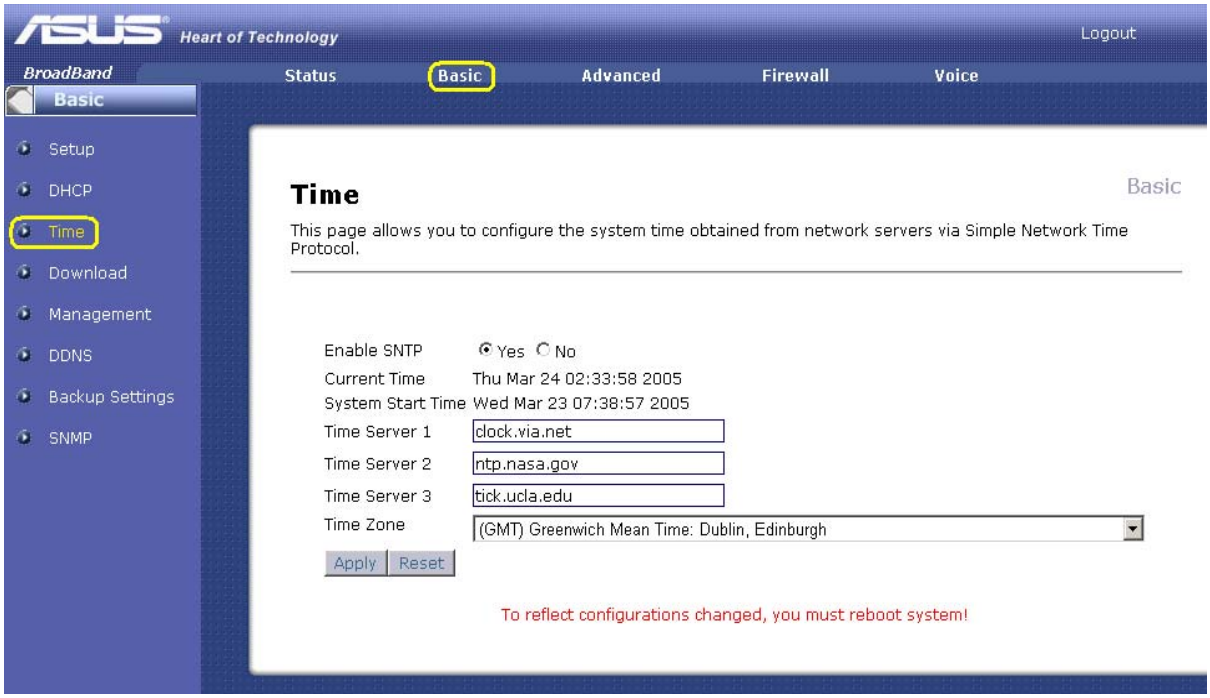


If you have your own DHCP server servicing the LAN side, you can disable the internal DHCP server by selecting the 'no' radio button. If you do this, make sure the LAN IP address of the SMTA is on the same subnet as the external DHCP server (the subnet mask is always 255.255.255.0), or you will not be able to access the SMTA from the LAN. The IP address of the SMTA can be set from the Basic Setup page.

You can also set the starting IP address for IP leases available to the LAN, and change the number of PCs supported on the LAN.

3.6 Configure System Current Time

Your SMTA uses SNTP (Simple Network Time Protocol) to retrieve accurate system time for the device. This page will display both the current system time and system up time. After modifying the configuration of this page, you need to restart the STMA for the changes to take effect.



- **Enable SNTP**–select 'yes' to turn on the feature of automatically retrieving system time.
- **Current Time**–this is the system's current time
- **System Start Time**–this is the system up time
- **Time Server [1-3]**–these are time servers that the system will synchronize with, starting with Time Server 1. The system will try the next timer server if the first one is down, and so on.

> ***NOTE:*** *Time Server 1-3 will display pre-set time servers that may be changed depending on your preferences.*

- **Time Zone**–select the time zone of your location

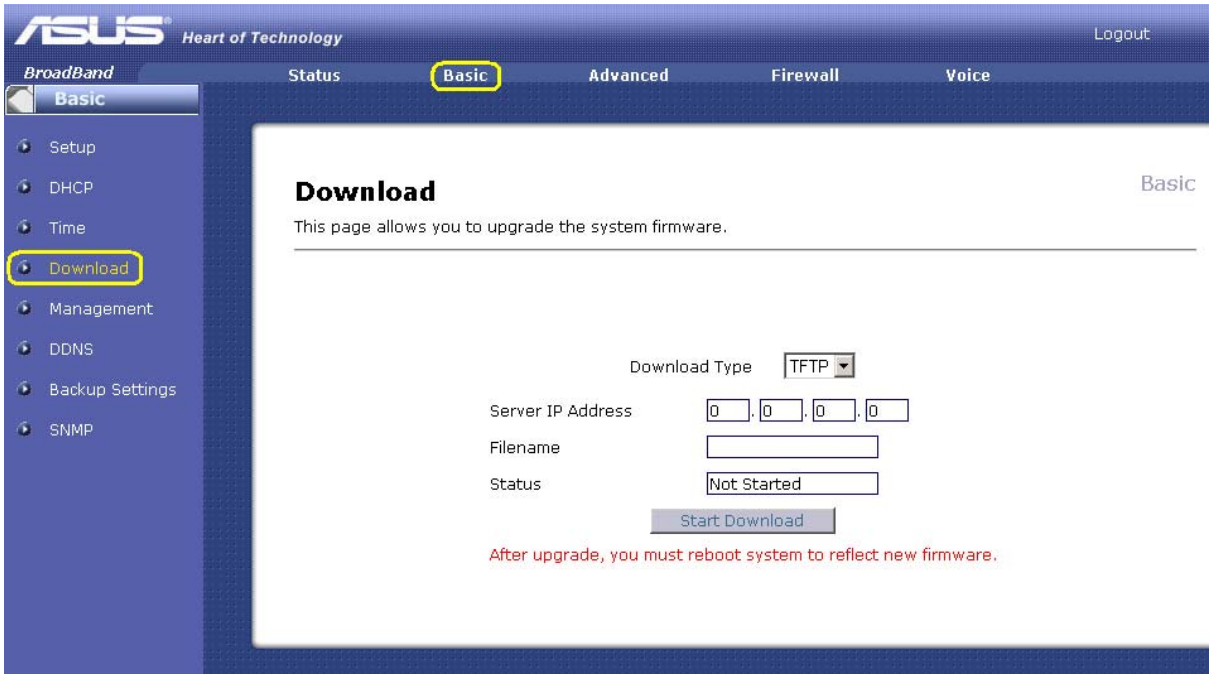
3.7 Upgrade Firmware

To update your SMTA with upgrades, you will first need to download the firmware upgrade from the Internet. After you successfully download the file, upgrade your system with the update by one of two methods–**TFTP** or **HTTP**.

To download by TFTP–

1. Select TFTP from the pull-down menu
2. Enter the IP Address of the TFTP server that you downloaded the file to
3. Enter the filename of the firmware upgrade
4. Click on the **Start Download** button

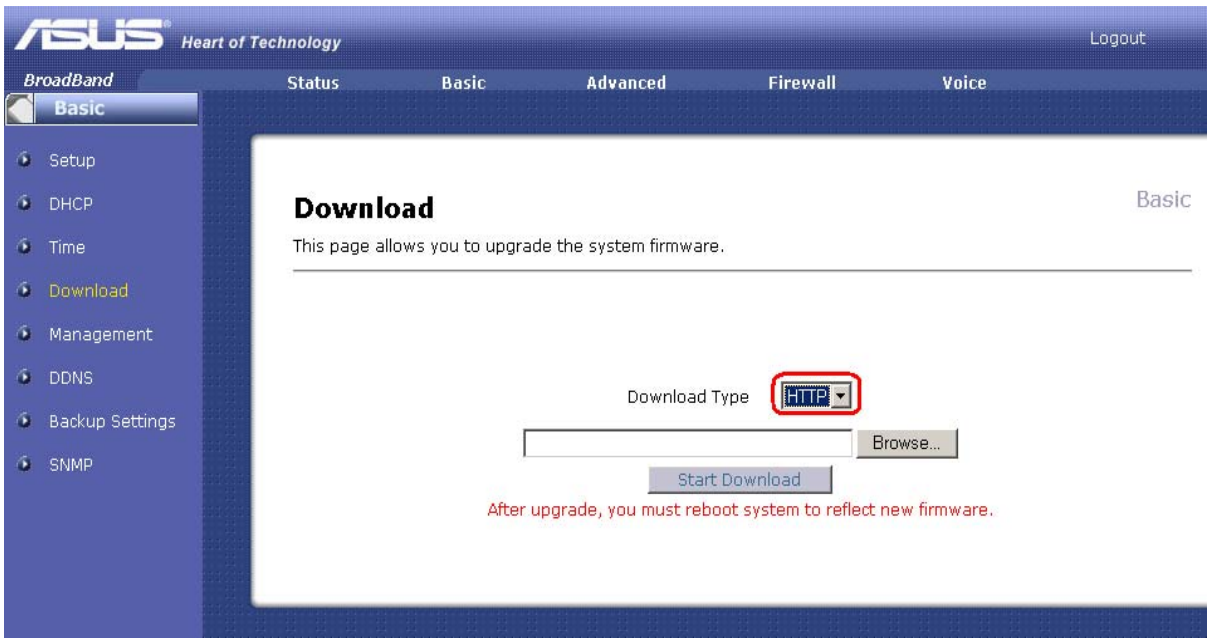
> ***NOTE:*** *After the file is successfully downloaded, a message prompt will appear on your screen for you to restart the device.*



To download by HTTP–

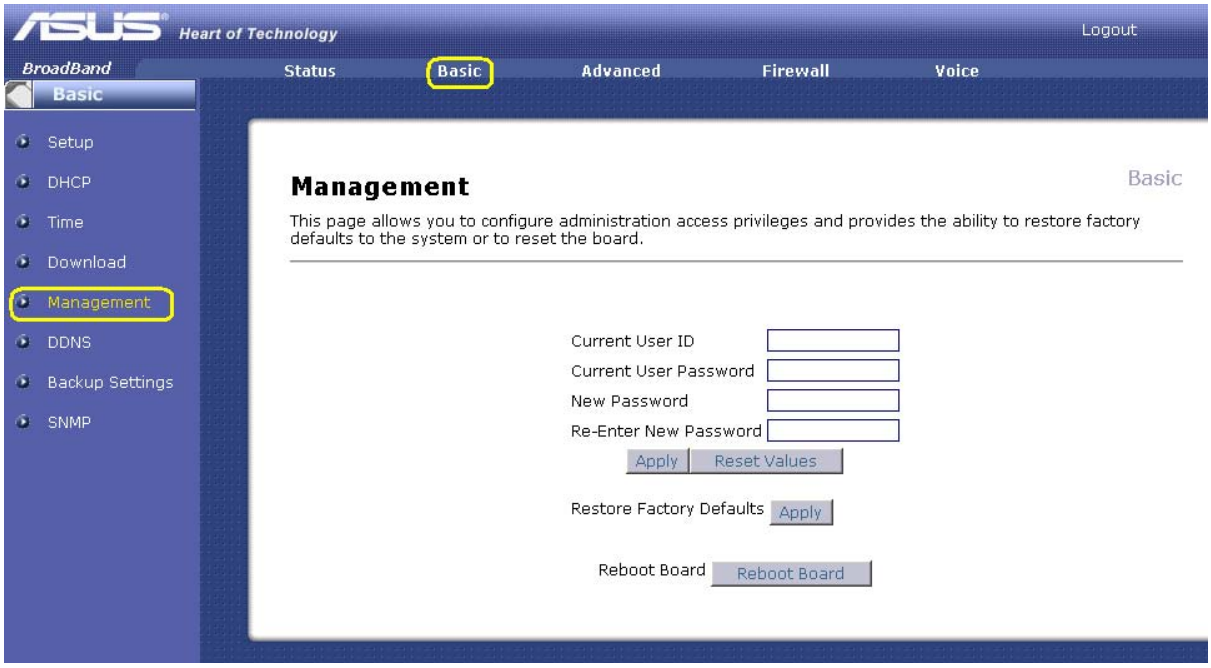
1. Select HTTP from the pull-down menu
2. Click on the **Browse** button to find the file on your PC
3. Click on the **Start Download** button

The following illustration shows the download screen for HTTP download–



3.8 Management Page

Restoring the SMTA to factory default settings may be necessary on occasion. This can be done from the Management Page, which can be accessed from the Basic Menu as illustrated below–



Changing the User Password–

NOTE: *The user ID cannot be changed from* ***admin*** *and* ***user****. Only the password can be changed.*

1. Enter the current user ID and user password
2. Enter the new password
3. Re-enter the new password again to verify that it is correct
4. Click **Apply** to change the password to the new one
5. Click **Reset Values** if you want to clear above fields and begin again

Restore Factory Defaults–

To restore factory defaults settings, click the second **Apply** button. This will cause the device to reset back to its original settings.

Reboot Board–

This function is the same as pressing the reset button on the back panel of your SMTA. This will save all changes before the device is restarted.

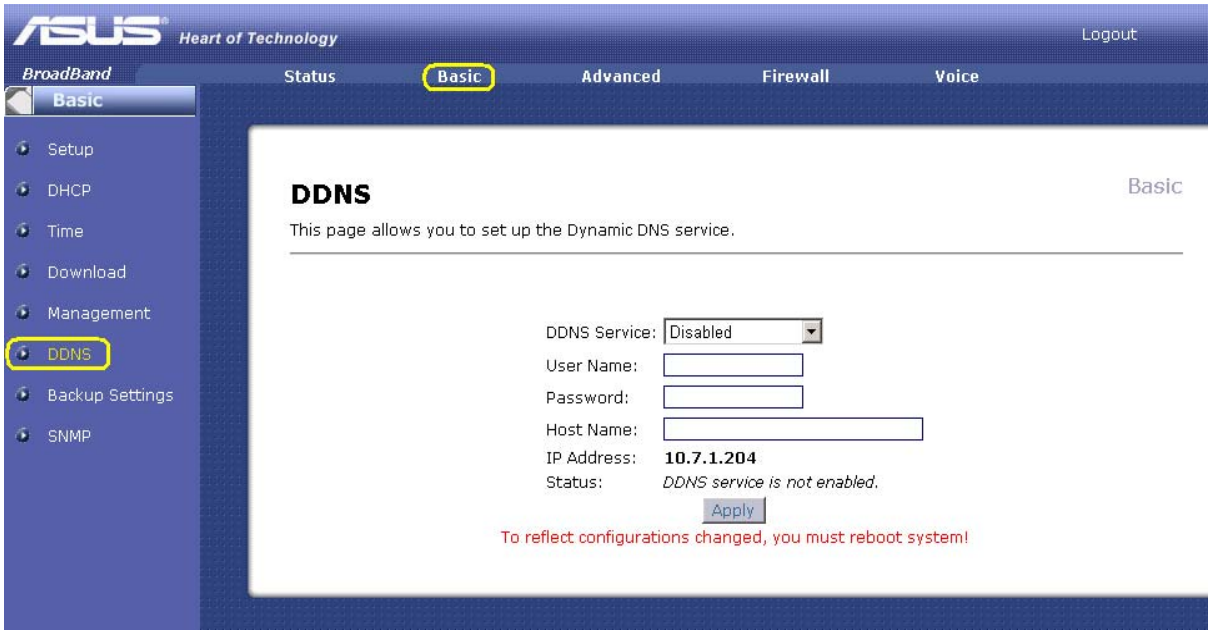
3.9 DDNS Setup

If you are using a DDNS (Dynamic Domain Name System) service to monitor the IP address of your web or FTP server, then you can enter the information provided by your DDNS service provider here. The default DDNS service provider is www.DynDNS.org.

- **DDNS Service:** Select the default DDNS service provider: www.DynDNS.org
- **User Name:** Enter the user name that is given by the service provider
- **Password:** Enter the password that is given by the service provider
- **Host Name:** This is registered on the DDNS service provider website

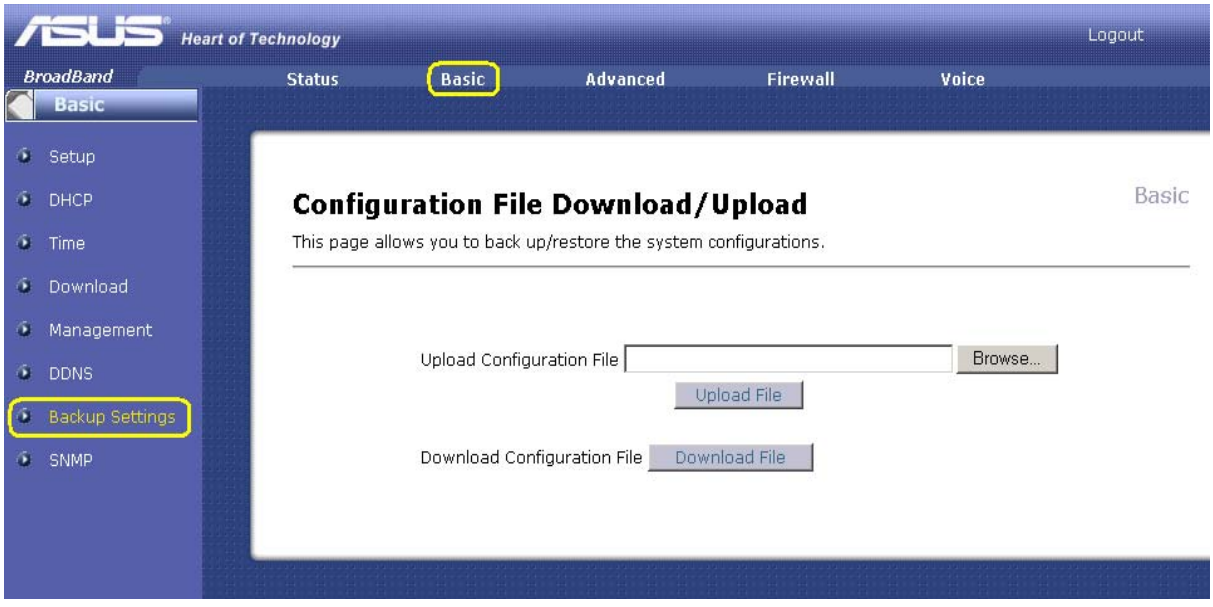
- **IP Address:** Enter the WAN IP address (same IP address as indicated on the Information page
- **Status:** Indicates the status of the DDNS service

Click on the **Apply** button when all the applicable information is entered.



3.10 Backup Settings

This page allows you to either upload or download configuration settings. If you want to use configurations that you previously saved, you can upload the configuration file. Browse your PC for the file name and click on the **Upload File** button. To save a copy of your current system configurations, click on the **Download File** button.

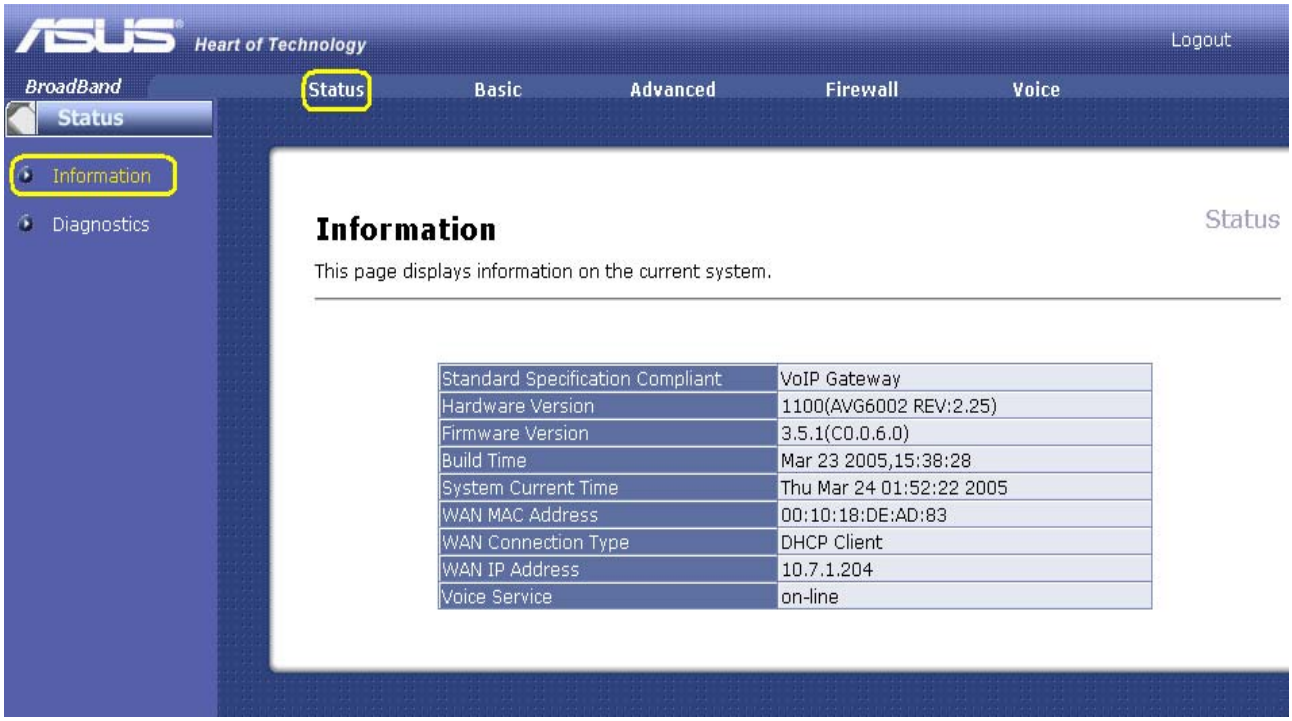


4. Troubleshooting

Several status pages are available from the web server to aid in troubleshooting problems with the SMTA. General information about the SMTA is found on the Information Page and troubleshooting is found on Diagnostic Pages.

4.1 Information Page

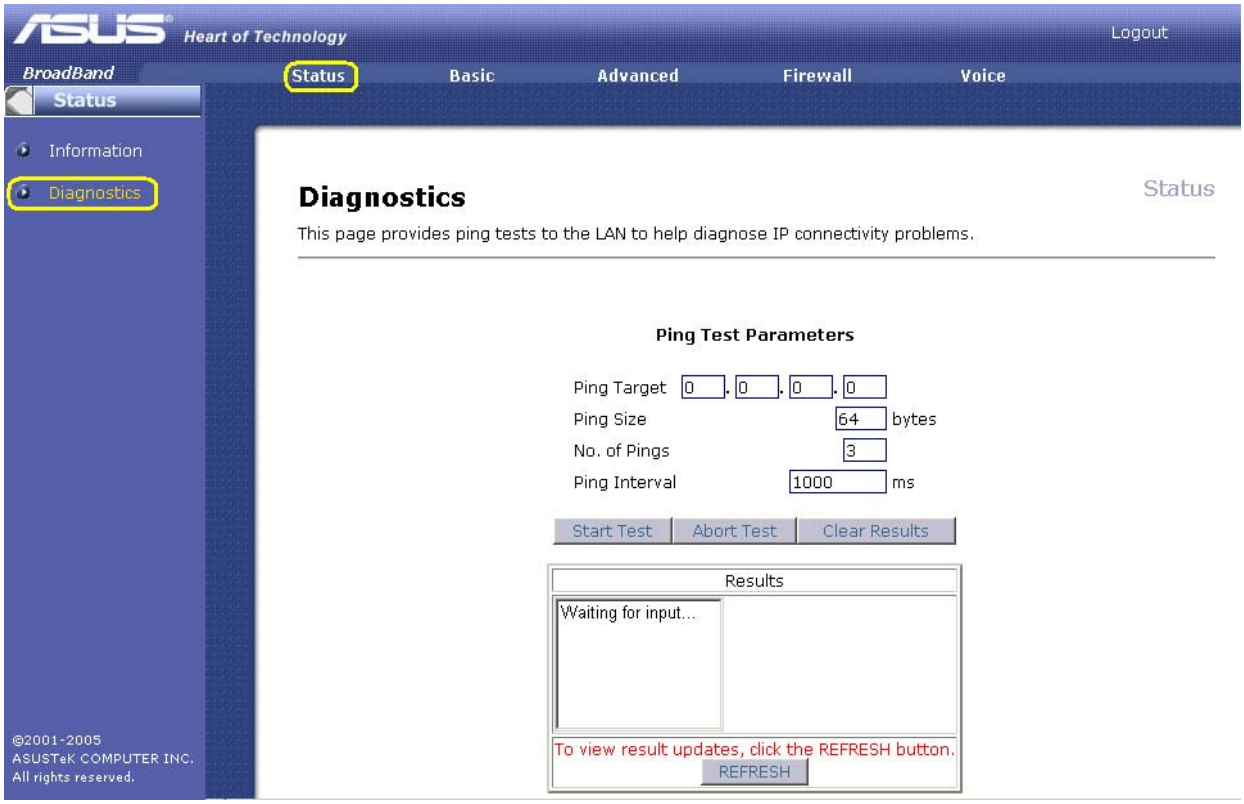
The Information page is the first page displayed in the Status section. The purpose of this page is to provide you with general system information relating to the version of the hardware and firmware, WAN information, etc. The information on this page can be refreshed at any time by clicking your web browser's Refresh button.



- **Standard Specification Compliant**–the name of the device
- **Hardware Version**–the version and model number of the device
- **Firmware Version**–the firmware version being used
- **Build Time**–when the firmware was built
- **System Current Time**–the current time on your system
- **WAN MAC Address**–Media Access Control address of the WAN; a unique identifier for each device
- **WAN Connection Type**–the connection type (DHCP Client, Static IP, or PPPoE) being used to connect to the WAN
- **WAN IP Address**–the IP address of the WAN
- **Voice Service**–the status (on-line or off-line) of the SMTA

4.2 Diagnostics Page

The Diagnostics page allows you to troubleshoot any problems with your IP connection by using a ping test.



This information may be useful to technical support representatives if you need their assistance in troubleshooting a problem with the WAN connection. Computers on the external WAN and internal Private LAN can be pinged.

- **Ping Target**–Enter the IP address of the network device you wish to check connectivity to
- **Ping Size**– the size of each packet for the ping test
- **No. of Pings**–the number of times you wish to ping the device
- **Ping Interval**–the number of times (in milliseconds; 1000 ms=1 sec) in between each ping

NOTE: *To view all the ping results in the window, click on the* ***Refresh*** *button.*

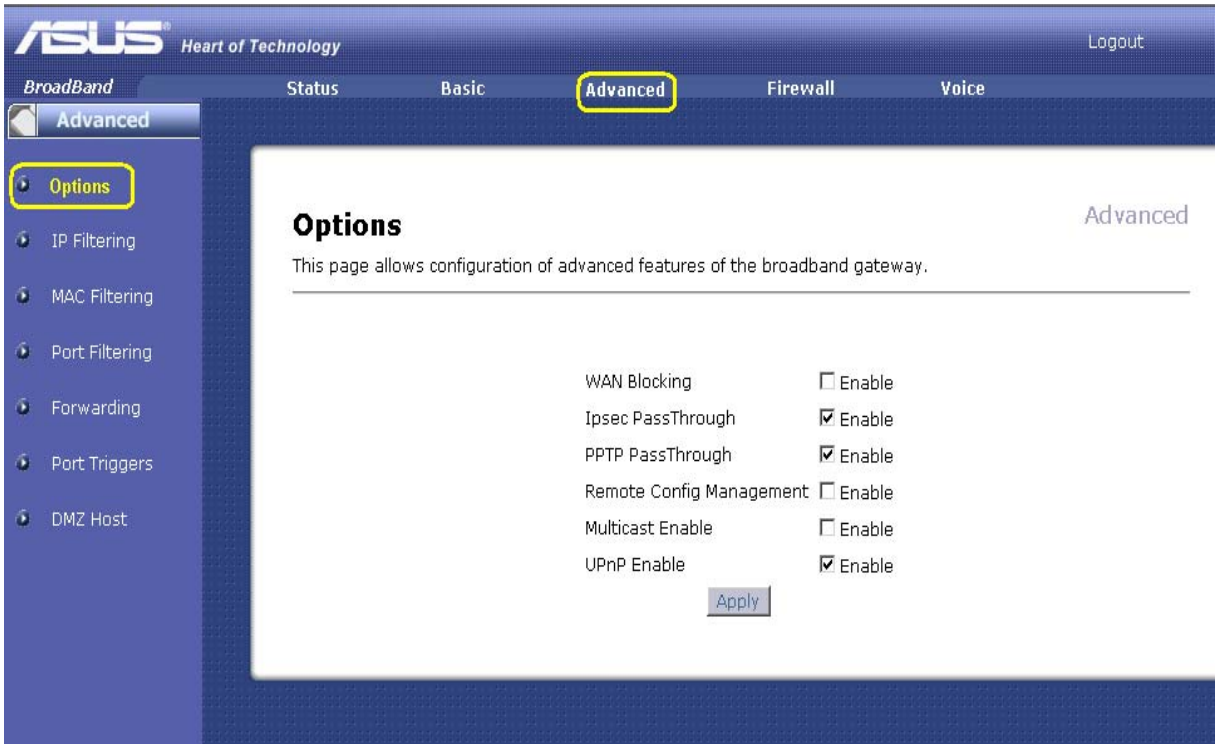
5. Advanced Configuration

There are many advanced router features supported by the SMTA. These features are documented in this section, and include:

1. Optional WAN blocking, IpSec pass-through, PPTP pass-through, remote administration, multicast enable modes and UPnP (universal plug and play)
2. LAN IP address, MAC address, and port number filtering
3. WAN to LAN port forwarding and triggers
4. DMZ hosting (or exposed host)

5.1 Optional Modes

The SMTA is capable of operating in several modes that adjust how the device routes IP traffic. These features are accessible from the Advanced Menu on the Options page.



To enable a feature, click on the appropriate check box. When you are satisfied with your selections, click on the **Apply** button. These features can be applied quickly without a system reset.

- **WAN Blocking** prevents the SMTA or the PCs behind it from being visible to the WAN. For instance, pings to the SMTA's WAN IP address or the PCs behind it are not returned. Therefore, it will be more difficult for a hacker to discover your WAN IP address to begin an attack on your private LAN.

- **IpSec / PPTP** (Point-to-Point Tunneling Protocol) **PassThrough** modes enable these protocols to be used through the SMTA such that a VPN device (or software) may communicate properly with the WAN.

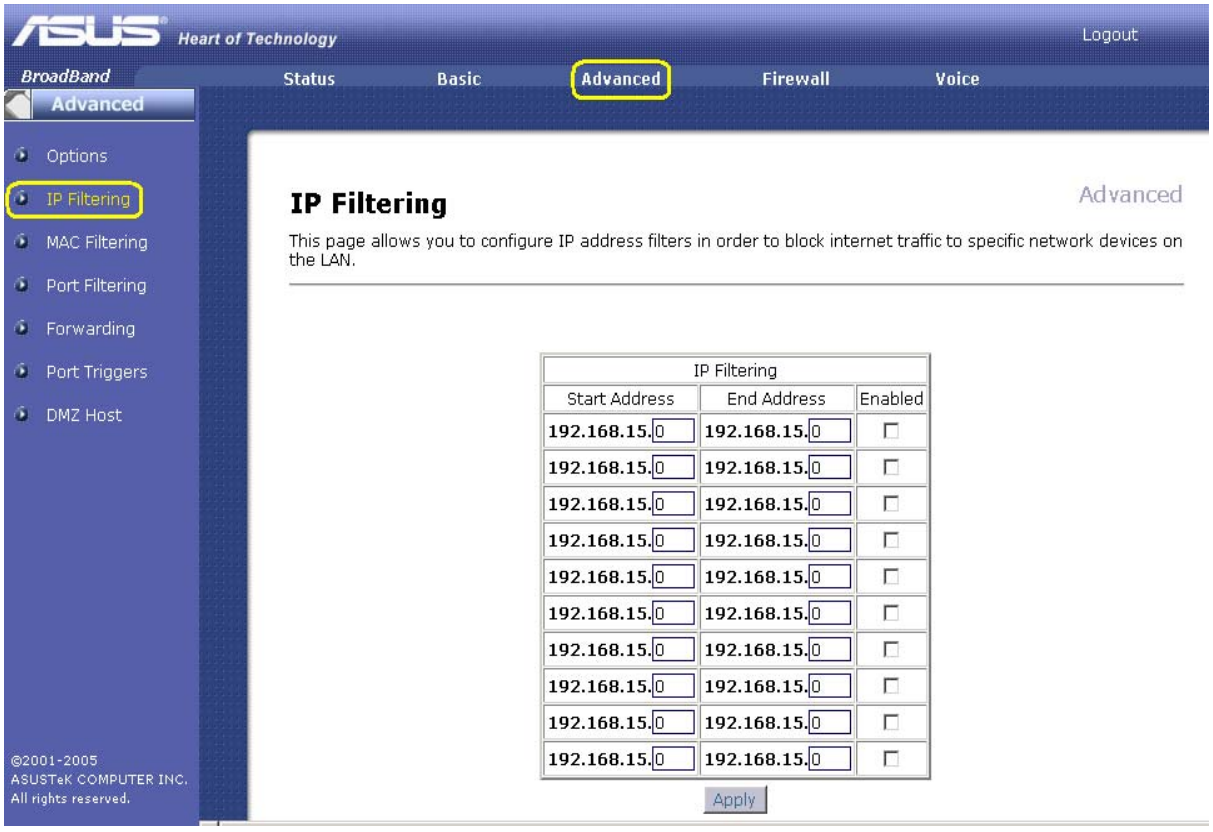
- **Remote Configuration Management** allows the SMTA to be administered (configured) from the WAN via surfing to the WAN IP address of the SMTA from anywhere on the Internet.

- **Multicast Enable** allows multicast-specific traffic (denoted by a multicast-specific address) to be passed to and from the PCs on the private network behind the SMTA.

- **UPnP Enable** allows PCs behind the SMTA to control the SMTA as a NAT traversal device.

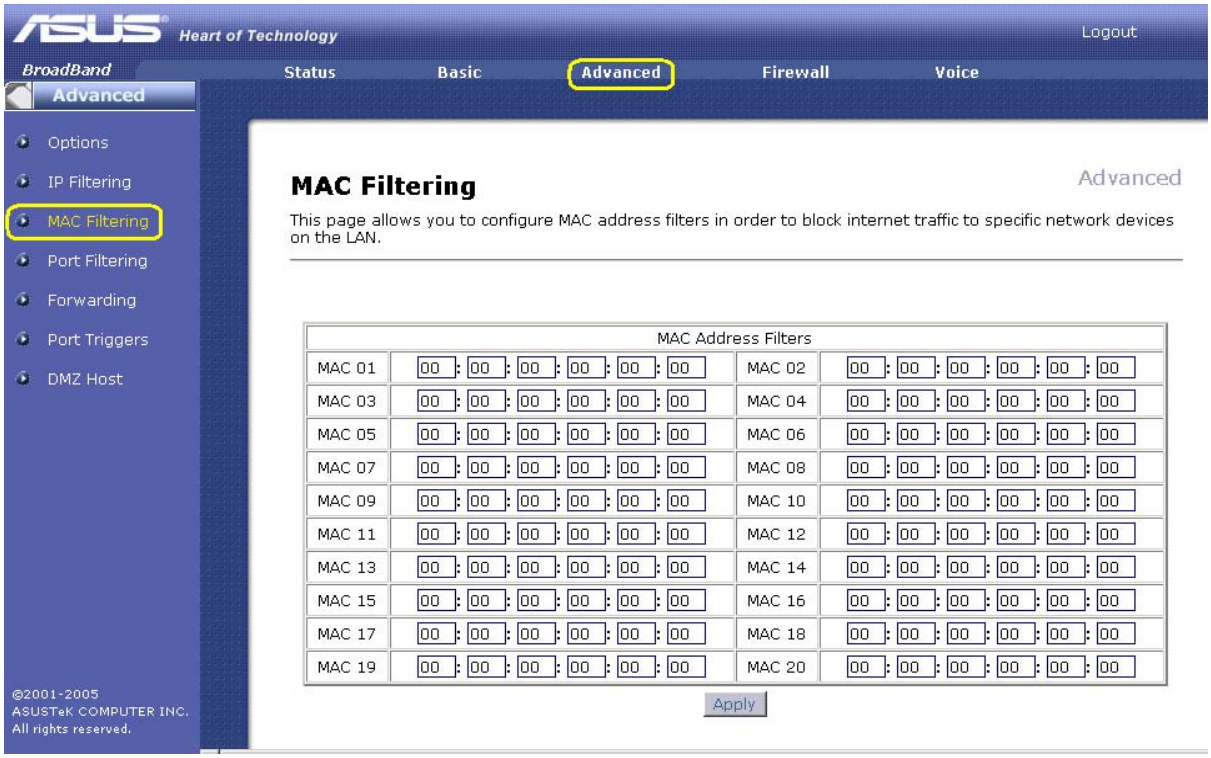
5.2 LAN IP Address, MAC Address, and Port Filtering

The SMTA can be configured to prevent local PCs from getting access to the WAN by specifying those IP addresses that should be filtered. This can be done from the IP Filtering page (shown below) in the Advanced Menu.



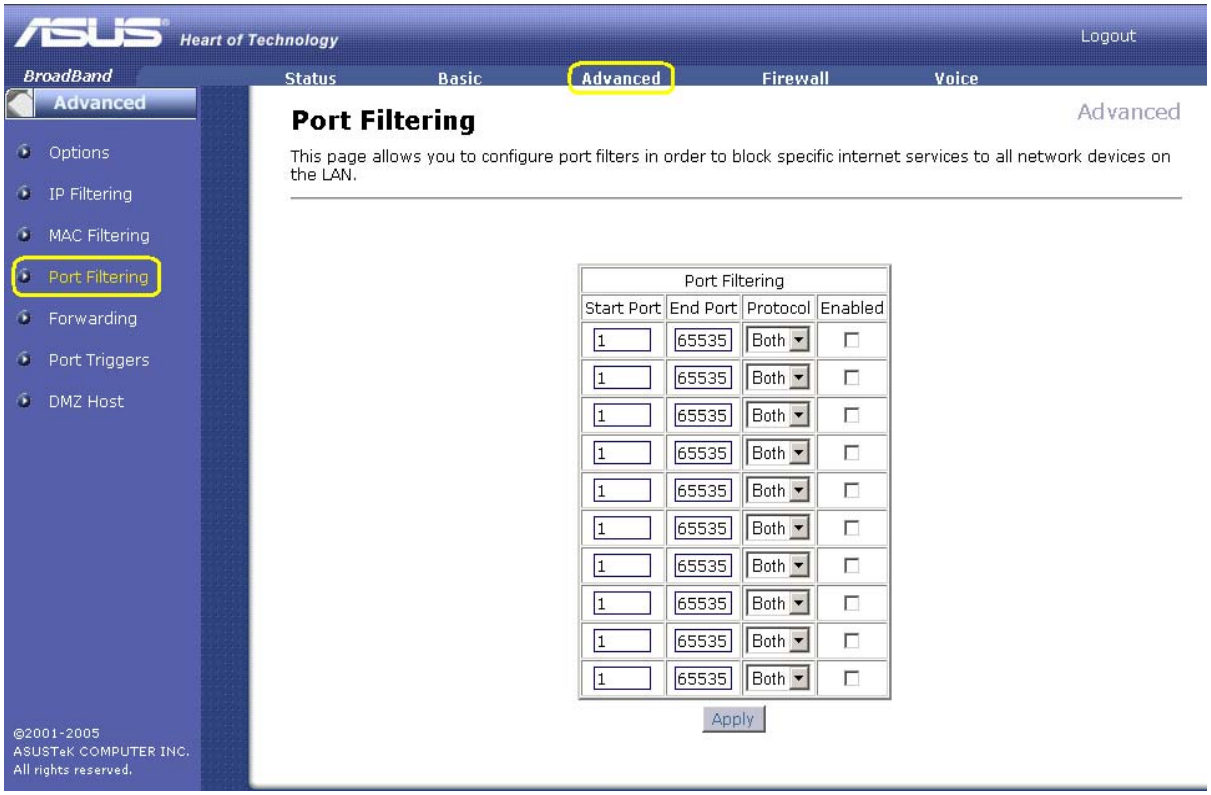
By entering starting and ending IP address ranges, you can configure which local PCs are denied access to the WAN. Note that you only need to enter the LSB (least-significant byte) of the IP address. The upper bytes of the IP address are set automatically from the SMTA IP address. To activate the IP address filter, you must also check the "enable" box and click on the **Apply** button. The enable box allows you to store filter settings commonly used but not have them active.

You can also prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC address. This can be configured using the MAC Filtering page, shown below.



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

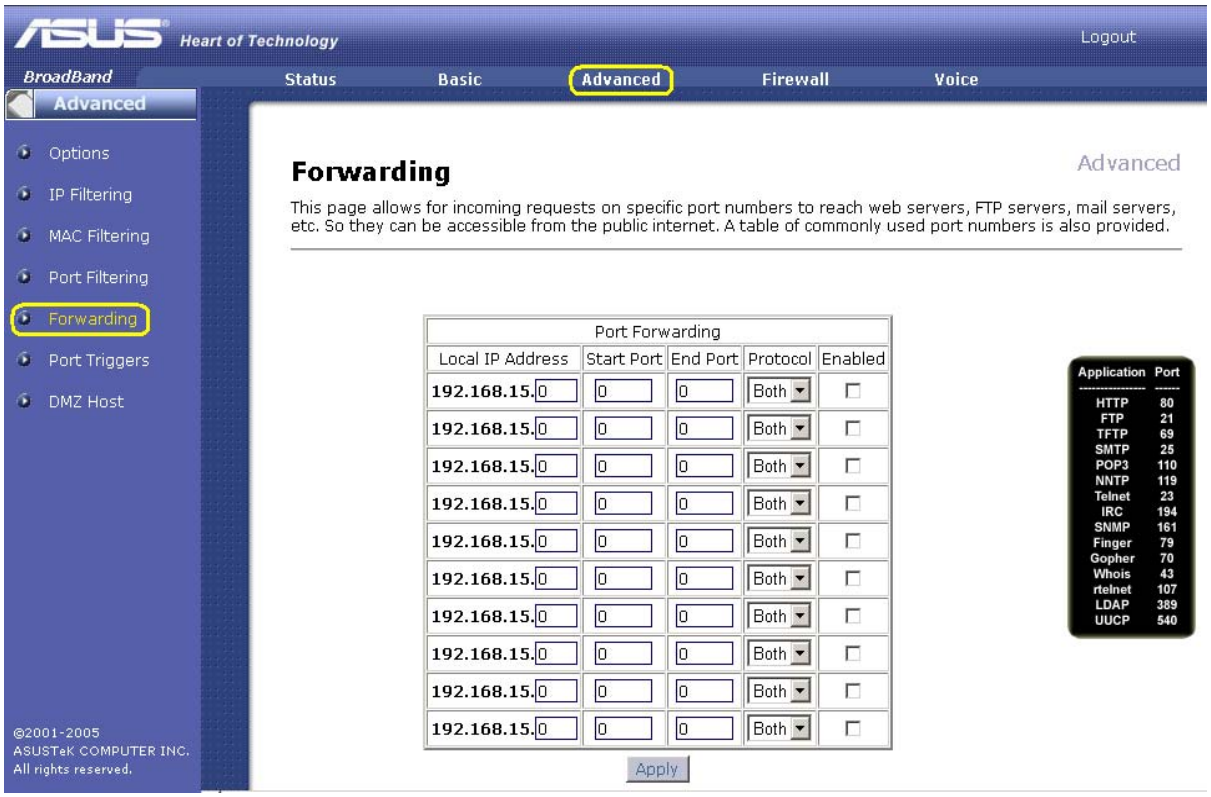
Similarly, you can prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. This can be configured using the Port Filtering page, shown below.



By specifying a starting and ending port range, you may determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis. Note the specified port ranges are blocked for ALL PCs and this setting is not IP address or MAC address specific. For instance, if you would like to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), you would set the "Start Port" to 80, the "End Port" to 80, the "Protocol" to TCP, check the "Enabled" box, and click the **Apply** button.

5.3 Port Forwarding

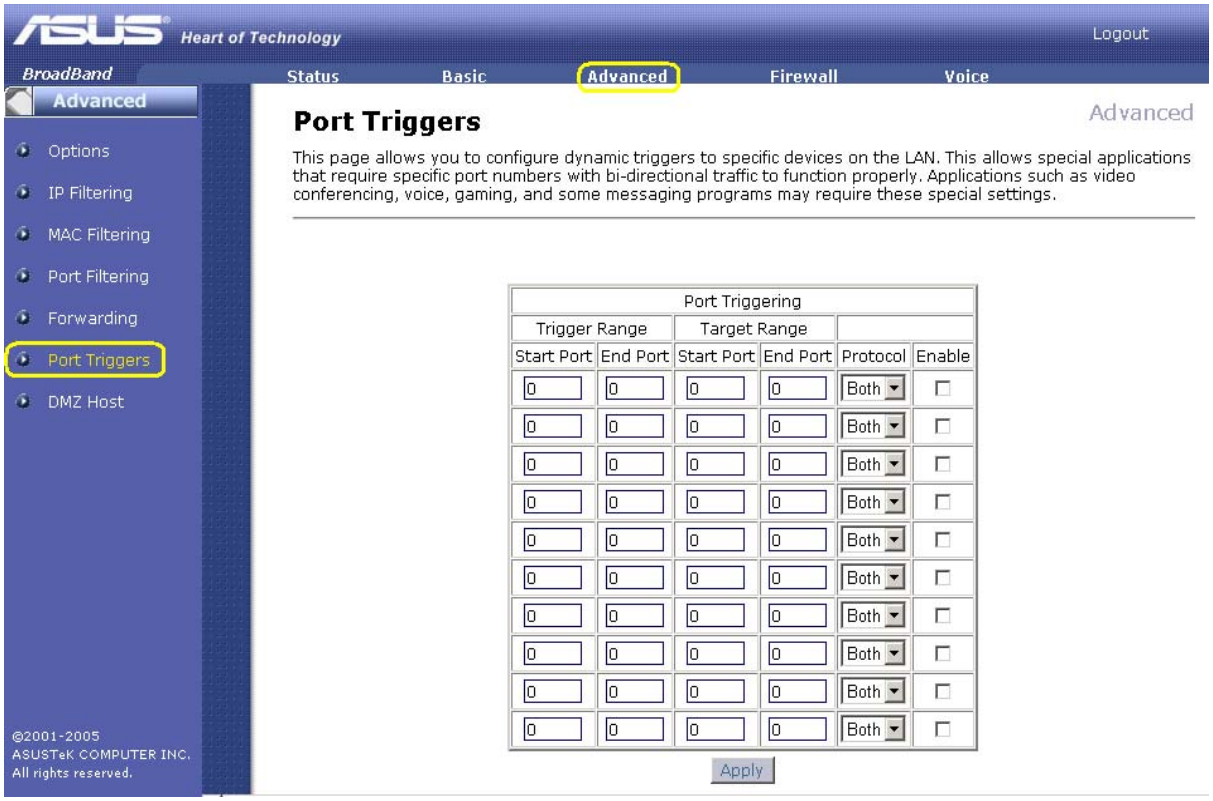
Forwarding allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC. The Forwarding page is shown below.



To specify a mapping, you must enter the range of port numbers that should be forwarded locally, and the IP address to which traffic to those ports should be sent. If only a single port specification is desired, enter the same port number in the "start" and "end" locations for that IP address. A table of commonly used Port numbers is supplied on the page for convenience.

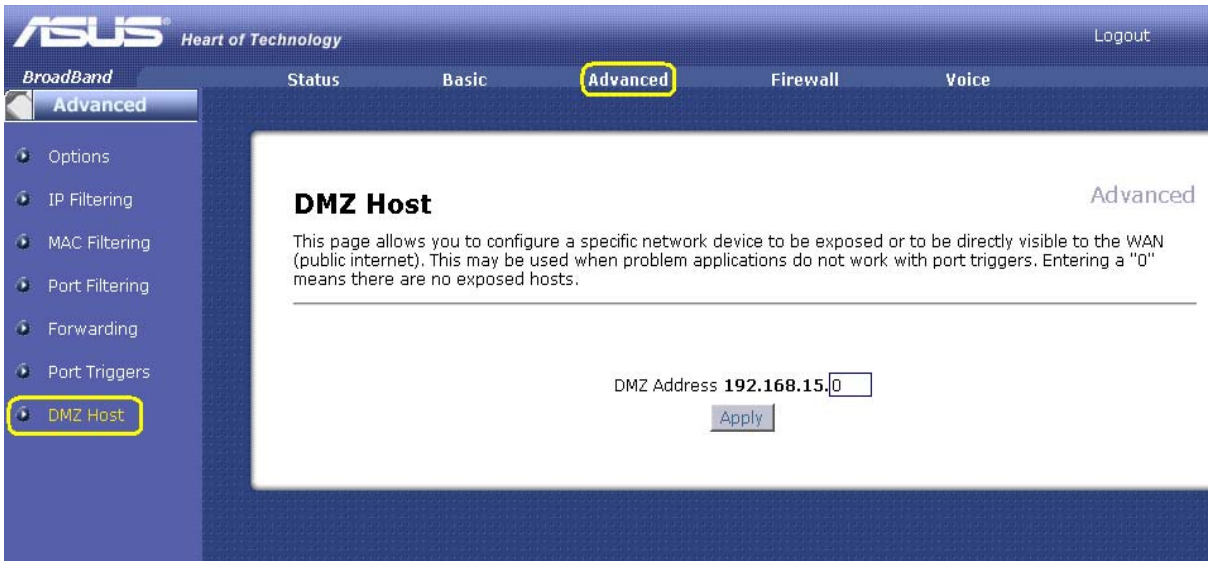
5.4 Port Triggering

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the SMTA detects outgoing data on a specific IP port number set in the "Trigger Range", the resulting ports set in the "Target Range" are opened for incoming (or sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the "Trigger Range" ports for 10 minutes, the "Target Range" ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.



5.5 DMZ Hosting

DMZ (De-militarized Zone) hosting (also commonly referred to as “Exposed Host”) allows you to specify the “default” recipient of WAN traffic that NAT is unable to translate to a known local PC. This can also be described as a computer or small sub-network that sits between the trusted internal private LAN, and the untrusted public Internet. The DMZ Host page is shown below.



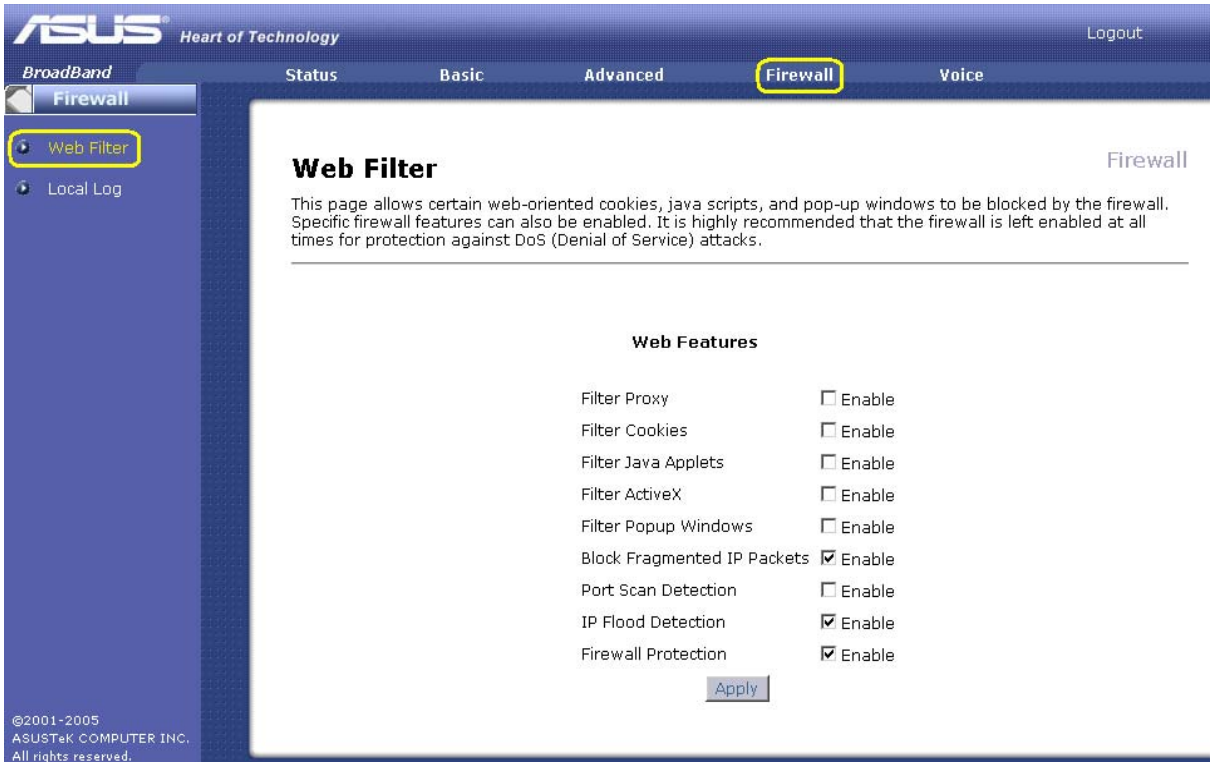
You may configure one PC to be the DMZ host. This setting is generally used for PCs using “problem” applications that use random port numbers and do not function correctly with specific port triggers or port forwarding setups mentioned earlier. If a specific PC is set as a DMZ Host, remember to set this back to “0” when finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the firewall.

6. Firewall Configuration

The SMTA contains an embedded firewall application to protect the Private LAN from malicious attacks (DoS, etc.) from the WAN interface.

6.1 Web Filter

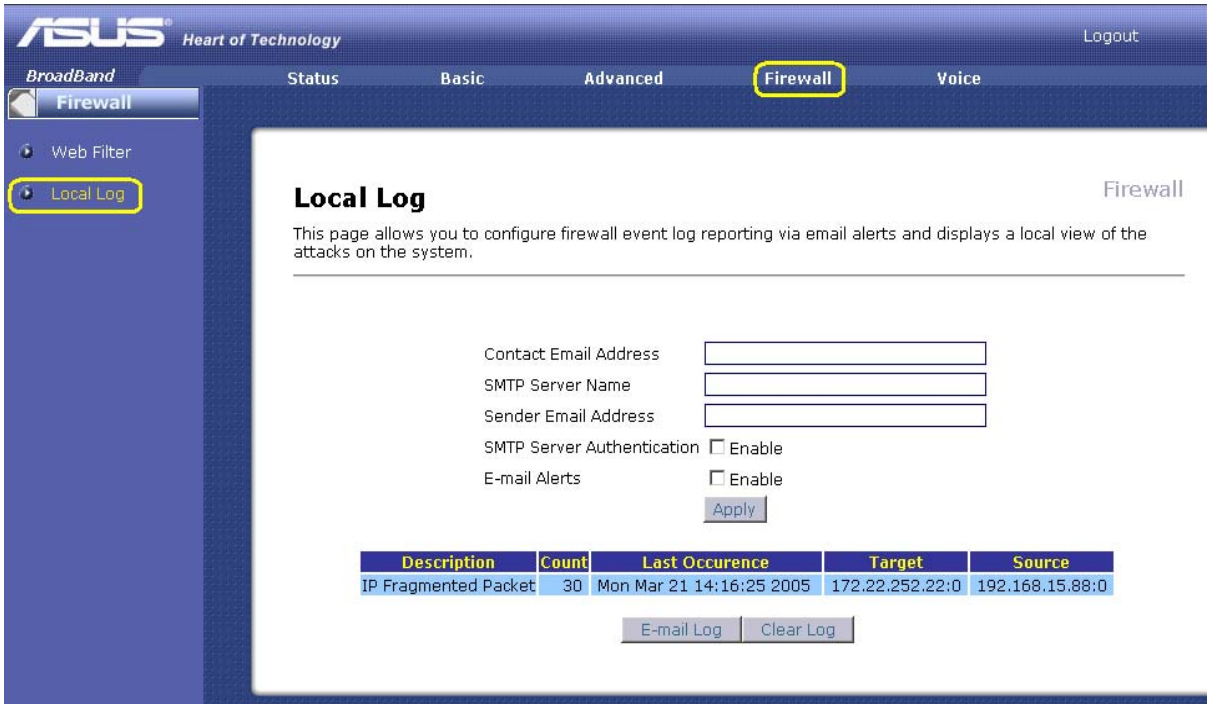
The Web Filter page has various settings related to blocking or exclusively allowing different types of data through the SMTA from the WAN to the LAN. The firewall enable checkbox is also present to allow enabling or disabling the firewall.



- **Proxies, Cookies, Java Applets, ActiveX controls,** and **Popup Windows** can all be blocked from this page.
- **Block Fragmented IP Packets** prevents all fragmented IP packets from passing through the firewall.
- **Port Scan Detection** detects and blocks port scan activity originating on both the LAN and WAN.
- **IP Flood Detection** detects and blocks packet floods originating on both the LAN and WAN. The Apply button must be clicked in order to activate any of the checkbox items. All of these settings can be activated quickly without rebooting the SMTA.
- **Firewall Protection** turns on the Stateful Packet Inspection (SPI) firewall features.

6.2 Local Event Log

The Local Log page can send firewall attack reports in two different ways. Individual emails can be sent out automatically each time the firewall is under attack, and also a local log is stored within the modem and displayed in table form on the Local Log page.



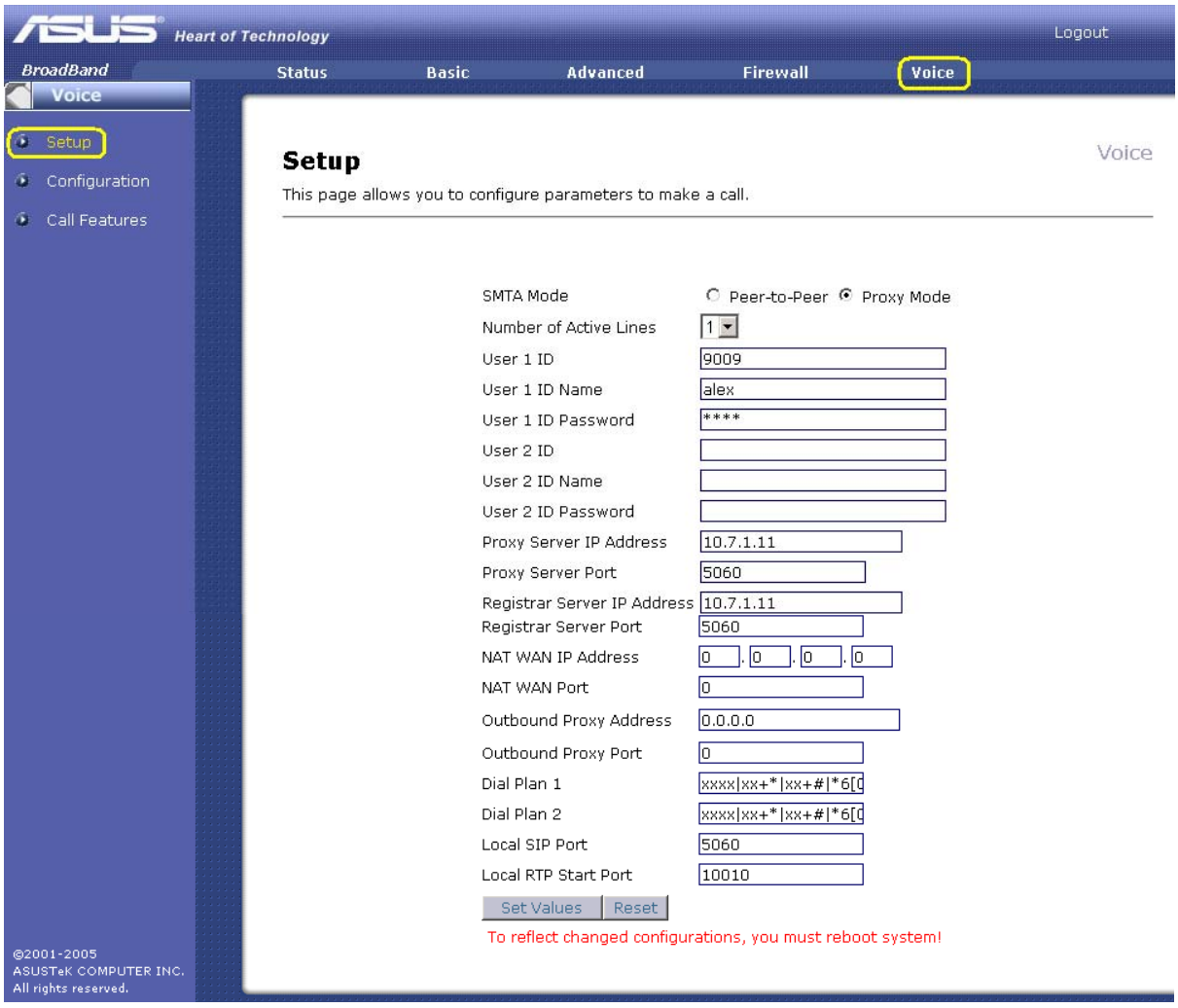
To enable the automatic email alerts, enter your email address in the space provided, enter that email account's email server address (provided by your ISP), check the "enable" box and click on the **Apply** button. Individual emails will now be sent to the specified address each time an attack is detected. Each attack is also logged in the table on the Event Log page. If desired, a summary of the Event Log Table can be sent to the specified contact email address by clicking on the Email Log button. Clicking on the Clear Log button can also clear the table.

7. Voice Setup

The SMTA contains a SIP user agent application to provide VoIP service on the Internet. This section will cover SIP user account, proxy server, register server and DSP feature settings.

7.1 Setup

The following is the screen for voice setup.



- **SMTA Mode: Peer-to-Peer:** Using Peer-to-Peer mode requires no additional setup. Just click on the radio button.
- **Proxy Mode:** If you are using proxy mode, then follow the below steps for setup.

    1. **Number of Active Lines**–this is the number of telephone lines or ports being used
    2. **User 1 ID**–this is the phone number
    3. **User 1 ID Name**–the name that appears on caller ID when you call out
    4. **User 1 Password**–the password for the User 1 ID

5. **User 2 ID / Name / Password**–enter info only if you have a second telephone line

6. **Proxy Server IP Address**–enter **0.0.0.0** if no proxy server is desired or enter the IP address that was issued by the VoIP service provider when you signed up

7. **Proxy Server Port**–this number is optional or if you obtained one from the VoIP service provider, enter it here

8. **Registrar Server IP Address**–enter **0.0.0.0** if no Registrar server is desired, however by registering, you can allow others to see your information

9. **Registrar Server Port**–this number is optional

10. **Outbound Proxy Address / Port**–this is provided by your service provider

11. **Dial Plan 1 / 2**–option of two plans for how numbers are dialed

12. **Local SIP Port**–5060 is the typical SIP port number, but it depends on your service provider

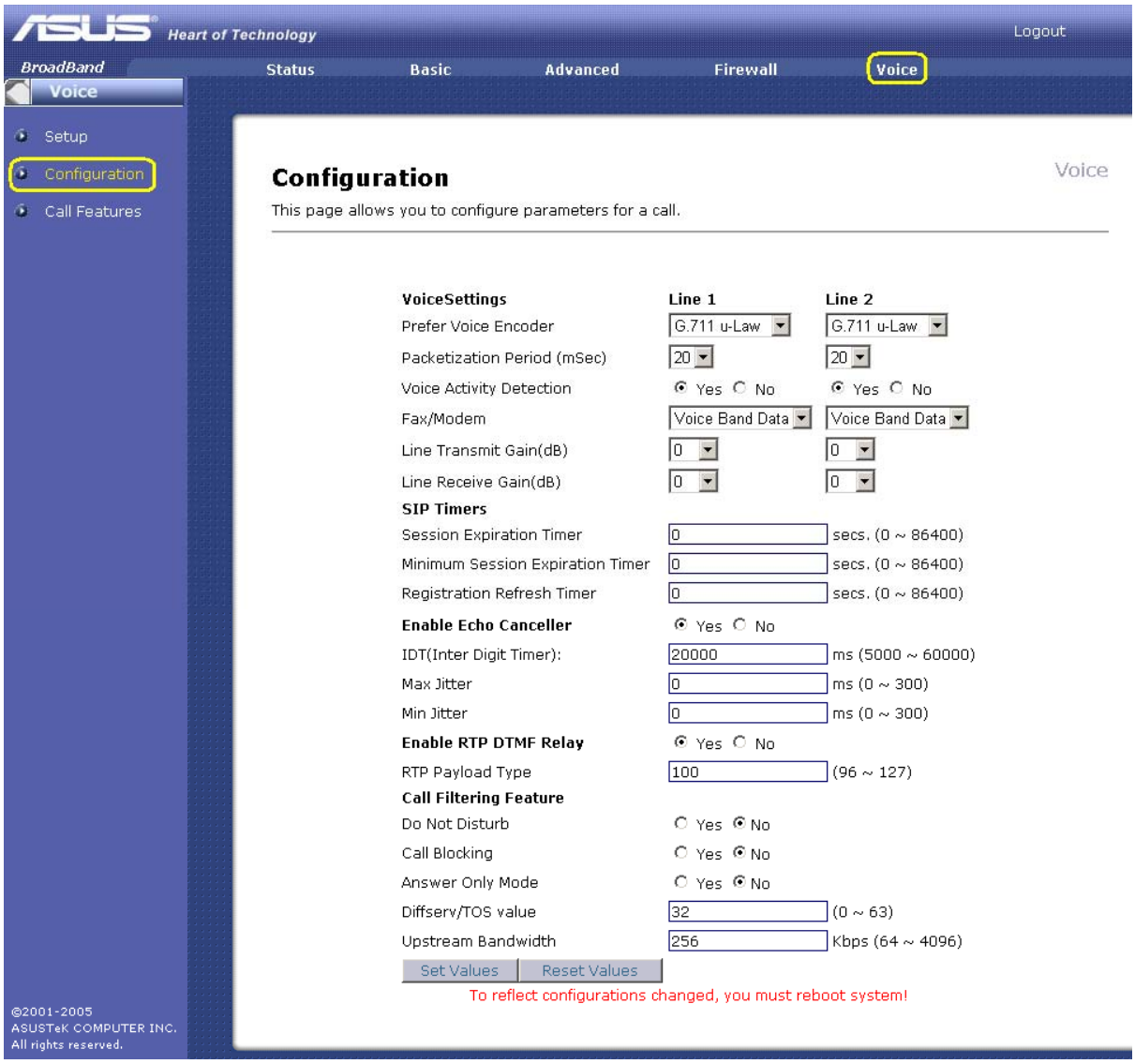
13. **Local RTP Start Port**–this is a starting parameter, usually a number in the 10000s

14. Click on the **Set Values** button when setup is complete

NOTE: *You must reboot the system in order for these settings to take effect.*

7.2 Voice Configuration

This page allows you to configure how to send and receive voice activity.



- **Prefer Voice Encoder**–select the voice encoder that you prefer. This does not guarantee that this encoder will be used, but will be taken into consideration when deciding which voice encoder to use. Each voice encoder varies by the amount of compression on the voice.

- **Packetization Period**–(in microseconds) this is how often a packet should be sent. This can increase or decrease the time duration between each packet sent.

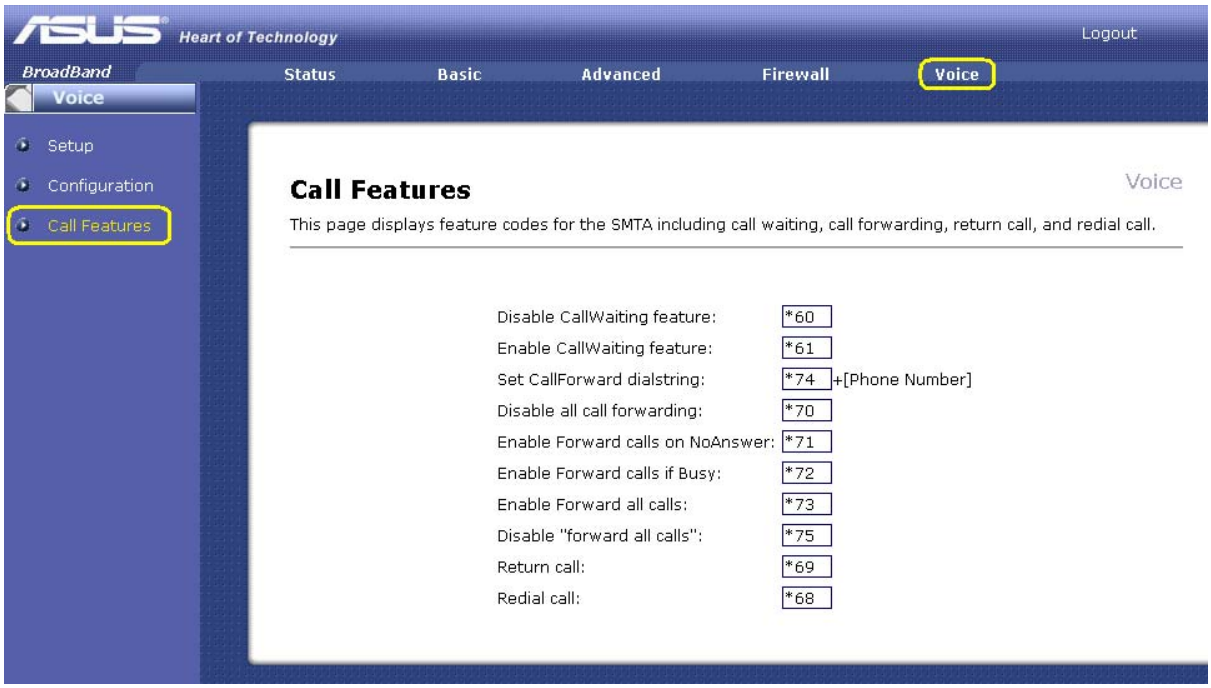
- **Voice Activity Detection**–enabling will control voice information to be sent based on voice activity, which can reduce voice traffic

- **Fax/Modem**–selecting *None* means that the codec will not be automatically adjusted, which may cause faxes to not be sent. *Voice Band Data* means that the codec will adjust for a successful fax transmission. Selecting *T.38* means that faxes being sent will not be affected by the codec selected. *T.38* is a special codec to send faxes. Voice Band Data is commonly used when faxes need to be sent.

- **Line Transmit Gain (db)**—the number of decibels that the volume of the voice being sent should be increased or decreased
- **Line Receive Gain (db)**—the number of decibels that the volume of the received voice should be increased or decreased
- **SIP Timers**—SIP register expiration timer and re-register timer setting
- **Session Expiration Timer (in microseconds)**—when a call session will end
- **Minimum Session Expiration Timer**—the shortest length of time that a call session will end
- **Registration Refresh Timer (in microseconds)**—the amount of time before registration is required again
- **Enable Echo Canceller**—enabling this feature will cancel out any echo in the call
- **IDT (Inter Digit Timer)**—length of wait time in between each number dialed before the numbers dialed are void and a busy tone is heard
- **Max / Min Jitter**—maximum/minimum time a packet is kept in buffer before it is converted from data back to voice. If this field is left at '0', then the system will use the defaults.
- **Enable RTP DTMF Relay**— Enabling DTMF relay and specify payload type can translate DTMF tone to a special RTP (real-time transport protocol) packet
- **RTP Payload Type**—works with RTP DTMF Relay
- **Do Not Disturb**—this call-filtering feature prevents incoming calls from coming through. Callers will hear a busy signal when you have the Do Not Disturb featured enabled.
- **Call Blocking**—this call-filtering feature allows you to restrict incoming calls from numbers on block list.
- **Answer Only Mode**— this mode is useful when you are unable to answer your phone for a long time and do not want to have voice messages accumulate. By turning on the Answer Only Mode, callers will hear a pre-recorded message and the call will be disconnected. The caller will not be able to leave a message.
- **Diffserv/ToS Value**—the value assigned to voice data in relation to the transmission requirement of voice so that the routing network has the capabilities to treat the transmission voice data differently from other data being sent on the network. The higher the value the greater the importance that voice data will have when being transmitted across the network.
- **Upstream Bandwidth**—the bandwidth in kbps (kilo-bits/sec) of upstream activity such as making outgoing calls or sending data. Enter a maximum bandwidth. If no call is being made, then the upstream bandwidth will be given entirely to Internet use.

7.3 Call Features

This page allows you see the feature codes for different call features such as call waiting, call forwarding, etc.



Call Feature	Function	Dial String
Call Waiting	Notifies you with beeps when you have another call on the line so you can take the call while placing the first caller on hold	• To Disable, dial ***60** • To Enable, dial ***61**
Set Call Forwarding dialstring	Enables you to set the dialstring of the designated phone number for which calls will be forwarded to	• To set the dialstring *ONLY*, dial ***74** and the phone number for which calls should be forwarded to • To Disable *ALL* CallForwarding, dial ***70**
Call Forward on No Answer	Enables you to forward incoming calls to another number when you do not answer	• To Enable, dial ***71**
Call Forward if Busy	Enables you to forward incoming calls to the designated number when you are on the line	• To Enable, dial ***72**
Forward all Calls	Enables you to forward ***ALL*** incoming calls (whether it is no answer or busy) to the designated phone number	• To Enable, dial ***73** • To Disable, dial ***75**
Return Call	Enables you to hear the number of the last incoming call	• To hear the number, dial ***69**
Redial Call	Enables you to redial the last number that you dialed	• To redial the last number dialed, press ***68**