

Wireless

This section allows you to configure wireless settings on your router.

Basic

The below Wireless - Basic screen lets you enable or disable wireless. The default setting for wireless is enabled. You can also hide the access point so others cannot see your ID on the network.

The screenshot shows the 'Wireless -- Basic' configuration page. On the left is a navigation tree with 'Wireless' expanded and 'Basic' selected. The main content area has a title 'Wireless -- Basic' and a description: '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" to configure the basic wireless options.' Below this are three settings: 'Enable Wireless' (checked), 'Hide Access Point' (unchecked), 'SSID' (text field with 'Broadcom'), 'BSSID' (text field with '12:E0:18:00:00:01'), and 'Country' (dropdown menu with 'ALL' selected). A 'Save/Apply' button is at the bottom right.

Security

The next screen is the Wireless - Security screen which allows you to select the network authentication method and to enable or disable WEP encryption. Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

The screenshot shows the 'Wireless -- Security' configuration page. On the left is a navigation tree with 'Wireless' expanded and 'Security' selected. The main content area has a title 'Wireless -- Security' and a description: 'This page allows you to configure security features of the wireless LAN interface. 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" to configure the wireless security options.' Below this are two settings: 'Network Authentication' (dropdown menu with 'Open' selected, showing a list of options: Open, Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, Mixed WPA2/WPA-PSK) and 'WEP Encryption' (dropdown menu with 'Disabled' selected). A 'Save/Apply' button is at the bottom right.

Network authentication methods include the following—

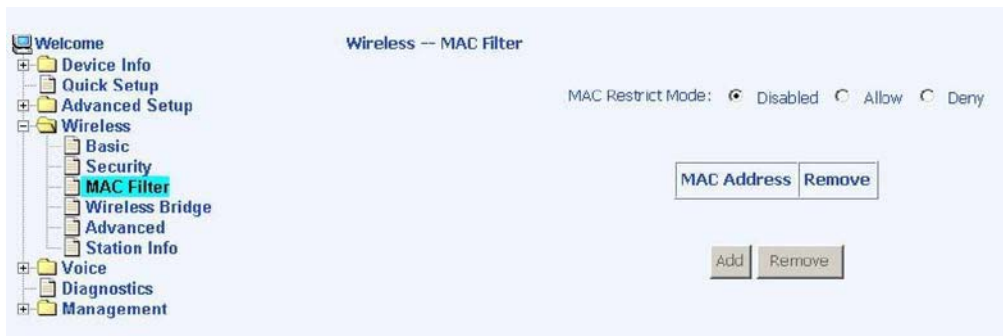
- Open—anyone can access the network. The default is a disabled WEP encryption setting.
- Shared—WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on Set Encryption Keys to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.
- 802.1X—requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.
- WPA—(Wi-Fi Protected Access)— usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses 128-bit dynamic session keys (per user, per session, and per packet keys).
- WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)— WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.
- WPA2 (Wi-Fi Protected Access 2)—second generation of WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-auth interval is the time in which another key needs to be dynamically issued.
- WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key)— suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and an re-key interval time.
- Mixed WPA2 / WPA—during transitional times for upgrades in the enterprise environment, this mixed authentication method allows “upgraded” and users not yet “upgraded” to

access the network via the router. RADIUS server information must be entered for WPA and as well as a group re-key interval time. Both TKIP and AES are used.

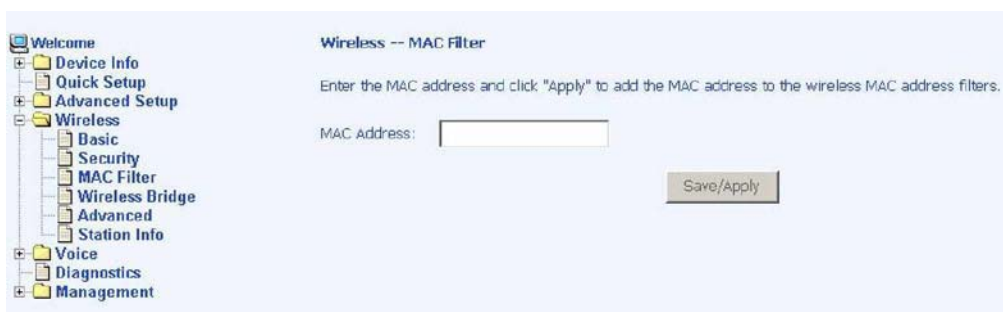
- Mixed WPA2 / WPA-PSK—useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.

MAC Filter

The MAC filter screen allows you to manage MAC address filters. Add the MAC addresses that you want to manage and then select the mode that you want to use to manage them. You can disable this feature or you can allow or deny access to the MAC addresses that you add to the list.



The following screen allows you to add a MAC address to the filter. When completed, click on the Save / Apply button.



Wireless Bridge

In this next screen you can select the mode, either access point or wireless bridge that you want the router to be in. In the screen below, bridge restrict is enabled, therefore you see the remote bridges MAC address fields. If bridge restrict is disabled, then there is nothing left to do afterwards. Click on Save / Apply to continue.

The screenshot shows a web interface for configuring a wireless bridge. On the left is a navigation menu with options: Welcome, Device Info, Quick Setup, Advanced Setup, Wireless (selected), Basic, Security, MAC Filter, Advanced, Station Info, Voice, Diagnostics, and Management. The main content area is titled 'Wireless -- Bridge'. It contains a paragraph explaining the configuration options: 'This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. 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: "Save/Apply" to configure the wireless bridge options.'

Below the text are three configuration fields:

- AP Mode:** A dropdown menu currently set to 'Access Point'.
- Bridge Restrict:** A dropdown menu currently set to 'Enabled'.
- Remote Bridges MAC Address:** A field containing the MAC address '02:50:C9:08:66:9C' with two empty input boxes next to it for additional addresses.

At the bottom right of the configuration area are two buttons: 'Refresh' and 'Save/Apply'.

Advanced

Advanced features of the wireless LAN interface can be configured in this section.

Settings can be configured for the following—

- **AP Isolation**—if you select enable, then each of your wireless clients will not be able to communicate with each other.
- **Band**—a default setting at 2.4GHz - 802.11g
- **Channel**— 802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your router.
- **Multicast Rate**—the rate at which a message is sent to a specified group of recipients.

- **Basic Rate**—the set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium.
- **Fragmentation Threshold**—used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
- **RTS Threshold (Request to Send Threshold)**—determines the packet size of a transmission through the use of the router to help control traffic flow.
- **DTIM Interval**—sets the Wake-up interval for clients in power-saving mode.
- **Beacon Interval**—a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
- **Xpress Technology**—a technology that utilizes standards based on framebursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b equipment.
- **54g Mode**— 54g is a Broadcom Wi-Fi technology.
- **54g Protection**—the 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS (Request to Send / Clear to Send) to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **WMM (Wi-Fi Multimedia)**—feature that improves the your experience for audio, video and voice applications over a Wi-Fi network.

Welcome

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
 - Basic
 - Security
 - MAC Filter
 - Wireless Bridge
 - Advanced**
 - Station Info
- Voice
- Diagnostics
- Management

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" to configure the advanced wireless options.

AP Isolation:

Band:

Channel:

Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

XPress™ Technology:

54g™ Mode:

54g Protection:

WMM(Wi-Fi Multimedia):

Station Info

This screen shows computers or other devices accessing your router through its wireless connection.

Welcome

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
 - Basic
 - Security
 - MAC Filter
 - Wireless Bridge
 - Advanced
 - Station Info**
- Voice
- Diagnostics
- Management

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status

BSSID	Associated	Authorized
00:11:2F:9D:1A:55		

Voice

This section explains the configuration of the voice function of your router. Configurations include basic and advanced SIP setup, phonebook, and call history.

SIP Basic

Following is the screen for SIP configuration.

The screenshot shows a web-based configuration interface for SIP. On the left is a navigation tree with the following items: Welcome, Device Info, Quick Setup, Advanced Setup, Wireless, Voice (selected), SIP Basic, SIP Adv, Phonebook, Call History, Diagnostics, and Management. The main area is titled "Voice -- SIP configuration" and contains the instruction "Enter the SIP Basic parameters." Below this are various configuration fields:

- Interface name: Br0 - Bridge (dropdown)
- SIP mode: Peer-to-Peer (dropdown)
- SIP Proxy: 0.0.0.0
- SIP Proxy port: 5060
- SIP Registrar: 0.0.0.0
- SIP Registrar port: 5060
- SIP domain name: (empty)
- SIP Outbound Proxy: 0.0.0.0
- SIP Outbound Proxy port: 5060
- User 1 ID: 1001
- User 1 ID Name: 1001
- User 1 Authentication Name: (empty)
- User 1 ID Password: ****
- User 2 ID: 2001
- User 2 ID Name: 2001
- User 2 Authentication Name: (empty)
- User 2 ID Password: ****
- ☐ FXO Enabled
- Dial plan: |xxx|xx.*|xx.#|*6[01234589]|*7[0-35]|*74xxx|*90|*
- SIP local port: 5060
- RTP start port: 10010

At the bottom right are two buttons: "Save Config" and "Stop SIP client".

- Interface Name— select the name of the interface that you are using.
- SIP Mode— includes peer-to-peer or proxy mode.

- SIP Proxy– enter 0.0.0.0 if no proxy server is being used or enter the IP address that was issued by the VoIP service provider when you signed up.
- SIP Proxy Port– this number is optional or if you obtained one from the VoIP service provider, enter it here.
- SIP Registrar– enter 0.0.0.0 if no proxy server is being used or enter the IP address that was issued by the VoIP service provider when you signed up.
- SIP Registrar Port–this number is optional
- SIP Domain Name– enter the domain name of the SIP server if you are using one
- SIP Outbound Proxy– provided by your service provider
- SIP Outbound Proxy Port– provided by your service provider
- User 1 ID– this is the phone number
- User 1 ID Name– the name that appears on caller ID when you call out
- User 1 Authentication Name– the user name provided by your service provider.
- User 1 ID Password–the password for the User 1 ID
- User 2 ID / ID Name / Authentication Name / ID Password– enter info only if you have a second telephone line
- FXO Enabled– check this box to enable FXO and allow for configuration of FXO. Enabling FXO means that you have the FXS (the phone jack on the wall) attached to the LINE port on the router. Essentially, you have telephone service to your router.

- FXO Call ID— the telephone number to access the PSTN line.
- FXO Call ID Name— the default is 3001, but you can change it to the name that appears on caller ID
- FXO Authentication Name— the name of the user that is allowed to access the voice function of the router
- FXO Call ID Password— the password for the FXO call ID
- Dial Plan— plan for how numbers are dialed when using VoIP. General characters in a dial plan are 0,1,2,3,4,5,6,7,8,9,*,#. Special characters in the dial plan include the following—

Special Characters in Dial Plan	
[]	Any one of the characters in brackets
X	Any digit character
+	Zero or more repetitions of previous expression
.	Zero or more repetitions of previous expression, same as +
()	Expression grouping, all digits in parentheses must exist and the order should match too
	Either, or

Below is an example of how a dial plan works—

With the dial plan `xxxx | xx+* | xx+# | *6[0189] | *7[0-35] | *74xxxx`, you can dial the following 6 types of phone numbers.

- (1) 4 arbitrary digits
- (2) arbitrary length of digits (at least one) with last input equal to *
- (3) arbitrary length of digits (at least one) with last input equal to #
- (4) *60, *61, *68, or *69
- (5) *70, *71, *72, *73, or *75
- (6) *74 and followed by 4 arbitrary digits

- SIP Local Port– 5060 is the typical SIP port number, but it depends on your service provider
- RTP Start Port– this is a starting parameter, usually a number in the 10000s for Real-Time Transport Protocol

SIP Advanced

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

Voice -- SIP Advanced configuration

Enter the SIP Advanced parameters.

Preferred codec: G711U
 Packetisation time: 20
 VAD state: Enable
 ECAN state: Enable
 DTMF relay state: RFC 2833
 Fax mode: Voice Band Data

SIP re-register timer: 300 (0-86400)
 Session expire timer: 0 (0-86400)
 Signaling/Voice TOS: 32 / 32 (0-63)/(0-63)
 Inter/Critical digit timer: 16 / 4 (4-60)/(4-16)

Do Not Disturb: ☐ Enable ☒ Disable
 Answer Only: ☐ Enable ☒ Disable

Prefix for switch VOIP to PSTN: 00
 PSTN Dialplan: 911
 PSTN route rule: Auto

Locale selection: USA - United States

☒ Remote server for SIP log messages.
 Log IP Address: 192.168.1.100
 Log port: 55555

Save Config Stop SIP client

- Preferred Codec– 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.

- Packetisation Time— (in microseconds) this is how often a packet should be sent. This can increase or decrease the time duration between each packet sent.
- VAD State— Voice Activity Detection—enabling will control voice information to be sent based on voice activity, which can reduce voice traffic
- ECAN State— Echo Canceller— enabling this feature will cancel out any echo in the call
- DTMF Relay State— select between voice band and RFC 2833. RFC 2833 describes how to carry out DTMF signaling, other tone signals, and telephony events in RTP packets.
- Fax Mode— select between none or voice band data. Voice band data is data being passed as audio using an audio codec. Voice and voice band data have different trade-offs—voice requires low delay, but voice band data requires low packet loss.
- SIP Re-register Timer— (in microseconds)—the amount of time before registration is required again
- Session Expire Timer— (in microseconds)—when a call session will end
- Signaling / Voice TOS— type of service for signaling and voice. A signaling transmission is used for building a voice connection. Voice TOS is used for voice transmission. Each call has two parts—first part involves the signaling transmission when a call is made or received. The second part is when the call is connected, it transfers voice in voice transmission.
- Inter / Critical Digit Timer— inter-digit timer (IDT) is used as timeout check between each digit dialed, while the critical digit timer (CDT) is used for "almost completed" dialing to wait for more digits. Essentially, CDT is the time that the device waits after the digits are dialed before it dials the numbers.

- 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.
- Answer Only— 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.
- Prefix for Switch VOIP to PSTN— one of the ways that a phone number can be dialed using PSTN (and not VoIP). It is the number prefix that you must enter in order to switch from using VOIP to your regular phone (public switched telephone network).
- PSTN Dialplan— the PSTN dial plan is the first dial plan that the device will look at before dialing. If the numbers match the PSTN dial plan, then the PSTN line, not VoIP line, will be used. Therefore, you should be careful when selecting your PSTN dial plan to prevent VoIP calls from being dialed from your PSTN line.
- PSTN Route Rule— for incoming or outgoing calls using PSTN, this is the line (line 1 or line 2) that the call is sent or received through. You can select auto so that it automatically selects an open line.
- Locale Selection— the location that you are using the router
- Remote Server for SIP Log Messages— if you enable the remote server, then fill out the following two fields—log IP address and log port.
- Log IP Address— the IP address of the remote server for SIP log message
- Log Port— the port number of the remote server

Phonebook

The phonebook allows you to filter calls from specified IP addresses. Enter the IP addresses in the Call ID field and then decide whether you want to allow or deny those enabled callers. You can also organize the calls by ring group (default, family, friend, and colleague).

Welcome

- + Device Info
- + Quick Setup
- + Advanced Setup
- + Wireless
- + **Voice**
 - SIP Basic
 - SIP Adv
 - Phonebook
 - Call History
 - Diagnostics
 - + **Management**

Voice -- SIP Phonebook

Enter individually setup.

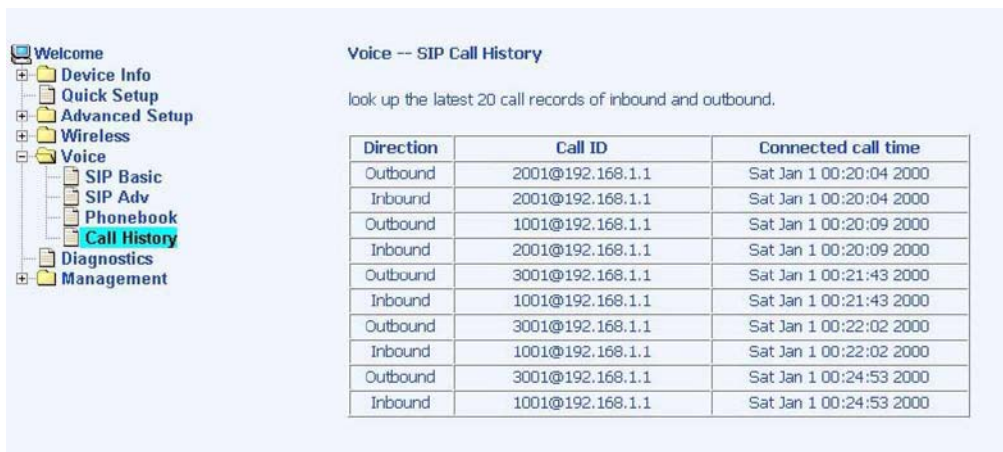
Call Filtering: ☐ Allow ☒ Deny

Call ID	SpeedDial	RingGroup	Enabled
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐
@ 0.0.0.0	N/A	Default	☐

Save Config
Stop SIP client

Call History

The SIP Call History screen allows you to view up to 20 of the latest inbound / outbound calls. You will see the phone numbers and IP addresses as the call ID as well as the call time and date.



Voice -- SIP Call History

look up the latest 20 call records of inbound and outbound.

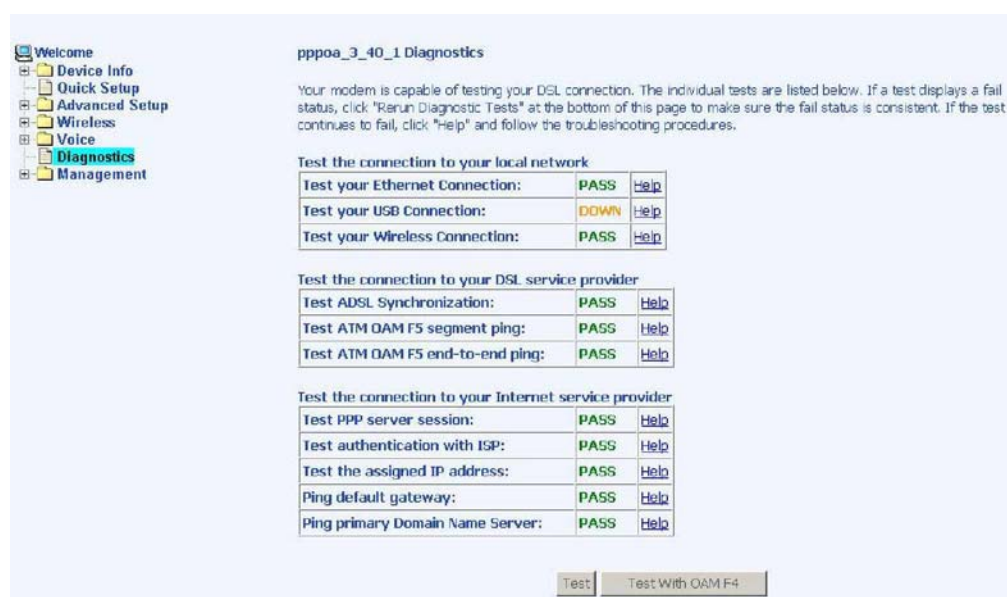
Direction	Call ID	Connected call time
Outbound	2001@192.168.1.1	Sat Jan 1 00:20:04 2000
Inbound	2001@192.168.1.1	Sat Jan 1 00:20:04 2000
Outbound	1001@192.168.1.1	Sat Jan 1 00:20:09 2000
Inbound	2001@192.168.1.1	Sat Jan 1 00:20:09 2000
Outbound	3001@192.168.1.1	Sat Jan 1 00:21:43 2000
Inbound	1001@192.168.1.1	Sat Jan 1 00:21:43 2000
Outbound	3001@192.168.1.1	Sat Jan 1 00:22:02 2000
Inbound	1001@192.168.1.1	Sat Jan 1 00:22:02 2000
Outbound	3001@192.168.1.1	Sat Jan 1 00:24:53 2000
Inbound	1001@192.168.1.1	Sat Jan 1 00:24:53 2000

Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. The results will show test results of three connections—

- Connection to your local network
- Connection to your DSL service provider
- Connection to your Internet service provider

There are two buttons at the bottom of the screen—Test and Test with OAM F4—which will allow you to retest if necessary.



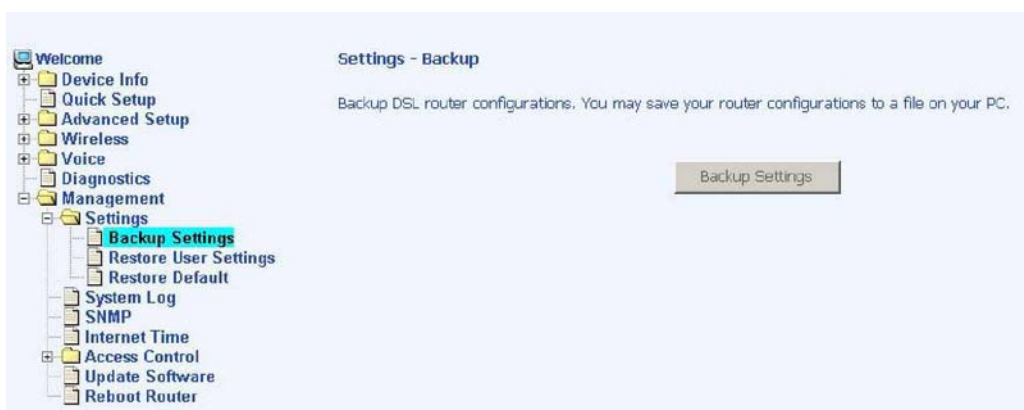
Management

The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

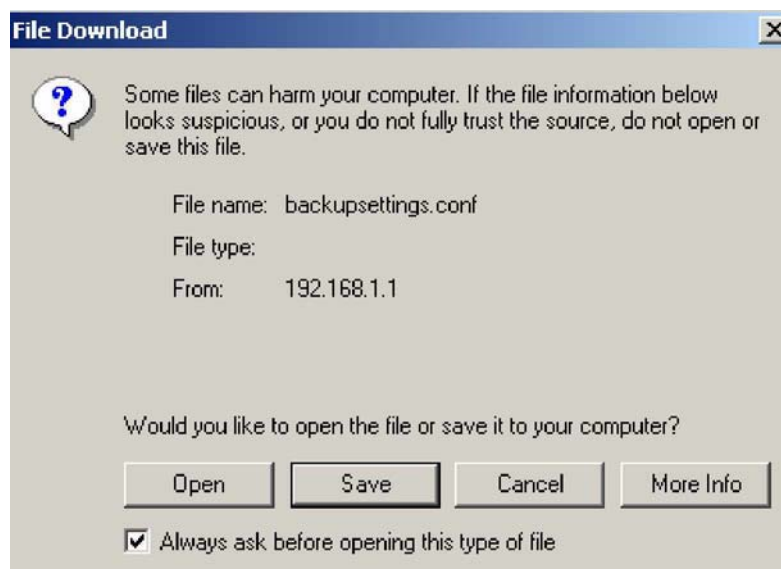
Settings

Backup Settings

To save a copy of the configurations that you have made on your router, click on the Backup Settings button.

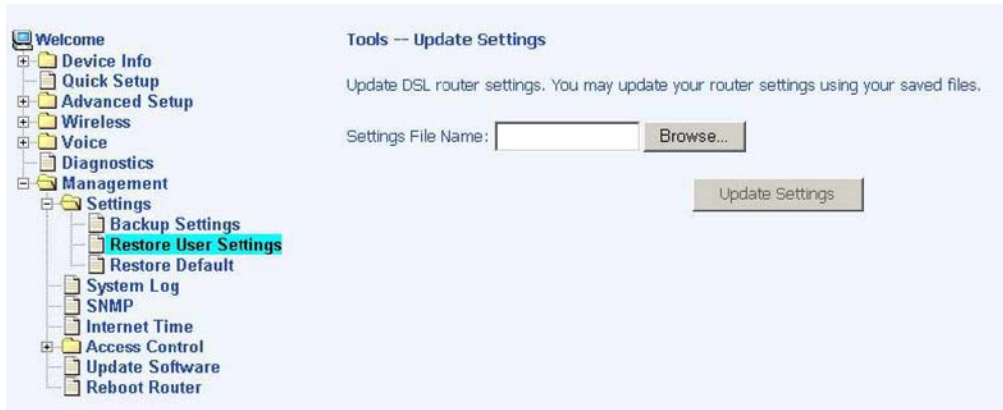


The below pop-up screen will appear with a prompt to open or save the file to your computer.



Restore User Settings

To load a previously saved configuration file onto your router, click Browse to find the file on your computer and click on Update Settings.



The router will restore settings and reboot to activate the restored settings.

Restore Default

Restore Default will delete all current settings and restore the router to factory default settings. Click on the Restore Default Settings button.



Click on OK when the pop-up window appears confirming that you want to restore factory default settings to your router.

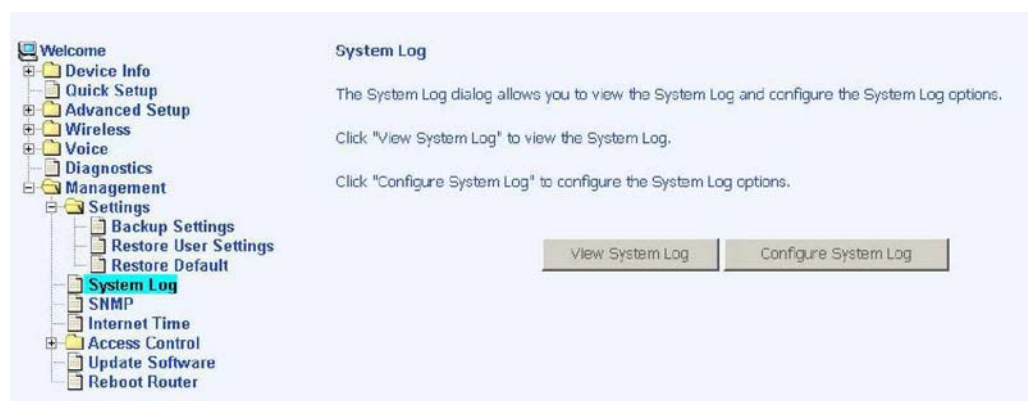


The router will restore the default settings and reboot.

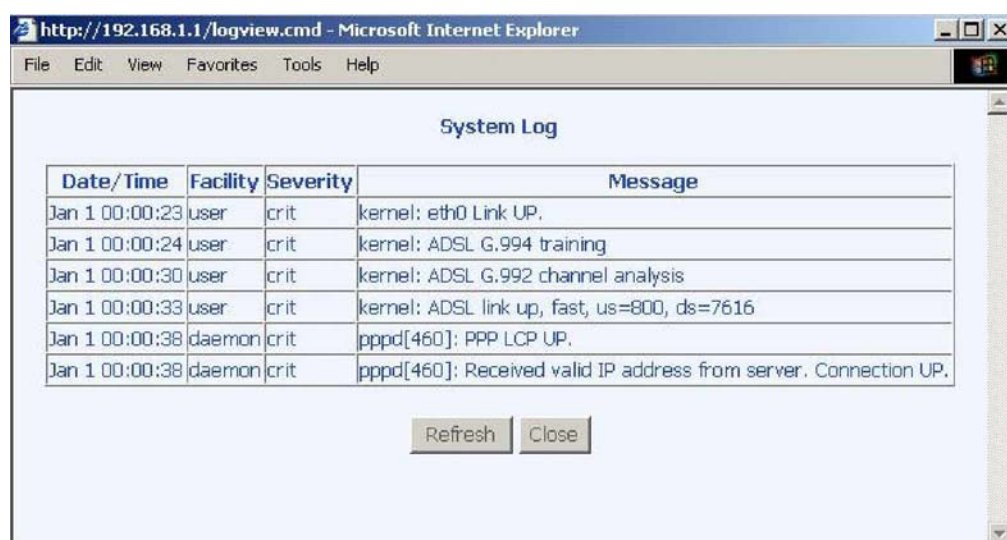
System Log

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

To view the System Log click on the View System Log button to check the log file.



Below is a view of the System Log.



Configure System Log

If the log is enabled, the system will log selected events including Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging. All events above or equal to the selected log level will be logged and displayed.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level:

Display Level:

Mode:

Save/Apply

If the selected mode is “Remote” or “Both”, events will be sent to the specified IP address and UDP port of a remote system log server. If the selected mode is “Local” or “Both”, events will be recorded in the local memory. Select the desired values and click on the “Save/Apply” button to configure the system log options.

SNMP

SNMP (Simple Network Management Protocol) provides a means to monitor status and performance as well as set configuration parameters. It enables a management station to configure, monitor and receive trap messages from network devices.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click 'Apply' to configure the SNMP options.

SNMP Agent ☒ Disable ☐ Enable

Read Community:

Set Community:

System Name:

System Location:

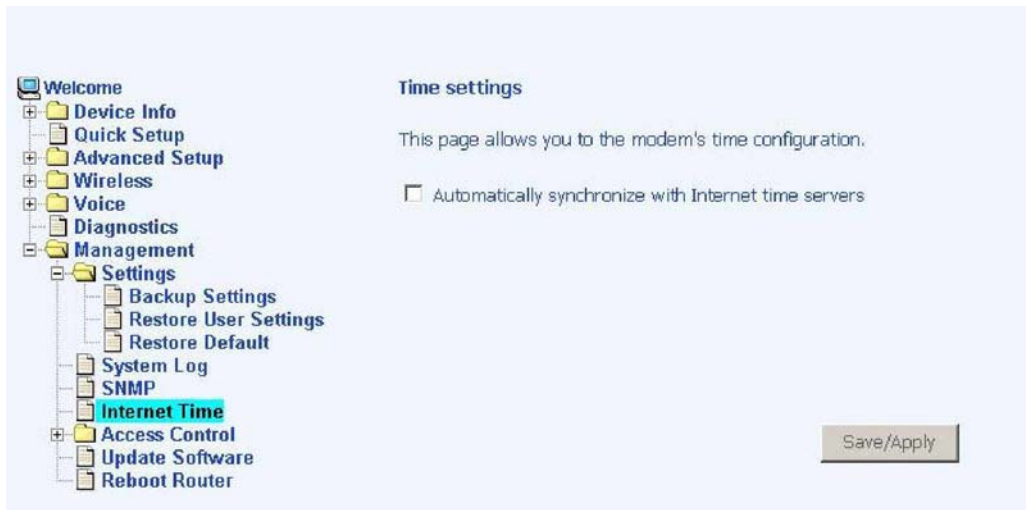
System Contact:

Trap Manager IP:

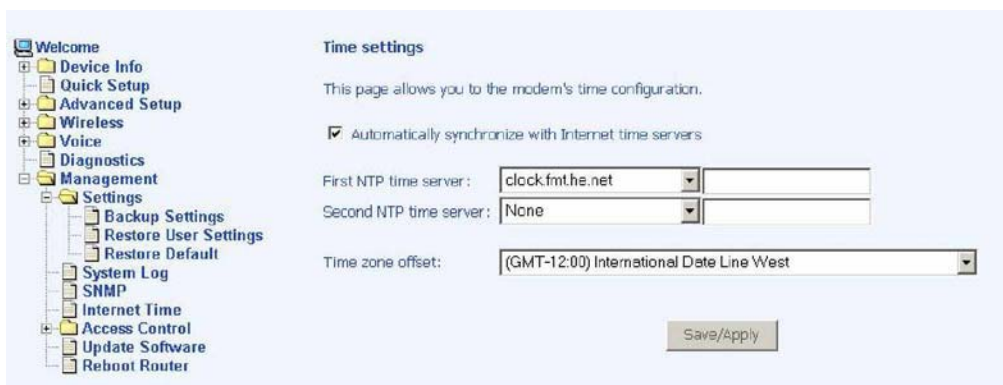
Save/Apply

Internet Time

The Time Settings screen allows you to automatically synchronize your time with a timeserver on the Internet.



If you choose to automatically synchronize with Internet time servers, then click on the box and the below fields appear. Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click on Save / Apply to save and complete your time settings.

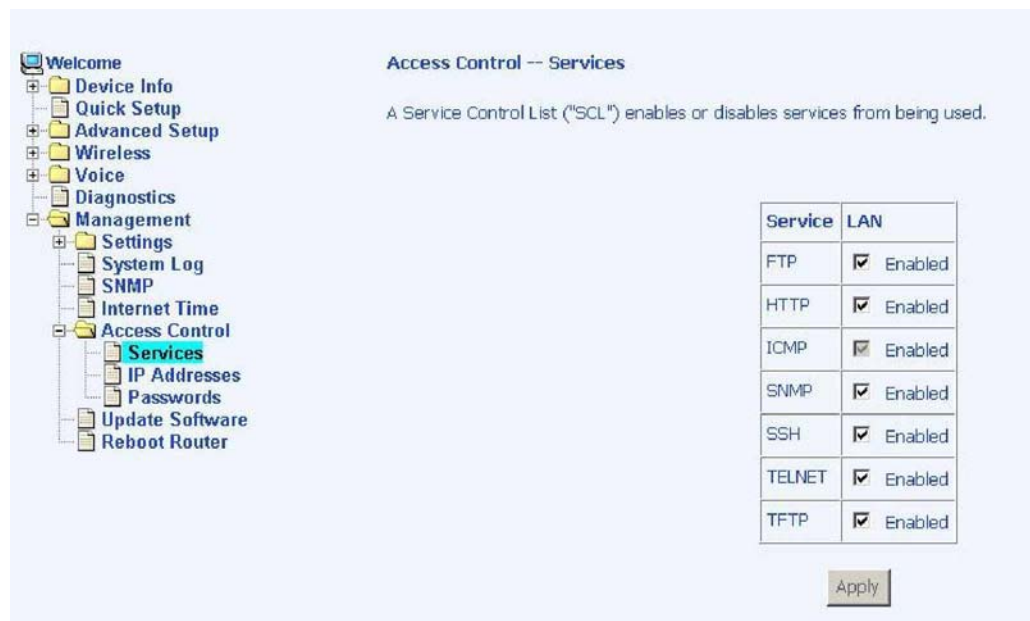


Access Control

You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, then only the LAN side can be configured.

Services

Services that can be enabled include FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Click on Apply when finished.



IP Addresses

Web access to the router can be limited when Access Control Mode is enabled. The IP addresses of allowed hosts can be added using Access Control  Address.

Add the IP address to the IP address list by clicking on the Add button, then select “Enabled” to enable Access Control Mode.



To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the Save / Apply button.

The screenshot shows the 'Access Control' configuration page. On the left is a navigation tree with categories like Welcome, Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. Under Management, 'Access Control' is expanded, showing sub-items: Settings, System Log, SNMP, Internet Time, Services, IP Addresses, Passwords, Update Software, and Reboot Router. The main content area is titled 'Access Control' and contains the instruction: 'Enter the IP address of the management station permitted to access the local management services, and click "Save/Apply."' Below this is a text input field labeled 'IP Address:' and a 'Save/Apply' button.

Passwords

Access the Passwords screen under the Access Control section to change a password. Select an account and enter the current password and the new password and then click on the Save / Apply button.

The screenshot shows the 'Access Control -- Passwords' configuration page. The left navigation tree is identical to the previous screenshot, but 'Passwords' is now selected under the 'Access Control' section. The main content area is titled 'Access Control -- Passwords' and contains the following text: 'Access to your DSL router is controlled through three user accounts: admin, support, and user.' It then lists the roles for 'admin', 'support', and 'user'. Below this, it says: 'Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.' There are four input fields: 'Username:' (a dropdown menu), 'Old Password:', 'New Password:', and 'Confirm Password:'. A 'Save/Apply' button is at the bottom right.

Update Software

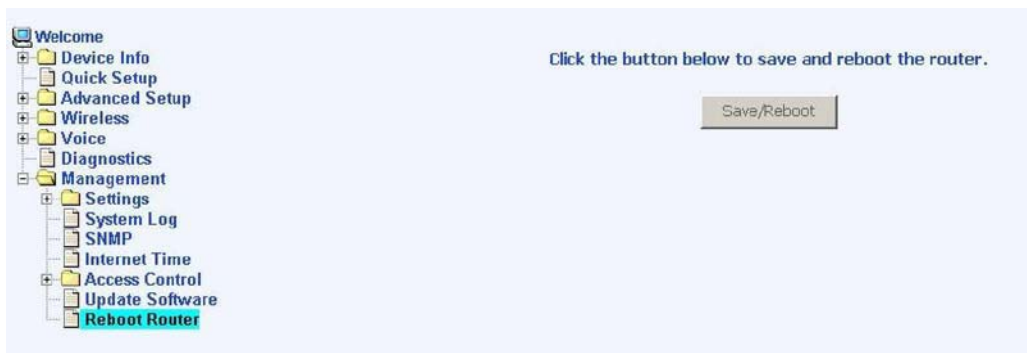
If your ISP releases new software for this router, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Enter the path to the image file location or click on the Browse button to locate the image file.
3. Click the Update Software button once to upload the new image file.



Reboot Router

Select “Reboot Router” under “Access Control” to reboot the router using the web interface. The router will save the current configuration and reboot itself using the new configuration.



FCC Warning Statement

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

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

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter

Safety Information

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. **Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.**

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 300 386 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 has been conducted. These are considered relevant and sufficient.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.