



WLR-2001/WLR3001

Wireless Broadband Router

(802.11b/g/n)



User Manual

TABLE OF CONTENTS

1	KEY FEATURES.....	4
2	PACKAGE CONTENTS.....	5
1	CAUTIONS.....	6
3	PRODUCT LAYOUT.....	7
4	NETWORK + SYSTEM REQUIREMENTS.....	10
5	WLR-2001/WLR3001 PLACEMENT.....	10
6	SETUP LAN, WAN.....	11
7	PC NETWORK ADAPTER SETUP.....	12
8	BRING UP THE WLR-2001/WLR3001.....	16
9	INITIAL SETUP WLR-2001/WLR3001.....	16
10	CONFIGURATION WIZARD.....	25
11	WIRELESS SETTINGS.....	27
12	FIREWALL SETTINGS.....	37
13	ADVANCED SETTINGS.....	43
14	TOOLBOX SETTINGS.....	50

Revision 1.2

© Sitecom Europe BV 2011

Note: All the information contained in this manual was correct at the time of publication.

However, as our engineers are always updating and improving the product, your device's software may have a slightly different appearance or modified functionality than presented in this manual.

Introduction

Congratulations on your purchase of the WLR-2001/WLR3001 Wireless Network Broadband Router. The WLR-2001/WLR3001 is compliant with 802.11n and up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b. The WLR-2001/WLR3001 is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Switch that connects your wired-Ethernet devices together.

At 300 Mbps (150 Mbps for the WLR-2001/WLR3001) wireless transmission rate, the Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel, giving you seamless access to multimedia content. Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, the WLR-2001/WLR3001 encodes all wireless transmissions with WEP, WPA, and WPA2 encryption.

With the inbuilt DHCP Server & powerful SPI firewall, the WLR-2001/WLR3001 protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With incredible speed and QoS function of 802.11n(draft2.0), the WLR-2001/WLR3001 is ideal for media-centric applications like streaming video, gaming, and VoIP telephony to run multiple media-intensive data streams through the network at the same time, with no degradation in performance.

The router includes Sitecom Cloud Security to protect your home network against cybercrime.

1 Key Features

Features	Advantages
Incredible Data Rate up to 300Mbps* (150Mbps for WLR-2001/WLR3001)	Heavy data payloads such as MPEG video streaming
IEEE 802.11n compliant and backwards compatible with 802.11b/g	Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices with legacy protection
Four 10/100 Mbps Fast Switch Ports (Auto-Crossover)	Scalability, extend your network.
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	Avoids the attacks of Hackers or Viruses from Internet
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security
WDS (Wireless Distribution System)	Make wireless AP and Bridge mode simultaneously as a wireless repeater
Sitecom Cloud Security	Security integrated in the router protects all the devices in your network against cybercrime when surfing the Internet.

** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLR-2001/WLR3001 Router
2. 5V 1A Power Adapter
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable

1 Cautions

This router's design and manufacturer has your safety in mind. In order to safely and effectively use this router, please read the following before usage.

3.1 Usage Cautions

The user should not modify this router. The environmental temperature should be within +5 ~ +35 degrees Celsius.

3.2 Power

The router's power voltage is DC 5V 1A.

When using this router, please connect the supplied AC adapter or AC adapter cable to the router's power jack. When placing the adapter cable, make sure it can not get damaged or be subject to pressure. To reduce the risk of electric shock, unplug the adapter first before cleaning it. Never connect the adapter to the router in a humid or dusty area. Do not replace the adapter or cable's wire or connector.

3.3 Repair

If the router has a problem, you should take it to an appointed repair centre and let the specialists do the repair. Never repair the router yourself, you might damage the router or endanger yourself.

3.4 Disposing of the Router

When you dispose of the router, be sure to dispose it appropriately. Some countries may regulate disposal of an electrical device, please consult with your local authority.

3.5 Others

When using this router, please do not let it come into contact with water or other liquids. If water is accidentally spilled on the router, please use a dry cloth to absorb the spillage. Electronic products are vulnerable, when using please avoid shaking or hitting the router, and do not press the buttons too hard.

- Do not let the router come into contact with water or other liquid.
- Do not disassemble the router; repair the router or change the design of the router, any damage done will not be included in the repair policy.
- Avoid hitting the router with a hard object, avoid shaking the router and stay away from magnetic fields.
- If during electrostatic discharge or a strong electromagnetic field the product will malfunction, unplug the power cable. The product will return to normal performance the next time it is powered on.

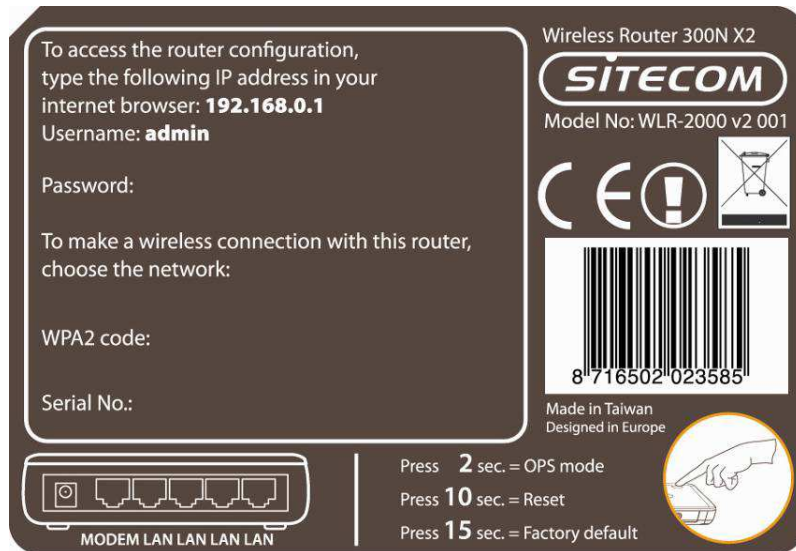
3 Product Layout



Port	Description
Power connector	Connect the 5V DC adapter to this port
WAN (Blue)	Connect your ADSL/Cable modem to this port
LAN (Yellow)	Connect your PC's or network devices to this port

Backlabel

The backlabel describes the IP address, login details, SSID, security code and WPS button functionality.



Button	Description
WPS BUTTON	Press 2 seconds for WPS mode Press 10 seconds to reset the router Press 15 Seconds to reset the router to factory defaults.

LED Definition

From left to right.

Port	Description
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
LAN (Blue)	Shows the cable is connected.
WAN (Blue)	Shows the cable is connected.
WiFi (Blue)	Shows WiFi activity and WPS.
Power (Red)	Shows the device is turned on.



4 Network + System Requirements

To begin using the WLR-2001/WLR3001, make sure you meet the following as minimum requirements:

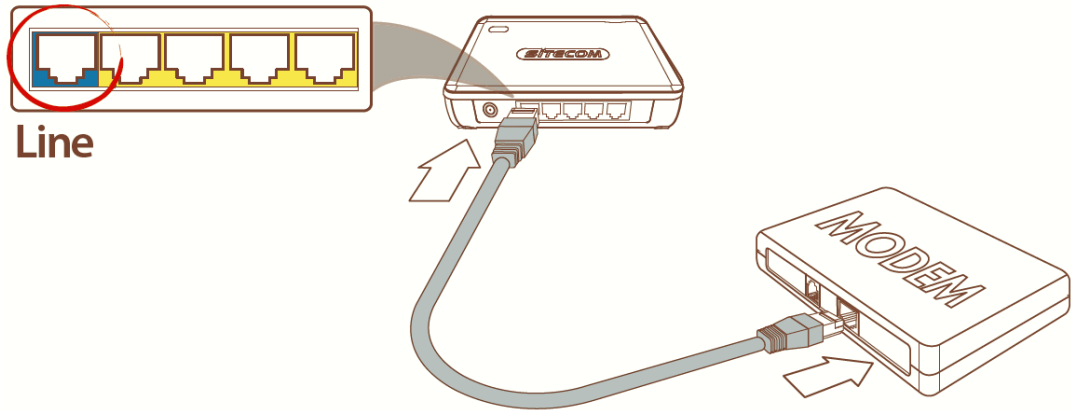
- PC/Notebook.
- Operating System – Microsoft Windows XP/VISTA/7
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11 b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5 cables.

5 WLR-2001/WLR3001 Placement

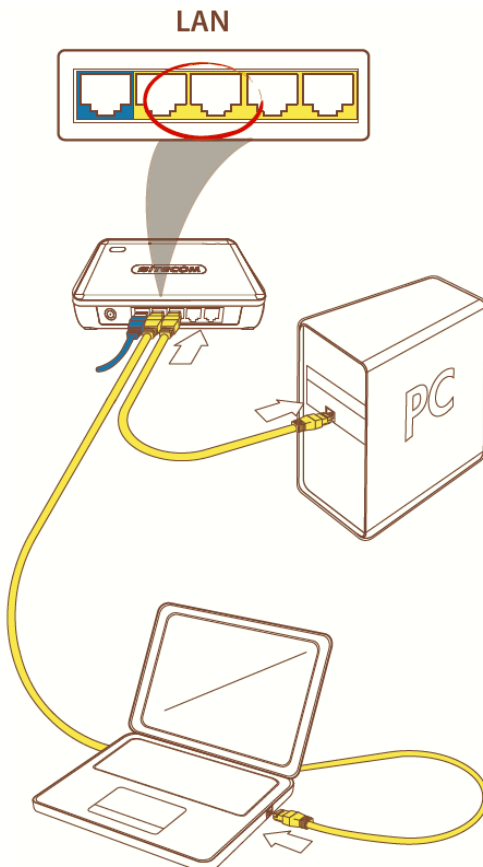
You can place the WLR-2001/WLR3001 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem.

6 Setup LAN, WAN

WAN connection:



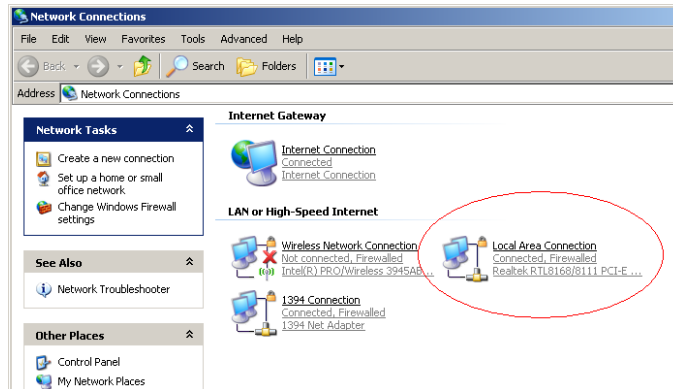
LAN connection:



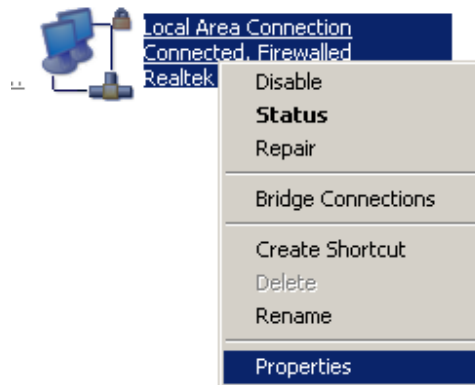
7 PC Network Adapter setup

Windows XP

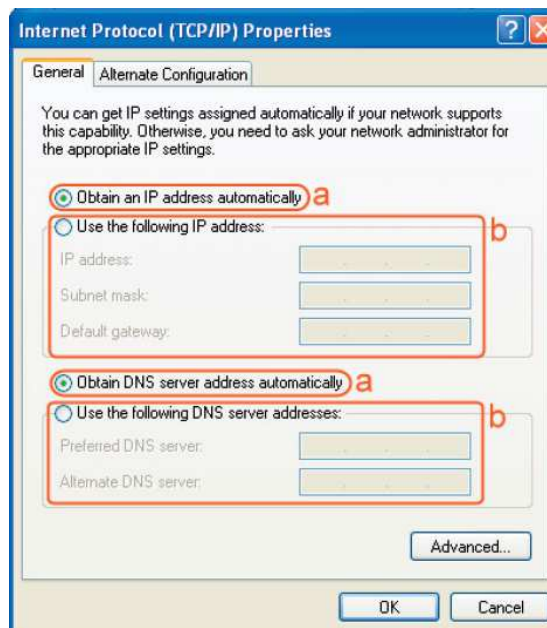
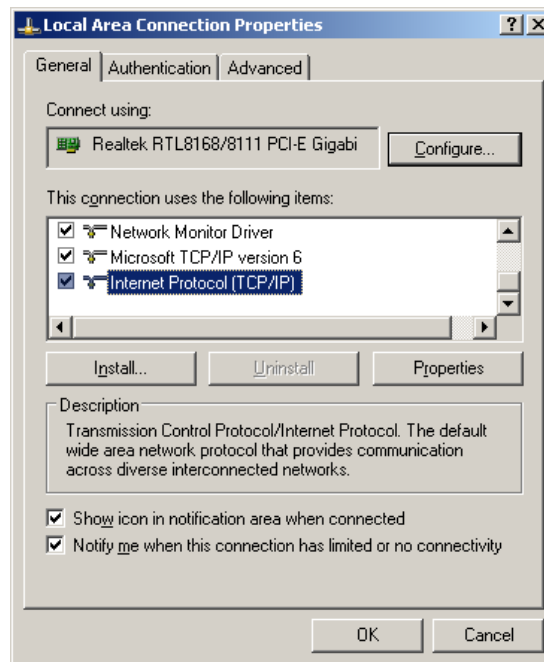
- Enter [Start Menu] → select [Control panel] → select [Network].



- Select [Local Area Connection]) icon=>select [properties]



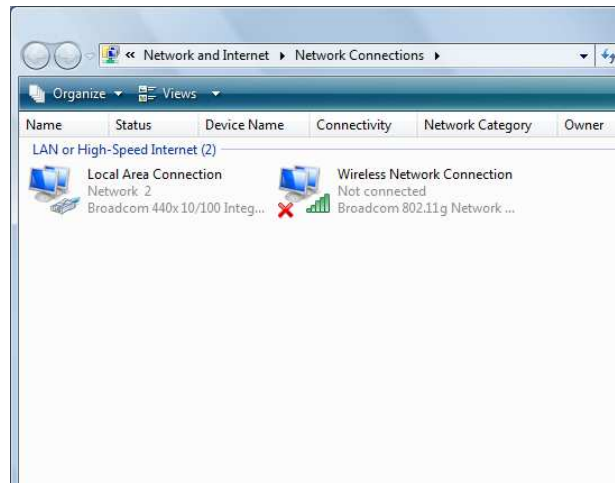
- Select [Internet Protocol (TCP/IP)] =>Click [Properties].



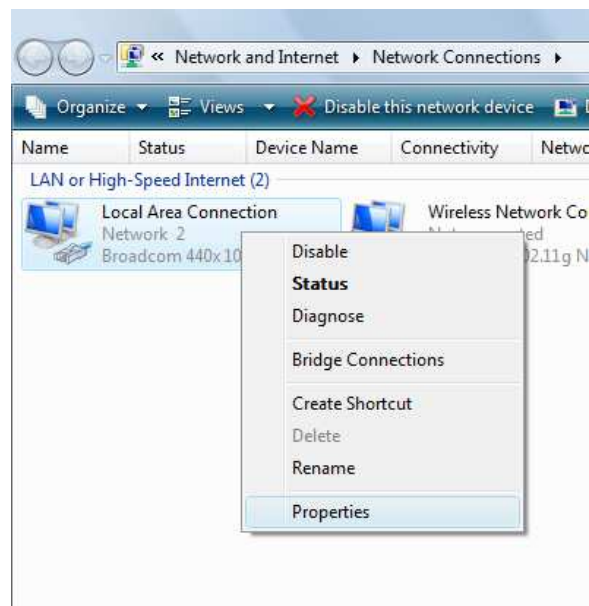
- Select the [General] tab.
The router supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

Windows Vista/Seven

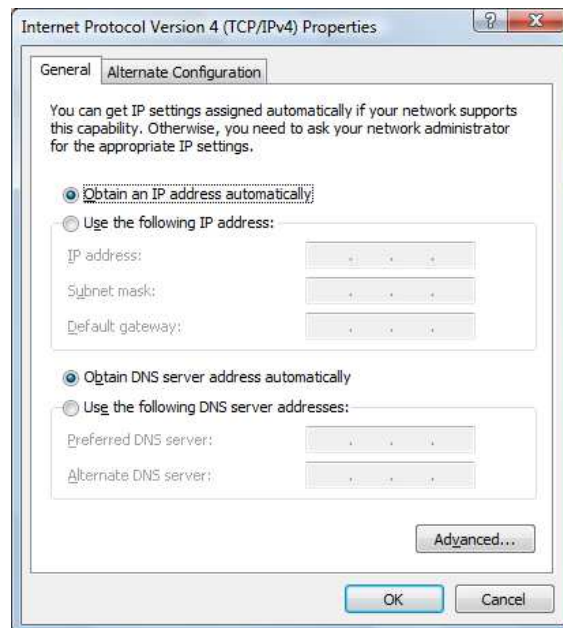
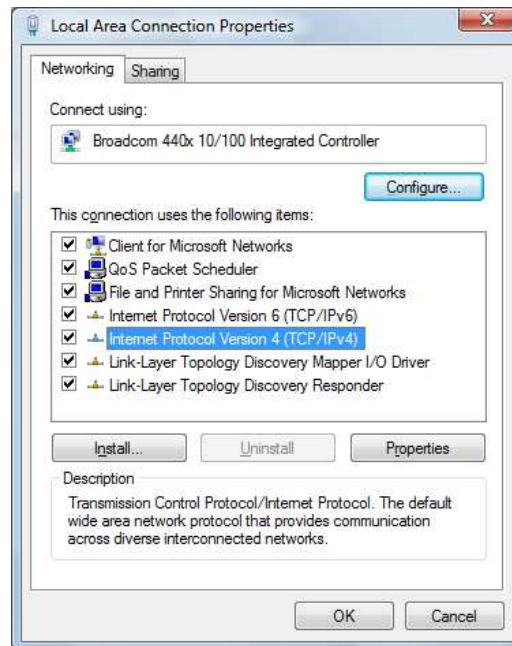
- Enter [Start Menu] → select [Control panel] → select [View network status and tasks] -> select [Manage network connections].



- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol Version 4 (TCP/IPv4)] =>Click [Properties].



- Select the [General] tab.

The router supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

8 Bring up the WLR-2001/WLR3001

Connect the supplied power-adaptor to the power inlet port and connect it to a wall outlet. The WLR-2001/WLR3001 automatically enters the self-test phase. During self-test phase, the Power LED will be lit continuously to indicate that this product is in normal operation.

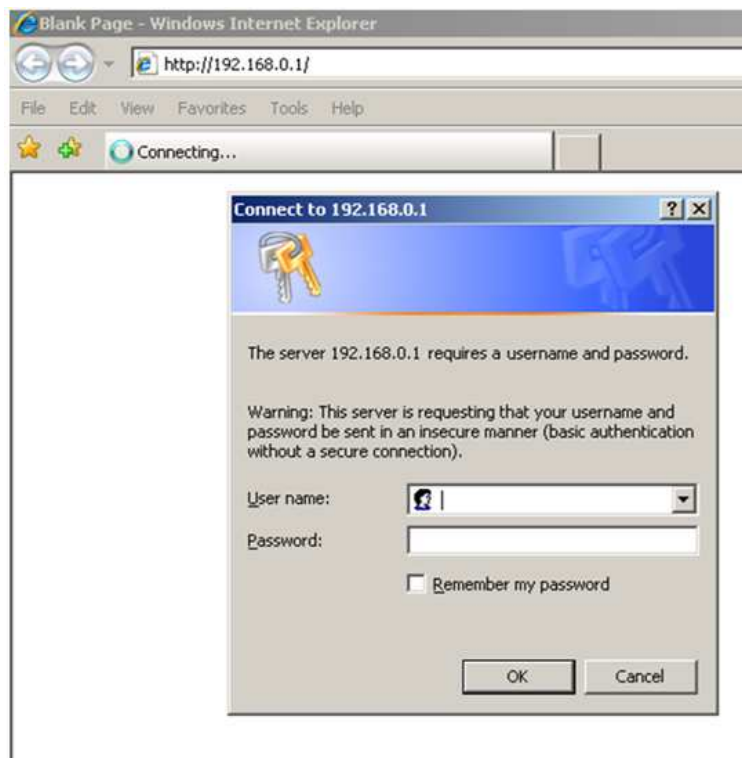
9 Initial Setup WLR-2001/WLR3001

LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).



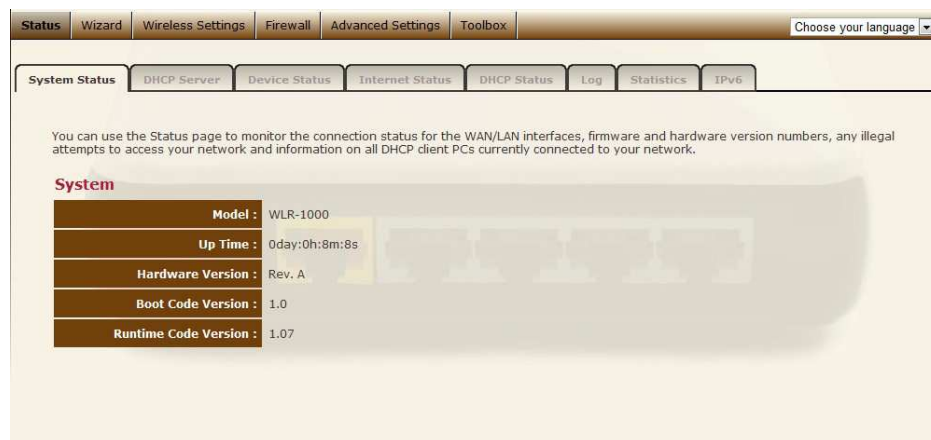
2. Type **http://192.168.0.1** in the address bar and press [Enter]



3. Type user name and password (default username is admin. The password can be found on the backlabel on the bottom of your router).



4. Click **OK**.
5. You will see the home page of the WLR-2001/WLR3001.



The System status section allows you to monitor the current status of your router.

The UP time, hardware information, serial number as well as firmware version information is displayed here.

DHCP Server

The LAN tab gives you the opportunity to change the IP settings of the WLR-2001/WLR3001.

Status Wizard Wireless Settings Firewall Advanced Settings Toolbox Choose your language

System Status **DHCP Server** Device Status Internet Status DHCP Status Log Statistics IPv6

You can enable the Wireless Router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The Wireless Router must have an IP Address in the Local Area Network.

LAN IP

IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disable
DHCP Server :	Enable
Lease Time :	Forever

DHCP Server

DHCP Client Start IP :	192.168.0.100
DHCP Client End IP :	192.168.0.200
Domain Name :	sitecomwlr1000

Apply Cancel

Click **<Apply>** at the bottom of this screen to save any changes.

IP address 192.168.0.1. It is the router's LAN IP address (Your LAN clients default gateway IP address).

IP Subnet Mask 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree is Disabled by default. If the 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no ip-addresses are assigned to clients and you have to use static ip-addresses. When DHCP server is enabled your computers will be assigned an ip-address automatically until the lease time expires.

Lease Time Forever. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

DHCP START client IP/DHCP Client end IP You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.

Note: *default IP range 192.168.0.100 ↔ 192.168.0.200. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool*

Domain Name You can specify a Domain Name for your LAN. Or just keep the default (sitecomwlrxxxx).

Device Status

View the Broadband router's current configuration settings. Device Status displays the configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section.

View the current setting status of this device.

Wireless Configuration

Mode :	Access Point
ESSID :	SitecomC7A7B0
Channel Number :	auto
Security :	WPA pre-shared key

LAN Configuration

IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enable
MAC Address :	00:0C:F6:00:00:00

Internet Status

This page displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **Renew** button to renew your WAN IP address.



The screenshot shows a web interface with a navigation bar at the top containing tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar is a secondary menu with tabs for System Status, DHCP Server, Device Status, Internet Status (selected), DHCP Status, Log, Statistics, and IPv6. The main content area displays the following information:

Attain IP Protocol :	Dynamic IP disconnect
IP Address :	
Subnet Mask :	
Default Gateway :	
MAC Address :	00:0C:F6:6A:D2:91
Primary DNS :	
Secondary DNS :	

A Refresh button is located at the bottom right of the information area.

DHCP Client Status

DHCP This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the Refresh button to update the available information.

You can check **Enable Static DHCP IP**. It is possible to add more static DHCP IPs.

They are listed in the table **Static DHCP Lease Table**. IP can be deleted at will from the table.

Click the **'apply'** button to save the changed configuration.

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired (Second)
192.168.0.100	00:26:22:ac:5f:2a	forever

Enable Static DHCP Leases

IP Address	MAC Address
<input type="text"/>	<input type="text"/>

Static DHCP Lease Table :

NO.	MAC Address	IP Address	Select
<input type="button" value="Delete"/>	<input type="button" value="Delete All"/>		

WLR-2001/WLR3001 Log

View the operation **log of the WLR-2001/WLR3001**. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



The screenshot shows a web interface for a Broadband router. At the top, there is a navigation bar with tabs: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below this is a secondary navigation bar with tabs: System Status, DHCP Server, Device Status, Internet Status, DHCP Status, Log (selected), Statistics, and IPv6. The main content area has a heading: "View the system operation information. You can see the system start up time, connection process, etc." Below the heading is a text area containing the log entry: "Jul 28 00:00:01 (none) syslog.info syslogd started: BusyBox v1.15.2". At the bottom of the text area are three buttons: Save, Clear, and Refresh.

WLR-2001/WLR3001 Statistics

Shows the counters of packets sent and received on WAN, LAN & WLAN.

The screenshot displays the 'Statistics' page of a router's web interface. The navigation bar includes 'Status', 'Wizard', 'Wireless Settings', 'Firewall', 'Advanced Settings', 'Toolbox', and a language selection dropdown. The main menu contains 'System Status', 'DHCP Server', 'Device Status', 'Internet Status', 'DHCP Status', 'Log', 'Statistics', and 'IPv6'. The page content includes a descriptive sentence and a table of network statistics.

This page shows the packet counters for transmission and reception regarding to networks.

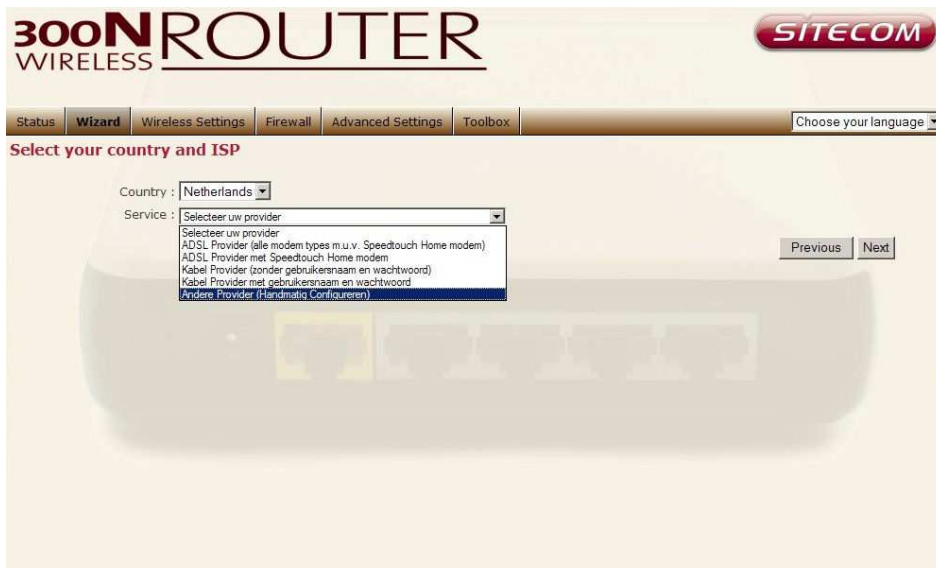
Wireless LAN :	<i>Packets Sent</i>	440
	<i>Packets Received</i>	0
Ethernet LAN :	<i>Packets Sent</i>	1639
	<i>Packets Received</i>	2192
Ethernet WAN :	<i>Packets Sent</i>	0
	<i>Packets Received</i>	0

10 Configuration Wizard

Click **Wizard** to configure the router. The Setup wizard will now be displayed; check that the modem is connected and click **Next**.



Select your country from the Country list. Select your internet provider. Click **Next**.



Depending on the chosen provider, you may need to enter your user name and password, MAC address or hostname in the following window. After you have entered the correct information, click **Next**.

300N WIRELESS ROUTER **SITECOM**

Status **Wizard** Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▾

Please, enter the data which is supplied by your ISP.

Hostname : (Alleen voor oudere @home verbindingen)

MAC Address :



300N WIRELESS ROUTER **SITECOM**

Status **Wizard** Wireless Settings Firewall Advanced Settings Toolbox Choose your language ▾

Please, enter the data which is supplied by your ISP.

Login Method : PPP over Ethernet

Username :

Password :

Service :

MTU : (512<=MTU Value<=1492)

Connection Type :

Idle Time : (1-1000 Minutes)



Click **APPLY** to complete the configuration.

11 Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function



Enable or Disable Wireless function here. Click **Apply** and wait for module to be ready and loaded.

Basic Settings

The screenshot shows a web interface for configuring wireless settings. At the top, there is a navigation bar with tabs for Status, Wizard, **Wireless Settings**, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, there are sub-tabs: Enable, **Basic**, Advanced, Security, ACL, and WPS. The main content area contains a descriptive paragraph: "This page allows you to define the ESSID and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point." Below this are four configuration fields: Mode (set to Access Point), Band (set to 2.4 GHz (B+G+N)), SSID (set to SitecomC7A7B0), and Channel (set to Auto). At the bottom right, there are Apply and Cancel buttons.

Mode Allows you to set the AP to AP or WDS mode.

Band Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.

SSID This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same SSID.

Channel The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Advanced

This tab allows you to set the advanced wireless options. The options included are, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.

The screenshot shows the 'Advanced' tab of the 'Wireless Settings' page. The page has a navigation bar with tabs for 'Status', 'Wizard', 'Wireless Settings', 'Firewall', 'Advanced Settings', and 'Toolbox'. Below the navigation bar are sub-tabs: 'Enable', 'Basic', 'Advanced', 'Security', 'ACL', and 'WPS'. The 'Advanced' sub-tab is selected. A warning message states: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.' The settings are as follows:

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2347	(0-2347)
Beacon Interval :	100	(20-1024 ms)
DTIM Period :	1	(1-10)
Data Rate :	Auto	
N Data Rate :	Auto	
Channel Bandwidth :	<input checked="" type="radio"/> Auto 20/40 MHz	<input type="radio"/> 20 MHz
Preamble Type :	<input checked="" type="radio"/> Short Preamble	<input type="radio"/> Long Preamble
CTS Protection :	<input type="radio"/> Always	<input checked="" type="radio"/> None

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the settings area.

Fragment Threshold "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate The "Data Rate" is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth is the range of frequencies that will be used.

Preamble Type The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Disable

When you choose to disable encryption, it is very insecure to operate the WLR-2001/WLR3001.



The screenshot shows a web interface for configuring wireless security. At the top, there are tabs: Enable, Basic, Advanced, Security (selected), ACL, and WPS. Below the tabs, a message states: "This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network." The main configuration area has a label "Encryption:" followed by a dropdown menu set to "Disable". Below this is a checkbox labeled "Enable 802.1x Authentication" which is unchecked. At the bottom right, there are "Apply" and "Cancel" buttons.

WPA Radius

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication



The screenshot shows a web interface for configuring wireless security. At the top, there are tabs: Status, Wizard, Wireless Settings (selected), Firewall, Advanced Settings, and Toolbox. A "Choose your language" dropdown is on the right. Below the tabs, a message states: "This page allows you to setup the wireless security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network." The main configuration area has tabs: Enable, Basic, Advanced, Security (selected), ACL, and WPS. The configuration options are: "WMM:" set to "Enable"; "Broadcast Essid:" set to "Enable"; "Encryption:" set to "WPA RADIUS"; "WPA Unicast Cipher Suite:" with radio buttons for "WPA(TKIP)", "WPA2(AES)" (selected), and "WPA2 Mixed"; "RADIUS Server IP Address:" with an empty text input; "RADIUS Server Port:" set to "1812"; and "RADIUS Server Password:" with an empty text input. At the bottom right, there are "Apply" and "Cancel" buttons.

WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.



The image shows a configuration interface for WEP encryption. It features several dropdown menus and input fields. The 'Encryption' dropdown is set to 'WEP'. The 'Key Length' dropdown is set to '64-bit'. The 'Key Type' dropdown is set to 'ASCII (5 characters)'. The 'Default Key' dropdown is set to 'Key 1'. Below these are four input fields labeled 'Encryption Key 1', 'Encryption Key 2', 'Encryption Key 3', and 'Encryption Key 4', all of which are currently empty.

Key Length You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Format You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Key1 - Key4 The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.



The screenshot shows a configuration window for WPA Pre-shared Key. It features four rows of settings:

- Encryption :** A dropdown menu set to "WPA pre-shared key".
- WPA Type :** Three radio buttons: "WPA(TKIP)" (selected), "WPA2(AES)", and "WPA2 Mixed".
- Pre-shared Key Type :** A dropdown menu set to "Passphrase".
- Pre-sharedKey :** An empty text input field.

At the bottom right, there are two buttons: "Apply" and "Cancel".

WPA-Radius

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses **TKIP** or CCMP (**AES**) to change the encryption key frequently. Press **Apply** button when you are done.



The screenshot shows a configuration window for WPA-Radius. It features five rows of settings:

- Encryption :** A dropdown menu set to "WPA RADIUS".
- WPA Type :** Three radio buttons: "WPA(TKIP)" (selected), "WPA2(AES)", and "WPA2 Mixed".
- RADIUS Server IP Address :** An empty text input field.
- RADIUS Server Port :** A text input field containing "1812".
- RADIUS Server Password :** An empty text input field.

At the bottom right, there are two buttons: "Apply" and "Cancel".

ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

For security reasons, the Wireless Router features MAC Address Filtering that only allows authorized MAC Addresses to associate with the Wireless Router.

MAC Address Filtering Table

NO.	MAC Address	Comment	Select
-----	-------------	---------	--------

Delete Delete All

Enable Access Control

New : MAC Address : Comment : Add Reset

Apply Cancel

Enable wireless access control Enables the wireless access control function

Adding an address into the list Enter the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

Remove an address from the list If you want to remove a MAC address from the "Current Access Control List", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.



The screenshot shows the WPS configuration interface of a wireless router. At the top, there is a navigation bar with tabs for Status, Wizard, **Wireless Settings**, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar are sub-tabs for Enable, Basic, Advanced, Security, ACL, and **WPS**. The WPS section is active, showing a 'WPS' toggle set to 'Enable'. Under 'WPS Information', there are fields for WPS Current Status (Configured), PinCode Self (04534082), SSID (SitecomC7A7B0), Authentication Mode (WPA pre-shared key), PassphraseKey (masked with asterisks), WPS Via Push Button (Start to Process), and WPS Via PIN (Start PIN).

WPS Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID This is the network broadcast name (SSID) of the router.

Authentication Mode It shows the active authentication mode for the wireless connection.

Passphrase Key It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

WPS via Push Button Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

12 Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click Apply



DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

The screenshot shows the 'Firewall' configuration page with the 'DMZ' tab selected. The page includes a navigation bar with 'Status', 'Wizard', 'Wireless Settings', 'Firewall', 'Advanced Settings', and 'Toolbox'. Below the navigation bar are tabs for 'Enable', 'DMZ', 'DoS', 'Access', and 'URL block'. The main content area contains a descriptive paragraph, an 'Enable DMZ' checkbox, and a table for defining DMZ hosts. The table has columns for 'Public IP Address' and 'Client PC IP Address'. Below the table are radio buttons for 'Dynamic IP' (selected) and 'Static IP', along with an 'Add' button and a 'Reset' button. Below the table is a 'Current DMZ Table' section with a table header and buttons for 'Delete', 'Delete All', and 'Reset'. At the bottom right are 'Apply' and 'Cancel' buttons.

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ

Public IP Address	Client PC IP Address
<input checked="" type="radio"/> Dynamic IP Session 1 <input type="text"/>	<input type="text"/>
<input type="radio"/> Static IP <input type="text"/>	<input type="text"/>

Current DMZ Table:

NO.	Public IP Address	Client PC IP Address	Select
-----	-------------------	----------------------	--------

Enable DMZ Enable/disable DMZ

Public IP Address The IP address of the WAN port or any other Public IP addresses given to you by your ISP

Client PC IP Address Fill-in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



Ping of Death Protections from Ping of Death attack

Discard Ping From WAN The router's WAN port will not respond to any Ping requests

Port Scan Protects the router from Port Scans.

Sync Flood Protects the router from Sync Flood attack.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services. If both MAC filtering and IP filtering are enabled simultaneously, the MAC filtering table will be checked first and then the IP filtering table.

Enable MAC Filtering Deny Allow

Client PC MAC Address	Comment
<input type="text"/>	<input type="text"/>

Current MAC Filtering Table

NO.	Client PC MAC Address	Comment	Select
-----	-----------------------	---------	--------

Enable IP Filtering Deny Allow

NO.	PC Description	PC IP Address	Client Service	Protocol	Port Range	Select
-----	----------------	---------------	----------------	----------	------------	--------

Deny If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.

Allow If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.

Filter client PCs by IP Fill in "IP Filtering Table" to filter PC clients by IP.

Add PC You can click Add PC to add an access control rule for users by IP addresses.

Remove PC If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.

Filter client PC by MAC Check "Enable MAC Filtering" to enable MAC Filtering.

Add PC Fill in "Client PC MAC Address" and "Comment" of the PC that is allowed to access the Internet, and then click "Add". If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

Remove PC If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

Enable URL block

URL/Keyword :

Current URL Blocking Table

NO.	URL/Keyword	Select
-----	-------------	--------

Enable URL Blocking Enable/disable URL Blocking

Add URL Keyword Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block.

Remove URL Keyword If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configurations

13 Advanced Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.

Port Forwarding

Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.



Enable Port Forwarding Enable Port Forwarding

Local IP This is the **local** IP of the server behind the NAT firewall.

Type This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only, or select "both" to forward both "TCP" and "UDP" packets.

Port Range The range of ports to be forward to the private IP.

Comment description of this setting.

Add Port Forwarding Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below.

Remove Port Forwarding If you want to remove a Port Forwarding setting from the "Current Port Forwarding Table", select the Port Forwarding setting that you want to remove in the table and then click "Delete Selected". If you want to remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections.

Special Applications

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Enable Trigger Port Enable the Special Application function.

TCP Port to open This is the range of TCP port numbers for this particular application.

UDP Port to Open This is the range of UDP port numbers for this particular application.

The screenshot shows the 'Special Applications' configuration page. At the top, there are navigation tabs: Status, Wizard, Wireless Settings, Firewall, **Advanced Settings**, and Toolbox. A language dropdown menu is on the right. Below the navigation, there are sub-tabs: NAT Enable, Port Forwarding, **Special Applications**, UPnP, and Quality of Service. The main content area contains a text block explaining that some applications require multiple connections and that NAT must be enabled. Below this is a checkbox for 'Enable Trigger port'. A table with columns 'IP Address', 'TCP Port to Open', 'UDP Port to Open', and 'Comment' is shown, with '0.0.0.0' entered in the IP Address field. Below the table is a 'Popular Applications' section with a dropdown menu and an 'Add' button. At the bottom, there is a 'Current Trigger-Port Table' with columns 'NO.', 'IP Address', 'TCP Port to Open', 'UDP Port to Open', 'Comment', and 'Select'. There are 'Delete', 'Delete All', and 'Reset' buttons below this table. 'Apply' and 'Cancel' buttons are at the bottom right.

Comment The description of this setting.

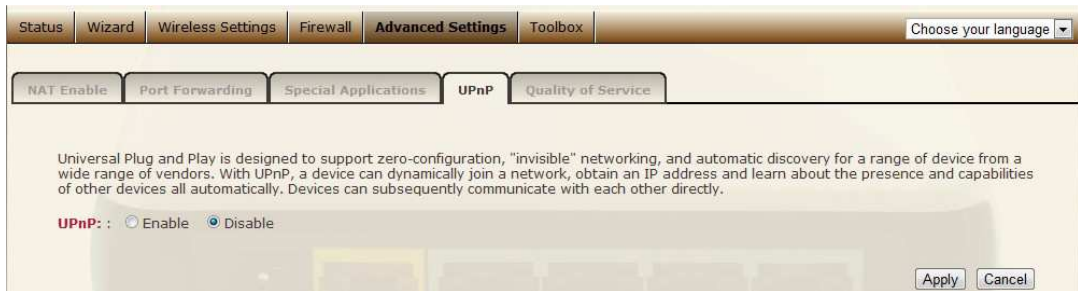
Popular applications This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

Add Special Application Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.

Delete If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

UPnP

With UPnP, all PCs in your Intranet will discover this router automatically, so you don't have to configure your PC and it can easily access the Internet through this router.



UPnP Feature You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

The screenshot shows the 'Quality of Service' configuration page. At the top, there is a navigation bar with tabs for 'Status', 'Wizard', 'Wireless Settings', 'Firewall', 'Advanced Settings', and 'Toolbox'. Below this, there are sub-tabs for 'NAT Enable', 'Port Forwarding', 'Special Applications', 'UPnP', and 'Quality of Service'. The main content area contains a description of QoS, a checkbox for 'Enable QoS', and a table titled 'Current QoS Table'. The table has columns for 'Priority', 'Rule Name', 'Upload Bandwidth', 'Download Bandwidth', and 'Select'. Below the table are buttons for 'Add', 'Edit', 'Delete', 'Delete All', 'Move Up', and 'Move Down'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Enable/Disable QoS You can check "Enable QoS" to enable QoS functionality for the WAN port.

Add a QoS rule into the table Click "Add" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.

Remove QoS rules from the table If you want to remove QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete Selected". If you want remove all QoS rules from the table, just click the "Delete All" button. Clicking "Reset" will clear your current selections.

Edit a QoS rule Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

Adjust QoS rule priority You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

14 TOOLBOX Settings

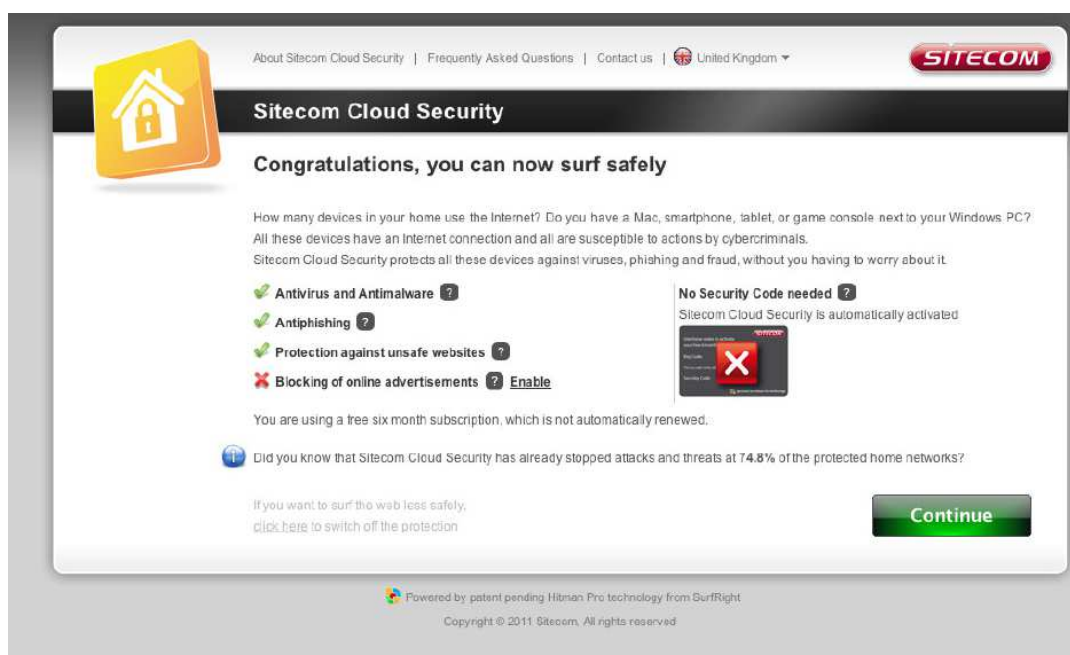
Sitecom Cloud Security

Antivirus software alone is not safe enough. You can now benefit from additional built-in security in your modem or router. Protect all devices in your home network against cybercrime while browsing. Activated automatically, your network and devices are better secured than ever before.

Your Sitecom device comes with a 6 month free *Sitecom cloud security* subscription.

After you have set up your Sitecom device for internet access, open the webbrowser and enter <http://www.sitecomcloudsecurity.com> in the address bar.

If the device has been properly configured the following web page should be shown.

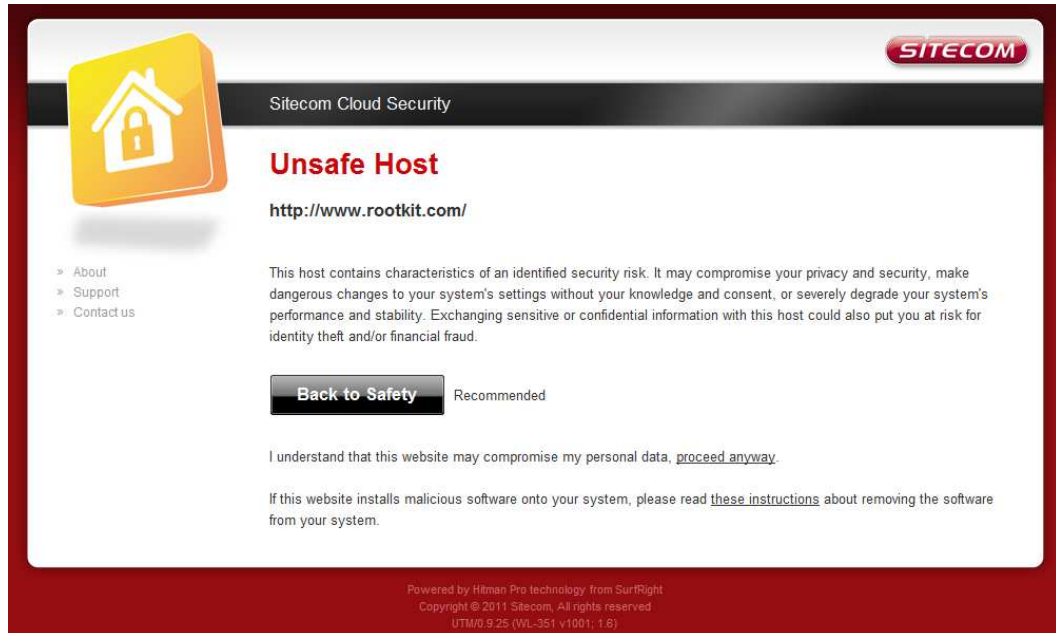


Here you can see which security features are activated.

The *Sitcom Cloud Security* service offers the following protection options:

- Anti-Malware
- Anti-Phishing
- Protection against unsafe websites
- Advertisement blocking

With the protection of *unsafe websites* activated the *Sitecom Cloud Security* will always check if a website is safe. If it is not safe it will inform you that is not safe to enter.

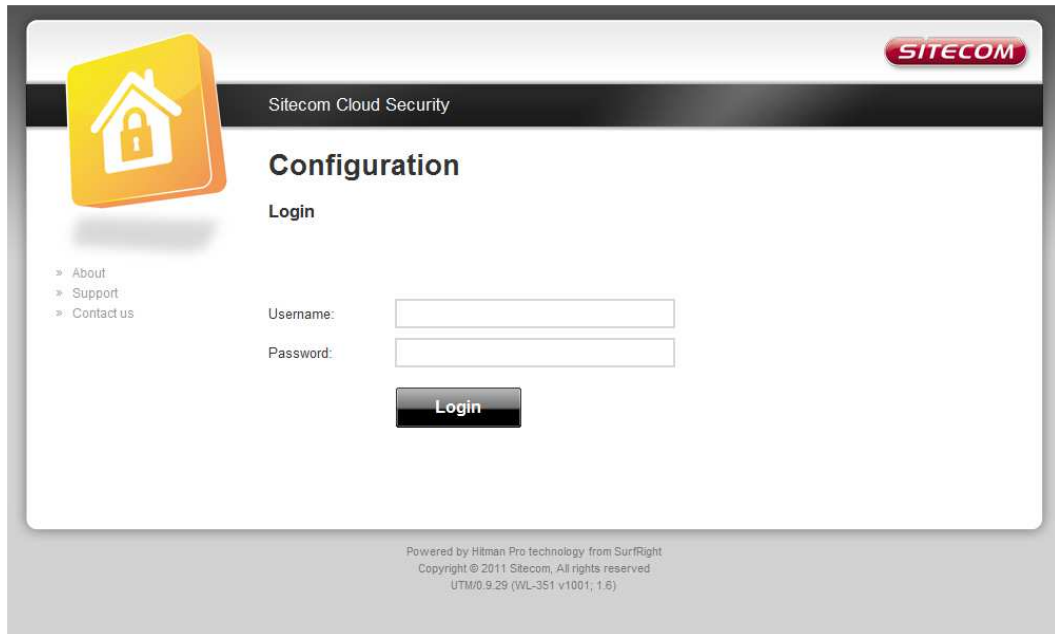


The screenshot shows a warning interface for Sitecom Cloud Security. At the top right is the SITECOM logo. Below it, the text 'Sitecom Cloud Security' is displayed. On the left is a yellow house icon with a padlock. The main heading is 'Unsafe Host' in red, followed by the URL 'http://www.rootkit.com/'. A warning message states: 'This host contains characteristics of an identified security risk. It may compromise your privacy and security, make dangerous changes to your system's settings without your knowledge and consent, or severely degrade your system's performance and stability. Exchanging sensitive or confidential information with this host could also put you at risk for identity theft and/or financial fraud.' Below this is a 'Back to Safety' button and the text 'Recommended'. A link 'proceed anyway' is provided for users who understand the risk. At the bottom, there is a link to 'these instructions' for removing malicious software. The footer contains technical details: 'Powered by Hman Pro technology from SurRight', 'Copyright © 2011 Sitecom. All rights reserved', and 'UTM/0.9.25 (VL-351 v1001, 1.6)'.

If you still wish to visit this webpage click on 'proceed anyway'. Alternatively click 'Back to Safety' so that your security will not be breached.

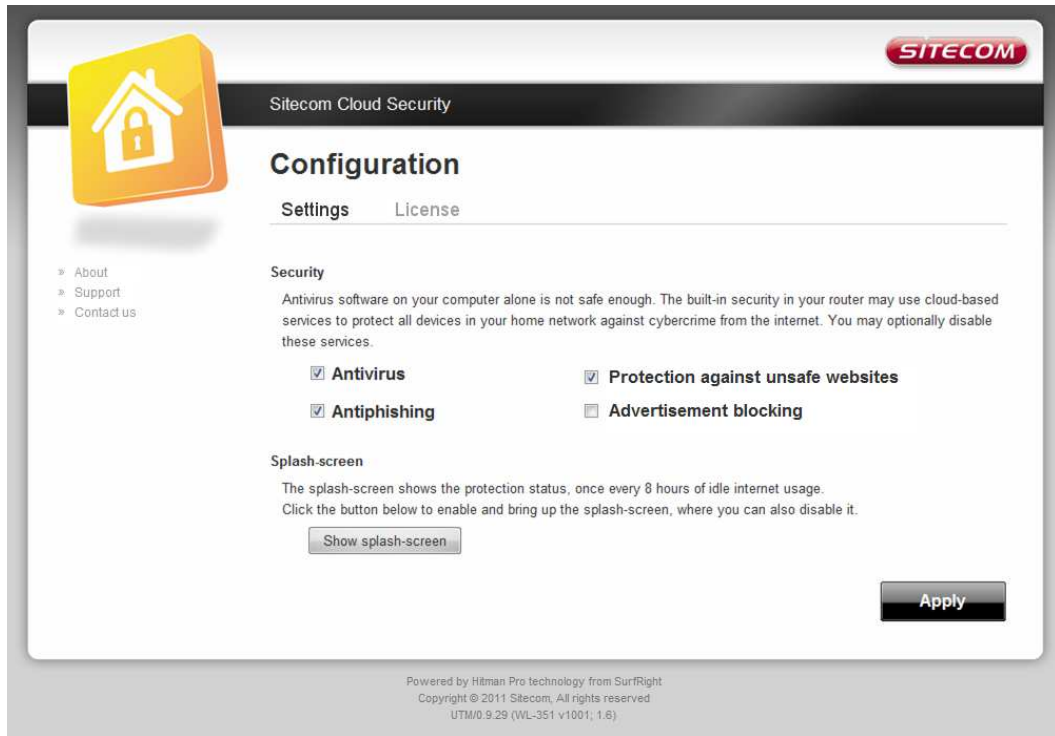
If you wish to change your security options or to extend your subscription at any time, open <http://www.sitecomcloudsecurity.com> from your web browser.

You will be asked for a username and password. These can be found on the backlabel on the bottom of your Sitecom router or modem.

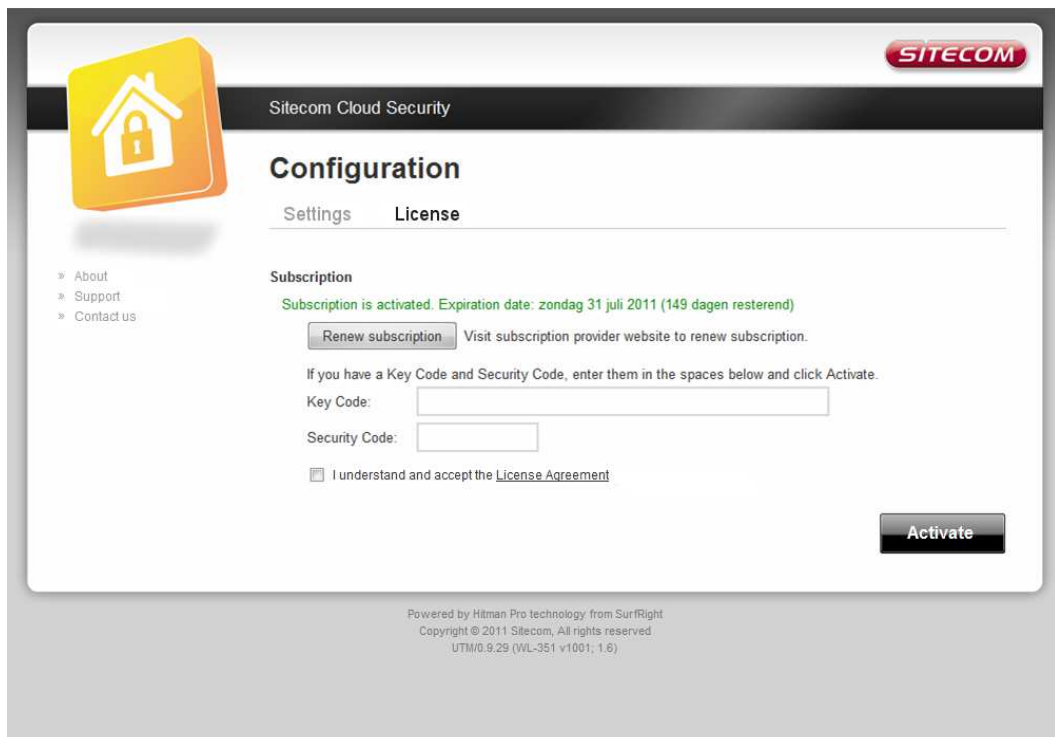


The screenshot displays the 'Sitecom Cloud Security' configuration interface. At the top right is the 'SITECOM' logo. Below it, the text 'Sitecom Cloud Security' is centered. On the left, there is a large orange icon of a house with a padlock. Below the icon are three links: 'About', 'Support', and 'Contact us'. The main heading is 'Configuration', followed by a sub-heading 'Login'. The login section contains two input fields: 'Username:' and 'Password:'. Below these fields is a black 'Login' button. At the bottom of the page, there is small text: 'Powered by Hitman Pro technology from SurfRight', 'Copyright © 2011 Sitecom, All rights reserved', and 'UTM/0.9.29 (WL-351 v1001; 1.6)'.

If the login succeeded you can click on 'Settings' to change your security options.



Or click 'License' to renew your subscription.



If you wish to disable Sitecom cloud security at any time, open the webpage of your Sitecom product and log in with the supplied credentials (these can be

found on the back label on the bottom of your Sitecom device).

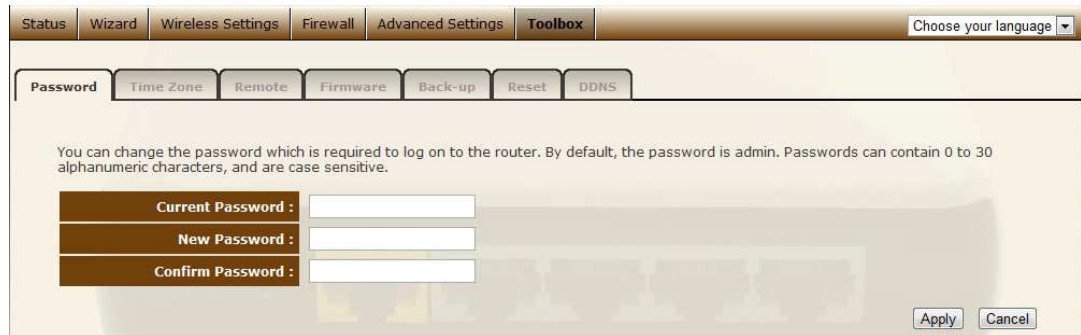
Go to Toolbox and select "Sitecom Cloud Security".



Click the "Disable" radio button and click 'Apply' for the settings to take effect.

Password change options

You can change the password required to log into the broadband router's system web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.



The screenshot shows a web-based management interface for a broadband router. At the top, there is a navigation bar with tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, there is a sub-menu with tabs for Password, Time Zone, Remote, Firmware, Back-up, Reset, and DDNS. The main content area contains the following text: "You can change the password which is required to log on to the router. By default, the password is admin. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive." Below this text are three input fields: "Current Password:", "New Password:", and "Confirm Password:". At the bottom right of the form are "Apply" and "Cancel" buttons.

Current Password Fill in the current password to allow changing to a new password.

New Password Enter your new password.

Confirm Password Enter your new password again for verification purposes.

Click <**Apply**> at the bottom of the screen to save the above configurations

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

The screenshot shows a web interface for configuring the Time Zone. At the top, there is a navigation bar with tabs: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A 'Choose your language' dropdown is on the right. Below the navigation bar, there are sub-tabs: Password, Time Zone (selected), Remote, Firmware, Back-up, Reset, and DDNS. The main content area has a heading: 'Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.' Below this, there are three rows of configuration options: 1. 'Time Zone' with a dropdown menu showing '(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'. 2. 'Time Server Address' with a text input field containing '192.43.244.18'. 3. 'Daylight Savings' with a checkbox labeled 'Enable' (which is unchecked), followed by 'Time From' with a dropdown for 'January' and a spinner for '1', and 'To' with a dropdown for 'January' and a spinner for '1'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Set Time Zone Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address You can set an NTP server address.

Enable Daylight Savings The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

Start Daylight Savings Time Select the period in which you wish to start daylight Savings Time

End Daylight Savings Time Select the period in which you wish to end daylight Savings Time

Click <**Apply**> at the bottom of the screen to save the above configurations

Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.



The screenshot shows a web interface for configuring a router. At the top, there is a navigation bar with tabs: Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, there are sub-tabs: Password, Time Zone, Remote, Firmware, Back-up, Reset, and DDNS. The 'Remote' tab is selected. The main content area contains the following text: "The remote management function allows you to designate a host on the Internet to have management/configuration access to the Wireless Router from a remote site. Enter the designated host IP Address in the Host IP Address field." Below this text is a table with three columns: Host Address, Port, and Enable. The 'Host Address' field contains '0.0.0.0', the 'Port' field contains '8080', and the 'Enable' column has an unchecked checkbox. At the bottom right of the table, there are 'Apply' and 'Cancel' buttons.

Host Address	Port	Enable
0.0.0.0	8080	<input type="checkbox"/>

Host Address This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port The port number of the remote management web interface.

Check "**Enabled**" to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Firmware Upgrade

This page allows you to upgrade the router's firmware.

The screenshot shows the 'Firmware' tab selected in the router's configuration interface. The page provides instructions for upgrading the system firmware and includes options to enable or disable automatic updates. A file selection field is present but currently empty.

Enable or disable Sitecom Auto Upgrade if Enabled the router will automatically check for firmware updates. If a new firmware has been detected a pop/up will appear in the webbrowser and inform the user about the new firmware and the changes and allows to Install the update.

Select **Enable** or **Disable** and click apply for the settings to take effect.

Firmware Upgrade This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click **<Apply>** at the bottom of the screen to start the upgrade process.

Backup Settings

The Backup screen allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



Use the "Backup" tool to save the Broadband router current configuration to a file named "**config.bin**" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.



DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.



The screenshot shows the DDNS configuration page in a router's web interface. The top navigation bar includes tabs for Status, Wizard, Wireless Settings, Firewall, Advanced Settings, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, a sub-menu contains tabs for Password, Time Zone, Remote, Firmware, Back-up, Reset, and DDNS. The DDNS tab is active. The main content area contains a descriptive paragraph: "DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service provider." Below this is a form with the following fields: "Dynamic DNS" with radio buttons for "Enable" and "Disable" (selected); "Provider" with a dropdown menu showing "DynDNS"; "Domain Name" with a text input field; "Account / E-mail" with a text input field; and "Password / Key" with a text input field. "Apply" and "Cancel" buttons are at the bottom right.

Enable/Disable Enable or disable the DDNS function of this router

Provider Select a DDNS service provider

Domain name Fill in your static domain name that uses DDNS

Account/E-mail The account that your DDNS service provider assigned to you

Password/Key The password you set for the DDNS service account above

Click <**Apply**> at the bottom of the screen to save the above configurations.