AirTies

300 Mbps Wireless ADSL2+ Router

User manual

Air 5450

7/24 people support
801 100 0911

Contents

Manual Overview

This manual guides you through the steps necessary for setting up and configuring your AirTies device. Please read this manual carefully before beginning the installation process.

The Warranty does not cover failure or damage as a result of not following the instructions in the manual. AirTies will not be held responsible in such circumstances.

The User Manual is an important resource you can refer to for safe and proper use of your device. Please retain it for future reference.

Safety and Maintenance

- In order to prevent damage to your device, be sure to keep it in its original box during transportation.
- The device must be used solely with its original power adapter.
- Do not insert a PSTN (phone) plug into the LAN port.
- If you encounter any problems, do not open or disassemble the device. Call AirTies Technical Support.
- In order to prevent electric shock, do not operate the device in wet or damp areas.
- In the event of a gas leak, do not use the device. Do not turn the device on or off. Do not plug or unplug the power cord.
- Avoid using the device in dusty environments. If dust buildup should occur, use a dry cloth to remove the dust.
- To clean the exterior of the device use a dry cloth. Do not attempt to clean the interior. There are no user serviceable components inside.
- For information regarding the installation and configuration of the device consult the remainder of this manual.
- Remove all protective plastic on the top and bottom of your device before you start using it.
- The average usage life of the device is 7 years as determined by the Authority of Industry and Trade.

1 INTRODUCTION

With Air 5450 which uses 802.11n technology, transfer wireless data, watch videos or upload your pictures to the Internet at speeds of up to 300Mbps. Backward compatible with the wireless 802.11b/g devices, the Air 5450 provides 6 times faster wireless communications compared to earlier technologies. Dead spots and packet losses on your wireless network becomes a thing of the past with the MIMO (Multiple Input Multiple Output) technology and the advanced error recovery system contained in the 802.11n standard.

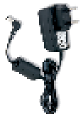
1.1 Minimum System Requirements

- For installation and configuration: a computer that has an Ethernet interface or wireless capability that is compatible with 802.11b/g/n standards, and is running any version of Windows, UNIX, Linux or Mac Operating Systems
- For the AirTies ADSL Utility: 32 bit Windows (98/ME/2000/XP/Vista)
- **The router does not need to be connected to a computer during normal operation.**

1.2 Package Contents

1. Air 5450 300Mbps Wireless ADSL2+ Router
2.Power adapter
3. Ethernet cable
4.Telephone cables (1 long, 1 short)
5. Splitter (ISDN&PSTN)
6. Easy Setup CD
7. Quick Installation Guide
8. Warranty Card

1



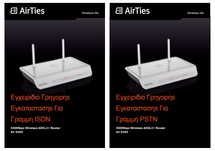
2

3

4

5

6

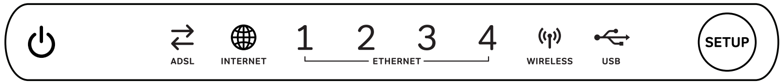


AirTies
Εγχειρίδιο Γρηγορης Εγκαταστασης Για Γραμμη ISDN
Εγχειρίδιο Γρηγορης Εγκαταστασης Για Γραμμη PSTN

7

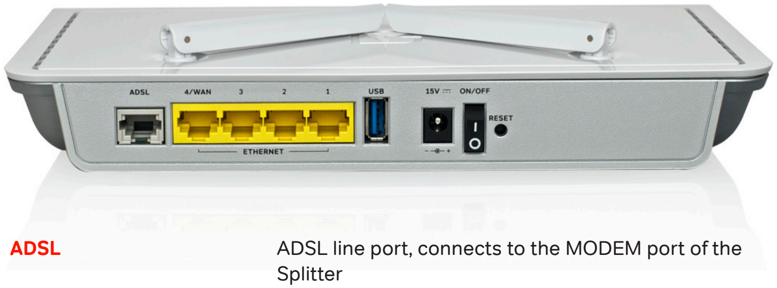
8

1.3 Front Panel



LED	Light	Status
POWER	Blue	AirTies router is “ON”.
	Off	AirTies router is “OFF”..
ADSL	Red	ADSL connection established and active
	Red Flashing	An ADSL connection is being negotiated
	Off	No ADSL connection
INTERNET	Red	Internet connection established and active
	Off	No Internet connection
1 2 3 4 ETHERNET	Red	LAN connection is ready to use
	Red Flashing	LAN connection active. There is data exchange.
	Off	LAN connection is not active
WIRELESS	Red	Wireless connection is ready to use
	Red Flashing	Wireless connection active. There is data exchange.
	Off	Wireless connection is disabled
USB	Red	USB connection establis hed
	Red flashing	USB connection active. There is data exchange.
	Off	No USB connection

1.4 Back Panel



ADSL	ADSL line port, connects to the MODEM port of the Splitter
Ethernet 4 - 1	Ethernet ports
Reset	Button to reset your device to default factory settings
USB	USB port
ON/OFF	Button to turn your device on and off
15V	15V power port, connects to the power adapter

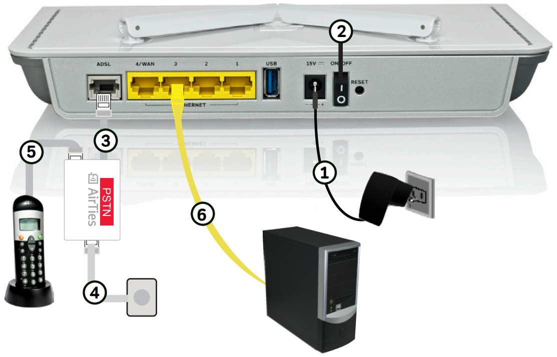
1.5 Main Features

- **All-in-one solution:** ADSL2+ Router, 300Mbps wireless access point, Firewall, 4 Ethernet ports
- **High speed wireless:** 300 Mbps wireless access point compliant with the 802.11n (Draft2.0) standard
- **ADSL2+ technology for high speed Internet** (24Mbps download/ 4Mbps upload)
- **Wireless Access range and Mesh Technology:** AirTies Mesh Technology support for extending coverage area by using additional AirTies wireless access point devices.
- **IPTV-ready!!:** The Air 5450, with its IP QoS, VLAN, PVC-Port mapping and IGMP support, is ready for the newest, state of the art services offered over the Internet such as IPTV*
- **USB Plug and Share** feature gives you printer and file sharing capability throughout your entire network from a single point*
- **Advanced Wireless Security:** WPA2-PSK, WPA2-802.1x, WPA-PSK, WPA-802.1x, WEP wireless encryption standards support
- **Automatic Wireless Security configuration:** The AirTies ADSL Utility automatically configures wireless security settings for the router and the PC that is used for setup.
- **Firewall:** Advanced anti-DoS SPI Firewall; MAC, URL and IP address based filtering for Internet access
- Easy installation with animated instructions with the **Easy Setup CD**
- **Automatic Firmware Upgrade:** Automatic firmware upgrade capability with the AirTies ADSL Utility. It is important to use the latest firmware to get the best possible performance out of your router.
- **ADSL Usage Monitor:** Especially useful for limited quota ADSL subscribers, making it easy to track monthly total download and upload amounts
- **Router:** Advanced router with DHCP server, NAT, NAPT, DMZ, VLAN*, RIPv1/v2 support
- **8 Channel PVC support**
- **Robust against voltage fluctuations:** Specially designed to withstand wide voltage fluctuations
- **Remote management:** Web and TR-069 support for remote management
- **7/24 AirTies Call Center and Technical Support** (engineering support by the AirTies R&D team when needed)
- **3 year extended warranty**
- Designed to be compatible with your local ADSL infrastructure

***Features to be added with a firmware upgrade**

2 INSTALLATION

2 1.Basic Cabling Procedure



Connecting the Cables (PSTN)

All wiring and configuration procedures explained in this document are also demonstrated with the animation that starts when you run the Air 5450 Easy Setup CD. Please run the **Easy Setup CD first.**

1- Connect the power adapter provided to the power port of your router and plug it into the wall outlet.

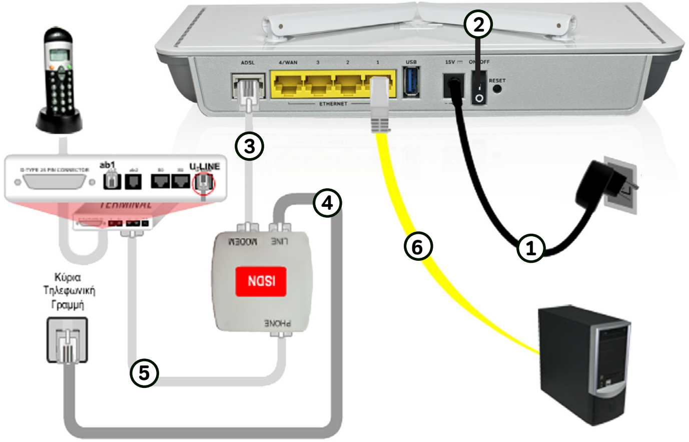
2- Turn on the Air 5450 by setting the On/Off switch to the "|" position.

3- Using the short telephone cable provided, connect the Modem port of the Splitter to the ADSL port of your router.

4- Connect the main phone line to the Line port of the Splitter. If the main phone line is currently connected to your phone, first disconnect it from your phone, and then connect it to the Line port of the Splitter.

5- Using the long telephone cable provided, connect your phone to the Phone port of the Splitter.

6- Using the Ethernet cable provided in the box, connect your PC to any of the four Ethernet ports of your router.



Connecting the Cables (ISDN)

All wiring and configuration procedures explained in this document are also demonstrated with the animation that starts when you run the Air 5450 Easy Setup CD. Please run the **Easy Setup CD first.**

1- Connect the power adapter provided to the power port of your router and plug it into the wall outlet.

2- Turn on the Air 5450 by setting the On/Off switch to the "|" position.

3- Using the short telephone cable supplied in the box, connect the "MODEM" port of the ISDN Splitter with the "ADSL" port of the Air 5450.

4- Using the longer telephone cable supplied in the box, connect the telephone wall socket to the "LINE" port of the ISDN Splitter. If your main phone line is connected to an ISDN terminal, disconnect it from the terminal and connect it to the "LINE" port of the ISDN Splitter.

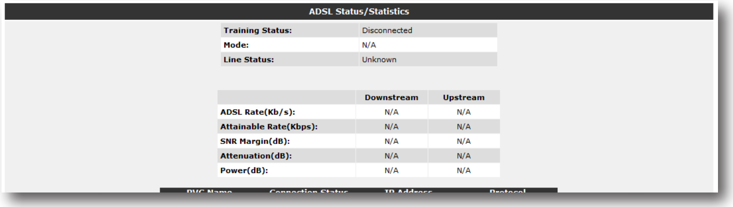
5- Using the phone cable, connect the "PHONE" port of the ISDN line Splitter to the ISDN terminal.

6- Using the Ethernet cable provided in the box, connect your PC to any of the four Ethernet ports of your router.

3 ADSL SETTINGS

3.1 ADSL Status and Statistics

When you click “**ADSL**” on the main menu of your router’s Web interface, the “**ADSL Status/Statistics**” page will come up. Here, you can see detailed information about your router’s ADSL connection and upstream/ downstream data rates. You can also check the status of your current PVC connection.



ADSL Status/Statistics

Training Status:	Disconnected
Mode:	N/A
Line Status:	Unknown

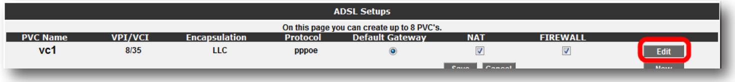
	Downstream	Upstream
ADSL Rate(Kb/s):	N/A	N/A
Attainable Rate(Kbps):	N/A	N/A
SNR Margin(dB):	N/A	N/A
Attenuation(dB):	N/A	N/A
Power(dB):	N/A	N/A

PVC Name	Connection Status	IP Address	Protocol

3.2 ADSL setup

When you click “**ADSL**” on the left menu of your router’s Web interface, you will see “**ADSL Setup**” as the first sub menu. Go to “**ADSL Setup**” to configure your router’s ADSL settings and follow the steps below:

1. When you click on the “**ADSL Setup**” submenu, a table showing your default PVC settings will be displayed.



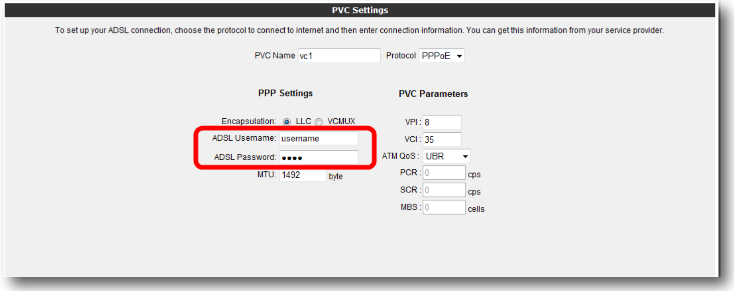
ADSL Setups

On this page you can create up to 8 PVC's.

PVC Name	VPI/VCI	Encapsulation	Protocol	Default Gateway	NAT	FIREWALL	
vc1	8/35	LLC	pppoe	●	☑	☑	Edit

2. To enter your ADSL settings click the “**Edit**” button in this table. The “PVC Settings” screen will come up.

3. On the “**PVC Settings**” screen, enter the user name and password given to you by your ADSL service provider in the “**ADSL Username**” and “**ADSL Password**” fields, respectively. Click “**Save**” to complete your ADSL setup.



PVC Settings

To set up your ADSL connection, choose the protocol to connect to internet and then enter connection information. You can get this information from your service provider.

PVC Name: vc1   Protocol: PPPoE

PPP Settings

Encapsulation: ● LLC ○ VCMUX
ADSL Username: username
ADSL Password: ••••
MTU: 1492 byte

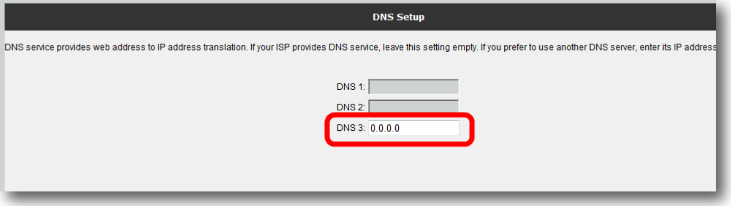
PVC Parameters

VPI : 8
VCI : 35
ATM QoS : UBR
PCR : 0 cps
SCR : 0 cps
MBS : 0 cells

3.3 DNS setup

DNS (Domain Name Service) is an Internet service that translates domain names into IP addresses. For example, when you try to go to the www.airties.com address, first your Internet service provider’s DNS will try to translate it to the corresponding IP address. The DNS system is, in fact, its own network. If one DNS server doesn’t know how to translate a particular domain name, it asks another one, and so on, all the way to the main InterNIC DNS server, until the correct address is returned. Most service providers will provide Domain Name services for security and speed.

Go to “**DNS Setup**” under the “**ADSL**” menu of your router’s Web interface. On the screen that comes up, you will see three DNS fields. The first two are your service provider’s DNS addresses and cannot be changed. If you prefer to use a different DNS server, enter its IP address in the “**DNS 3**” field.



DNS Setup

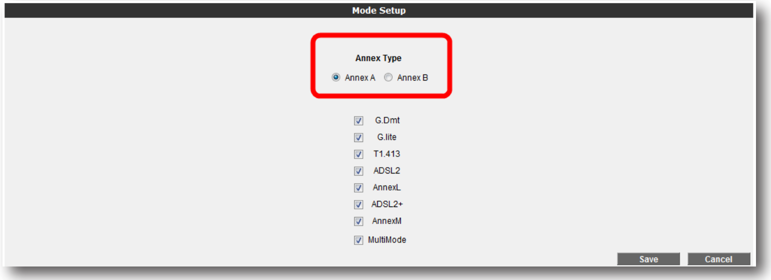
DNS service provides web address to IP address translation. If your ISP provides DNS service, leave this setting empty. If you prefer to use another DNS server, enter its IP address

DNS 1:
DNS 2:
DNS 3: 0.0.0.0

3.4 Mode setup

Different Internet service providers may differ in terms of modes of the ADSL service they offer. Some only provide basic ADSL service, while others provide different modes of ADSL such as ADSL2, ADLS2+, etc..

Your router supports multiple ADSL modes. You can see the ADSL modes supported and change settings by going to “**Mode Setup**” under the “**ADSL**” menu of your router’s Web interface. All ADSL modes are enabled by default. On this screen, you can disable/enable the modes as you choose. Click “**Save**” when you are done with the mode setup.



Mode Setup

Annex Type

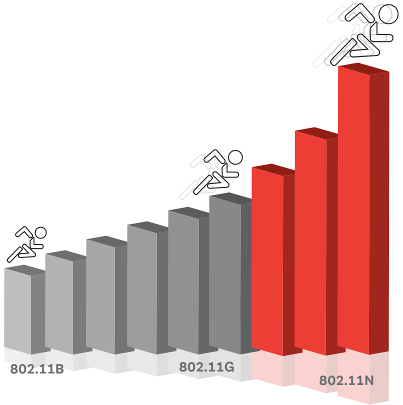
● Annex A ○ Annex B

☑ G.Dmt
☑ G.lite
☑ T1.413
☑ ADSL2
☑ AnnexL
☑ ADSL2+
☑ AnnexM
☑ MultiMode

Important: Please choose your Annex Type as Annex A (PSTN) or Annex B (ISDN) according to your line type on Mode Setup screen

4 WIRELESS SETTINGS

Your AirTies router can be used as a wireless access point to set up a wireless hotspot. With the 802.11g standard it supports, you can setup a wireless network with data rates of up to 54Mbps allowing you to share files between PCs at very high speeds. Your router is backward compatible with the 802.11b standard and can also work with 802.11b devices without affecting the performance of 802.11g devices.

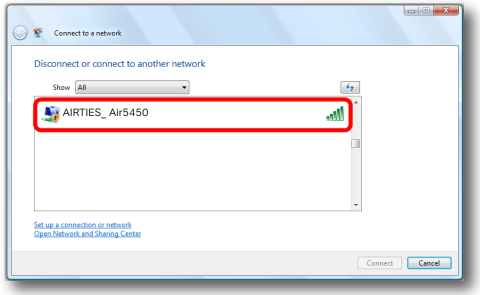


4.1 Setting up a wireless connection

Your router has Wireless networking enabled by default. No additional router configuration is needed for your wireless computers to access the Internet. It is recommended that you configure wireless security as explained in the sections that follow.

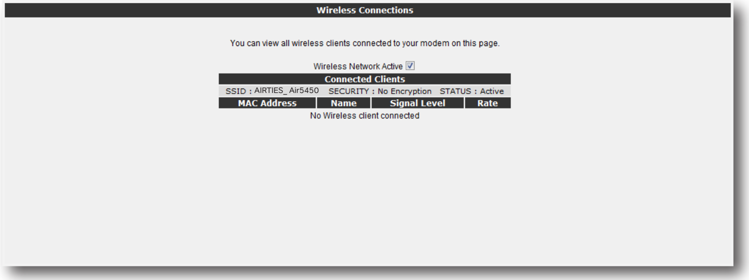
In order to connect your laptop to the AirTies router wirelessly:

Go to Start-Settings-Network Connections- Wireless Network Connection-View Wireless Networks. On the "**Wireless Network Connection**" screen, select the wireless network named AIRTIES_ 5450 and click "**Connect**".


Connect to a network
Disconnect or connect to another network
Show
All
AIRTIES_ Air5450
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

4.2 Wireless Network Settings

When you click the "**WIRELESS**" menu of your router's Web interface, you will be in the "Wireless Connections" screen that lists all the wireless clients connected to the router. You can block the access of any client to your wireless network by using the "**MAC Filtering**" option.



Wireless Connections

You can view all wireless clients connected to your modem on this page.

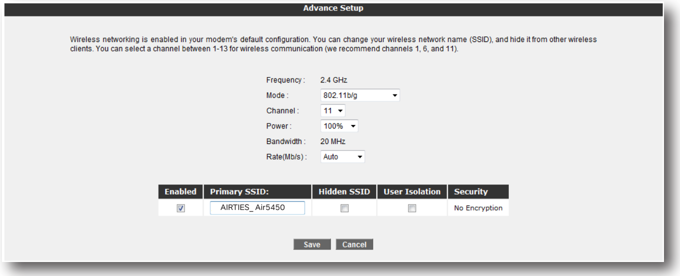
Wireless Network Active ☑

Connected Clients

SSID : AIRTIES_ Air5450   SECURITY : No Encryption   STATUS : Active

MAC Address	Name	Signal Level	Rate
No Wireless client connected			

To configure your wireless network settings, go to "**Wireless Setup**" under the "**WIRELESS**" menu. On the screen that comes up you can see whether wireless networking is enabled or not.



Advance Setup

Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency : 2.4 GHz
Mode : 802.11b/g
Channel : 11
Power : 100%
Bandwidth : 20 MHz
Rate(Mb/s) : Auto

Enabled	Primary SSID:	Hidden SSID	User Isolation	Security
☑	AIRTIES_ Air5450	□	□	No Encryption

Wireless settings are in two different categories: General wireless settings for your router and settings for your particular wireless network (SSID).

- "**Frequency**" shows the main frequency band your router is using. Depending on the frequencies supported it could be 2.4GHz or 5GHZ.
- "**Mode**" shows the IEEE 802.11 mode actively used by your router. The default mode is 802.11b/g, supporting both 802.11b and 802.11g devices.
- "**Channel**" field allows you to choose the channel your router will broadcast in. It is recommended that you choose one of channels 1,6, or 11.
- "**Power**" displays the total transmitted power from the device
- "**Rate**" shows the highest wireless data transfer rate supported by your router. It is set to "Auto" by default. This allows for automatic adjustment of data transfer rate based on distance and signal quality.

4.3 Wireless Security Settings

It is not necessary to configure wireless security to enable wireless communication. However, for your data security, it is recommended that you choose one of the security protocols described below that best fits your needs.

WPA2, WPA, and WEP are wireless encryption protocols used to encrypt the data traffic within the wireless network. MAC Address Filtering allows you to control which wireless terminals can connect to the AirTies router and share your Internet access. Access to the router by unauthorized terminals is blocked.

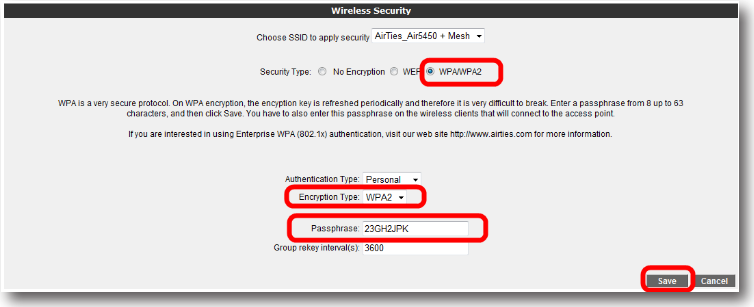
For your wireless network security, it is recommended that both MAC Address filtering and one of WPA, WPA2 or WEP wireless encryption protocols be activated.

4.3.1 WPA2 Security Settings

WPA2, defined by the IEEE 802.11i standard, is one of the latest wireless encryption methods. If you would like to use WPA2 in your wireless network, all the wireless adapters in your network must support WPA2. For Centrino platform computers, it is necessary to download the WPA2 updates for the Windows XP operating system to be able to use WPA2 (www.microsoft.com).

To enable WPA2 encryption and configure the necessary settings:

1. Go to “**Wireless Security Settings**” under the “**WIRELESS**” menu of the Web interface of your router.
2. Click on the “**WPA/WPA2**” button in the “**Security Type**” section of the “**Wireless Security**” screen.
3. Select “**Personal**” as “**Authentication Type**”.
4. In the “**Encryption Type**” field you can choose between “**WPA2**” and “**Both**”. If all the wireless devices on your network support WPA2, then select “**WPA2**”. If some of the wireless clients support WPA only, then select “**Both**” in which case the devices that support WPA2 will use WPA2 and those that do not support it will use WPA over their wireless connection.
5. Enter a network key that is 8 to 63 characters long (use a combination of letters and digits) in the “**Passphrase**” field. Make sure you choose a key that is not easy to guess. Click “**Save**”.
6. You must enter the same passphrase for all the wireless clients that will communicate with your device.



Wireless Security

Choose SSID to apply security: AirTies_Air5450 + Mesh

Security Type: ○ No Encryption ○ WEP ● WPA/WPA2

WPA is a very secure protocol. On WPA encryption, the encyption key is refreshed periodically and therefore it is very difficult to break. Enter a passphrase from 8 up to 63 characters, and then click Save. You have to also enter this passphrase on the wireless clients that will connect to the access point.

If you are interested in using Enterprise WPA (802.1x) authentication, visit our web site http://www.airties.com for more information.

Authentication Type: Personal

Encryption Type: WPA2

Passphrase: 23GH2JPK

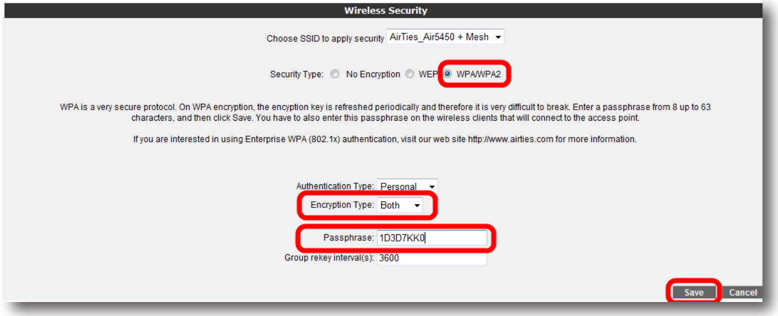
Group rekey interval(s): 3600

4.3.2 WPA Security Settings

WPA (Wi-Fi Protected Access) encryption standard is one of the current wireless encryption standards that provide a high level of data protection. All AirTies wireless products and 802.11g compliant wireless communication devices support WPA. If you would like to use WPA on your wireless network, all the wireless adapters on your network must support WPA.

To enable WPA encryption and configure the necessary settings:

1. Go to “**Wireless Security Settings**” under the “**WIRELESS**” menu of the Web interface of your router.
2. Click on the “**WPA/WPA2**” button in the “**Security Type**” section of the “**Wireless Security**” screen.
3. Select “**Persona**l” as “**Authentication Type**”.
4. In the “**Encryption Type**” field you have two choices: “**WPA2**” and “**Both**”. To be able to use WPA encryption, select “**Both**” in which case the devices that support WPA2 will use WPA2 and those that do not support it will use WPA over their wireless connection.
5. Enter a network key that is 8 to 63 characters long (use a combination of letters and digits) in the “**Passphrase**” field. Make sure you choose a key that is not easy to guess. Click “**Save**”.
6. You must enter the same passphrase for all the wireless clients that will communicate with your device.



Wireless Security

Choose SSID to apply security: AirTies_Air5450 + Mesh

Security Type: ○ No Encryption ○ WEP ● WPA/WPA2

WPA is a very secure protocol. On WPA encryption, the encyption key is refreshed periodically and therefore it is very difficult to break. Enter a passphrase from 8 up to 63 characters, and then click Save. You have to also enter this passphrase on the wireless clients that will connect to the access point.

If you are interested in using Enterprise WPA (802.1x) authentication, visit our web site http://www.airties.com for more information.

Authentication Type: Personal

Encryption Type: Both

Passphrase: 1D3D7KK0

Group rekey interval(s): 3600

4.3.3 WEP Security Settings

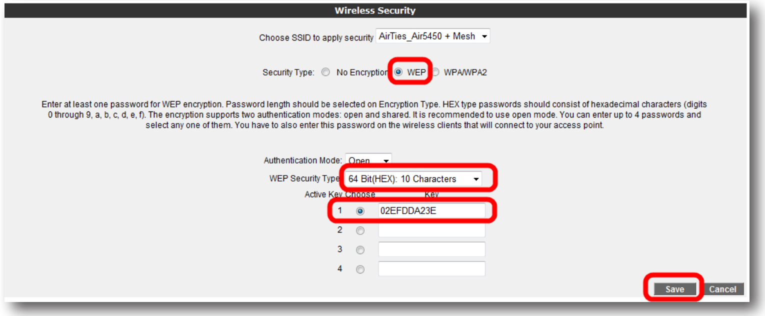
Your AirTies router supports WEP encryption in addition to the WPA and WPA2 encryption standards. If any of the devices in your wireless network does not support WPA or WPA2, it is recommended that you choose WEP encryption.

To enable WEP encryption and configure the necessary settings:

1. Go to "**Wireless Security Settings**" under the "**WIRELESS**" menu of the Web interface of your router.
2. Click on the "**WEP**" button in the "**Security Type**" section of the "**Wireless Security**" screen.
3. Select "**Open**" for "**Authentication Mode**".
4. In the "**WEP Security Type**" field, there are four choices for specifying a network key.
    1. 10 hexadecimal characters(A-F and 0-9) for 64-bit encryption
    2. 5 ASCII characters for 64-bit encryption
    3. 26 hexadecimal characters(A-F and 0-9) for 128-bit encryption
    4. 13 ASCII characters for 128-bit encryption

You can enter up to 4 network keys and also choose the one you want to use. Click "**Save**".

5. You must enter the same password for all the wireless clients that will communicate with your device.



Wireless Security

Choose SSID to apply security: AirTies_Air5450 + Mesh

Security Type: ○ No Encryption ● WEP ○ WPA/WPA2

Enter at least one password for WEP encryption. Password length should be selected on Encryption Type. HEX type passwords should consist of hexadecimal characters (digits 0 through 9, a, b, c, d, e, f). The encryption supports two authentication modes: open and shared. It is recommended to use open mode. You can enter up to 4 passwords and select any one of them. You have to also enter this password on the wireless clients that will connect to your access point.

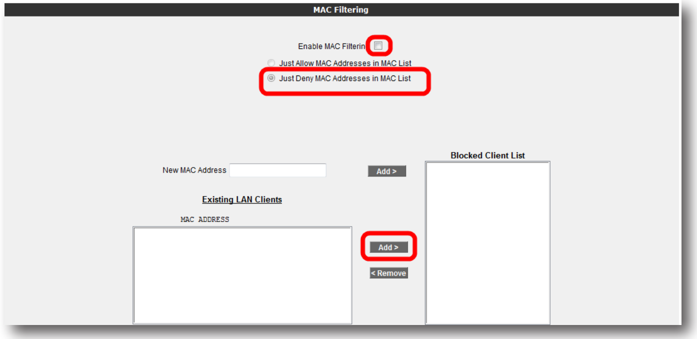
Authentication Mode: Open

WEP Security Type: 64 Bit(HEX): 10 Characters

Active Key	Choose	Key
1	●	02EFDDA23E
2	○	
3	○	
4	○	

4.4 MAC Filtering

You can specify those clients that will be allowed access to your network using MAC Filtering. MAC Filtering is not required for wireless security, but it is recommended that you use it in addition to encryption for your data protection.



MAC Filtering

Enable MAC Filterin □

○ Just Allow MAC Addresses in MAC List

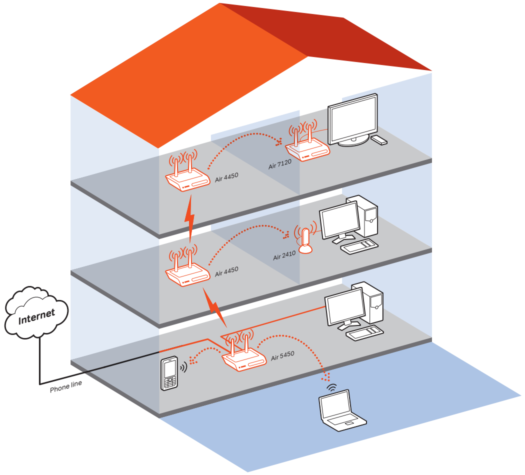
● Just Deny MAC Addresses in MAC List

To enable MAC Address filtering and make the necessary settings for blocking clients:

1. Click on "**MAC Filtering**" under the "**WIRELESS**" menu of the Web interface of your router.
2. In the window that appears, check the "**Enable MAC Filtering**" box.
3. Select "**Just Deny MAC Addresses in MAC List**".
4. For each device to be denied access, enter the wireless MAC address of the device in the "**New MAC Address**" field or select from "**Existing LAN Clients**" and then click the "**ADD**" button.
5. When you are done entering the MAC addresses, click "**Save**".
6. To add the devices that will be allowed access to the wireless network, select "**Just Allow MAC Addresses in MAC List**" instead of "**Just Deny MAC Addresses in MAC List**" and enter the MAC addresses.

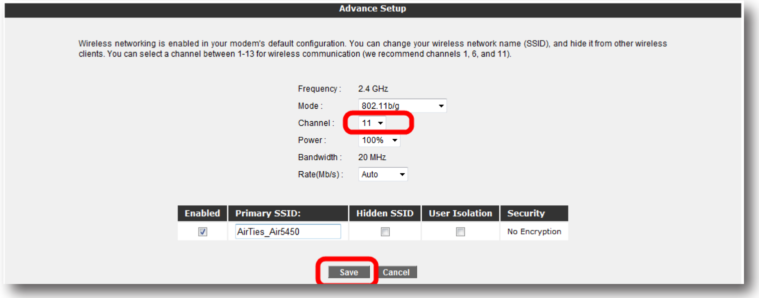
4.5 AirTies Mesh settings

AirTies Mesh Technology® resolves the signal loss and limited coverage area problems often encountered in multi-story concrete buildings. To extend wireless coverage area, one or more AirTies wireless access point devices functioning in repeater mode are connected to your device to set up a “**Mesh Network**”. The wireless access points communicate with each other via the Mesh protocol and boost the signal wherever signal strength is low thus increasing wireless range. Computers connect to the access point with the strongest signal and get to the router over the Mesh Network. Thus, the weak signal or dead spots due to barriers such as concrete walls are eliminated and the coverage area can be expanded to the maximum.



To setup a Mesh Network with your device:

1. Go to “**Wireless Setup**” under the “**WIRELESS**” menu of the Web interface of your router. Select a channel for your “**Mesh Network**” to operate in (it is recommended that you use one of channels “**1**”, “**6**”, or “**11**”) from the ones listed in the “**Channel**” field. You should select the same channel on all the wireless access point devices that form the “**Mesh Network**”.



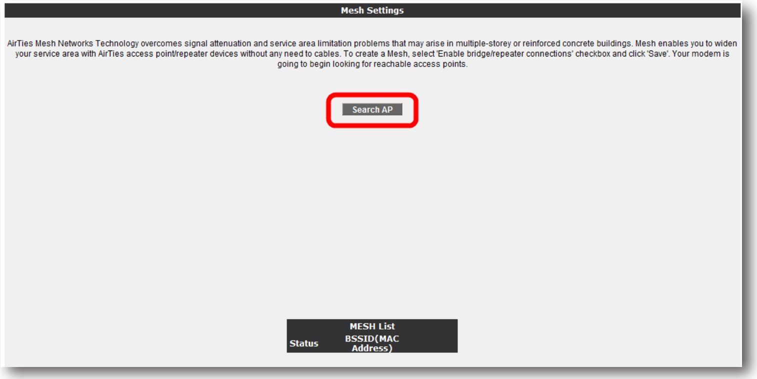
Advance Setup

Wireless networking is enabled in your modem's default configuration. You can change your wireless network name (SSID), and hide it from other wireless clients. You can select a channel between 1-13 for wireless communication (we recommend channels 1, 6, and 11).

Frequency : 2.4 GHz
Mode : 802.11b/g
Channel : 11
Power : 100%
Bandwidth : 20 MHz
Rate(Mb/s) : Auto

Enabled	Primary SSID:	Hidden SSID	User Isolation	Security
☑	AirTies_Air5450	□	□	No Encryption

2. Go to “**MESH**” under the “**WIRELESS**” menu of the Web interface of your router. In the “**Mesh Settings**” screen that comes up, click the “**Search AP**” button.

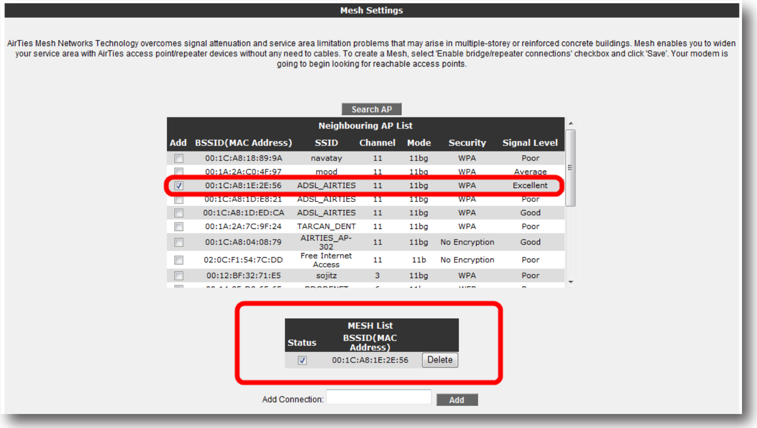


Mesh Settings

AirTies Mesh Networks Technology overcomes signal attenuation and service area limitation problems that may arise in multiple-storey or reinforced concrete buildings. Mesh enables you to widen your service area with AirTies access point/repeater devices without any need to cables. To create a Mesh, select 'Enable bridge/repeater connections' checkbox and click 'Save'. Your modem is going to begin looking for reachable access points.

MESH List	
Status	BSSID(MAC Address)

3. When you click the "**Search AP**" button, the router will start searching for wireless access points to connect to within its range and list the access points detected.



Mesh Settings

AirTies Mesh Networks Technology overcomes signal attenuation and service area limitation problems that may arise in multiple-storey or reinforced concrete buildings. Mesh enables you to widen your service area with AirTies access point/repeater devices without any need to cables. To create a Mesh, select 'Enable bridge/repeater connections' checkbox and click 'Save'. Your modem is going to begin looking for reachable access points.

Neighbouring AP List

Add	BSSID(MAC Address)	SSID	Channel	Mode	Security	Signal Level
□	00:1C:A8:18:89:9A	navatay	11	11bg	WPA	Poor
□	00:1A:2A:C0:4F:97	mood	11	11bg	WPA	Average
☑	00:1C:A8:1E:2E:56	ADSL_AIRTIES	11	11bg	WPA	Excellent
□	00:1C:A8:1D:E8:21	ADSL_AIRTIES	11	11bg	WPA	Poor
□	00:1C:A8:1D:ED:CA	ADSL_AIRTIES	11	11bg	WPA	Good
□	00:1A:2A:7C:9F:24	TARCAN_DENT	11	11bg	WPA	Poor
□	00:1C:A8:04:08:79	AIRTIES_AP-302	11	11bg	No Encryption	Good
□	02:0C:F1:54:7C:DD	Free Internet Access	11	11b	No Encryption	Poor
□	00:12:BF:32:71:E5	sojitz	3	11bg	WPA	Poor

MESH List

Status	BSSID(MAC Address)	
☑	00:1C:A8:1E:2E:56	Delete

Add Connection:

4. Check the box for the access point(s) that you would like your router to setup a Mesh connection with. Select only those access points that have a signal level of "**Average**" or better. Click "**Save**" to complete the Mesh settings of your device.

5. The same Mesh settings should be made on all the AirTies access points selected above. You can find detailed information about Mesh settings for each type of access point device in their user manuals.

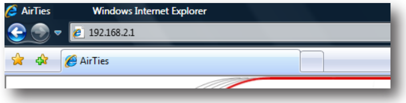
Important: All AirTies devices that form the Mesh Network should operate on the same channel.

5 ADVANCED SETTINGS

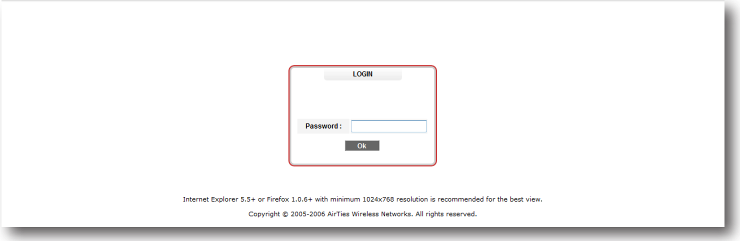
You can do the installation and basic connection settings (ADSL and Wireless) of your router using the Easy Setup CD included with your product. The Easy Setup CD helps you do the initial installation of your device quickly and easily. In addition to the CD, your router has an easy to use Web interface you can directly connect to and configure the basic and advanced settings. You do not need to be connected to the Internet to use the Web interface of your router. It is sufficient to have your computer connected to the router. Follow the steps listed below to access the Web interface:

1- Open your web browser (Internet Explorer, Mozilla Firefox, etc.).

2- In the Address bar, enter **192.168.2.1,** the default IP address of your device. This will launch the Web interface of your router.



3- In the "**LOGIN**" screen that comes up you will be prompted for a password to login. Your router does not have a default password. Initially, leave this field blank and continue by clicking "**OK**".



LOGIN

Password :

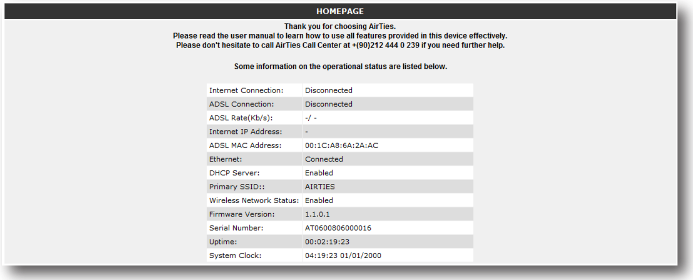
Internet Explorer 5.5+ or Firefox 1.0.6+ with minimum 1024x768 resolution is recommended for the best view.

Copyright © 2005-2006 AirTies Wireless Networks. All rights reserved.

Note: How to set a password for logging into the Web interface is explained in the "**Password Settings**" sub section under the "**MANAGEMENT**" section.

5.1 HOMEPAGE

The "**HOMEPAGE**" is the first screen that comes up after logging in. On this screen you can find information on the general settings and current operating status of your device.



HOMEPAGE

Thank you for choosing AirTies.
Please read the user manual to learn how to use all features provided in this device effectively.
Please don't hesitate to call AirTies Call Center at +(90)212 444 0 239 if you need further help.

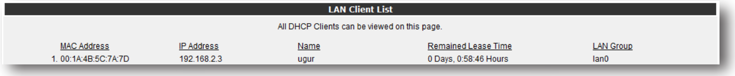
Some information on the operational status are listed below.

Internet Connection:	Disconnected
ADSL Connection:	Disconnected
ADSL Rate(Kb/s):	-/ -
Internet IP Address:	-
ADSL MAC Address:	00:1C:A8:6A:2A:AC
Ethernet:	Connected
DHCP Server:	Enabled
Primary SSID::	AIRTIES
Wireless Network Status:	Enabled
Firmware Version:	1.1.0.1
Serial Number:	AT0600806000016
Uptime:	00:02:19:23
System Clock:	04:19:23 01/01/2000

5.2 LAN

Any device that you connect to your router, such as PCs, network printers, IP cameras, etc., is a client. Any operation related to clients that will have a local network connection to your router can be done through the “**LAN**” menu of the Web interface and its submenus.

When you click on the “**LAN**” menu, the “**LAN Client List**” screen will come up. All clients that are connected to your router and their connection details are shown on this screen.



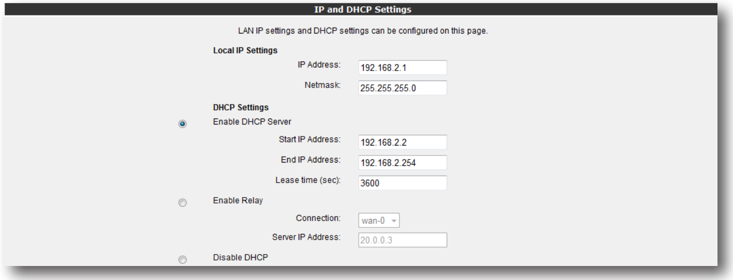
LAN Client List

All DHCP Clients can be viewed on this page.

	MAC Address	IP Address	Name	Remained Lease Time	LAN Group
1.	00:1A:4B:5C:7A:7D	192.168.2.3	ugur	0 Days, 0:58:46 Hours	lan0

5.2.1 IP and DHCP Settings

Every client that is connected to your router is given a local IP address. The module that assigns these IP addresses is the DHCP (Dynamic Host Configuration Protocol) module. For IP and DHCP configuration of your router, go to “**IP and DHCP Settings**” under the “**LAN**” menu.



IP and DHCP Settings

LAN IP settings and DHCP settings can be configured on this page.

Local IP Settings

IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Settings

● Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Lease time (sec): 3600

○ Enable Relay

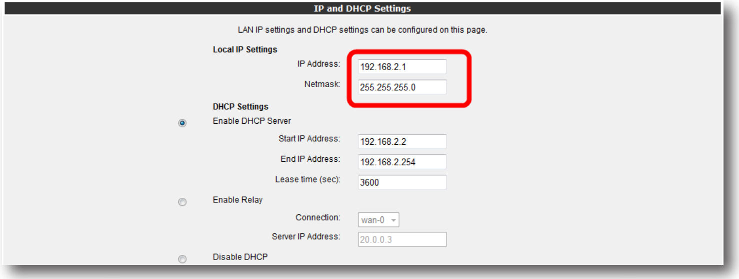
Connection: wan-0

Server IP Address: 20.0.0.3

○ Disable DHCP

Local IP Settings

You can change the IP address and Netmask of your router in this section. The default IP Address of your device is 192.168.2.1, and the default Netmask is 255.255.255.0. You can change these values based on the needs of your existing network.



IP and DHCP Settings

LAN IP settings and DHCP settings can be configured on this page.

Local IP Settings

IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Settings

● Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Lease time (sec): 3600

○ Enable Relay

Connection: wan-0

Server IP Address: 20.0.0.3

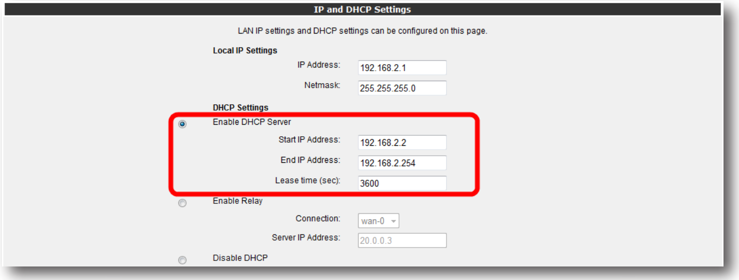
○ Disable DHCP

DHCP Settings

This section is for DHCP related settings. The settings you can change are the following:

Enable DHCP Server

DHCP is enabled by default. In this section you can assign an address range from which the router can assign local IP addresses to clients and the lease time. The default IP address range for your router is 192.168.2.2 through 192.168.2.254. Maximum lease time for an IP address is set as 3600 seconds, which means the assigned IP address will be renewed every 3600 seconds.



IP and DHCP Settings

LAN IP settings and DHCP settings can be configured on this page.

Local IP Settings

IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Settings

● Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Lease time (sec): 3600

○ Enable Relay

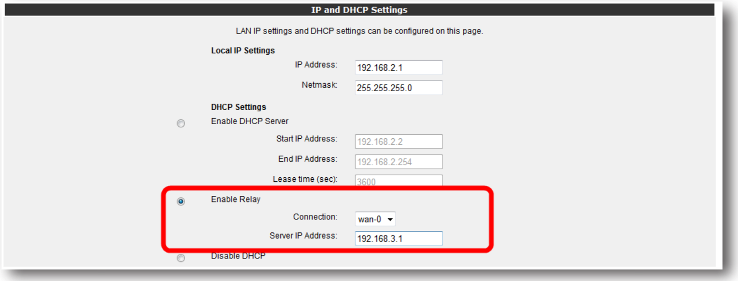
Connection: wan-0

Server IP Address: 20.0.0.3

○ Disable DHCP

Enable DHCP Relay

DHCP relay makes it possible for a DHCP server on a different network to assign local IP addresses to clients connected to the router. To do this, the address of the device (modem, server, etc.) that runs the DHCP service needs to be known.



IP and DHCP Settings

LAN IP settings and DHCP settings can be configured on this page.

Local IP Settings

IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Settings

○ Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Lease time (sec): 3600

● Enable Relay

Connection: wan-0

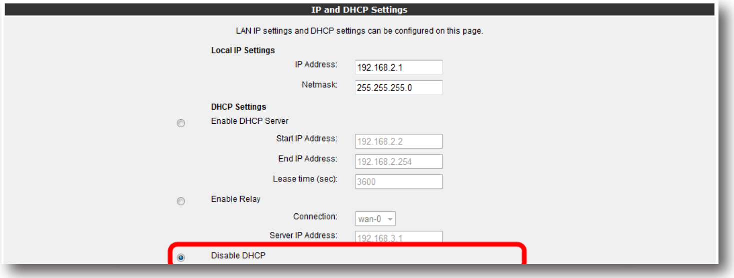
Server IP Address: 192.168.3.1

○ Disable DHCP

Important: If DHCP Relay is enabled, the DHCP server of your router is disabled and does not assign IP addresses to clients

Disable DHCP

Stops all DHCP activity on the device. When in this mode, clients connected to the router need to be assigned an IP address manually or they have to get an IP address from another DHCP server in order to communicate with the network.



IP and DHCP Settings

LAN IP settings and DHCP settings can be configured on this page.

Local IP Settings

IP Address: 192.168.2.1

Netmask: 255.255.255.0

DHCP Settings

○ Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Lease time (sec): 3600

○ Enable Relay

Connection: wan-0

Server IP Address: 192.168.3.1

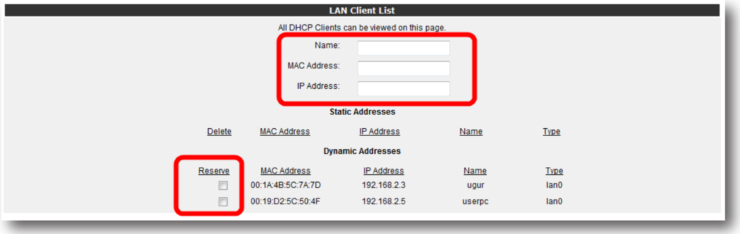
● Disable DHCP

In order for any changes made to the IP or DHCP settings to take effect, you need to click “**Save**”.

5.2.2 LAN Clients

You can see all the clients connected to your router and their connection details by selecting “**LAN Clients**” under the **“LAN”** menu of your router’s Web interface. Through this menu, you can also reserve an IP address for a client. When an IP address is reserved for a client, it cannot be assigned to any other client. Whenever the client connects to the router, it can get the IP address reserved for it.

You can see the IP addresses that are reserved in the “**Static Addresses**” table. “**Dynamic Addresses**” table shows the IP addresses assigned but not reserved.



LAN Client List

All DHCP Clients can be viewed on this page.

Name:

MAC Address:

IP Address:

Static Addresses

Delete	MAC Address	IP Address	Name	Type

Dynamic Addresses

Reserve	MAC Address	IP Address	Name	Type
□	00:1A:4B:5C:7A:7D	192.168.2.3	ugur	lan0
□	00:19:D2:5C:50:4F	192.168.2.5	userpc	lan0

Click “**Save**” for the changes you have made in the “**LAN Clients**” page to take effect.

5.3 FIREWALL settings

A firewall prevents unauthorized Internet users from accessing your local network and computer.

AirTies Firewall has SPI (Stateful Packet Inspection) feature. SPI monitors the protocol and packet addresses being received to determine if the information should be passed through the firewall to the connected computers. Internet addresses that are a source of malicious attacks are permanently blocked from accessing your network.

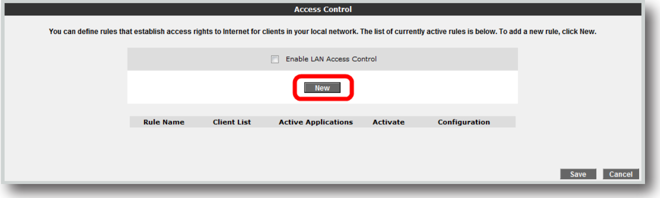
You can also limit or block the Internet access of any local user by defining advanced rules for Internet access.

The following sections describe the submenus under the “**FIREWALL**” menu of the Web interface.

5.3.1 Access control

You can allow or block Internet access of any computer on your local network using the Access Control feature. These access restrictions can be based on IP address as well as MAC address.

Click “**New**” to define a new access rule.



Access Control

You can define rules that establish access rights to Internet for clients in your local network. The list of currently active rules is below. To add a new rule, click New.

□ Enable LAN Access Control

Rule Name	Client List	Active Applications	Activate	Configuration

In the window that appears:

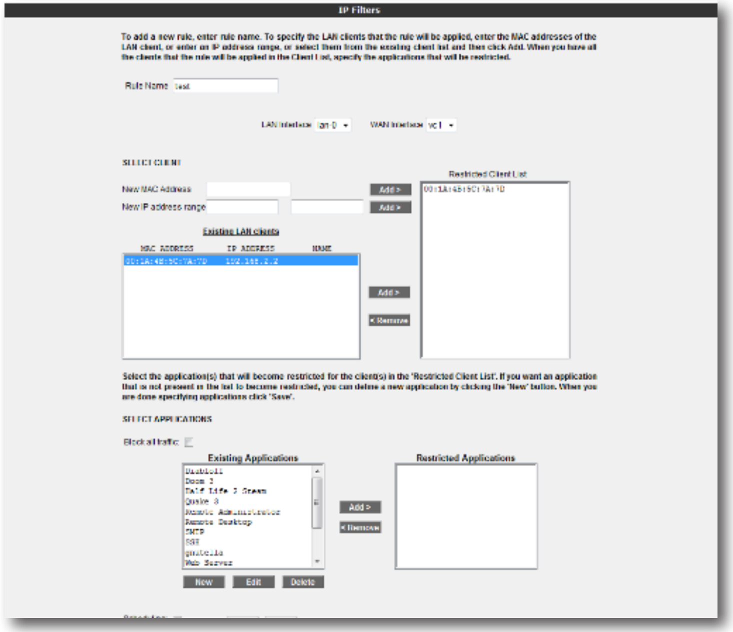
- Enter a name for the access rule you would like to define in the “**RULE NAME**” field. Choose a name that is easy to remember.
- In the “**LAN Interface**” field, enter the LAN interface to which the rule will apply. (Routers that support VLAN have more than one LAN interface.)
- Select the PVC to which the access rule will apply in the “**WAN Interface**” field.
- In the “**Select Client**” section, enter the IP or MAC addresses of the clients whose access you would like to restrict with this rule and click “**Add >**”.
- In the “**Select Applications**” section, specify the applications you would like to block access to by the clients you have defined in the “**Select Clients**” section previously. You can select the application from the “**Existing Applications**” list and click “**Add >**””.
- You can specify the times that the Access Rule will be in effect by checking the “**Schedule**” box. If you define scheduling rules, then the access rule will be in effect only during the times specified.

- To add a new application to the “**Existing Applications**” list, click “**New**”. In the window that appears:

  o Enter a name for the application you are going to define in the “**Application Name**” field.

  o Enter the LAN and WAN ports the application uses and click “**Save**”.

- Click “**Save**” when you are done.



IP Filters

To add a new rule, enter rule name. To specify the LAN clients that the rule will be applied, enter the MAC addresses of the LAN client, or enter an IP address range, or select them from the existing client list and then click Add. When you have all the clients that the rule will be applied in the Client List, specify the applications that will be restricted.

Rule Name: test

LAN Interface: lan-0 WAN Interface: vc1

SELECT CLIENT

New MAC Address

New IP address range

Existing LAN clients

MAC ADDRESS	IP ADDRESS	NAME
00:1A:4B:5C:7A:7D	192.168.2.2	

Restricted Client List

00:1A:4B:5C:7A:7D

Select the application(s) that will become restricted for the client(s) in the 'Restricted Client List'. If you want an application that is not present in the list to become restricted, you can define a new application by clicking the 'New' button. When you are done specifying applications click 'Save'.

SELECT APPLICATIONS

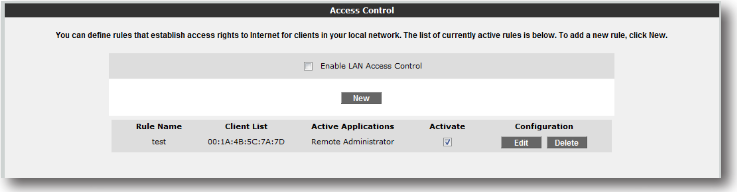
Block all traffic □

Existing Applications

Diablo II
Doom 3
Half Life 2 Steam
Quake 3
Remote Administrator
Remote Desktop
SMTP
SSH
gnutella
Web Server

Restricted Applications

• To activate the rule you have defined, check the “**Enable Access Control**” box and click “**Save**”.



Access Control

You can define rules that establish access rights to Internet for clients in your local network. The list of currently active rules is below. To add a new rule, click New.

□ Enable LAN Access Control

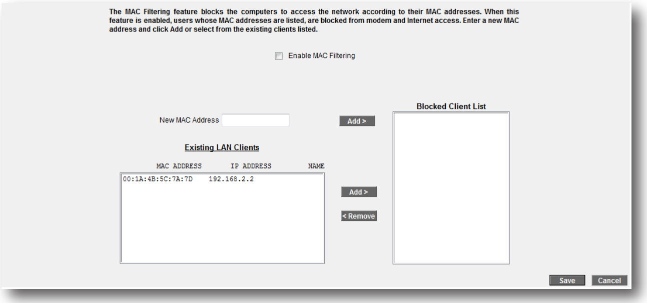
Rule Name	Client List	Active Applications	Activate	Configuration
test	00:1A:4B:5C:7A:7D	Remote Administrator	☑	Edit Delete

5.3.2 MAC address filtering

MAC Address Filtering allows you to restrict network access based on MAC addresses. When this feature is activated, the clients whose MAC addresses are on the list will have their access to the router blocked.

To restrict access based on MAC Address:

- Check the “**Enable MAC Filtering**” box.
- Enter a MAC address or choose from the list of existing clients and click “ **Add**”.
- Click “**Save**”.



The MAC Filtering feature blocks the computers to access the network according to their MAC addresses. When this feature is enabled, users whose MAC addresses are listed, are blocked from modem and Internet access. Enter a new MAC address and click Add or select from the existing clients listed.

□ Enable MAC Filtering

New MAC Address

Existing LAN Clients

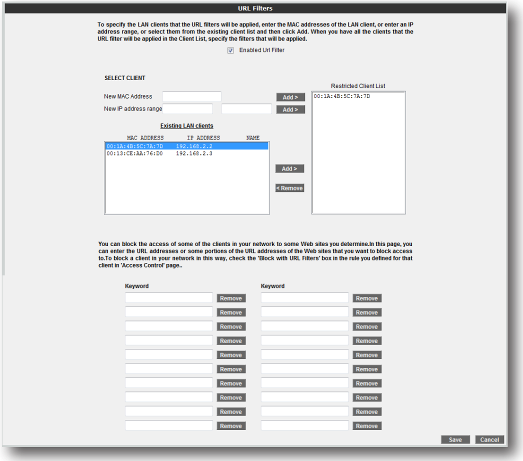
MAC ADDRESS	IP ADDRESS	NAME
00:1A:4B:5C:7A:7D	192.168.2.2	

Blocked Client List

5.3.3 URL filters

You can block access of any computer in your local network to the websites you specify. In this window, you can enter the URL or any keyword that is part of the URL for websites you would like to block access to.

- To activate the URL filtering feature check the “**Enable URL Filter**” box.
- In the “**SELECT CLIENT**” section, specify the IP or MAC addresses of the clients that the URL filtering rule will apply to, clicking the “**Add**” button after each entry.
- Enter the URL’s you would like to block access to in the “**Keyword**” list.
- Click “**Save**”.



URL Filters

To specify the LAN clients that the URL filters will be applied, enter the MAC addresses of the LAN client, or enter an IP address range, or select them from the existing client list and then click Add. When you have all the clients that the URL filter will be applied in the Client List, specify the filters that will be applied.

☑ Enabled Url Filter

SELECT CLIENT

New MAC Address

New IP address range

Existing LAN clients

```
MAC ADDRESS          IP ADDRESS       NAME
00:1A:4B:5C:7A:7D    192.168.2.2
00:13:CE:AA:76:D0    192.168.2.3
```

Restricted Client List

```
00:1A:4B:5C:7A:7D
```

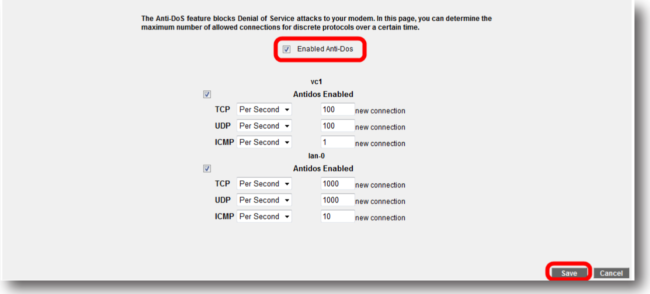
You can block the access of some of the clients in your network to some Web sites you determine.In this page, you can enter the URL addresses or some portions of the URL addresses of the Web sites that you want to block access to.To block a client in your network in this way, check the 'Block with URL Filters' box in the rule you defined for that client in 'Access Control' page..

5.3.4 Anti-DoS

The Anti-DOS feature prevents “**Denial of Service**” attacks that aim to disable your router by flooding it with connection requests. In this window, you can set the maximum number of connections that will be allowed from the Internet for a specified time interval for each protocol.

The Anti-DoS feature is disabled by default. To enable Anti-DoS and configure the necessary settings:

- Check the “**Enable Anti-DoS**” box.
- Enter the maximum number of connections that will be allowed over the LAN and Internet.
- Click “**Save**”.



The Anti-DoS feature blocks Denial of Service attacks to your modem. In this page, you can determine the maximum number of allowed connections for discrete protocols over a certain time.

☑ Enabled Anti-Dos

vc1

☑ Antidos Enabled

TCP	Per Second	100	new connection
UDP	Per Second	100	new connection
ICMP	Per Second	1	new connection

lan-0

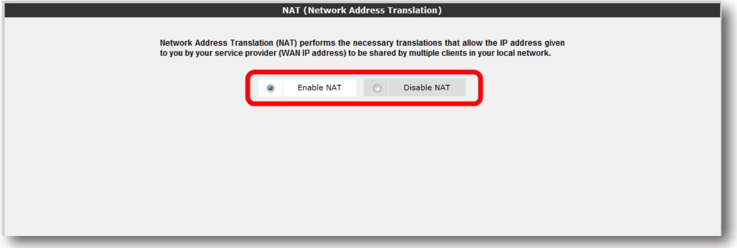
☑ Antidos Enabled

TCP	Per Second	1000	new connection
UDP	Per Second	1000	new connection
ICMP	Per Second	10	new connection

5.4 NAT

Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address. NAT allows multiple clients in your local network to access the Internet through a single global IP address (WAN IP) assigned to you by your Internet service provider.

You can enable/disable NAT using the “**NAT**” menu of your router’s Web interface. NAT is enabled by default.



NAT (Network Address Translation)

Network Address Translation (NAT) performs the necessary translations that allow the IP address given to you by your service provider (WAN IP address) to be shared by multiple clients in your local network.

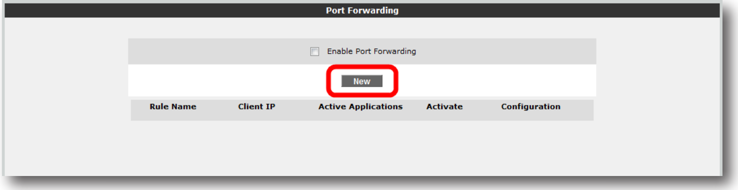
● Enable NAT ○ Disable NAT

5.4.1 Port Forwarding

“**Port Forwarding**” is used in order for a host outside your local network to access a host on your local network.

To configure Port Forwarding on your router, go to “**Port Forwarding**” under the “**NAT**” menu of the Web interface of your router.

On the screen that appears, you will see the list of currently defined port forwarding rules. If no rules have been defined yet, then the list will be empty. To define a new port forwarding rule, click “**New**”



Port Forwarding

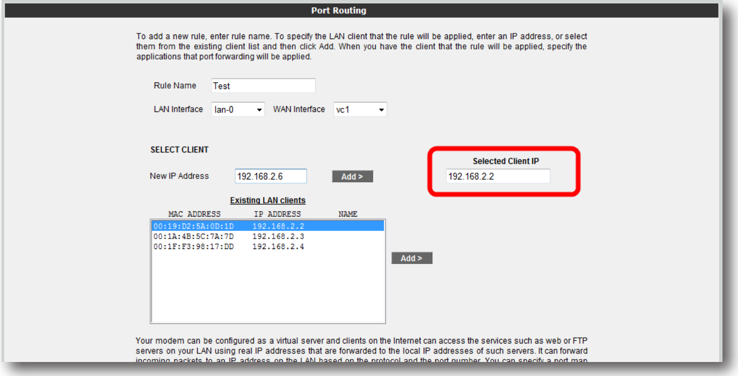
□ Enable Port Forwarding

Rule Name	Client IP	Active Applications	Activate	Configuration

On the top section of the page that comes up, fill out the fields related to the forwarding rule and the client PC’s the rule will apply to.

Rule Name: Enter a name for the new rule you are defining.

SELECT CLIENT: This section is for specifying the clients that the port forwarding rule will apply to. Enter the IP address of the client in the “**New IP Address**” field or select the IP address from the “**Existing LAN Clients**” list and click “**Add>**”. You will see the new IP address in the “**Selected Client IP**” field.



Port Routing

To add a new rule, enter rule name. To specify the LAN client that the rule will be applied, enter an IP address, or select them from the existing client list and then click Add. When you have the client that the rule will be applied, specify the applications that port forwarding will be applied.

Rule Name: Test

LAN Interface: lan-0 WAN Interface: vc1

SELECT CLIENT

New IP Address: 192.168.2.6 Add >

Selected Client IP: 192.168.2.2

Existing LAN clients

MAC ADDRESS	IP ADDRESS	NAME
00:19:D2:5A:0D:1D	192.168.2.2	
00:1A:4B:5C:7A:7D	192.168.2.3	
00:1F:F3:98:17:DD	192.168.2.4	

Add >

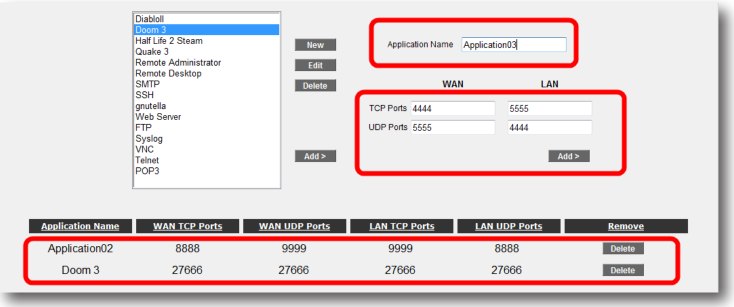
Your modem can be configured as a virtual server and clients on the Internet can access the services such as web or FTP servers on your LAN using real IP addresses that are forwarded to the local IP addresses of such servers. It can forward incoming packets to an IP address on the LAN based on the protocol and the port number. You can specify a port map

On the lower half of the screen, you can enter the port forwarding rule parameters.

- In the "**Application Name**" field, enter the name of the application for the port forwarding rule you are creating.
- In the "**TCP Ports**" fields, enter the WAN and LAN TCP port numbers. (WAN and LAN port numbers are determined by the application designer and are usually the same)
- In the "**UDP Ports**" fields, enter the WAN and LAN UDP port numbers. (WAN and LAN port numbers are determined by the application designer and are usually the same) Click "**Add>**".

All the values you have entered for the application will show up in the table below. If the application for which you'd like to setup port forwarding is already on the application list to the left of the page, you can just select it and click "**Add>**". The port numbers will be filled in automatically.

Click "**Save**" after you've entered all the parameters.

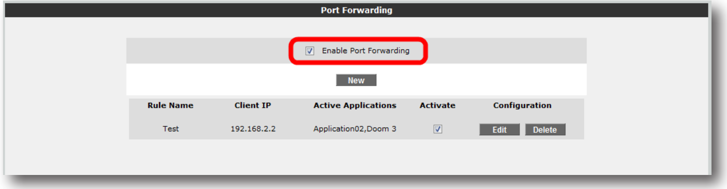


Application Name: Application03

	WAN	LAN
TCP Ports	4444	5555
UDP Ports	5555	4444

Application Name	WAN TCP Ports	WAN UDP Ports	LAN TCP Ports	LAN UDP Ports	Remove
Application02	8888	9999	9999	8888	Delete
Doom 3	27666	27666	27666	27666	Delete

After you click "**Save**", the following "**Port Forwarding**" screen will come up. Here, you will see the port forwarding rule you have defined. After checking that all the values displayed are correct, check the "**Enable Port Forwarding**" box. Then, click "**Save**".



Port Forwarding

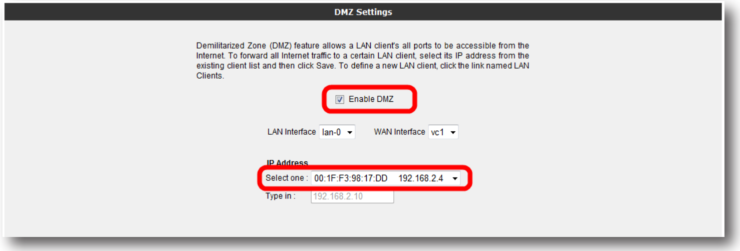
☑ Enable Port Forwarding

Rule Name	Client IP	Active Applications	Activate	Configuration
Test	192.168.2.2	Application02,Doom 3	☑	Edit Delete

5.4.2 DMZ

The DeMilitarized Zone (DMZ) feature opens up all the ports of a single local network host for unrestricted access from the Internet.

On your router, DMZ is disabled by default. To enable DMZ, go to the "**DMZ**" sub-menu under the "**NAT**" menu of your router's Web interface. On the "DMZ Settings" screen that comes up, check the "**Enable DMZ**" check box. Specify the local IP address of the network host that you would like traffic to be forwarded to in the "**IP Address**" field either by typing it in or selecting from the list. Click "**Save**". From now on, all packets coming from the Internet to your router's WAN IP (no matter which port) will be directed to the local client with the IP address you have specified."



DMZ Settings

Demilitarized Zone (DMZ) feature allows a LAN client's all ports to be accessible from the Internet. To forward all Internet traffic to a certain LAN client, select its IP address from the existing client list and then click Save. To define a new LAN client, click the link named LAN Clients.

☑ Enable DMZ

LAN Interface: lan-0 WAN Interface: vc1

IP Address

Select one : 00:1F:F3:98:17:DD 192.168.2.4

Type in : 192.168.2.10

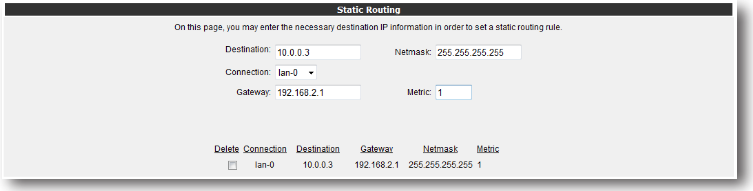
5.5 Routing

Routing defines the rules that determine how IP packets reach their destination on the Internet. You can either define static routing where you specify the target IP addresses, and how to get to them or use RIP dynamic routing protocol which updates the routing rules automatically. To specify which routing to use and set the necessary parameters, click on the "**ROUTING**" menu of your router's Web interface.

5.5.1 Static routing

To define a static routing rule, go to "**Static Routing**" under the "**ROUTING**" menu of the Web interface. You now need to enter a destination IP and how to get to it.

- **Destination IP:** Enter the IP address of the destination
- **Netmask:** Enter the Netmask for the destination IP address
- **Connection:** Enter the interface that will be used for the data transfer. It should be set to "**lan**" for local IP addresses and "**wan**" for remote IP addresses.
- **Gateway:** Enter the IP address of the host that can transfer the data to the "**Destination IP**". This can be a WAN IP or a LAN IP address depending on the connection type.
- **Metric**: In this field, you can specify the number of hops (how many gateways the data needs to go through) to get to the destination IP.



Static Routing

On this page, you may enter the necessary destination IP information in order to set a static routing rule.

Destination: 10.0.0.3 Netmask: 255.255.255.255

Connection: lan-0

Gateway: 192.168.2.1 Metric: 1

Delete	Connection	Destination	Gateway	Netmask	Metric
□	lan-0	10.0.0.3	192.168.2.1	255.255.255.255	1

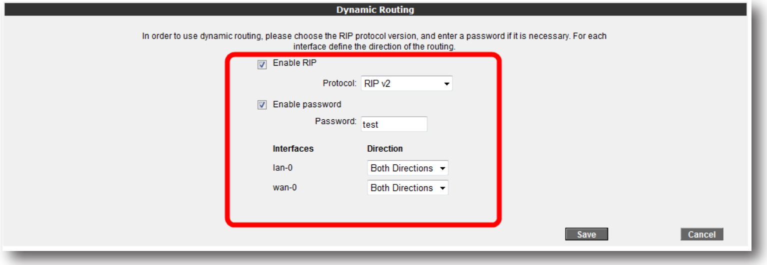
5.5.2 Dinamik routing

Dynamic Routing uses RIP protocol to determine and update the routing rules automatically based on the local and remote networks connected. There are two versions of the routing protocol: RIP v1 and RIP v2. RIP v2 allows for encryption between two routers.

To configure Dynamic Routing go to **"Dynamic Routing**" under the "**ROUTING**" menu of your router's Web interface and enter the following information:

- **Enable RIP:** Click this check box to enable dynamic routing.
- **Protocol:** If you would like to use RIP v2 and also have RIP v1 supported for backward compatibility, then select "**RIP v1 compatible**".
- **Enable password:** Check this box if you have chosen RIP v2 as the protocol and you would like to use encryption between routers.
- **Password:** Enter a password. The same password must be used in all the other routers.

When you use Dynamic Routing, for each of the LAN and WAN interfaces you can specify in which direction data can be sent. You can select "**inward**", "**outward**" or "**Both Directions**".



Dynamic Routing

In order to use dynamic routing, please choose the RIP protocol version, and enter a password if it is necessary. For each interface define the direction of the routing.

☑ Enable RIP

Protocol: RIP v2

☑ Enable password

Password: test

Interfaces	Direction
lan-0	Both Directions
wan-0	Both Directions

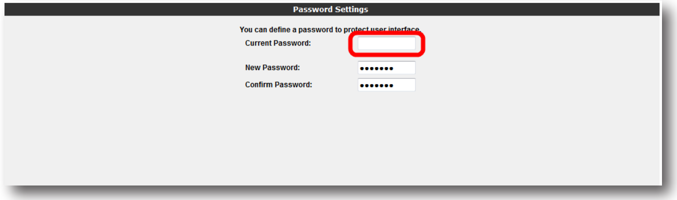
5.6 MANAGEMENT

The “**MANAGEMENT**” menu of your router’s Web interface lets you configure local and remote management settings

5.6.1 Password Settings

Your router does not have a default password for login. To login to the Web user interface leave the “**password**” field blank and click “**OK**”. You can define a password for the Web interface or change the existing password from the “**Password Settings**” menu.

When you are assigning a password to the Web interface for the first time, on the “**Password Settings**” screen, leave the “**Current Password**” field blank and enter the password you would like to use in the “**New Password**” and once more in the “**Confirm Password**” field. Click “**Save**”. From now on, you will have to use this new password to login to the Web interface.



Password Settings

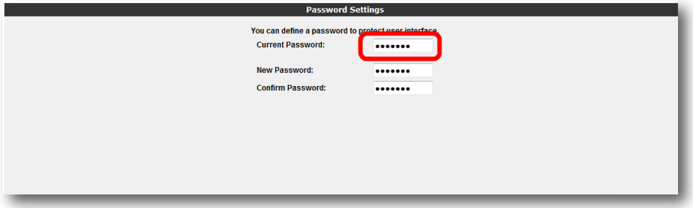
You can define a password to protect user interface.

Current Password:

New Password: •••••••

Confirm Password: •••••••

If you want to change your existing password, enter the password you’re currently using in the “**Current Password**” field and the new password in the “**New Password**” and “**Confirm Password**” fields, and click “**Save**”.



Password Settings

You can define a password to protect user interface.

Current Password: •••••••

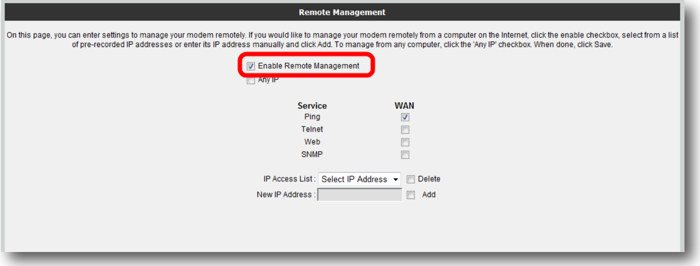
New Password: •••••••

Confirm Password: •••••••

5.6.2 Remote Management

To enter the settings related to the remote management of your device, go to “**Remote Management**” under the “**MANAGEMENT**” menu.

To enable remote management of your device, click the “**Enable Remote Management**” check box.



Remote Management

On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

☑ Enable Remote Management

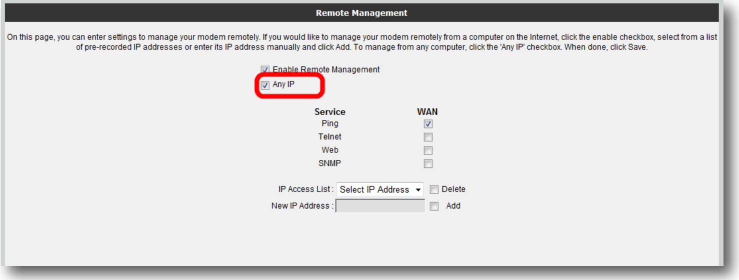
□ Any IP

Service	WAN
Ping	☑
Telnet	□
Web	□
SNMP	□

IP Access List : Select IP Address □ Delete

New IP Address : □ Add

If you check the “**Any IP**” box, your router can be managed remotely from any computer.



Remote Management

On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

☑ Enable Remote Management

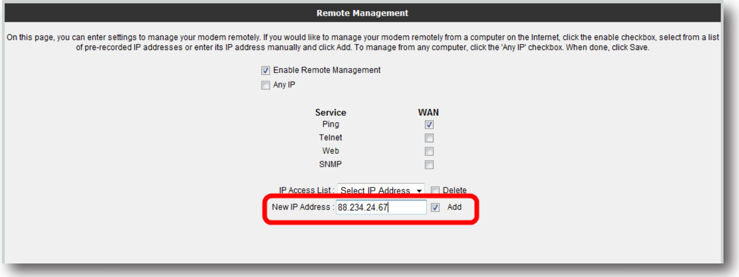
☑ Any IP

Service	WAN
Ping	☑
Telnet	□
Web	□
SNMP	□

IP Access List : Select IP Address □ Delete

New IP Address : □ Add

If “**Any IP**” is not checked, you have to add the WAN IP address of the computer from which you would like to remotely manage your device to the “**IP Access List**”. To do this, enter the WAN IP address in the “**New IP Address**” field and click the “Add” box.



Remote Management

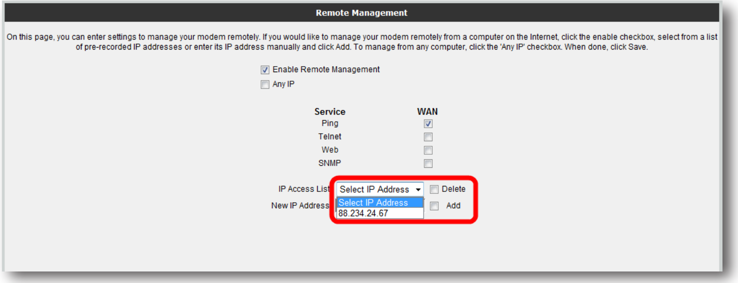
On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

☑ Enable Remote Management
☐ Any IP

Service	WAN
Ping	☑
Telnet	☐
Web	☐
SNMP	☐

IP Access List : Select IP Address ☐ Delete
New IP Address : 88.234.24.67 ☑ Add

After saving, the WAN IP address you have entered will appear in the **“IP Access List**”. If you select this address from the list and click “**Save**”, remote management will be activated for this address. If you want to remove an IP address from the list, select the address from the list, click on the “**Delete**” checkbox and then click “**Save**”.



Remote Management

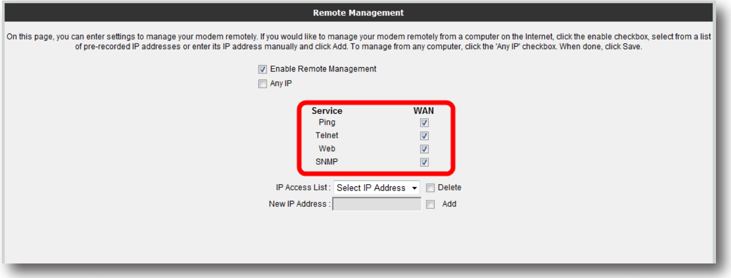
On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

☑ Enable Remote Management
☐ Any IP

Service	WAN
Ping	☑
Telnet	☐
Web	☐
SNMP	☐

IP Access List : Select IP Address ☐ Delete
New IP Address : ☐ Add

You can also specify which services will be available to the remote management computers on this page.



Remote Management

On this page, you can enter settings to manage your modem remotely. If you would like to manage your modem remotely from a computer on the Internet, click the enable checkbox, select from a list of pre-recorded IP addresses or enter its IP address manually and click Add. To manage from any computer, click the 'Any IP' checkbox. When done, click Save.

☑ Enable Remote Management
☐ Any IP

Service	WAN
Ping	☑
Telnet	☑
Web	☑
SNMP	☑

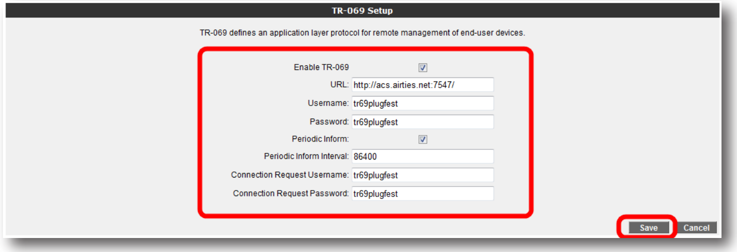
IP Access List : Select IP Address ☐ Delete
New IP Address : ☐ Add

<span style="color:red">5.6.3</span> TR-069 Settings

TR-069 is an application layer protocol for remote management of end-user devices. With TR-069, all the settings that can be configured over a local area connection can be done automatically via remote Automatic Configuration Servers (ACS). There are a few simple settings to be configured to use TR-069 for automatic configuration. For these settings, go to “**TR-069 Settings**” under the “**MANAGEMENT**” menu.

- **Enable TR-069:** Check this box to enable TR-069.
- **URL:** The ACS address the router will connect to (given to the user by the ACS provider)
- **User Name:** The user name to be used by the router to connect to the ACS server (assigned to the user by the ACS provider)
- **Password:** The password to be used by the router to connect to the ACS server (assigned to the user by the ACS provider)
- **Periodic Inform Interval:** the time in seconds after which the router and the ACS server will check their connection status. The default period is set to 86400 seconds for your router.
- **Connection Request User Name:** The user name that the ACS will use to connect to the router.
- **Connection Request Password:** The password that the ACS will use to connect to the router.

After entering all the values, click “**Save**”.



TR-069 Setup

TR-069 defines an application layer protocol for remote management of end-user devices.

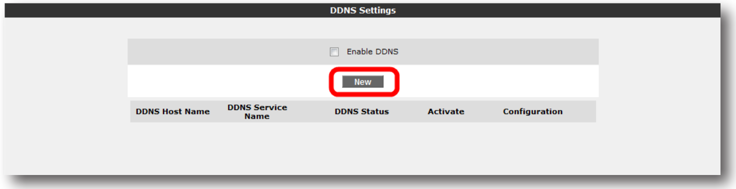
Enable TR-069	☑
URL:	http://acs.airties.net:7547/
Username:	tr69plugfest
Password:	tr69plugfest
Periodic Inform:	☑
Periodic Inform Interval:	86400
Connection Request Username:	tr69plugfest
Connection Request Password:	tr69plugfest

5.7 DDNS

Dynamic DNS (DDNS), ensures that your hostname and IP address in the Internet name servers are always current. It's primarily used to associate a domain name with a dynamic IP address which makes it possible to access a computer with a dynamic IP address over the Internet. It also allows you to run a server on a computer with a dynamic IP address.

5.7.1 DDNS Settings

To configure the DDNS settings of your router, go to "**DDNS Settings**" under the "**DDNS**" menu of the Web interface. On the "**DDNS Settings**" screen that comes up, you can see the current DDNS account information. To enter a new DDNS account, click "**New**".

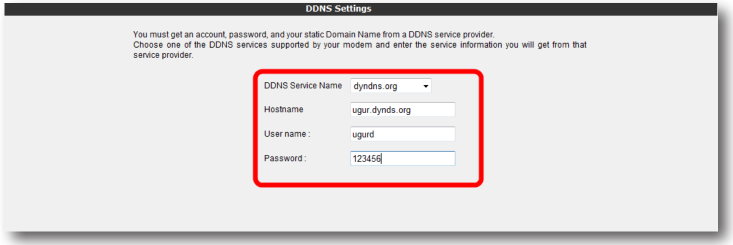


DDNS Settings

☐ Enable DDNS

DDNS Host Name	DDNS Service Name	DDNS Status	Activate	Configuration

To use the Dynamic DNS feature, you need to setup an account with a DDNS service provider. On the screen that comes up, select a DDNS service provider and enter your account information (**Hostname**, **Username**, **Password**). Click "**Save**" after you have filled in the necessary fields.



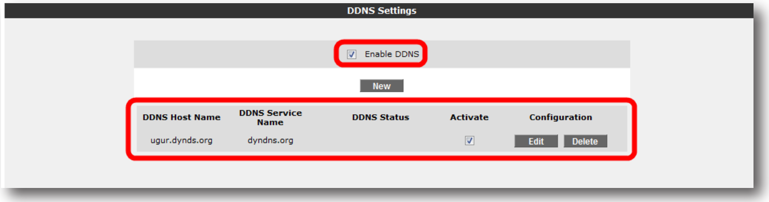
DDNS Settings

You must get an account, password, and your static Domain Name from a DDNS service provider.
Choose one of the DDNS services supported by your modem and enter the service information you will get from that service provider.

DDNS Service Name: dyndns.org
Hostname: ugur.dynds.org
User name : ugurd
Password : 123456

Clicking "**Save**" will take you to the "**DDNS Settings**" screen again. Here you can see the account information you have entered and account status, and if you have more than one DDNS service entry, you can change the active account. You can also edit or delete the DDNS accounts you have previously entered.

To enable DDNS, check the "**Enable DDNS**" box and click "**Save**".



DDNS Settings

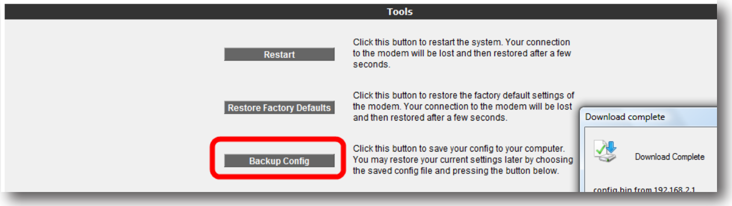
☑ Enable DDNS

DDNS Host Name	DDNS Service Name	DDNS Status	Activate	Configuration
ugur.dynds.org	dyndns.org		☑	Edit Delete

5.8 Tools

On this page, you can restart your router, reset it to factory defaults, backup your router's current configuration or restore from a previous backup. To get to the "**Tools**" screen, select "**TOOLS**" from the main menu of the Web interface.

- The "**Restart**" button restarts your router remotely. During this operation, your connection to the router will be lost. You can reconnect after the router comes back up.
- The "**Restore Factory Defaults**" button allows you to reset your router back to factory defaults remotely. This will clear all the current settings on your router.
- "**Backup Config**" lets you save the current settings of your router onto your computer. When you click the "**Backup Config**" button, your router will create a file called "**config.bin**" to be saved on your computer. You can restore this configuration later using the "**Restore Config**" button.



Tools

Restart — Click this button to restart the system. Your connection to the modem will be lost and then restored after a few seconds.

Restore Factory Defaults — Click this button to restore the factory default settings of the modem. Your connection to the modem will be lost and then restored after a few seconds.

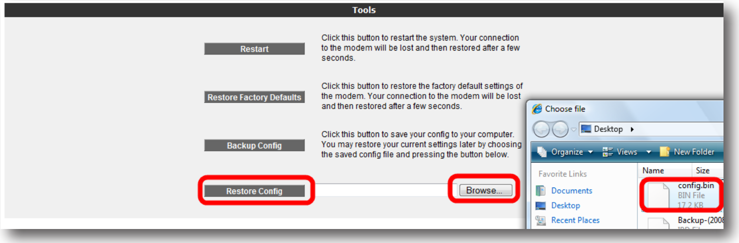
Backup Config — Click this button to save your config to your computer. You may restore your current settings later by choosing the saved config file and pressing the button below.

Download complete

Download Complete

config.bin from 192.168.2.1

- "**Restore Config**" lets you restore a previously saved configuration onto your router Click the "**Browse**" button to locate the config.bin file that was previously saved, and then press the "**Restore Config**" button to restore your settings from this file onto your router.



Tools

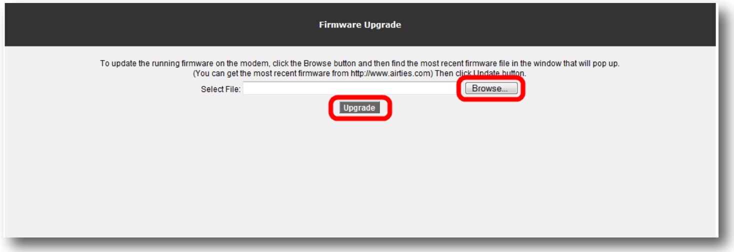
Click this button to restart the system. Your connection to the modem will be lost and then restored after a few seconds.

Click this button to restore the factory default settings of the modem. Your connection to the modem will be lost and then restored after a few seconds.

Click this button to save your config to your computer. You may restore your current settings later by choosing the saved config file and pressing the button below.

5.8.1 Firmware Upgrade

In order to update the firmware running on the router, go to "**Firmware Upgrade**" under the "**TOOLS**" menu. Click "**Browse**" and locate the most recent router firmware file on your computer in the pop-up window that appears. (You can download the most recent firmware file from the AirTies website www.airties.com). Then click "Upgrade".



Firmware Upgrade

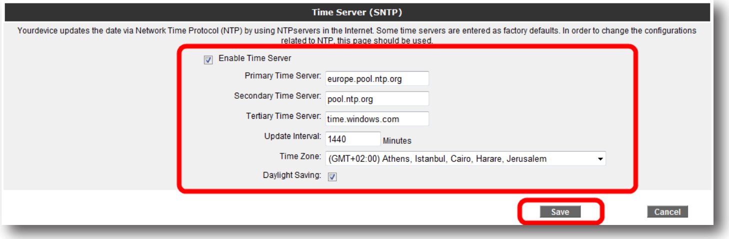
To update the running firmware on the modem, click the Browse button and then find the most recent firmware file in the window that will pop up.
(You can get the most recent firmware from http://www.airties.com) Then click Update button.

Select File:

After the firmware is successfully installed, the system will restart automatically. Therefore, connection to the device will be lost. You will need to reconnect if you would like to reconfigure any settings. Your router must stay ON during the upgrade.

5.8.2 Time Settings

Your router gets the current time and date from Internet time servers using the SNTP protocol. Default factory settings include some time servers. To change the time servers used by your router go to "Time Settings" under the "**TOOLS**" menu of the Web interface. In the "**Time Server (SNTP)**" window that comes up, enter the time server information and click "**Save**".



Time Server (SNTP)

Yourdevice updates the date via Network Time Protocol (NTP) by using NTPservers in the Internet. Some time servers are entered as factory defaults. In order to change the configurations related to NTP, this page should be used.

☑ Enable Time Server

Primary Time Server: europe.pool.ntp.org

Secondary Time Server: pool.ntp.org

Tertiary Time Server: time.windows.com

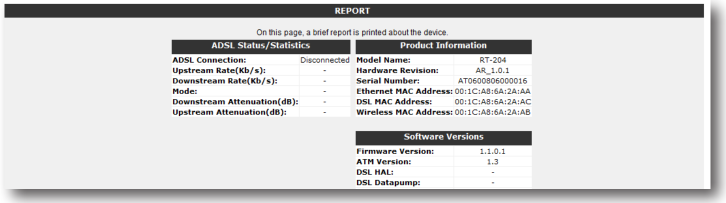
Update Interval: 1440 Minutes

Time Zone: (GMT+02:00) Athens, Istanbul, Cairo, Harare, Jerusalem

Daylight Saving: ☑

5.9 REPORTS

The "**REPORTS**" menu displays information about the main characteristics of your router such as ADSL Status and Statistics, Product Information and Software Versions.



REPORT

On this page, a brief report is printed about the device.

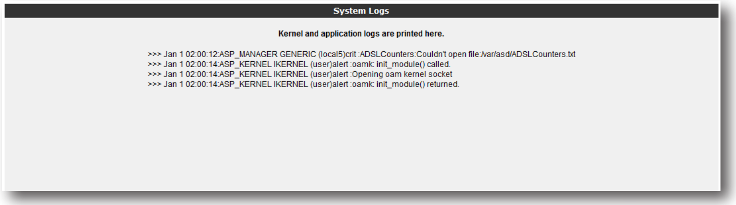
ADSL Status/Statistics	
ADSL Connection:	Disconnected
Upstream Rate(Kb/s):	-
Downstream Rate(Kb/s):	-
Mode:	-
Downstream Attenuation(dB):	-
Upstream Attenuation(dB):	-

Product Information	
Model Name:	RT-204
Hardware Revision:	AR_1.0.1
Serial Number:	AT0600806000016
Ethernet MAC Address:	00:1C:A8:6A:2A:AA
DSL MAC Address:	00:1C:A8:6A:2A:AC
Wireless MAC Address:	00:1C:A8:6A:2A:AB

Software Versions	
Firmware Version:	1.1.0.1
ATM Version:	1.3
DSL HAL:	-
DSL Datapump:	-

5.9.1 System Logs

The "**System Logs**" under the "**REPORTS**" menu displays detailed system logs about system activity and the applcations that were active since the router was last started.



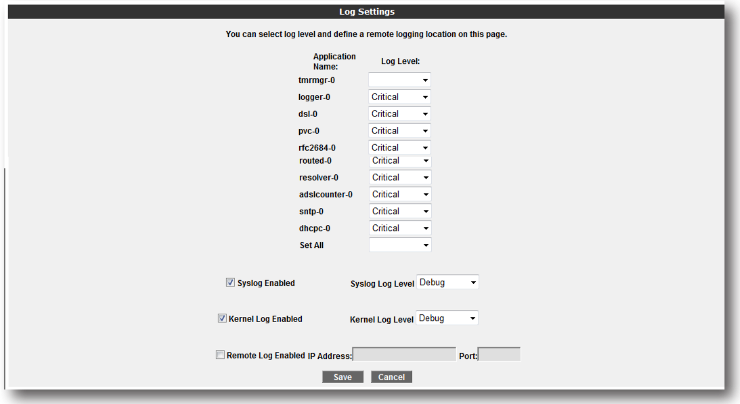
System Logs

Kernel and application logs are printed here.

```
>>> Jan 1 02:00:12:ASP_MANAGER GENERIC (local5)crit :ADSLCounters:Couldn't open file:/var/asd/ADSLCounters.txt
>>> Jan 1 02:00:14:ASP_KERNEL IKERNEL (user)alert :oamk: init_module() called.
>>> Jan 1 02:00:14:ASP_KERNEL IKERNEL (user)alert :Opening oam kernel socket
>>> Jan 1 02:00:14:ASP_KERNEL IKERNEL (user)alert :oamk: init_module() returned.
```

5.9.2 Log Settings

"**Log Settings**" allows you to set log detail levels. You can also specify a remote logging destination.



Log Settings

You can select log level and define a remote logging location on this page.

Application Name:	Log Level:
tmrmgr-0	
logger-0	Critical
dsl-0	Critical
pvc-0	Critical
rfc2684-0	Critical
routed-0	Critical
resolver-0	Critical
adslcounter-0	Critical
sntp-0	Critical
dhcpc-0	Critical
Set All	

☑ Syslog Enabled — Syslog Log Level: Debug

☑ Kernel Log Enabled — Kernel Log Level: Debug

□ Remote Log Enabled IP Address: Port:

6 TECHNICAL PROPERTIES

- **ADSL properties:** G.992.1 Annex A (G.DMT), G.992.2 (G.Lite), G.992.3 (ADSL2), G992.4 (G.Lite.bis), G.992.5 (ADSL2+),Rate Adaptive DSL (RADSL), READSL, Traffic shaping UBR/CBR, OAM (I.610)
- **Connection protocols:** PPPoE, PPPoA, RFC1483 Bridging, RFC1483 Routing, classical IP over ATM, PAP/CHAP, RFC 2364 PPP over AAL5, RFC2366 Multicast over ATM
- **Wireless transmit power:** Max 16 dBm EIRP
- **Wireless security options:** WPA2, WPA, WEP, wireless MAC address filtering, SSID hiding
- **Frequency range:** ETSI 2400MHz - 2483.5MHz (13 channels with 3 non-overlapping), 20/40MHz channel bandwidth
- **Router and Firewall:** Anti-DoS SPI firewall; IP and MAC address filtering; URL filtering; Port forwarding; DMZ; Static Routing, RIPv1, RIPv2 routing; DNS Proxy; DHCP server and client; NAT/NAPT; PPP (PAP/CHAP/MSCHAP), IGMPv1/v2*
- **UPnP** (Universal Plug and Play)
- **Reset** button to return the router to factory settings
- **Operating voltage:** 100V AC - 240V AC
- **Cabling:** RJ-45 (Ethernet), RJ-11 (ADSL)
- **Ports:** ADSL, Power (15V DC), 4 x 10/100 Ethernet(RJ-45, auto MDI/MDIX), 1xUSB Host
- **LEDs:** Power, Internet, ADSL, Ethernet 1-4, USB, Wireless
- **Certificates:** CE

* Features to be added with a firmware upgrade

7 PHYSICAL CHARACTERISTICS

Dimensions: 255mm x170mm x 33mm

Weight: 350 g

Power: 15Volt DC, 1.2A

Operating Voltage: 100V - 240V AC

Operating Temperature: 0°C ~ 40°C

Storage Temperature: -40°C ~ 70°C

Humidity %10 - %90: non-condensing

AirTies

www.airties.com

Easy setup CD

Three year warranty

7/24 people support
801 100 0911

CE ⓘ