AirTies

300 Mbps Wireless 4-Port Router

User Manual

Air 4450

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 its Access Point and Router functionality, the Air 4450 provides wireless Internet access over ADSL and Cable modems. Air 4450 uses 802.11n technology thus providing wireless data transfer rates of up to 300 Mbps. Thus you can transfer data, watch videos or upload your pictures to the Internet at "N-speed". Providing 6 times faster wireless communications compared to earlier technologies, and 4 times greater wireless range through use of MIMO technology*, Air 4450 is developed to meet all your wireless needs.

You can resolve wireless coverage area problems, through use of AirTies Mesh Technology which allows you to expand wireless coverage area in concrete buildings and very large areas where signal range problems are common.

The Wireless Bridge feature lets you include devices with no wireless capability but with an Ethernet interface in your wireless network.

You can share files and printers over your entire network from a single point using the USB "Plug and Share" feature.

Air 4450 is fully compatible with all 802.11b/g devices and Centrino / Centrino 2 laptops.

* compared to the range of 54Mbps wireless communications on a 802.11b/g wireless network
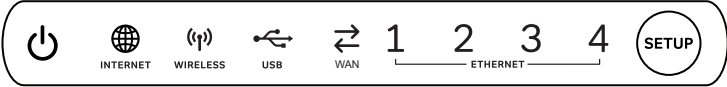
1.1 Minimum System Requirements

- For installation and configuration: a PC that has an Ethernet interface or 802.11 b/g/n compatible wireless capability, and is running any version of Windows, UNIX, Linux or Mac Operating Systems and a Web browser
- For the AirTies ADSL Utility: 32 bit Windows 98/ME/2000/XP/Vista

The device does not need to be connected to a PC during normal operation.

1.2 Package Contents

Please check to make sure all the parts listed below are included in the box:

1. Air 4450 300Mbps Wireless 4-port Router
2. 12V Power adapter
3. Ethernet cable
4. AirTies Easy Setup CD
5. Quick Installation Guide
6. Warranty Card and Certificate of Compliance

1.3 Front Panel

LED	LIGHT	STATUS
POWER	Blue	The device is "ON".
	Off	The device is "OFF".
INTERNET	Red	Internet connection established and active
	Red Flashing	Connecting to the Internet
	Off	No Internet connection
WIRELESS	Red	Wireless network connection established and active
	Red flashing	Data exchange on the wireless network connection
	Off	No wireless network connection
USB	Red	USB connection established
	Red flashing	USB connection active. There is data exchange.
	Off	No USB connection
WAN	Red	WAN connection established and active
	Red flashing	Data exchange on the WAN connection
	Off	No WAN connection.
ETHERNET 1 2 3 4	Red	LAN connection established and active
	Red flashing	LAN connection active. There is data exchange.
	Off	No LAN connection

1.4 Back Panel

WAN	Internet line port, connects to Internet gateway devices
ETHERNET 1-4	Ethernet ports
Reset	Button to reset your device to default factory settings
USB	USB Plug and Share port
ON/OFF	Button to turn your device on and off
12V Power Port	12V power port, connects to the power adapter

1.5 Main Features

- **Multi-function:** Router, 300Mbps Wireless Access Point, Repeater
- **"N-speed" wireless communications:** 300 Mbps wireless access point compliant with the 802.11n (Draft2.0) standard
- **Repeater:** AirTies Mesh Technology support for extending wireless coverage area in concrete buildings where signal range problems are common.
- **Router:** Advanced router with DHCP server, NAT, NAPT, DMZ, VLAN*, RIPv1/v2 support
- **USB Plug and Share** feature gives you printer and file sharing capability throughout your entire network from a single point*
- **Backward Compatible:** fully compatible with 802.11b/g devices
- Advanced Wireless Security: WPA2- PSK, WPA2-802.1x, WPA-PSK, WPA-802.1x, WEP wireless encryption standards support
- **Firewall:** Advanced anti-DoS SPI Firewall; MAC and IP address based filtering for Internet access
- **Uninterrupted technical support:** 7/24 AirTies Call Center and Technical Support (engineering support by the AirTies R&D team when needed)
- **3 year extended warranty**

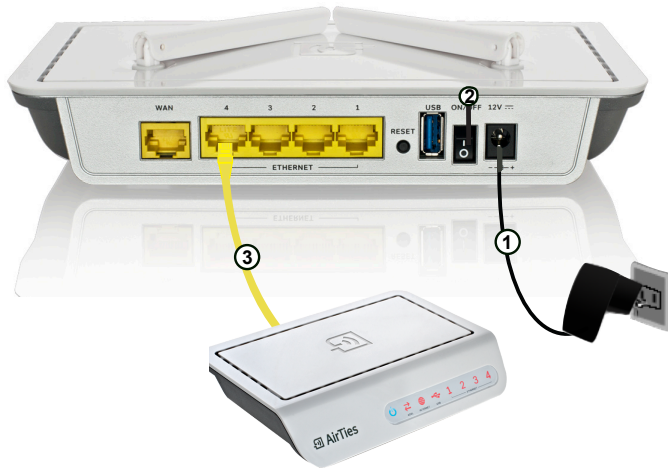*** To be added with a firmware upgrade**

2. INSTALLATION

2.1 Installing the Air 4450 as an Access Point

In Access Point mode, the Air 4450 provides wireless access capability on any network where access to the Internet is through a wired ADSL modem, essentially making a wired network wireless.

Note: How to change the mode of your device is explained in section 3.1 Operation Mode of this manual.

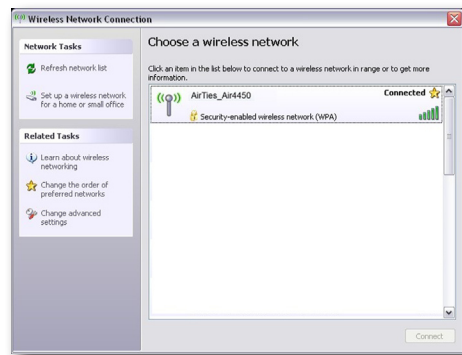### 2.1.1 Connecting the Cables for Access Point Mode

1. Connect the 12V power adapter included in the box to the power port of your device and plug it into the wall outlet.
2. Turn the Air 4450 on by switching the On/Off button to "|" position.
3. Using the Ethernet cable provided, connect one of the LAN ports of the Air 4450 to the Ethernet port of your ADSL modem or an Ethernet port of a Switch on your wired network.

2.1.2 Connecting to the Air 4450

The Air 4450 cable connections must be complete before you can establish a wireless connection to it.

1. First, check to make sure the wireless network client (802.11b/g or 802.11n) of your computer is enabled.
2. Find the "**AirTies_Air4450**" network (SSID) on the wireless network search page of your wireless network client and connect to it.
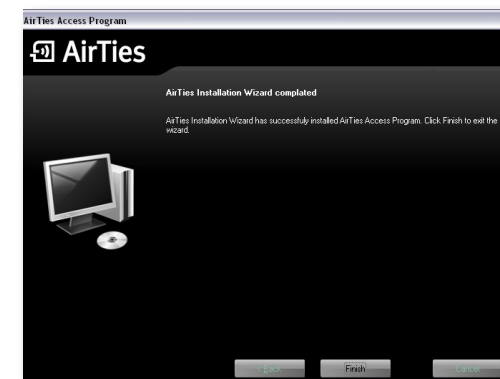

2.1. 3 Advanced Settings Using the AirTies Access Program

Important: To be able to use the AirTies Access Program, your device must be connected to an ADSL modem or a wired network and must have an IP address assigned to it.
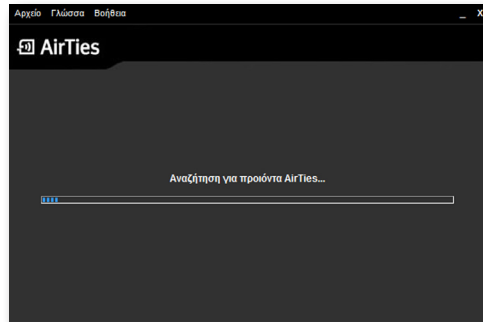
1. By using the AirTies Access Program you can access the Web interface of your device to configure the encryption settings and other advanced settings of your wireless network.
2. Insert the Air 4450 Easy setup CD into your computer.
3. The AirTies Access Program installation wizard will start automatically. Click Next> to start the installation.
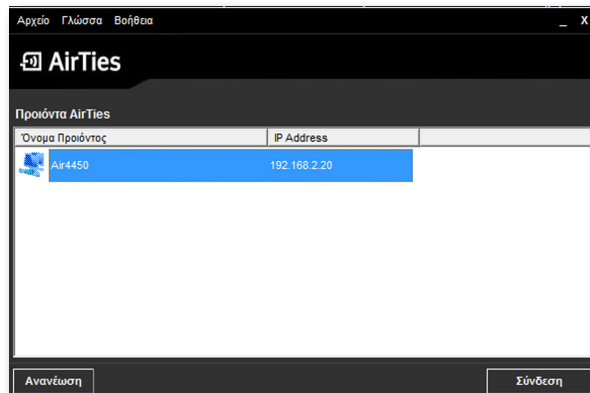

4. To complete the installation process, click "**Finish**" in the installation wizard.
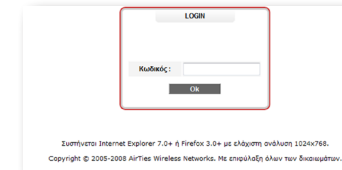
5. Once the installation is complete, the AirTies Access Program will start looking for AirTies products that are connected to your computer.

6. At the end of the search, a list of all AirTies products connected to your computer will be displayed.

7. Select the AirTies product whose Web interface you'd like to access and click "**Σύνδεση**". The login screen will come up. You do not need a password to access the Web interface. Click "**OK**" to enter.
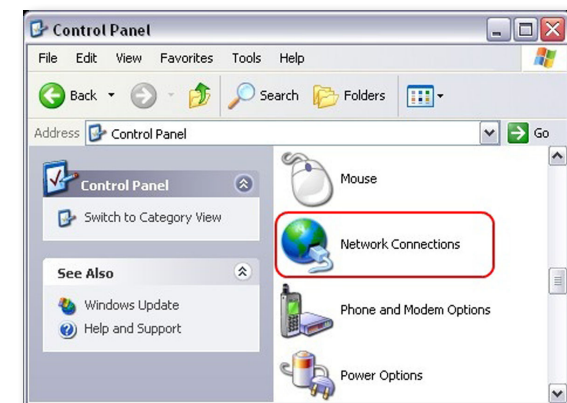

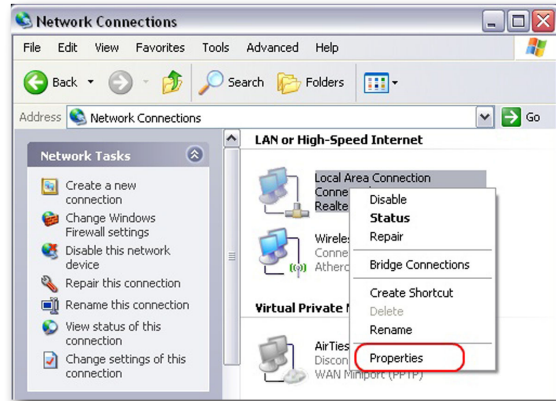**2.1.4** Accessing the advanced settings with a Static IP

In Access Point mode, you can configure the advanced settings by connecting the Air 4450 directly to your computer. For this, you need to assign a static IP address to your computer's network adapter. The IP address has to be within the same network block as the default IP address of the Air 4450 (192.168.2.254) and must be static (example: 192.168.2.5). Below you will find instructions for assigning a static IP address under various operating systems.
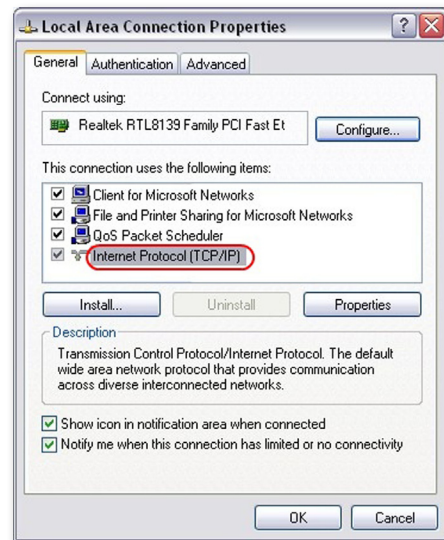
Windows XP

1. Go to **Start -> Control Panel.**
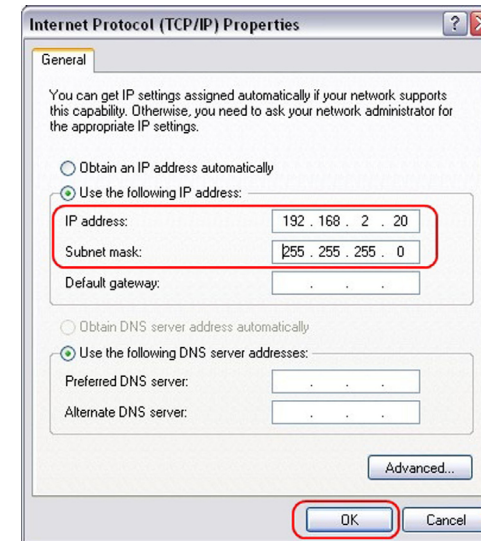2. Click **Network Connections.**

3. In the Network Connections window, right-click on the network adapter from which you will connect to the Air 4450 (Wireless Network Connection, Local Area Connection) and select **Properties**.

4. Right-click on **Internet Protocol (TCP/IP) and select Properties.**

5. In the **Internet Protocol (TCP/IP) Properties** window click on the **Use the following IP address** button and enter an address in the 192.168.2.1 – 192.168.2.253 range in the **IP address** field.

6. The **Subnet mask** field will have a default value of 255.255.255.0. You do not need to change this value.
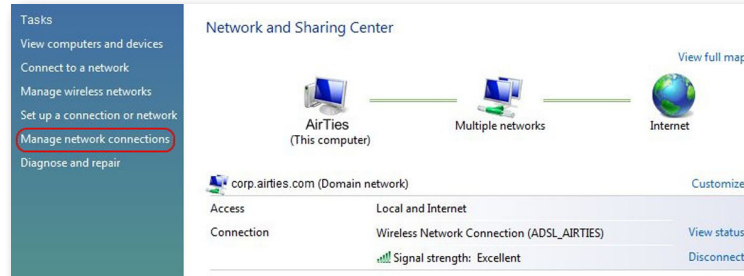

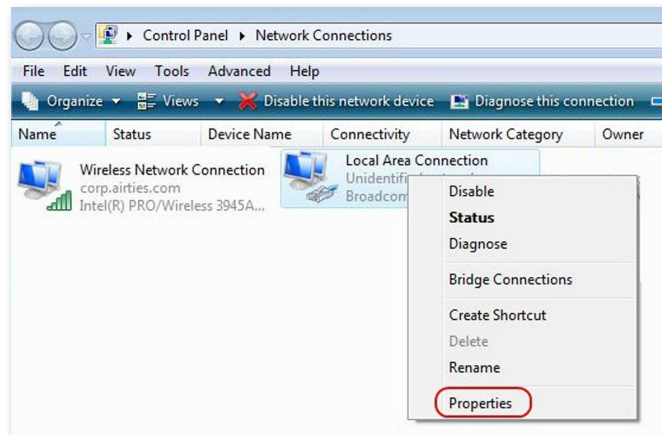7. Click the **OK** button at the bottom of the window

Windows Vista

1. Go to **Start -> Control Panel.**
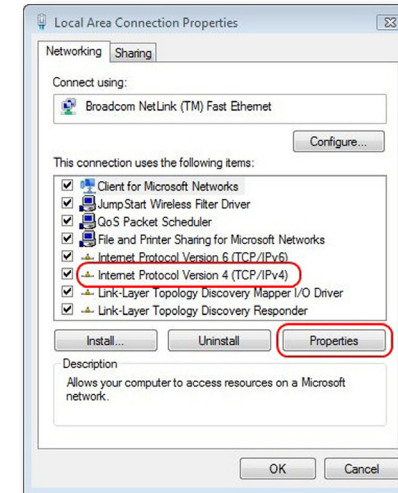2. Select **Network and Sharing Center.**

8

3. At the **Network and Sharing Center,** select **Manage network connections** from the menu on the left.

4. In the window that comes up, right-click on the network adapter from which you will connect to the Air 4450 (Wireless Network Connection, Local Area Connection) and select **Properties**.

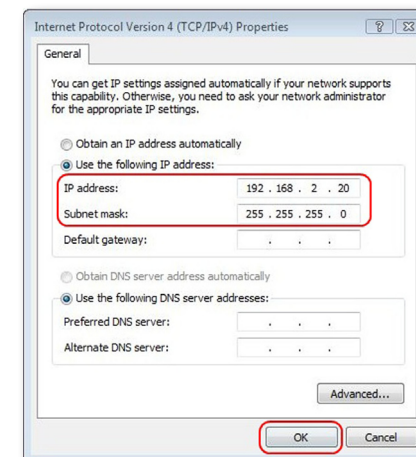5. In the **Network Connection Properties** window, double-click on **Internet Protocol version 4 (TCP/IPv4)**.

6. In the Internet Protocol version 4 (TCP/IPv4) window click on the Use the following IP address button and enter an address in the 192.168.2.1 – 192.168.2.253 range in the IP address field.

7. The Subnet mask field will have a default value of 255.255.255.0. You do not need to change this value.

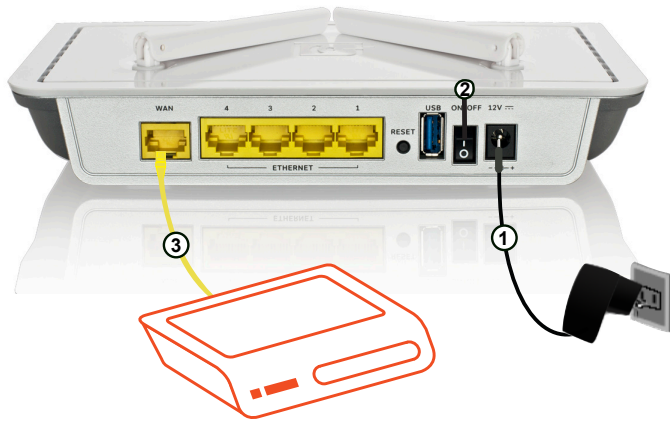8.Click the **OK button** at the bottom of the window.

When finished, you can open a browser window (e.g. Internet Explorer, Firefox) and enter 192.168.2.254 in the address field to access the Web interface for configuring advanced settings

2.2 Installing the Air 4450 as a Router

In Router mode, the Air 4450 allows you to connect your entire wired network to the Internet wirelessly through a modem that does not have NAT or Firewall features.

Note: How to change the mode of your device is explained in section 3.1 Operation Mode of this manual.

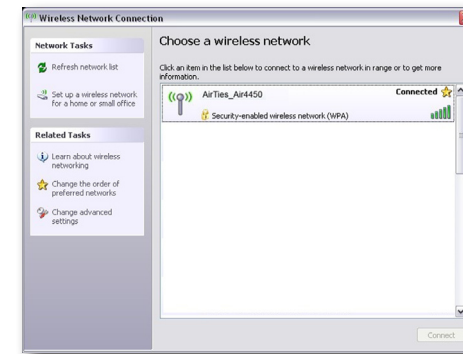## 2.2.1 Connecting the Cables for the Router Mode

1. Connect the 12V power adapter included in the box to the power port of your device and plug it into the wall outlet.

2. Turn the Air 4450 on by switching the On/Off button to "|" position.

3. Using the Ethernet cable provided, connect the WAN port of the Air 4450 to a cable modem or Internet gateway.

2.2.2 Connecting to the Air 4450 (In Router mode)

The Air 4450 cable connections must be complete before you can establish a wireless connection to it.

1. First, check to make sure the wireless network client (802.11b/g or 802.11n) of your computer is enabled.

2. Find the "**AirTies_Air4450**" network (SSID) on the wireless network search page of your wireless network client and connect to it.
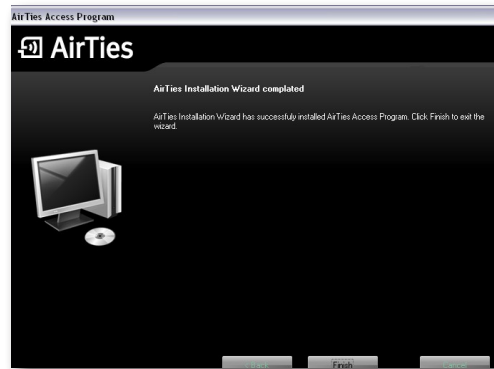

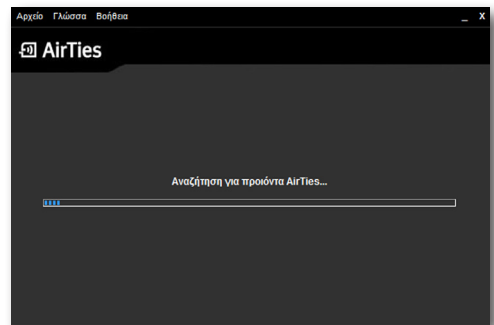## 2.2.3 Advanced Settings Using the AirTies Access Program (in Router mode)

1. By using the AirTies Access Program you can access the Web interface of your device to configure the encryption settings and other advanced settings of your wireless network.

2. Insert the Air 4450 Easy setup CD into your computer.

3. The AirTies Access Program installation wizard will start automatically. Click **Next>** to start the installation.
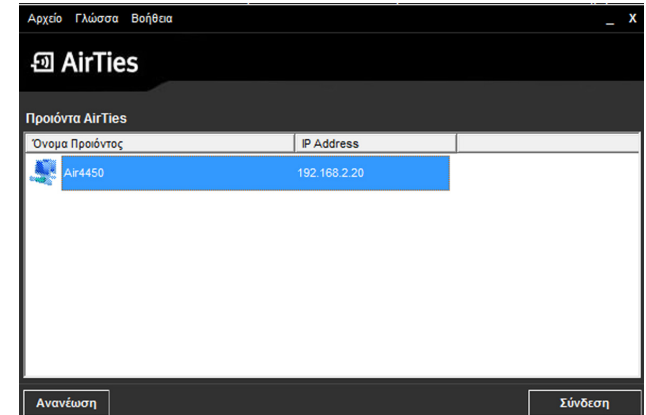
4. To complete the installation process, click "Finish" in the installation wizard.

5. Once the installation is complete, the AirTies Access Program will start looking for AirTies products that are connected to your computer.

6. At the end of the search, a list of all AirTies products connected to your computer will be displayed.

7. Select the AirTies product whose Web interface you'd like to access and click "Σύνδεση". The login screen will come up. You do not need a password to access the Web interface. Click "**OK**" to enter.
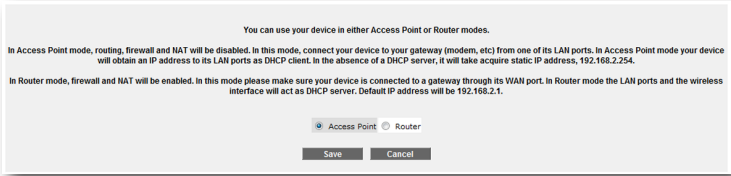

Σημείωση: Στον τρόπο λειτουργίας router, η προεπιλεγμένη διεύθυνση του Web interface για το Air 4450 είναι 192.168.2.1.

3 ADVANCED SETTINGS

3.1. Operation Mode

On this screen you can choose the operation mode of your device as either an Access Point or Router. Choose the operation mode of your device and click "**Save**".

3.2 Internet settings
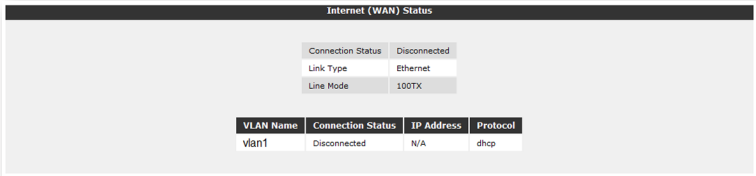
3.2.1 Internet status and statistics

When you click "Internet" on the main menu of your device's Web interface, the "Internet (WAN) Status" page will come up. Here, you can see detailed information about your Internet connection and upstream/ downstream data rates. You can also check the status of your current PVC connection.

Connection Status shows whether your device and the devices connected to it have Internet access or not.

Link Type shows the type of connection your device has to the Internet. Your device **connects to the Internet over Ethernet.**

Link Mode is the connection mode. It also indicates the maximum data rate for the connection.
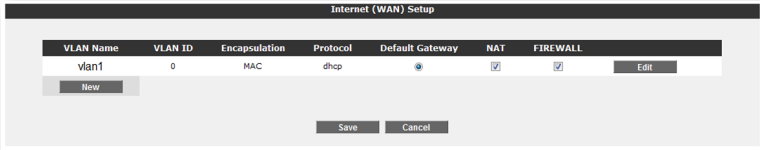
Internet Connection Speed shows the speed of upload and download traffic (in Kbps) measured at every refresh.
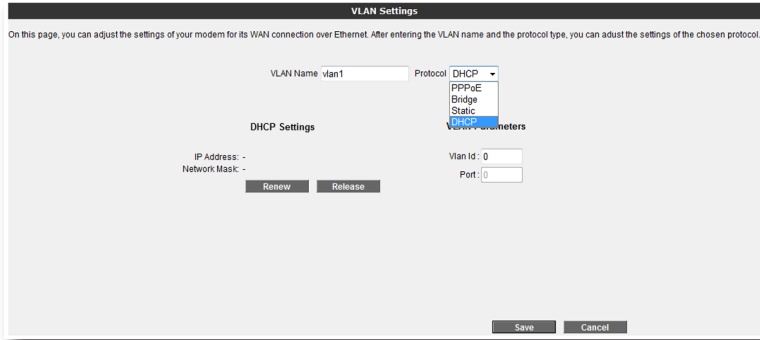

3.2.2 Internet Settings

When you click INTERNET on the main menu of the Web interface, you will see Internet Settings as the first submenu. Go to Internet Settings to configure the Internet settings of your device. If you are connected to the Internet through a direct connection to a cable modem, then the information necessary for configuring the settings must be on your computer. If you are a first time user, you can obtain the necessary information from your Internet Service Provider.

1. When you click on the Internet Settings submenu, a table showing your default PVC settings will be displayed.

2. To enter your Internet settings, click the "Edit" button in this table. The "**VLAN Settings**" screen will come up.

3. First, you need to know which connection protocol your connection supports (PPPoE, DHCP, Bridge or static).

4. Depending on the protocol you choose, your Internet provider must have given you the necessary information to enter on this page. After you enter the necessary values, click "**Save**".

12

3.2.3 DNS Settings

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 **INTERNET** menu of your device's Web interface. Check the "**Use ISP assigned DNS Servers**" checkbox if you'd like to use the DNS servers assigned by your Service Provider. If you prefer to use DNS servers of your choice, do not check this box, and enter the IP address(es) of the server(s) you would like to use in the "201.11.43.11" format.

3.3 LAN

Any device that you connect to your Air 4450, such as a PC, network printer, IP camera, etc., is a **client**. For settings related to clients that will have a local network connection to your device, you can use the LAN menu and its submenus.

When you click on the LAN menu, the "**LAN Client List**" screen will come up. On this screen, all clients that are connected to your device and their connection details are listed.

3.3.1 IP and DHCP Settings

Every client that is connected to your Air 4450 is given a local IP address. The module that assigns these IP addresses is the DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) module. You can configure the IP and DHCP settings of your device, from the **IP and DHCP Settings** submenu under the **LAN** menu.

Local IP Settings

You can change the IP address and Netmask of your device in this section. The default IP Address of your Air 4450 when it is not connected to any other network device is 192.168.2.254 in Access Point mode and 192.168.2.1 in Router mode. The default Netmask is 255.255.255.0 in either case. You can change these values based on the needs of your existing network.

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 your device can assign local IP addresses to clients and the lease time. The default IP address range is 192.168.2.2 through 192.168.2.254. Maximum lease time for an assigned IP address is set as 3600 seconds, which means the assigned IP address will be renewed every 3600 seconds.

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 your device. To enable this, the address of the device (modem, server, etc.) that runs the DHCP service needs to be known.

Important: If DHCP Relay is enabled, the DHCP server on your device is disabled and can not assign IP addresses to clients.

Disable DHCP

Stops all DHCP activity on the device. When in this mode, clients connected to the Air 4450 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.

Πρέπει να κάνετε κλικ στο "**Save**" για να αποθηκεύσετε οποιεσδήποτε αλλαγές στις ρυθμίσεις IP ή DHCP.

3.3.2 LAN Clients

You can see all the clients connected to your device and their connection details by selecting **LAN Clients** under the **LAN** menu of the 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 gets 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.
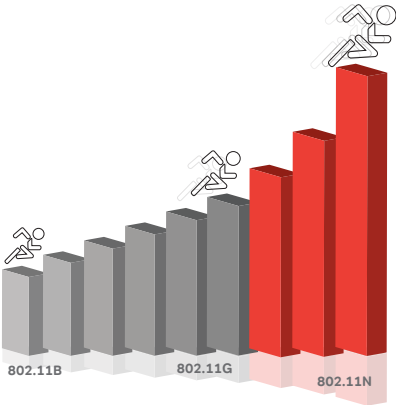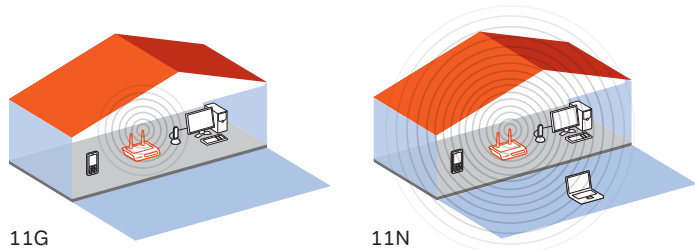

Click "**Save**" for the changes you have made in the "**LAN Clients**" page to take effect.

3.4 Wireless Settings

With the 802.11n standard, you can setup a wireless network with data rates of up to 300Mbps allowing you to share files between PCs at very high speeds. Your Air 4450 is backward compatible with the 802.11b/g standards and can also work with 802.11b/g devices without affecting the performance of 802.11n devices.

By using clients and access points that support 802.11n, you can achieve wireless transfer rates of up to 300 Mbps. Additionally, the MIMO mode supported by the 802.11n standard gives you a much broader wireless range than 802.11b/g devices do.
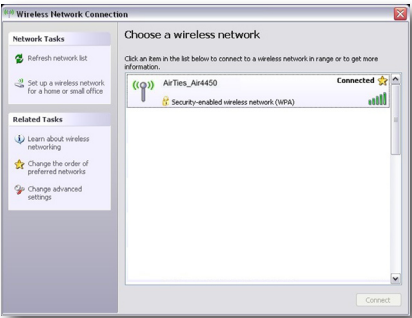

11G   11N

3.4.1 Connecting to the Air 4450 Wirelessly

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

In order to connect your laptop to the Air 4450 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_ Air4450** and click "**Connect**".

3.4.2 Wireless Network Settings

Clicking on the **WIRELESS** menu of the Web user interface takes you to the "**Wireless Connections**" screen which lists all the wireless clients connected to your device. You can block the access of any client to your wireless network by using the "**MAC Filtering**" option.

15

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

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

- "**Frequency**" shows the main frequency band your device uses. Depending on the frequencies supported, it could be 2.4GHz or 5GHZ.
- "**Mode**" shows the IEEE 802.11 mode actively used by your device. The default mode is 802.11b/g/n, supporting 802.11n as well as 802.11b and 802.11g devices.
- "**Channel**" field allows you to choose the channel the Air 4450 will broadcast in. It is recommended that you choose one of channels 1, 6, or 11.
- "**Power**" displays the total transmitted power from your device.
- "**Bandwidth**" field allows you to specify whether to use 20MHz or 40MHz when in 802.11n mode. 40MHz should be selected to achieve 300Mbps wireless data rates.
- "**Rate**" shows the highest wireless data transfer rate supported by your device. It is set to "**Auto**" by default. This allows for automatic adjustment of data transfer rate based on distance and signal quality.

The next set of settings is for configuring your wireless network.

- "**Primary SSID**": Enter a wireless network name (SSID). This is the name your device broadcasts.
- "**Hidden SSID**": Checking this box will hide your SSID during broadcast. This is not recommended since hiding the SSID will prevent laptops from seeing your network within their range.
- "**User Isolation**": Checking this box will prevent wireless clients connected to your network from accessing other client PCs on the network.
- "**Security**": Shows the security protocol currently used by your network.

Click "**Save**" to store your settings.

3.4.3 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 that are used to encrypt the data traffic within a wireless network.

MAC Address Filtering allows you to control which wireless terminals can connect to your AirTies device. Access to the device by unauthorized terminals is blocked. For your wireless network security, it is recommended that both MAC Address filtering and WPA2 wireless encryption protocol be activated.

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 user interface of your device.
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 "**WPA and WPA2** . 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**".

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

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 user interface of your device.
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 have two choices: "**WPA2**" and "**WPA and WPA2**". 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.

WEP Security Settings

Your Air 4450 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 device.
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.
   a. 10 hexadecimal characters(A-F and 0-9) for 64-bit encryption
   b. 5 ASCII characters for 64-bit encryption
   c. 26 hexadecimal characters(A-F and 0-9) for 128-bit encryption
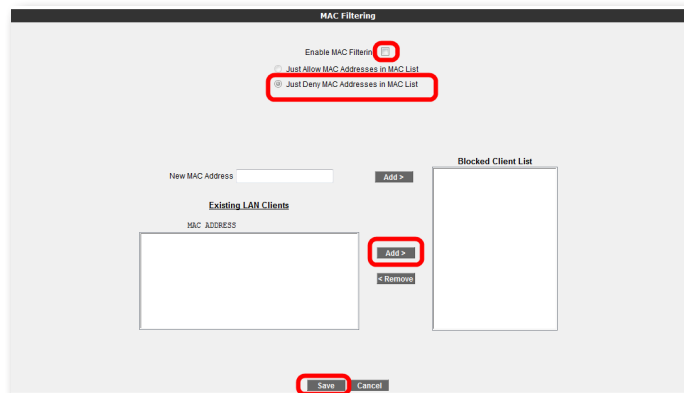   d. 13 ASCII characters for 128-bit encryption

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.

3.4.4 MAC Address Filtering

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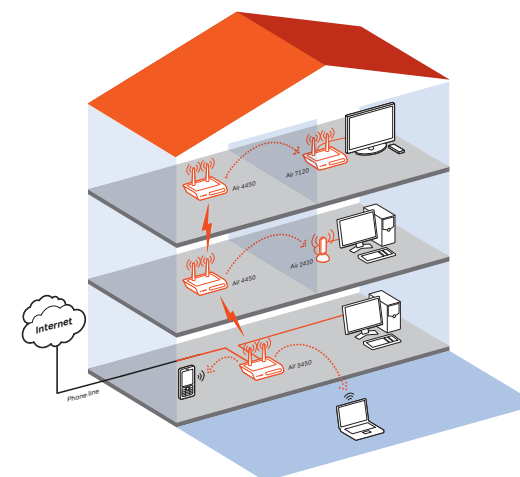

To enable MAC Address filtering and make the necessary settings for blocking clients:

1. Select MAC Filtering under the WIRELESS menu of the Web interface of your device.

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.

3.4.5 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 the 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. In this way, 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. Select a channel for your "**Mesh Networ**k" 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**".

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

3. When you click the **"Search AP"** button, the Air 4450 will start searching for wireless access points to connect to within its range and list the access points detected.

4. Check the box for the access point(s) that you would like your device 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 respective user manuals.

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

3.5 FIREWALL Settings

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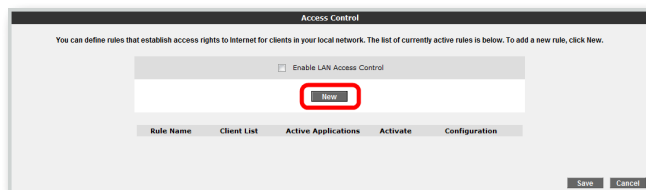
AirTies Firewall has SPI (Stateful Packet Inspection) feature. SPI monitors the protocol and packet addresses being received to determine if the information should be passed through the firewall to the connected computers. Internet addresses that are a source of malicious attacks are permanently blocked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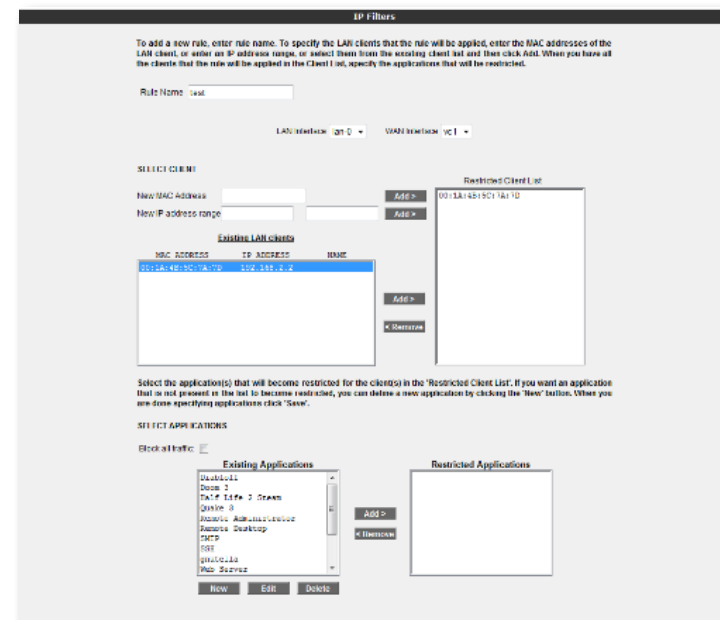
3.5.1 Access Control

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 or MAC address.
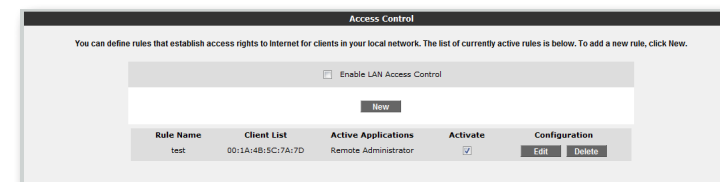
Click "**New"** to define a new access rule.

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 "**Scheduling**" 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.

- To activate the rule you have defined, check the "**Enable Access Control**" box and click "**Save**".
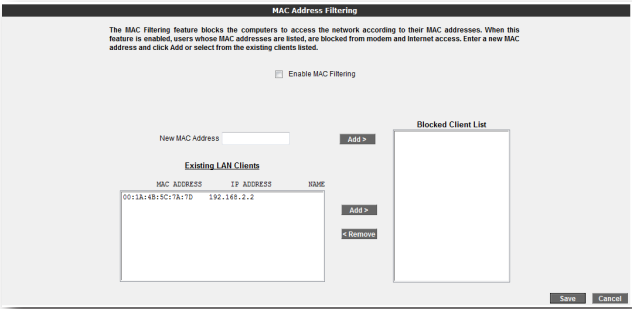
3.5.2 MAC Address Filtering

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 Air 4450 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**".

3.5.3 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.
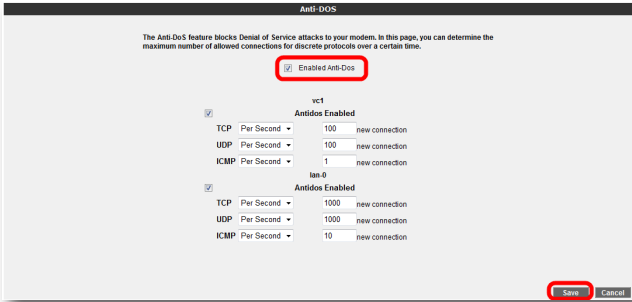
- To activate the URL filtering feature check the "**Enable URL Filter**" box.
- In the "**SELECT CLIENT**" section, specify the IP or MAC addresses of the clients that the URL filtering rule will apply to, clicking the "**Add**" button after each entry.
- Enter the URL's you would like to block access to in the "**Keyword**" list.
- Click "**Save**".

3.5.4 Anti-DoS

The Anti-DOS feature prevents "Denial of Service" attacks that aim to disable your device 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.
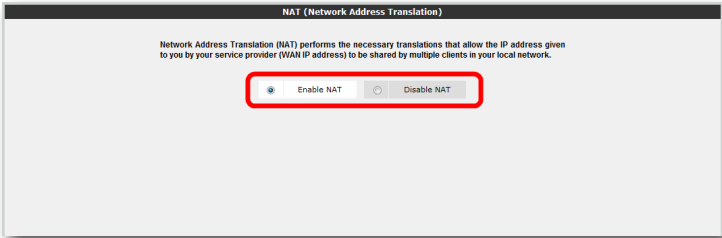
The Anti-DoS feature is disabled by default. To enable Anti-DoS and configure the necessary settings:

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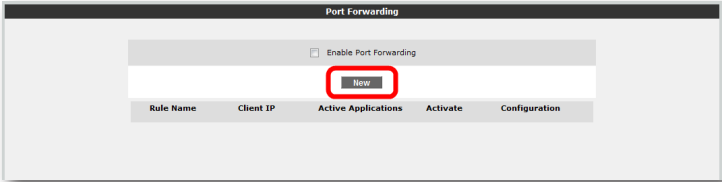- Click "**Save**".

3.6 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 the Web user interface. NAT is enabled by default.
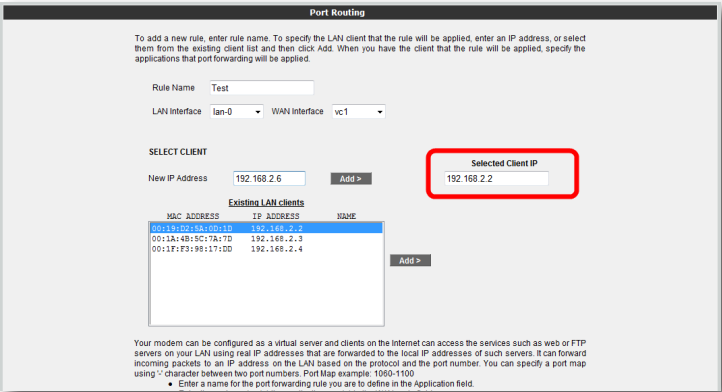

3.6.1 Port Forwarding

"**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 device, go to Port Forwarding under the NAT menu of the Web interface.

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**".

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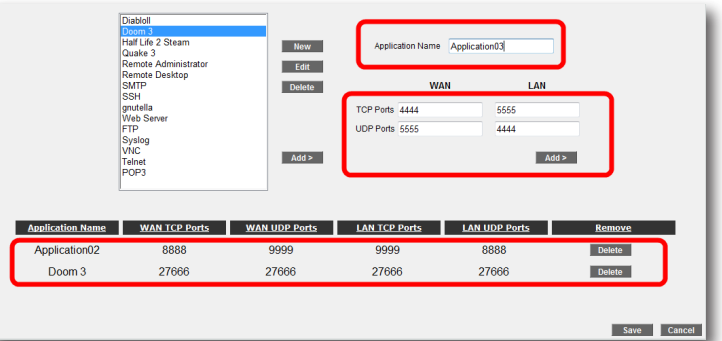
SELECT CLIENT: This section is for specifying the clients that the port forwarding rule will apply to. Enter the IP address of the client in the "**New IP Address**" field or select the IP address from the "**Existing LAN Clients**" list and click "**Add>**". You will see the new IP address in the "**Selected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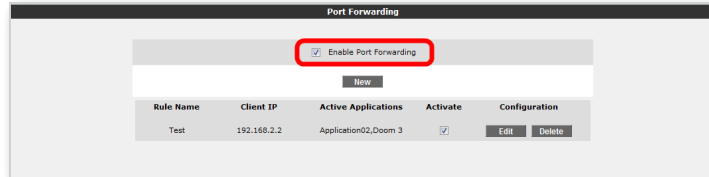

On the lower half of the screen, you can enter the port forwarding rule parameters.

- 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 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.

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**".
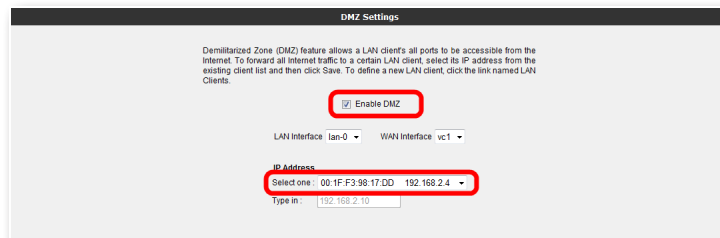

3.6.2 DMZ

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

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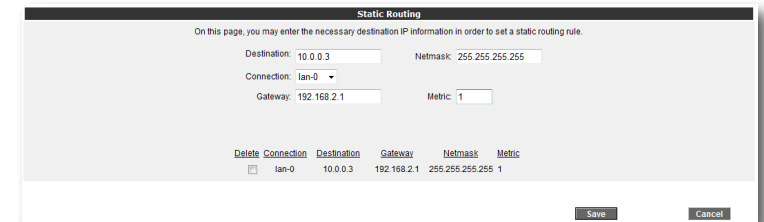

3.7 Routing

Routing defines the rules determining how IP packets reach their destination on the Internet. The Air 4450 supports "static routing" where you specify the target IP addresses and how to get to them. To specify the type of routing to use and set the necessary parameters, use the **ROUTING** menu of the Web interface.

3.7.1 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.

3.8 Management

The **MANAGEMENT** menu of the Web interface lets you configure local and remote management settings of your device.

3.81 Password Settings

Your device 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**" fields. Click "**Save**". From now on, you will have to use this new password to login to the Web interface.

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**".

3.8.2 Remote Management

To configure 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, first click the "**Enable Remote Management**" check box.

If you check the "**Any IP**" box, your device can be managed remotely from any computer that has a WAN IP.

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.

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**".

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

3.9 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.

3.9.1 Password Settings

To configure the DDNS settings of your device, 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**".

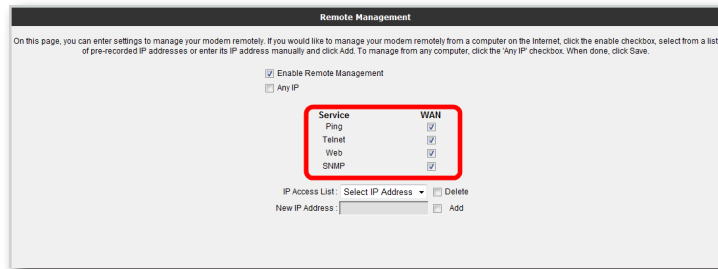To use the Dynamic DNS feature, you need to setup an account with a DDNS service provider. On the screen that comes up, select a DDNS service provider and enter your account information (**Hostname**, **Username**, and **Password**). Click "**Save**" after you have filled in the necessary fields.

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**" checkbox and click "**Save**".

3.10 Tools

On this page, you can restart your device, reset it to factory defaults, backup its current configuration or restore from a previous backup. To get to the "**Tools**" screen, select **TOOLS** from the main menu of the Web interface.
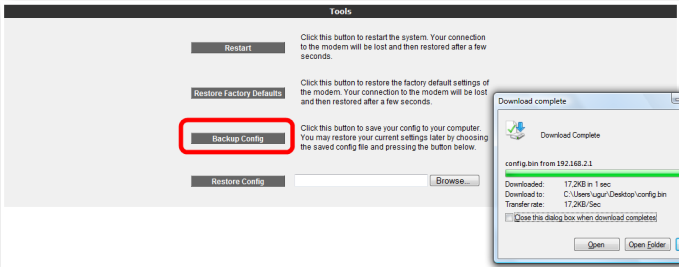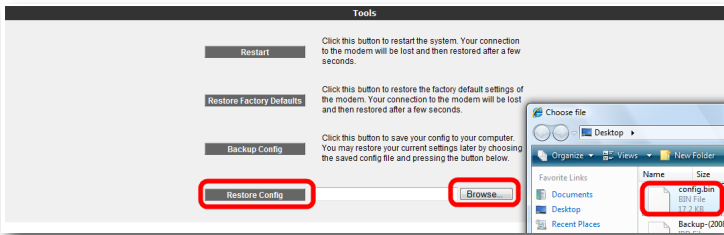
- The "**Restart**" button restarts the device remotely. During this operation, your connection to the Air 4450 will be lost. You can reconnect after the device comes back up.

- The "**Restore Factory Defaults**" button allows you to reset the device back to factory defaults remotely. This will clear all the current settings on your Air 4450.

- "**Backup Config**" lets you save the current settings of your Air 4450 onto your computer. When you click the "**Backup Config**" button, your device will create a file called "config. bin" to be saved on your computer. You can restore this configuration later using the "**Restore Config**" button.
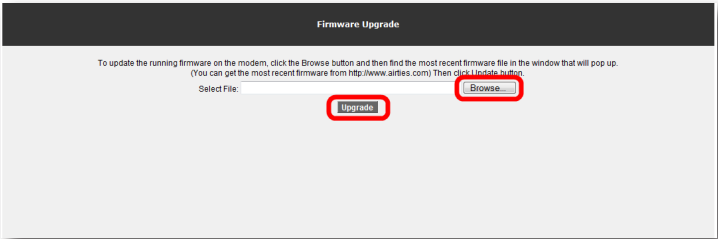

- "**Restore Config**" lets you restore a previously saved configuration onto your device. Click the "**Browse**" button to locate the config.bin file that was previously saved, and then press the "**Restore Confi**g" button to restore your settings from this file onto your Air 4450.

3.10.1 Firmware Upgrade

In order to update the firmware running on the device, go to Firmware Upgrade under the TOOLS menu. Click "**Browse**" and locate the most recent Air 4450 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**".

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. The device must stay ON during the upgrade.

3.10.2 Time Settings

The Air 4450 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 device 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**".

3.11 Reports

The **REPORTS** menu displays information about the main characteristics of your device such as **ADSL Status and Statistic**s, Product Information and **Software Versions**.

3.11.1 System Logs

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

System Logs

Kernel and application logs are printed here.

3.11.2 Log Settings

"**Log Settings**" screen allows you to set detail levels for application logs. You can also specify a remote logging destination.

Log Settings

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

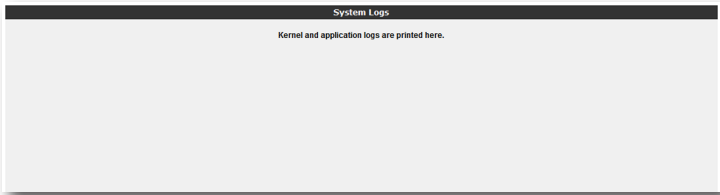| Application Name:	Log Level:
tmrmgr-0	
logger-0	Critical
dsl-0	Critical
pvc-0	Critical
rfc2684-0	Critical
routed-0	Critical
resolver-0	Critical
adslcounter-0	Critical
sntp-0	Critical
dhcpc-0	Critical
Set All	

☑ Syslog Enabled   Syslog Log Level Debug

☑ Kernel Log Enabled   Kernel Log Level Debug

☐ Remote Log Enabled IP Address: Port:

Save   Cancel

4 Technical Properties

- **Ports:** Power (12V DC), 5 x 10/100 Ethernet(RJ-45, auto MDI/MDIX), USB
- **Connection protocols:** PPPoE, RFC1483 Bridging, RFC1483 Routing, classical IP over ATM, PAP/CHAP
- **Other supported protocols**: RFC2684, RFC2364, RFC2516, RFC1577, IEEE802.1d, RFC1631
- **Router and Firewall:** Anti-DoS SPI firewall; IP and MAC address based filtering; Port forwarding; DMZ; Static Routing; DNS Proxy; DHCP server and client; PPP (PAP/CHAP/MSCHAP)
- **Wireless transmit power:** 19 dBm EIRP (max.)
- **Wireless security options:** WPA2-Enterprise, WPA2-Personal, WPA-Enterprise, WPA-Personal, WEP (64/128 bit), MAC address filtering, SSID hiding
- **Wireless Standards:** IEEE 802.1b, 802.1g, 802.11n, 802.11d, 802.11e, 802.11i standards compliant
- **Wireless data rates:** 1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54, 72, 144, 150, 300
- **Frequency range:** ETSI 2400MHz - 2483.5MHz (13 channels with 3 not overlapping)
- **UPnP** (Universal Plug and Play) feature
- **LEDs:** Power, Internet, Wireless Network, USB, WAN, Ethernet, Setup
- **Reset button** to return the device to factory settings
- **Power:** External 12V power adapter
- **Mounting:** Wall or desktop
- **Class 2 device**

5 Physical Characteristics

- **Dimensions:** 180mm x 122mm x 33mm
- **Weight:** 220 g
- **Power:** 12V DC
- **Adapter Operating Voltage: 100V - 240V AC**
- **Operating Temperature:** between 0°C and 40°C
- **Storage Temperature:** between -40°C and 70°C
- **Humidity:** between 10% and 90% non-condensing

AirTies

Easy setup CD

3 Three year warranty

7/24 people support
801 100 0911

CE ①