

125 Mbps Wireless ADSL2+ 1 Port Modem



RT-205

USER MANUAL

This document is prepared by AirTies Wireless Networks Corporation. All rights reserved.

Manual Overview

This manual guides you through the steps necessary for setting up the AirTies RT-205 125Mbps Wireless ADSL2+ Modem. 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.

If any questions or problems arise during installation or use of this product, contact AirTies Wireless Networks Technical Support

TABLE OF CONTENTS

1. INTRODUTION	3
1.1 Main Features	3
1.2 Minimum System Requirements	4
1.3 Package Contents.	4
1.4 Front Panel	5
1.5 Back Panel	5
2. SAFETY AND MAINTENANCE.	6
3. INSTALLATION	6
3.1. Connecting the Cables	6
3.2. Installation Settings	7
3.2.1 Installation Settings Using the Easy Setup CD	7
3.2.2 Installation Settings via the Web Interface	10
4. RT-205 WIRELESS SETTINGS	12
4.1. Wireless Security	12
4.1.1 WPA Security Settings	13
4.1.2 WEP Security Settings	14
4.2. AirTies Mesh Technology	15
4.2.1 Important Guidelines for Mesh Network Setup	15
4.2.2 Mesh Network Settings of RT-205	16
5. FIREWALL.	17
5.1. Access Control	17
5.2. Applications	19
5.3. MAC Address Filtering	20
5.4. Web Filtering	20
5.5. URL Filters	21
5.6. DMZ	21
6. OTHER SETTINGS	22
6.1. NAT (Network Address Translation) and Port Forwarding Settings	22
7. RT-205 SPECIAL APPLICATIONS	23
7.1. ADSL Usage Monitor	23
8. TROUBLESHOOTING	24
9. TECHNICAL AND PHYSICAL SPECIFICATIONS	25
10.0THER INFORMATION	26

1. Introdution

Congratulations on your purchase of AirTies RT-205 125 Mbps Wireless ADSL2+ 1 Port Modem. AirTies RT-205 combines the functions of an ADSL2+ modem (24 Mbps download/4 Mbps upload), advanced wireless router, and firewall. In addition, the RT-205 uses G++ technology enabling you to setup a 125 Mbps wireless local network and have up to 253 devices, such as PCs, terminals, and printers share your Internet connection.

Furthermore, the RT-205 offers SNMP support for remote network management.



1.1 Main Features

 \bullet All-in-one solution: ADSL2+ Modem, 125Mbps Wireless Access Point, 1 Ethernet port, Router and Firewall

• Modem: ADSL2+ modem (24Mbps download/ 4Mbps upload) optimized for your local ADSL service provider

• Router: DHCP server, NAT, NAPT, RIPv1/v2 specified router, VPN pass-through

• Firewall: Advanced anti-DoS SPI Firewall; URL, IP and MAC address based filtering, DMZ

• High speed wireless with G++: 125 Mbps wireless Access Point provides an actual throughput of up to 45 Mbps (with other wireless devices that also support 125Mbps). Also, backward compatible with 802.11b/g.

• Wireless range and Mesh Technology: Ranges of up to 400 meters outdoors and 100 meters indoors standard. Extendible with AirTies Mesh technology, using additional wireless access point devices such as the AirTies AP-300.

• Wireless security: WPA, WPA2-AES, 64/128 bit WEP and 802.1x standards

• Wired device support: Connect a single wired device directly to the 10/100Mbps Ethernet port.

• ADSL Usage Monitor: Especially useful for limited quota ADSL subscribers. Reports monthly total download and upload amounts and current download rate.

Robust against voltage fluctuations: Specially designed to withstand wide voltage fluctuations
 Easy setup and management: Universal Plug and Play (UPnP), Easy Setup CD (with animated

instructions), user-friendly ADSL Utility Program and User Manual

• Easy Update: Firmware (software) upgrades via the Web interface.

Remote Management: SNMP based remote inspection and management

 \bullet 24x7 technical support: by a highly trained AirTies support team and backed up by the AirTies R&D team

Extended warranty: 3 years

1.2 Minimum System Requirements

- ADSL service on your phone line must be active and working properly,
- For wired use: a computer with an Ethernet adaptor that supports the TCP/IP
- For wireless use: 802.11b or 802.11g wireless adapter or computer with wireless capabilities.
- Any version of Windows or Unix, Linux, Mac operating systems
- For the AirTies Utility Program: Windows 98 / ME / 2000/ 2003 or XP operating systems

1.3 Package Contents

Please ensure that the package contains all of the items listed below. Contact your dealer immediately if any of the following items are missing or damaged.

- 1. AirTies RT-205 125Mbps Wireless ADSL2+ 1 Port Modem
- 2. Power adapter and power cord
- 3. Ethernet cable
- Standard telephone/ADSL cable (1 long and 1 short)
 Telephone/ADSL line splitter
- 6. AirTies Easy Setup CD
- 7. User Manual (this document)
- 8. Warranty Card (3 years)



1.4 Front Panel

The LEDs on the front panel show modem status. When the modem is configured and functioning properly, all LED indicators are green. The following table shows the states indicated by the LEDs.

125 AD	MirTies Mbps Wireless SL2+ 1 Port Router	ADSL PPP WLAN LAN			
LED	Light	Status			
PWR	Green RT-205 is powered ON.				
	Off RT-205 is powered OFF.				
ADSL	Green	ADSL connection is established.			
	Flashing Green	AirTies RT-205 is negotiating an ADSL connection.			
Off No ADSL connection.					
PPP	Green	Internet connection is established.			
	Off No Internet connection.				
WLAN	Green	A wireless connection is established			
Flashing Green A wireless connection is established and data transfer is o					
	Off	No wireless connection			
LAN Green Local Area Network (LAN) connection is estab					
	Flashing Green	Local Area Network (LAN) connection is established and data			
		transfer is occurring.			
	OffA	No Local Area Network (LAN) connection.			

1.5 Back Panel

Interfaces for data and power (ports) are located on the back of the AirTies RT-205.



Number	Port	Description
1	ADSL	ADSL line port.
		To be connected to the MODEM port of the splitter.
2	PWR	12 Volt DC port. To be connected to the supplied AC/DC adapter.
3	Reset	To reset the custom configuration of your modem and return to factory
		settings.
4	1/0	Power switch to turn the device ON or OFF.
5	LAN	Ethernet port (10/100). To be connected to the Ethernet Port of the PC.

2. Safety and Maintenance

When operating the AirTies RT-205, please follow these safety guidelines:

• 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. Please note that the adapter

is 220V only. Do not use with 110V AC.

• Do not insert a PSTN (phone) plug into the LAN port.

• If you encounter any problems, do not open or disassamble the device. Instead, 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 further information regarding the installation and configuration of the device consult the remainder of this manual.

• In order to ensure the best care for your device, retain this manual as a guide for future reference.

3. Installation

3.1 Connecting the Cables

This chapter describes how to set up and configure your RT-205.

How to connect the cables is also explained in detail by the animated instructions that automatically start when you insert the Easy Setup CD into the CD drive of your PC.

1. Connect your ADSL telephone plug to the "LINE" port of the splitter 2. Connect the "PHONE" port of the splitter with your regular telephone device.

3. Using the short telephone/ADSL cable provided, connect the "MODEM" port of the splitter with the "ADSL" port of your RT-205 modem.

4. You can connect your PC to the Ethernet port of the AirTies RT-205. Alternatively, you can connect your PC wirelessly to the local wireless network set up by the AirTies RT-205.

5. Plug the power adapter provided into the 220V wall outlet and the other end of the power cord to the RT-205 modem.

Make sure all cabling is done properly before turning the power on. Turn your modem on.



3.2 Installation Settings

Completing the hardware connections in the previous section is necessary before modifying the installation settings. After the hardware setup is complete, turn the RT-205 on and wait about 30 seconds for the modem to initialize.

You can modify the installation settings in one of two ways:

- 1. By using the Easy Setup CD with animated instructions, or,
- 2. By using the Web User Interface

Both methods are described in the following sections.

* It is recommended that you use the AirTies Easy Installation CD for the initial installation.

3.2.1 Installation Settings Using the Easy Setup CD

The AirTies ADSL Utility Software provides you with the easiest way to complete the installation of your modem and activation of its ADSL access.

Once the cabling is completed, insert the Easy Setup CD into the CD drive of your PC. The AirTies ADSL Utility Software Installation program will start automatically. If it does not start automatically, please run the program "installation.exe" on the CD.

1. Click on the RT-205 picture. A sequence of animated instructions will guide you through the cabling of your RT-205 modem. Please verify that you have connected the cables as shown in this presentation.

You can skip this animation at any time and proceed with setup by clicking the Setup link in the upper right hand corner of the window.



2. Once the presentation is finished, click the "SETUP" button. This will launch the Airties ADSL Utility Setup Wizard.



3. Click "Next> " to proceed with setup.



- 4. In the section labeled "Customer Information" enter your
- First and Last name
- Phone number
- E-mail address
- 5. In the section labeled "ADSL User Information" enter your
- ADSL username
- ADSL password

If you do not know or do not remember your ADSL username or password, contact your ADSL service provider to get these values.

Do not change the value in the "Protocol" field (PPPoA) unless you are specifically advised to do so by your ADSL service provider.

6. Click "Save".

The basic installation settings of your RT-205 are now completed. Please wait until the LEDs on the front panel of the RT-205 labeled "ADSL" and "PPP" light up in solid green.

rnet Settings	
Costomer Informa	ation
Name Surname:	Ahmet Reis
Phone Number:	212 2128220
E-mail address:	ahmet@yahoo.com
ADSL User Infor	mation
Protocol:	PPPoE -
Username:	airties@ttnet
Password	

You can check the status of your Internet connection by clicking the "Status" button on the left menu bar of the AirTies ADSL Utility window.

If you cannot connect to Internet even though the LEDs are all green, contact your ADSL service provider.

- AirTie	es		
Status	A Internet	AirTies	My Computer
Settings		11/200	
Counter			
Info		Download: 1024 Kors Upload: 256 Kbrs	
Artian ATISI 1 Hilby			

3.2.2 Installation Settings via the Web Interface

Once the cabling of your RT-205 is completed, you can adjust the initial settings with the advanced web interface using any web browser (e.g.Internet explorerExplorer, Mozilla Firefox, Netscape). You don't need to be connected to the Internet to do this.

1. Open your web browser (e.g. Internet Explorer)

2. In the Address bar enter 192.168.2.1, the default IP address of your modem, and press Enter. This will launch the web interface of your AirTies RT-205 modem.

File	Edit	View	Favorites	Tools	Help		
0	EBRENK +	0	× × (1 🏠	Search	+ Favorites	e

3.You will be prompted for a password to login. Initially, leave this field blank and continue by clicking "Submit".

Atries RT-205 - Windows Internet Explorer		E (P 🔀
- E Http://192.168.2.1/	💌 🛃 🗙 Goope	2.
Ble Edit Yew Favorites Iools Help		
Arbes RT-205	1	Bage • 🎯 Tgok • 🤲
- AirTies	AirTies RT-205 Wireless ADSL2+ 1 Port Modern	
This	Inst Explorer 5.5+ or Firefox 1.0.4+ with minimum 1024/708 resolutions recommended for the best view. Copyright © 2006 2006 ArTiles Wireless Networks: All rights reserved.	
Done	🚷 Internet	₹100% ×

4. Go to "Connection Setup" under the "ADSL" main menu on the left menu bar. You are now in the "PPPoA Connection Setup" screen.

- AirTies	AirTies RT-205 Wirele	AirTies RT-205 Wireless ADSL2+ 1 Port Modem					
HOMEPAGE	We	Icome					
LAN	Thank you for using A4Tiles RF-206. It is recommended for ead the User's Manual widetail before you start using your modern. For any problems: please, contact A#Tiles Technical Support Center at +90-212-4440239.						
FIREWALL	Important Information on RT-21	75 is presented in the table below					
NAT	Internet Connection	Not Connected	1				
ROUTING	ADSL Connection:	Not connected					
MANAGEMENT	ADSL Speed	0/0 kbps					
DDNS	Internet IP Address.	N/A					
TOOLS	ADSL MAC Address	00.12.8F3FB1.0C					
REPORT	Wireless Network	Enabled					
	Wireless Network Name (SSID):	ARTES_RT-205					
	Ethernet	Connected					
	DHCP Server.	Running					
	Firmware Version:	10.23					
	Senat Number.	J644033460					
	System Uptime:	0 Hours 18 Minute					
	System Clock	Updating					

4. Enter your ADSL Username and Password. If you do not know or do not remember your ADSL username or password, contact your ADSL service provider to get these values.

Also, please check with your ADSL service provider to make sure the values for PVC settings (VPI=8 and VCI=35) are compliant with your ADSL service provider's infrastructure.

HOMEPAGE ADSL ADSL Settings ADSL Settings ADSL Setting ADSL Setting ADSL Mode LAN WIRELESS	el up your ADSL connection, choose the p mallori from your service provider. Nam	PPPc relacal to car e: [A Connectio	on Setup Land then ente	r connectio	n Information. You can get this
WIRELESS				Protokol	PPPoA	li i
FIREWALL NAT ROUTING	PP	P Setup	GINAT GIF	rewall PVC Setu	ıp	
DDNS TOOLS	Protocol Username: Password	user_name	/GMUX	VPI: VCI	8 35	
REPORT	MTU: Default Gateway	1500 I	byte	QoS PCR SCR MBS CDVT Auto PVC	0 0 0	cps cps cells usecs

Basic installation settings of your RT-205 are now complete. Please wait until the LEDs on the front panel of the RT-205 labeled "PPP" and "ADSL" light up in solid green. You should now be connected to the Internet. If you are not connected to the Internet even though the lights are green, contact your ADSL service provider.

ூ AirTies	PWR	ADSL	PPP	WLAN	LAN
125 Mbps Kablosuz ADSL2+ 1 Portlu Modem	•			•	•

4. RT-205 Wireless Settings

You can configure the wireless communication and security features of your RT-205 by choosing the "WIRELESS" menu on the left menu bar of the RT-205 web interface. Go to "Wireless Settings" under the "WIRELESS" menu. Check the "Activate Wireless Network" box.

You can assign a name to your wireless network by entering the name in the "Wireless Network Name (SSID)" field. If you check the "Hide Wireless Network Name (SSID)" box, the RT-205 will hide your SSID during broadcast.

You can enter a broadcast channel number (from 1 to 13) in the "Channel" field. The same channel should be selected on all devices in the wireless network.

The 125Mbps G++ feature can be activated by checking "G++" box. Note that a wireless USB adapter supporting 125Mbps is necessary on the receiver side to provide wireless communication at 125Mbps.

	es AirTies	RT-205 Wireless	ADSL2+11	Port Mod	dem, 🚽 🖉 EKIT 🍃 RE
IOMEPAGE		PPPoA Connec	tion Satur		
ADSL.		TTTON CONTINES	don sexup		
ADSL Settings	To set up your ADSL connection, choose the pr	otocol to connect to inter	net and then ente	r connectio	n information. You can get this
DNS Setup	information from your service provider.				
ADSL Mode	Name	27.	Protokol	PPPoA .	
AN					
VIRELESS		🗹 NAT 🗑	Firewall		
IREWALL					
IAT					
OUTING	PPP	Setup	PVC Set	up.	
ANAGEMENT	Protocol	O LLCO VOMUX			
IDMS	Usemane:	user name	VPI	8	
0016	Passwort		VCI	35	
COLS		1500	QoS:	UBR	×
EPORT	Datault Calavard	byte	PCR		cos
	Detaul Galeway, (•	SCR		cos
			LID9	lin.	
			MBS		Cells
			CDVT:	10	usecs
			Auto PVC	D	

4.1 Wireless Security

It is not necessary to configure wireless security to enable wireless communication. However, due to growing importance of data security, it is recommended that you choose a suitable security protocol and configure the RT-205 to use it.

Click on "Security" under the "WIRELESS" menu on the left menu bar of the RT-205 web interface. You will be presented with wireless security choices.

- AirTie	S AirTies RT-205 Wireless ADSL2+ 1 Port Modem						
HOMEPAGE							
ADSL	Wireless Security(Off)						
LAN	Select your wireless security level.						
WIRELESS	Off O WEP O WPA						
Wireless Setup							
Wireless Security	Wreless security is not required for access point or perate and is OT by default if you do not want unauthorized users to common to your access point read-adong on your writeses communications, it is recommended to use and VEP or VFP-writeses security protocols that encrypt you writese communications. RT-200° supports both protocols, IDPA (VIP) Protocols 4 access joint on the secure protocol and is write hard to breast, and access access and access access and access access access and access access access and access acce						
MAC Address Filtering							
MESH							
FIREWALL							
NAT	Townserver and discovery of						
ROUTING	Save Cancel						

Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP) are wireless encryption protocols used to encrypt the data traffic within the wireless network. AirTies RT-205 supports both encryption standards. WPA is the latest and most advanced wireless encryption standard and provides you with the highest level of data protection. All AirTies wireless products and the newly introduced 802.11g wireless communication devices support WPA. WEP is an earlier wireless security protocol. If one of the devices in your wireless network does not support WPA, it is recommended that you choose WEP encryption.

The AirTies RT-205 supports 802.1x Identity inspection as well. For detailed information about how to setup 802.1x security, please consult www.airties.com

MAC Address Filtering allows you to control which network cards can connect to the AirTies RT-205 and share your internet access. It is recommended to activate both MAC address filtering and one of the wireless encryption protocols WAP or WEP.

4.1.1 WPA Security Settings

To enable WPA encryption, check the "WPA" box in the "Wireless Security" screen.

Enter a network key that is 8 to 63 characters long (use a combination of letters and digits) in "password" section by marking "PSK password" and click "Save".You have to enter the same key for all devices within the wireless network.

In order to use WPA2, which is a more advanced version of the WPA encryption, all wireless receiver devices should also support WPA2.

HOMEPAGE	-		200					
IDSL			W	reless Security	y (WEP)			_
AN								
VIRELESS			Select	nur wireless s	ecurity leve	ŕ		
Wireless Setup	0	Off	() ()	WEP	O	WPA		
Nireless Security	- · · · · ·		, e	1.1.771				
in the second	WEP is a less secure s	security protocol	and may b	e broken. If any of	your clients do	not support	WPA, then a	consider using WE
IAC Address Milering								
IESH	Enter a 10 26, or 58 charac	der (64, 128, or)	256 bits) p;	assword that cons	ists of hexade	cima) charao	ders (diaits (othrough 9 a b c
AESH IREWALL	Enter a 10, 26, or 58 charac and select the size. The e	der (64, 128, or i ancryption suppr	256 bits) pr orts suppor	ssword that cons ts two authenticat	ists of hexade on modes, op	cima) charac en and shar	cters (digits (ed. It is reco	0 through 9, a, b, c, mmended to use c
MESH IREWALL	Enter a 10, 26, or 58 charac and select the size. The e mode. You can enter up to 4	der (64, 128, or) ancryption suppo passwords and	256 bits) pr orts suppor d select an	essword that cons ts two authenticat one of them. You connect to your acc	ists of hexade on modes: op have to also e ress point.	cima) charac en and shar nter this pas	cters (digits (ed. It is reco ssword on th	0 through 9, a, b, c, mmended to use c le wireless clients '
MAC ADDRESS FUTEPING MESH IREWALL IAT IOUTING	Enter a 10, 25, or 58 charac and select the size. The e mode. You can enter up to 4	der (64, 128, or) ancryption suppr passwords and	256 bits) pr orts suppor d select an	assword that cons ts two authentical one of them. You connect to your acc	ists of nexader on modes: op have to also e ress point.	cima) charao en and shar nter this par	cters (digits (ed. Il is reco ssword on th	0 through 9, a, b, c, mmerided to use c e wireless clients
MAGA AGGPESS FUERING MESH IREWALL AT OUTTING MANAGEMENT	Enter a 10, 26, or 58 charac and select the size. The e mode. You can enter up to 4	der (64, 128, or) ancryption suppo passwords and	256 bits) pro orts suppor d select an l Auth	assword that cons ts two authentical one of them. You connect to your act entication Mod	ists of hexade on modes op have to also e ress point.	cima) charao en and shar nter this pas	cters (digits (ed. Il is reco ssword on th	0 fhrough 9, a, b, c, mmended to use c ie wireless clients
IAG AGORESS FUTERING IESH REWALL AT DUITING ANAGEMENT DNS	Enter a 10, 26, or 58 charac and select the size. The e mode. You can enter up to 4	der (64, 128, or) ancryption suppr i passwords and	256 bits) pr orts suppor d select an f	assword that cons is two authentical rone of them. You connect to your acc entication Mod	ists of hexade on modes: op have to also e less point. e: Open	cima) charac en and shar nter this pas	cters (digits (ed. It is reco ssword on th	9 through 9, a, b, c, mmended to use c e wireless clients
AL AGDRESS FUREWAY ESH REWALL AT AT DUTING ANAGEMENT DNS DOLS	Enter a 10: 26, or 58 charac and select the size. The e mode You can enter up to 4 Selec	ter (64, 128, or) ancryption support passwords and it	256 bits) pr orts suppor d select an t Auth	assword that cons to two authentical one of them. You connect to your acc entication Mod Password	ists of hexade on modes op have to also e tess point. e Open	cimal charac en and shar Inter this pas	ters (digits (ed. II is reco ssword on th Lengti	0 through 9, a, b, c, mmended to use c ie witeless clients
AL AGUITAS FUREING ESH REVALL AT DUITING ANAGEMENT DOLS POOLS	Enter a 10, 26, or 58 charac and select the size. The e mode. You can enter up to 4 Selec Q	ter (64, 128, or) ancryption suppor passwords and 1 1234567690	256 bits) pro orts suppor d select an I	assword that cons to two authenticat rone of them. You connect to your acc entication Mod Password	ists of hexade on modes op have to also e ress point. e. Open S	cimal charac en and shar Inter this pas	ters (digits) ed. It is reco ssword on th Length	o through 9, a, b, c, mmended to use c e witeless clients
ACLADURES FUEEWING HESH IREWALL AT OUTING ANAGEMENT DNS OOLS EPORT	Enter a 10, 26, or 58 charact and select the size. The e- mode. You can enter up to 4 Selec O	ter (64, 128, or) ancryption support passwords and 1 1234567890	256 bits) pr orts suppor d select an Muthe	assword that cons ts two authenticati one of them. You connect to your acc entication Mod Password	ists of hexade on modes op have to also e ress point e. Open h	cima) charac en and shar Inter this pas	ters (digits (ed. It is reco ssword on th Length 64 bit 64 bit	0 through 9, a, b, c, mmended to use c e witeless clients M
Inc. Address Pillening HESH IREWALL AT OUTING ANAGEMENT DNS OOLS EPORT	Enter a 10, 26, or 58 charac and select the size. The e mode. You can enter up to 4 Selec O O	ter (64, 128, or 1 encryption suppr passwords and 1 1234567890	256 bits) pr orts suppor d select an Auth	essword that cons ts two authenticat one of them. You connect to your act entication Mod Password	ists of hexade on modes, op have to also e less point. e: Open in	cima) charac en and shar nter this pas	Length 64 bit 64 bit 64 bit 64 bit	0 through 9, a, b, c, mmended to use c re wireless clients

4.1.2 WEP Security Settings

To enable WEP encryption, check the "WEP" box in the "Wireless Security" screen.

Three levels of WEP encryption exists. 64-bit encryption uses a key of 10 hexadecimal digits. A hexadecimal digit is A-F and 0-9. 128-bit encryption uses 26 digits, and 256-bit encryption uses 58 digits. A key with more digits is more secure. After selecting the key length, enter the appropriate number of hexadecimal digits, any combination of (0-9, A-F), for the key.

There are two "Confirmation Mode"s that are supported in WEP encryption: "Open" and "Shared". Using "Open" mode is recommended.

Click "Save" after completing your WEP settings.

IOMEPAGE	-		11				
ADSL.		v	Vireless Securit	y (WEP)			
AN							
WIRELESS		Color	t vour wirelees s	ocurity lovel			
Wireless Setup	0 (0# 0	WEP		WPA		
Wireless Security	ý i	0,1	VVL.		111.75		
NAC Address Filtering	WEP is a less secure s	ecurity protocol and ma	be broken. If any of	your clients do	not support VV	PA, then col	nsider using VVE
NAC Address Filtering ME5H	WEP is a less secure s	ecurity protocol and maj	be broken. If any of	your clients do	not support W	PA, then col	nsiderusing Wi
NAC Address Filtering MESH IREWALL	WEP is a less secure s Enter a 10, 26, or 58 charact and select the size. The ei	ecurity protocol and ma er (64, 128, or 256 bits) noryption supports supp	be broken. If any of password that cons orts two authentical	your clients do ists of hexaded ion modes: ope	not support W uma) character in and shared	PA, then co rs (digits 0 ti It is recom	hrough 9, a, b, c mended to use
MAC Address Filtering MESH TREWALL IAT	WEP is a less secure s Enter a 10, 26, or 58 charact and select the size. The ei mode. You can enter up to 4	ecurity protocol and ma er (64, 128, or 256 bits) noryption supports supp passwords and select a	be broken. If any of password that cons orts two authentical iny one of them. You connect to your ac	your clients do ists of hexaded ion modes: ope have to also e cess point	not support W umal character in and shared inter this passy	PA, then co is (digits 0 t it is recom vord on the	nsider using Wi hrough 9, a, b, c mended to use wireless clients
NAC Address Filtering MESH IREWALL IAT IOUTING	WEP is a less secure s Enter a 10, 26, or 58 charact and select the size. The ei mode. You can enter up to 4	ecurity protocol and ma er (64, 128, or 256 bits) noryption supports supp passwords and select a	be broken. If any of password that cons orts two authentical my one of them. You connect to your act	your clients do ists of hexadec ion modes: ope have to also e cess point.	ndt support W umal character in and shared inter this passy	PA, then co is (digits 0 t It is recom vord on the	nsider using Wi hrough 9, a, b, c mended to use wireless clients
NAC Address Filtering MESH IREWALL IAT IOUTING IANAGEMENT	WEP is a less secure s Enter a 10, 26, or 58 charach and select the size. The el mode. You can enter up to 4	ecurity protocol and ma er (64, 129, or 256 bits) noryption supports supp passwords and select a Aut	be broken. If any of password that cons orts two authentical my one of them. You connect to your act hentication. Mord	your clients do lists of hexaded lon modes ope have to also e cess point.	not support W ima) character m and shared nter this passy	PA, then co is (digits 0 t It is recom vord on the	insider using Wi hrough 9, a, b, c mended to use wireless clients
NAC Address Filtering NESH IREWALL IAT OUTING IANAGEMENT IDNS	WEP is a less secure s Enter a 10.26, or 59 charact and select the size. The e mode. You can enter up to 4 i	ecurity protocol and maj er (64, 128, or 256 bits) norphion supports supp passwords and select o Aut	be broken. If any of password that cons orts two authenticat my one of them. You connect to your act hentication Mod	your clients do ists of hexadec ion modes ope have to also e cess point. le: Open s	not support W imal character in and shared inter this passy	PA, then co is (digits 0 t It is recom vord on the	nsider using Wi firough 9, a, b, c mended to use wireless clients
AC Address Filtering IESH IREWALL AT OUTING ANAGEMENT DNS DOLS	WEP is a less secure si Enter a 10.26, or 59 chand and select the size. The a mode. You can enter up to 4 (Select	ecurity protocol and maj er (64, 129, or 256 bits) horpflion supports supp passwords and select a Aut	be broken. If any of password that cons orts two authentical riv one of them. You connect to your aci hentication Mod Password	your clients do ists of hexaded for modes, ope have to also e cess point. le: Open S	not support W ima) character an and shared nter this passy	PA, then co is (digits 0 t It is recom yord on the Length	nsider using Wi fhrough 9, a, b, c mended to use wireless clients
HAC Address Filtering HESH IREWALL AT OUTING IANAGEMENT DNS OOLS EPORT	WEP is a less secure s Enter a 10.26, or 59 charact and select the size. The ex- mode You can enter up to 4 Select Q	ecurity protocol and maj er (64, 128, or 256 bits) nonption supports supp passwords and select of Aut 1234567890	be broken. If any of password that cons orts two authentical my one of them. You connect to your aci hentication Mod Password	your clients do lists of hexaded lion modes: ope have to also e cess point.	ndt support W ima) character an and shared. Inter this passy	PA then con the digits 0 the this recommission the vord on the Length	nteider using WI fnrough 9, a, b, c mended to use wireless clients
NAC Address Filtering NESH IREWALL AT OUTING UNING UNAGEMENT DDNS OOLS EPORT	WEP is a less secure s Enter a 10.26, or 56 charad and select the size. The e mode. You can enter up to 4 Select ©	ecurity protocol and maj er (64, 128, or 256 bits) noryption supports supp passwords and select of Aut 1234567890	be broken. If any of password that cons orts two authenticat in one of them. You connect to your and hentication Mod Password	your clients do ists of hexadect ion modes ope have to also e cess point.	ndt support W ima) character in and shared. Inter this passy	PA, then co is (digits 0 t it is recom- yord on the Length 64 bit	meider using WI mrough 9, a, b, c mended to use wireless clients
NAC Address Filtering NESH AT OUTING OUTING IANAGEMENT DDNS OOLS EPORT	WEP is a less secure s Enter a 10.26, or 56 charact and select the size. The se- mode. You can enter up to 4 Geographic select O O O	ecurity protocol and major er (54, 128, or 255 bits) porption supports supp passwords and select a Aut 1234567890	be broken. If any of password that cons orts two authenticators or the second second second connect to your act connect to your act hentication Mod Password	your clients do ists of hexadec ion modes: ope have to also e cess point. Ie: Open	ndt support W	PA, then co is (digits 0 till is recommy yord on the Length 64 bit 64 bit	meider using Wi through 9, a, b, c imended to use wireless clients

Click on "MAC Address Filtering" under the "WIRELESS" menu on the left menu bar of the RT-205 Web interface.

To activate MAC Address filtering, check the "Activate MAC Filtering" box.

To add the devices that will be permitted to access the RT-205:

• Check the "Permit" box.

• For each device to be allowed access, enter the wireless MAC address of the device (e.g. "00-14-38-15-60-DD") in the "ADD" field and then click the "ADD" button.

- AirTie	S AirTies RT-205 Wireless ADSL2+, 1 Port Modem
HOMEPAGE	
ADSL	MAC Address Hitering
LAN	rou can allow or block wreless clients to reach the access point based on them take, addresses, select allow or block driverso to create a list of clients that will be allowed or blocked access to the access point. Then enter the IAC addresses of the clients and click-Add, When all clients
WIRELESS	are added, click Save. Example: MAC address should be in this format 00-23-45-57-80-33
Wireless Setup	
Wireless Security	Enable MAC filtering 🗹
MAC Address Filtering	Access @Allow OBlock
MESH	
FIREWALL	ACO
NAT	
ROUTING	
MANAGEMENT	Save Cancel
1000 Marca 1000	International In

4.2 AirTies Mesh Technology

The Airties RT-205 has built-in Wireless Distribution System (WDS) Mesh Technology support. WDSMesh Technology simplifies setup of extended or completely wireless networks. AirTies Mesh Networks Technology that makes use of this WDS feature resolves problems such as loss of wireless signal or limited coverage area, often encountered in multiple-story or reinforced concrete buildings.

The Mesh Network consists of an AirTies RT-205 and one or more AirTies AP-300 Wireless Access Point devices. The AP-300s communicate with each other via wireless Mesh protocol and act as "repeaters"... Signals from wireless terminals reach the closest access point automatically, and then reach the RT-205 modem via the access points in between. In this manner, wireless coverage area can be expanded significantly.

The following figure depicts an AirTies Mesh Network consisting of an RT-205 and two AP-300s.

How to set up a Mesh Network with AP-300 devices and an AirTies modem supporting Mesh Network technology is explained in detail in the AirTies AP-300 User's Manual or on AirTies web site http://www.airties.com



4.2.1 Important Guidelines for Mesh Network Setup

 $1.\ \text{RT-205}$ and all repeaters should use the same wireless communication channel (for instance channel 6).

2. On the site survey page, available repeaters' MAC addresses can be seen. For each repeater select the MAC addresses of the other Repeaters that it will be directly communicating with via Mesh.

3. The signal level should not be below "Good" (%50) in the places where repeaters are located. 4. It is recommended that all devices be assigned t the same SSID .

4.2.2 Mesh Network Settings of RT-205

The Airties RT-205 has built-in Wireless Distribution System (WDS) Mesh Technology support. WDSMesh Technology simplifies setup of extended or completely wireless networks. AirTies Mesh Networks Technology that makes use of this WDS feature resolves problems such as loss of wireless signal or limited coverage area, often encountered in multiple-story or reinforced concrete buildings.

The Mesh Network consists of an AirTies RT-205 and one or more AirTies AP-300 Wireless Access Point devices. The AP-300s communicate with each other via wireless Mesh protocol and act as "repeaters". . Signals from wireless terminals reach the closest access point automatically, and then reach the RT-205 modem via the access points in between. In this manner, wireless coverage area can be expanded significantly.

The following figure depicts an AirTies Mesh Network consisting of an RT-205 and two AP-300s.

How to set up a Mesh Network with AP-300 devices and an AirTies modem supporting Mesh Network technology is explained in detail in the AirTies AP-300 User's Manual or on AirTies web site http://www.airties.com

AirTie:	AirTies RT-205 Wireless ADSL2+ 1 Port Modern
HOMEPAGE	
ADSL	MESH Settings
LAN	You can setup your mesh (WDS) connections on this page. Select one or more access points from the Access point list and click the
WIRELESS	checkbox hert to each access point's SSID, they will be added to the access points to connect list you can also enter the MAC address of the access point manually and click Add. When you finish the list of access points to connect, click Save.
Wireless Setup	
Wireless Security	Enable hydrolice and connections
HAC Address Filtering	Enavie unigenepeate connectoris . Co
MESH	
FIREWALL	Save Cancel
NAT	3019 50000
ROUTING	
MANAGEMENT	
DDNS	

You will see a list of all access points detected. Choose the access point(s) you would like to include in the Mesh network by checking the corresponding box(es).

1	1						_
ISL			MESH S	ettings			
LAN	You can setup you	r mesh (WBS) connection	ons on this page. Select	one or mor	e access points fr	om the	Access point li
WIRELESS	the	access point manually a	nd click Add. When you f	inish the lit	it of access points	to conn	ect, click Save
Wireless Setup							
Wireless Security			Enable bridge/repea	ter connect	ions 🗹		
MAC Address Filtering							
MESH			A000-00000			_	
FIREWALL			Access P	oint List			
NAT		SSIR	BSSID (MAC Address)	Channel	Signal Strength	Mode	Security Leve
ROUTING	0	Kat-1	00:12/BF 3D 28 A5	3	-57	bg	WPA
MANAGEMENT		cowav140j	00:C0:02:F8:E5:1C	1	-70	bg	WEP
DONS	Ő	halic_uni	00:12:BF:06:98:5D	8	-89	bg	WEP
REPORT		SPEEDLAN9200	SE 93:40.94 F9:07	9	-92	bg	ÓĦ
	D D	AIRTIES_VolP_Visitor	00:C0:02:F8:E0:48	-13	-51	bg	0#
	D	ozben	00 14:7C:52:DD A4	-13	-85	bg	ĊĦ
		ADSL_AIRTIES	00.12/BF.D0.89:43	-18	-22	bg	WEP
	D	Pos-Destek	00.00.49.F5.03.3F	-11	-85	bg	WEP
		AIRTIES_WAV-140	00:C0:02:F4:E4:39	-18	-42	bg	ÓĦ
	m	AIRTIES	00.12 BF 30.98:6D	-15	-91	bq	WEP

To complete setting up your Mesh network for each access point device you like this RT-205 to connect to you specify this RT-205 as an access point.

The access points you have chosen must use the same wireless channel as your RT-205 modem. To set the wireless channel of the access point device, go to "Settings" under the "Wireless" menu of the web interface of the device.

5. Firewall

A firewall is the primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer.

One of the methods used by the Airties RT-102 firewall to protect your network is SPI, Stateful Packet Inspection. SPI monitors the protocol and packet addresses being received to determine if the information should be passed through the firewall to the connected computers. The 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.

To activate the fi'ddrewall, go to "FIREWALL" under the left menu bar of the RT-205 web interface. Check the "Firewall is Active" box and click "Save".

- AirTies	AirTies RT-205 Wireless ADSL2+ 1 Port Modem
HOMEPAGE	
ADSL	Firewall
LAN	Firewall protects your computers and your network against harmful attacks from the internet. Your modem's
WIRELESS	firewall has Stateful Packet Inspection (SPI) feature that will inspect every packet coming from the Internet to your modem and will not allow any that is not authorized to pass through. Using the Firewall menu, you can
FIREWALL	also define advanced rules to allow or prohibit local users in your network to access the internet, to open
NAT	traffic to a certain computer
ROUTING	
MANAGEMENT	Enable Firewall O Disable Firewall
DDNS	
TOOLS	Save Cancel

5.1 Access Control

You can allow or block a user's access to certain Internet services by setting MAC or IP address filters.

Go to "Access Control" under the "FIREWALL" menu in the left menu bar of the Web interface. Check the "Activate Access Control" box. Click "New" to define a new access restriction. This will put you in the "IP Filters" window.

- AirTies	AirTies RT-205 Wireless ADSL2+ 1 Port Modem
HOMEPAGE	ACCESS CONTROL
ADSL	
LAN	
WIRELESS	You can define rules that establish access rights to Internet for client in your local network. The list of currently active rules is below. To add a new rule, click New.
FIREWALL	Finable LAN Access Control
Accuss Control	Navi
Applications	
MAC Filtering	Rule Name Client List Active Rules Configuration
Web Filters	
URL Filters	Block outgoing pings
DMZ	
Anti-Do5	
NAT	Save Cancel

Enter a name for the access rule you would like to define in the "Rule Name" field. Access control can be defined based on local IP or MAC address (uniquely identifies the network adapter of the device). If an access rule is defined by MAC address, the rule defined for the device will be valid even if the local IP address changes.

It is possible to enter the MAC or IP addresses individually or choose them from the list of client devices in the local network.

Enter the MAC address of the device you'd like to restrict traffic from in "New MAC Address" or IP address of the device in the "New IP Range" field. For a single IP address, enter the same value in the two boxes that define the range. (e.g. 192.168.2.2 and 192.168.2.2). To restrict access for all devices in an IP address range, enter the beginning and ending IP addresses (e.g. 192.168.2.2 and 192.168.2.50).

Clicking the "Add" button next to MAC Address or IP Range, will add the device to the restricted "Clients List.

HUMP YALE ADSL LAN SELECT CLENT WIRELESS FIREWAIL Access Control Applications Applications AAC Filtering Wire Filtering Management Dobs Tools REPORT Report Block all traffic Block vith URI, Filters: Block with URI, Filters: Block with URI, Filters: Block with URI, Filters: Uablof I Bloc	COMPANY AND CONT	
ANSK LAN WIRELESS FIREWALL Access Control Applications MAC Efficiency Web Filters URL, Elsters DME Anti-DoS Name Name Access Control Applications MAC Efficiency URL, Elsters DME Anti-DoS Name ROUTING MARAEMENT DONS TOOLS REPORT Elster Similations Math-DoS Block all traffic 2 Stern Block all traffic 2 Stern Block all traffic 2 Stern DADS DOOLS Block all traffic 2 Stern Block all traffic 2 Stern Block all traffic 2 Stern Block with URL, Fillers:	HUMEPAGE	SELECT CLIENT
LAN New MAC address WIRELESS Add2 REW MAL Add2 Accass Control Add2 Applications Mode 2016;52:17:13 MAC Filtering Add2 Web Filters Biock 2016;22:15:7:28 URL Filtering Add2 Web Filters Biock 2016;22:15:7:28 URL Filtering Add3 Work Filters Biock 2016;22:15:7:28 URL Filtering Add3 Work Filters Biock 2016;22:15:7:28 URL Filtering Add3 ROUTING Restricted applications that will be restricted select from Existing Applications list and click Add. To define a new application click New. When done specifying applications select select select from Existing Applications Biock all traffic Biock Pilles: Biock with URL; Ellers: CuRRL Fillers:	ADSL	
WIRELISS FIREWALL Access Centrel Access Centrel Applications Wirk Filters URL Filters MAX Filters URL Filters URL Filters MAX Report To select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New Wen one specifying applications click Select SELECT APPLICATIONS Block	LAN	New MAC address Add > Restricted Client List
FIRE WALL Access Control Access Control MAC Filtering Web Filters URL Filters URL Filters 00111185:25:57:83 DirZ Androw Anti-Dos Retify applications list and click Add. To define a new application click New. When done specifying applications list and click Add. To define a new application click New. When done specifying applications click Save. MAAGEMENT Dons TOOLS Block all traffic C Block Fings: REPORT Existing Applications Note: Block all traffic C Block Fings: Instrict C Block Add. It all traffic C Block Fings: Existing Applications Block with URL, Filters: (URL Filters should be set)	WIRELESS	New IP address range
Access Control Applications Applications Applications Applications Web Filters OPS Anti-DoS NAT ROUTING MAAGEMENT DOONS TOOLS REPORT ELECT APPLICATIONS Block all traffic Block with URL, Filters: U(RR, Filters basilities 1004 Block with URL, Filters: U(RR, Filters basilities 104 Block with URL, Filter	FIREWALL	Existing LAN clients
Applications 00151 vac besid:171 192,188,273 011gp2 MAC Filtering 00111/d51251571a3 192,188,274 turget Vide Filters 00111/d51251571a3 192,188,274 turget Nat To select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New When done specifying applications click Save NAAT Select applications that will be restricted Save Select Applications Statistics Block All traffic Block Pinges Existing Applications Statistics Save Save Add> Existing Applications Statistics Save Block Pinges Existing Applications Existing Applications Statistics Save Save Existing Applications Existing Applications	Access Control	MAC ADDRESS IF ADDRESS NAME
NAC Filtering 00:11:d8:25:57:a3 192,168.2.4 turgut: Web Filters Add 2 Remove OHZ Anti-toos Select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New When done specifying applications click Select Source SELECT APPLICATIONS Biodx all traffic: Biodx Pings; ERPORT Existing Applications Report Existing Applications Biodx all traffic: Biodx Pings; Now Edit Biodx with URI, Filters; (URIL Filters should be set)	Applications	00:18:de:b8:31:T1 192.168.Z.3 DilgeD
Web Filters Mall OVE Mall Anti-bas Remove NAT To select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New When done specifying applications click Select ANAGEMENT SELECT APPLICATIONS REPORT Block all traffic Block all traffic Block Pings: Number 2004 Add P Report Note: Note: Block Pings: Block with URL, Filters: (URL Filters should be set)	MAC Filtering	00:11:d6:25:57:a3 192.168.2.4 turgut
URL Filters DMZ ANT-DAS ANT-DAS ANT-DAS ANT-DAS NAT ROUTING TO select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New When done specifying applications dick Save SELECT APPLICATIONS Block all traffic Block Pings Auth-IdenED Auth-Iden	Web Filters	Add>
AND DAS ANT ANT ANT ROUTING NAAT ROUTING NAAACEMENT DOONS TOOLS REPORT Block all traffic Block Pings Listing Applications Block all traffic Block Pings Listing Applications Block all traffic Block Pings Listing Applications Butch-Identify Block Pings Listing Applications Butch-Identif	URL Filters	
Andros NAT NAT KOUTING MANAGEMENT DDNS TOOLS REPORT To select applications that will be restricted select from Existing Applications list and click Add. To define a new application click New When done specifying applications click Save SELECT APPLICATIONS Biock all traffic C Biock Pings: Diablo Clip Deak D 2 Diablo Clip Biock all traffic C 2 Biock with URI, Filters: U(URL Filters should be set) Biock with URI, Filters: U(URL Filters should be set)	DHZ	< Remove
NAT ROUTING MANAGEMENT DONS TOOLS REPORT Block all traffic Didations Add> Report	Anti-DoS	
ROUTING Into the set of applications into the origination of the set of the testing applications into the origination of the set o	NAT	To prove controllary for the control area for the second state of
MANAGEMENT DONS TGOLS Block all traffic Block Plugs B	ROUTING	New When done specifying applications click Save
DONS TOOLS REPORT Block all traffic: Block with URI, Filters: URING SELECT APPOCATIONS SELECT APPOCATIONS Sector 2 S	MANAGEMENT	
INDEX Block all traffic Block Pings; Restricted Applications Interview Data is all traffic Block Pings; Restricted Applications Interview Data is all traffic Block Pings; Restricted Applications Interview Data is all traffic Block Pings; Restricted Applications Interview Data is all traffic Interview Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Data is all traffic Restricted Applications Restricted Applications Interview Restricted Applications Restricted Applications Restricted Applications Interview Restricte	DDNS	SELECT APPLICATIONS
Existing Applications Restricted Applications Betticital 2 DiabioII Does Printing Similator 2004 Ref DiabioII Compose Quake 3 Remove Benote Dektop Compose Block with URL, Filters: D (URL Filters should be set)	TOOLS	Block all traffic Block Pinos:
Add> Bartifield 2. Distifield 2. Distifield 3. Distifield 3. Distifield 3. Pick 1. Add> CRamove Remote Administrator Benote Desktop Remote Desktop New Edit	REPORT	Existing Applications Restricted Applications
. Black with URI, Filters; 🗇 (URI, Filters should be set)		Auth-IdentO Betlefield 2 DiabloII Doom 3 Flight Simulator 2004 Half Life 3 Steam Quake 3 Remote Administrator Bemote Deaktop Remote Deaktop Remote Deaktop Remote Deaktop Remote Deaktop Remote Deaktop

In order to remove one of the previously added clients, select it from the "Client List" and click "Remove".

You can select the applications you would like to restrict access to from the "Current Applications" list. If the application you are looking for is not on the list, you can add it by clicking "New" and entering the new application. Clicking "Add" will move the applications selected to the "Blocked Applications" list. Don't forget that access to the applications in the "Blocked Applications" list will be blocked for only those clients in the "Client List".

To remove an application from the "Blocked Applications" list, select the application you would like to unblock and click "Remove".

5.2 Applications

You can add the applications of your choice to the predefined "Current Applications" list. To do this, go to "Applications" under the "FIREWALL" menu on the left menu bar of the Web interface.

In this window, you can add/remove definitions of the special programs, games and P2P software that can be used by the IP filters, or you can change the port numbers of the existing applications.

- AirTies	AirTies RT-205 Wireless ADSL2+ 1 Port-Modern			
HOMEPAGE ADSL LAN WIRELESS FIREWALL Accust Control Applications MAC Filtering Web Filters URL Filters DMZ AnthrDoS NAT ROUTING MANAGEMENT DDNS TOOLS	Applications The applications listed here are used in IP filtering. Here you can define new applications, each port values of existing applications or remove them. Frequently used applications are already added by AVTies. Existing Applications Existing Applications Battlefield 2 Diabioli Doon 3 Flight Simulator 2004 Half Life 2 Steam Quake 3 Remote Administrator. Remote Desktop SMTP SMTP SSH Vazza elonkey and clones; Now Edit Now Edit			
REPORT				

To add a new application to the "Current Applications" list click the "New" button. Enter the name of the application in "Application Name" field, external port number in the "Real Ports" field, and internal port number in the "LAN Ports" field. Click "Save".

AirTies	AirTies RT-20	S Wireless ADSL2+ 1 Port Modem		
HOMEPAGE		Uygulama		
LAN	Enter the port numbers and inten	vals seperated by commas. Example: 1234,4567-5678,3333		
FIREWALL	Application Name: emule			
Access Control	Actual Ports	LAN Ports		
MACFilturing	TCP Ports 4672	TCP Ports 4672		
Web Filters	UDP Parts:	UDP Ports		
URL Filters				
Anti-DoS				
NAT		Save Cancel		
ROUTING				

The rule / application you have defined is now added to the "Current Applications" list.

5.3 MAC Address Filtering

MAC Address Filtering allows you to permit network access based on MAC addresses. When this feature is activated, you can specify the MAC addresses of the computers that will be allowed access to the internet.

To activate the MAC Address filtering feature, go to "MAC Address Filtering" under the "FIREWALL" menu on the left menu bar of the AirTies RT-205 Web interface.

Air Ties	AirTies RT-205 Wireless ADSL2+1 Port Modem
Cardina estendo:	🤫 ERIT 🔮 REFRESH
ADEL	MAC Address Filtering
RUSE	The MAC Filtering feature allows the computers to access the network according to their MAC addresses. When this feature is
LAN	enabled, users except the ones whose MAC addresses are listed, are blocked from internet access. Enter a new MAC address
WIRELESS	C Enable MAC Address Filtering
FIREWALL	Filtered Client List
Access Control	Enter new MAC address
Applications	
MAC Filtering	Annual Annual Printers (Marine
Web Filters	MAC 2008F55 TE 2008F55 HEME
URL Filters	00:0e:35:96:70:05 192.368.2.2 turnut
DHZ	00:18:de:b0:31:71 192.168.2.3 DilgeD
Anti-DoS	00:11:d8:25:57:a3 192.168.2.4 turgut
NAT	< Remove
ROUTING	
MANAGEMENT	
2000	Save Cancel

• Check the "Activate MAC Address Filtering" box.

• Enter the MAC address of the computer you would like to allow Internet access to in the "Add New MAC Address" field (e.g. 00:12:34:56: ab: cd). You can also browse the "Clients List" and select the MAC addresses to be added from there.

• Click "Add". This will add the MAC address to the "Blocked Clients list". The entries in the "Filtered Clients" list will be granted access to the Internet.

In order to find out the MAC address of the Ethernet card or the wireless adapter of a computer, enter "ipconfig /all" in the DOS command line.

5.4 Web Filtering

With the Web Filtering feature, you can block some possibly risky web based application features before they reach the computers in your network. For example: cookies can cause your personal information to be obtained since they contain website entry information.

To define web filters, go to "Web Filters" under the "FIREWALL" menu on the left menu bar of the AirTies RT-205 web interface. For each web application feature you would like to block (proxy, cookie, java applet, activeX, pop-up), check the corresponding "Filter On" box.

AirTies	AirTies RT-205 Wireless ADSL2+ 1 Port Modem
HOMEPAGE ADSL	Web Filters
LAN WIRELESS	Web filters allow dangerous internet applications to be blocked even before they reach the computers on your LAN Select the applications that you would like be blocked and then click Save
FIREWALL Access Control Applications MAC Filtering	Proxy O Filter On O Filter Oft Cookies O Filter On O Filter Oft Java Applets O Filter On O Filter Oft ActiveX O Filter On O Filter Oft Peo-Unit O Filter On O Filter Oft
Web Filters URL Filters DNZ Anti-DoS	Save Cancel

5.5 URL Filters

You can block access of any computer in your local network to certain websites. To define the websites that you do not want users to access:

Go to "URL Filters" under the "FIREWALL" menu on the left menu bar of the web interface.
Specify the URL or any keyword that is part of a URL in the "URL Filters" window. For example, when "mars" is entered as a URL keyword, access to both www.marslilartraveltomars.com and www.marslilardunyadalifeonmars.com will be blocked.

• To block access of a computer in your local network to any of these sites, check "Http with URL Filters" box for the rule that you created for this computer in the "Access Control" page.

Air Ties	AirTies	RT-205 Wirele	ess ADSL2+ 1 Port	Modem				
HOMEPAGE								
ADSL		URL	Filters					
AN	You can specify filters that block	access from LAN cli	ents to certain URLs. To s	pecify a filter, enter a keyword				
WIRELESS	that exists within the URL Exam entered, click Save.	that exists within the URL. Example: enter "abcdefg" to block www.abcdefg.com. When all the keywords are, entered click Save.						
TREWALL								
Accuss Control	Keyword		Keyword					
Applications		Delete		Delete				
AC Filtering		Delete		Delete				
Web Filters		ALC: NOT OF REAL		In the second se				
URL Filters	-	Usiele	-	Loien				
DM2		Delete		Delete				
Anti-DoS	1	Delete		Delete				
AT	1	Incorrectable		Married States				
OUTING	1	Liesote		IJONGIO				
IANAGEMENT	L	Delete	_	Dislete				
DNS		Defete		Delete				
OOLS	-	Delete		Defete				
EPORT		Delete		Delete				

5.6 DMZ

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

Although it's a risky method, you can open and forward all the ports for a certain client at once with DMZ to resolve access problems resulting from firewall or NAT settings.

WARNING: It is not recommended to keep all the ports open for any client for an extended period.

To enable DMZ:

1- Go to "DMZ" under the "FIREWALL" menu on the left Menu bar.

2- Check the "Activate DMZ" box.

3- Enter the local IP address of the client that you would like traffic to be forwarded to in the "Select LAN IP Address" field and click "Save".

This way, all data packets directed to the global IP address of your RT-205, (i.e. your legal IP address on the Internet) will be forwarded to this local client, regardless of the port number.

- AirTies	AirTies RT-2	05 Wireless ADSL2 + 1 Port Mode	m
HOMEPAGE		DMZ Settings	
LAN WIRELESS FIREWALL	Demilitarized Zone (DMZ) feature Internet To forward all Internet tr existing client list and then click Clients.	e allows a LAN client's all ports to be accessit affic to a certain LAN client, select its iP addre Save. To define a new LAN client, click the link i	ve from the ss from the named LAN
Access Control		🗹 Enable DMZ	
MAC Filtering	Select your local IP Adress:	Select	LAN Clients
Web Filters	or	Select 192,168,2.2., turnut - 00.0e 35.96.70 p5	
URL Filters	Write an iP from your local network:	192 168 2 3 - DilgeD - 00 18 de:b8:31:71	
DHZ		192 168 2.4 - turgut - 00 11 d8 25 57 a3	
Anti-DoS			increased in second
NAT			Save Cancel

6. Other Settings

6.1 NAT (Network Address Translation) and Port Forwarding Settings

Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address. NAT allows multiple users in your local network to access the Internet through a single public IP address (the global or legal IP address) assigned to you by your Internet service provider. While your WAV-140 bears the global IP address, local IP addresses (like 192.168.2.4) are assigned to hosts on your local network.

For a host outside your local network to access a machine on your local network, "Port Forwarding" is used. Data packets sent from the Internet to your global IP address arrive at a certain port of your modem. If Port Forwarding is defined for that port, the incoming traffic is redirected to a machine inside the local network that has only a local IP address. Some popular peer-to-peer applications (e.g. E-mule, Kazaa, VPN, Remote desktop) rely on this technology.

To enable Port Forwarding on a port, go to "NAT" menu on the left menu bar and click on "Port Forwarding".

Mir Ties		AirTies I	RT-205	Wireles	s ADSL2+ 1 Pe	ort Modem	w B	(II) 💪
HOMEPAGE				Port Ro	uting			
ADSL			e contrat da la contrat	-		an		
LAN	RT-205 can be co servers on your L	onligured as a virtual se _AN using real IP addre	sses that	are forwar	ded to the local IP a	cess the services such a iddresses of such servers	RT-205	can
WIRELESS	forward incoming	packets to an IP addres	is on the l	LAN based	t on the protocol and	The port number. You can	specify a	port
FIREWALL	 In app 	dication textbox to description	ptport rout	ing rule en	ter name.			
NAT	 Targe As pro 	t IP Address textbox write stocol type select protoco	your loca (that is be	I network II sing used a	P that wants to conne application etc. TCP	ect Internet UDP: TCP&UDP (If you do	not know	
Port Forwarding	protocol	is being used by applica	lion pleas	e select TC	P&UDP)			
ROUTING	You si	hould enter port that is b	er port nu eing used	by applica	tion into target LAN p	ion (usualy it is the sama a	is really p	ort).
MANAGEMENT	 For m this texth 	iore port range you shoul iox	d use 🖓 F	or example	e between 23 and 80	ports range you can use 2	23-80 into	
DDNS	Se	elect from Existing Clier	nts 💌	Select fr	om Existing Applica	tions 💌 Add>		
DDNS TOOLS	Se	elect from Existing Clier	nts 💌	Select fr	om Existing Applica	itions 💌 🛛 Add >		
DDNS TOOLS REPORT	Application	elect from Existing Clier	Protoco	Select fr	om Existing Applica WAN Ports	tions 💌 🛛 Add> Target LAN Ports	Enable	- Delete
DDNS TOOLS REPORT	Se Application	elect from Existing Clier Target IP Address	Protoco TCP	Select fr	om Existing Applica WAN Ports	tions 💌 🛛 Add>: Target LAN Ports	Enable	Delete
DDNS TOOLS REPORT	Application	elect from Existing Clier Target IP Address	Protoco TCP TCP	Select fr	om Existing Applica WAN Ports	tions 💌 🛛 Add> Target LAN Ports	Enable	Delete
DDNS TOOLS REPORT	Application	Target IP Address	Protoco TCP TCP TCP	Select fr	om Existing Applica WAN Ports	Target LAN Ports	Enable	Delete
DDNS TOOLS REPORT	Application	elect from Existing Clier Target IP Address	Protoco TCP TCP TCP TCP	Select fm	om Existing Applica WAN Ports	Add > Target LAN Ports	Enable	Delete
DDNS TOOLS REPORT	Se Application	elect from Existing Clier Target IP Address	Protoco TCP TCP TCP TCP TCP	Select fm	om Existing Applica WAN Ports	Add > Target LAN Ports	Enable	Delete
DDNS TOOLS REPORT	Application	Alect from Existing Clien	rts Protoco TCP TCP TCP TCP TCP	Select fm	om Existing Applica WAN Ports	Add >> Target LAN Ports		
DONS TOOLS REPORT	Application	Alect from Existing Chier	Protoco TCP TCP TCP TCP TCP TCP TCP	Select fm	om Existing Applica WAN Ports	Add>		
DONS TOOLS REPORT	Application	elect from Existing Clier Target IP Address	Protoco TCP TCP TCP TCP TCP TCP TCP TCP	Select fm	om Existing Applica WAN Ports	Add>		Delete
DONS TOOLS REPORT	Se Application	elect from Existing Clier	Protoco TCP TCP TCP TCP TCP TCP TCP TCP TCP	Select fm M Type M M M M M M M M M M M M M M M M M M M	om Existing Applica WAN Ports	Add >> Target LAU Ports Target LAU Ports		
DONS TOOLS REPORT	Se Application	Terget IP Address	TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Select fm M Type M M M M M M M M M M	om Existing Applea	Add >> Target LAN Ports		

In the window titled "Port Routing", you can either find and select the client machine from the list of machines on the local network and the application from the "Current Applications" list, or you can enter a new application, and related forwarding information.

In the window titled "Port Routing":

• In the "Application" field, assign a name for the Port Forwarding rule you are creating.

• Enter the local IP address of the client that is to be accessible from the Internet in the "Target IP Address" field.

• Select the protocol that the application uses from the list of protocols in the "Protocol" box. If you are unsure of the protocol, select "TCP&UDP".

• Enter the real port number used by the application in the "Wan Ports" field.

• Enter the local port number for the application in the "Target LAN Ports" field. (can be the same as the Real Port)

• To forward a range of ports instead of a single port, use a dash (-) sign in between. For example to forward all ports between 23 and 80, enter "23-80".

• Check the "Énable" box.

Click "Save".

7. RT-205 Special Applications

7.1 ADSL Usage Monitor

The ADSL Usage Monitor reports monthly broadband usage (download and upload) and displays your current download rate. Click "Counter" on the left menu bar of the AirTies ADSL Utility Program to view the monthly usage summary for a 12-month period as well as the current download rate.

The ADSL Usage Monitor can be displayed on any of the PCs in your local network regardless of whether the PC is connected directly (via the Ethernet port) or remotely (by a switch, hub or access point) to the AirTies RT-205. The download and upload totals are for all Internet traffic that goes through the RT-205.



8. Troubleshooting

There is no Internet connection, and the ADSL LED flashes continuously (or is not on at all) Call your ADSL service provider and make sure your ADSL line is active. Note that the ADSL LED flashes for about a minute as the ADSL connection is being negotiated. Make sure the splitter connections are made correctly.

ADSL connection is established and the ADSL LED is on, but the Internet LED is off. Check that the settings specific to your ADSL service provider (e.g. PPPoA and PPPoE) are correct. Contact your service provider to verify your user name and password.

I forgot the password I set to access the web interface. Cannot access the device.

You will have to reset the AirTies RT-205 to its original factory settings. To do this, push and hold the "Reset" button on the back panel for several seconds with the tip of a pencil, or a similar object.

I keep losing my wireless connection

There may be a few reasons:

1. The most probable one: if there are any other devices (Dect /wireless phone, etc.) broadcasting in the same frequency as RT-205 (2.4 GHz), these devices may cause interference. Changing the channel in "Channel and SSID" section under the "Wireless" menu in the RT-205 web interface would solve this problem. In the factory settings, channel is set to "Auto". Try channels 1, 11 and 13. If the problem is channel interference, one of these channels will solve your problem. 2. If Windows manages you wireless network, the problem may be Windows based. 3. Make sure you have the latest driver updates for your wireless card.

During the setup with the CD I get the error message "cannot access the modem".

1. Check the connection between the PC and the modem.

2. The firewall on your PC may be preventing access to the modem. Turn off the firewall and try again.

You can contact AirTies Technical Support at any time (24x7) with any problems or questions related to your AirTies product.

9. Technical and Physical Specifications

• 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), support for 8 PVCs and 6 PPP sessions

• Connection protocols: PPPoE, PPPoA, RFC1483 Bridging, RFC1483 Routing, Classical IP over ATM, PAP/CHAP, RFC 2364 PPP over AAL5, RFC2366 Multicast over ATM, IP multicast IGMP v1&v2, snooping

 \bullet 802.11b/g and G++ wireless networks: 1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54 Mbps speed (automatic speed adjustment) and 125 Mbps G++ mode

- Frequency interval: ETSI 2400 MHz(min)- 2483.5 MHz(max) (13 channels with 3 not overlapping)
- "Reset" button to return the modem to default settings
- Operating Voltage Range: 170V AC to 260V AC
- Cabling: RJ-45 (Ethernet), RJ-11 (ADSL)
- LEDs: PWR Power, ADSL ADSL activity, PPP Internet connection, WLAN Wireless network activity, LAN Local network activity
- Antenna power: 19dBm EIRP

• Wireless security specifications: WPA (802.1x, TKIP, PSK) ; WPA2 (AES); 64/128 bit WEP, wireless MAC address filtering, SSID hiding

UPnP : Universal Plug&Play

• Router and Firewall: SPI firewall; IP and MAC address filtering; URL filtering; Port forwarding; DMZ; VPN pass-through (PPTP, L2TP, IPSec); Static Routing, RIPv1, RIPv2 forwarding; DNS Proxy; DHCP server and client; NAT/NAPT; PPP (PAP/CHAP/MSCHAP); up to 1024 NAT sessions

- Compatible with Windows 98, ME, 2000, 2003, XP, UNIX, Linux, MAC OS
- Certificates: CE
- Dimensions: 155mm x 125mm x 25mm
- Weight: 450 grams
- Power: 12Volt DC
- Operating Temperature: 0°'a1C 45°'a1C
- Storage Temperature: -40°'a1C 70°'a1C
- Humidity: %10 %90

10. Other Information

Designed by AirTies Wireless Networks Büyükdere Caddesi fiarl· df Merkezi No:103 Kat:5 Mecidiyeköy/Istanbul Turkey Tel :+90 212 444 0239 Fax :+90 212 318 6298

Maintenance & Repair Services Provided By AirTies Wireless Networks Büyükdere Caddesi fiarl> df Merkezi No:103 Kat:5 Mecidiyeköy/Istanbul Turkey Tel :+90 212 444 0239 Fax :+90 212 318 6298







7/24 AirTies Tech Support +90 212 444 0 239

www.airties.com