neµbeore



Fixed Wireless Terminal

July 2010

MRV7517PW22-B1 FW R01

Copyright Notice

Copyright of all the contents and materials published in the manual is owned by Arcadyan. None of the materials provided on this manual may be duplicated, reproduced or transmitted, either partially or completely, in any form or by any means. 2010 Copyright Arcadyan Technology Corporation

Disclaimers

Arcadyan makes no warranty as to the materials and information in this manual, including representations of the materials or information. The materials or information are provided "as is". There are no implied warranties or conditions of merchantability, fitness for particular purpose or noninfringement. Arcadyan assumes no responsibility for the accuracy and completeness of the information. Arcadyan may change the materials or products mentioned therein at any time without notice. Arcadyan shall not be liable for any special, indirect or consequential damages, including, without limitation, damages resulting from use of or reliance on the information presented, loss of profits or revenues or costs.

Submission of Information

Except as otherwise agreed by Arcadyan in writing, any material, information or other communication you transmit or post to this manual will be deemed non-confidential and non-proprietary ("Non-confidential Information"). Arcadyan shall have no obligations with respect to the Non-confidential Information. Arcadyan will be free to copy, disclose, distribute, incorporate and otherwise use the Non-confidential Information and all data, images, sounds, text, and other things embodied therein for any and all commercial or non-commercial purposes.

Manufactured by Arcadyan Technology Corporation

4F No. 9 Park Avenue II, Hsinchu Science Park Hsinchu, Taiwan

Trademarks:

The Arcadyan brand name, logos, trademarks and service marks ("Trademark") used and displayed in this manual are registered and unregistered trademark of Arcadyan. Arcadyan is not granting you a license to use them in any way or function.

Other product and company names are trademarks or registered trademarks of their respective holders.

Table of Contents

CHAPTER 1	Introduction	1
	About the Broadband Router	1
	Features and Benefits	
	Applications	3
CHAPTER 2	Installation	5
	Hardware Installation	5
	Package Contents	5
	System Requirements	6
	Hardware Description	7
	ISP Settings	11
	Connect the System	11
	Software Installation	13
	Configuring Client PC	13
	Window XP	14
	Window Vista	14
	Macintosh Computer	17
CHAPTER 3	Web Management	
	Navigating the Web Browser Interface	19
	Making Configuration Changes	
	Start	20
	Status	
	WLAN	

	LAN
D	ata
	Firewall
	DNS & DDNS
	NAT
	Wireless
E	xtras
	HSPA Modem
	Password Settings
	Time Settings
	Remote Management
	Firmware Upgrade
	Diagnostic Utility
	Reboot
	UPnP
Product Specifications	s75
Compliance	
	Federal Communication Commission Interference Statement 79

CHAPTER 1 Introduction

Thank you for your purchase of the Fixed Wireless Terminal. We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this Broadband Router provides a convenient and powerful solution. The Broadband Router also enables service providers to provide their residential and small office home office (SOHO) customers with 3G mobile phone service as well as the high-quality VoIP service using traditional analog telephones and fax machines.

About the Broadband Router

The Broadband Router provides Internet access to multiple users by sharing a single-user account. It provides many secure and cost-effective functions. It is simple to configure and can be up and running in minutes. Support is provided for both wired and wireless devices. The Broadband Router is compatible with 3GPP UMTS/HSPA+ and compliant with IEEE 802.11n specification while maintaining full backwards compatibility with the IEEE 802.11b/g standards. This wireless networking standard utilizes advanced MIMO (multiple-in, multiple-out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps - five times faster than 802.11g, the Broadband Router provides sufficient bandwidth to listen to digital music, play online games, transfer large files and surf the Internet simultaneously. This device also provides wireless security via Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2 encryption, and MAC address filtering.

Features and Benefits

- HSPA+ (High-Speed Packet Access) embedded for using mobile RAN (Radio Access Network)
- WCDMA/HSPA as primary radio access and GSM/GPRS/EDGE as fall-back
- Supports CSoHS (Circuit-Switched voice service over HSPA) air interface of improving data and voice service system capacity.
- IEEE802.11n compliant
- Wireless speeds up to 300 Mbps
- Increased speed and coverage up to 15 times the speed of IEEE 802.11g
- Fully backwards compatible with 802.11b/g wireless networks
- Allows you to stream HD video, listen to digital music, play online games, transfer large files, make VoIP calls and surf the Internet simultaneously
- Wi-Fi Multimedia (WMM) for wireless quality-of-service
- Local network connection via a 10/100 Mbps Ethernet port
- DHCP for dynamic IP configuration, and DNS for domain name mapping
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as web, FTP, email, and Telnet)

- VPN transparent pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP)
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

Applications

Many advanced networking features are provided by this Broadband Router:

• Wired and Wireless LAN

The Broadband Router provides connectivity to 10/100 Mbps devices, and wireless connection speed up to 300 Mbps. This router is fully compliant with specifications defined in IEEE 802.11b, IEEE 802.11g and IEEE 802.11n draft v2.0 standards, making it easy to create a network in small offices or homes.

• Internet Access

This device UMTS (Universal Mobile Telecommunication System) interface for your Internet connection.

• Shared IP Address

The Broadband Router provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web at the same time.

• Virtual Server

If you have a fixed IP address, you can set the Broadband Router to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Broadband Router can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

• DMZ Host Support

Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

• Security

The Broadband Router supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The Broadband Router's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. WPA/WPA2, IEEE802.1x, WEP, SSID, and MAC filtering provide security over the wireless network.

CHAPTER 2 Installation

Before installing the Broadband Router, verify that you have all the items listed under "Package Contents." If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Broadband Router. After installing the Broadband Router, refer to "Web Management" on page 18 for detailed configuration.

After unpacking the Broadband Router, check the contents of the box to be sure you have received the following components:

1.Fixed Wireless Terminal

- 2. Power adapter
- 3. One CAT-5 Ethernet cable (RJ-45)
- 4. One documentation CD

Immediately inform your dealer in the event of any incorrect, missing, or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

System Requirements

To install and connect to the Broadband Router, you must have:

- 3G SIM card for UMTS (Universal Mobile Telecommunication System) connection.
- A computer with a CD-ROM drive.
- Windows 2000 or later, or Mac OS 9.x or later.
- An up to date web browser: Internet Explorer 5.5 or later, or
- Mozilla 1.7/Firefox 1.0 or later.

Hardware Description

The Broadband Router connects to an Ethernet connection using it's RJ-45 LAN port. It can be connected directly to your PC or to a local area network using the Fast Ethernet LAN ports.

The Broadband Router contains an integrated modem and connects to the Internet or to a remote site using its RJ-11 port.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet port and up to 300 Mbps over the built-in wireless access point.

The HSPA+ implementation of this Broadband Router offers 5.36 Mbps in the uplink and 7.2 Mbps in the downlink.

The Broadband Router includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting.

LED Indicators

The status LED indicators on the front panel are illustrated in the following figure and table.



FIGURE 1. Front View

The LED indicators on the top panel are illustrated by the following
table.

LED	Status	Description	
Signal Quality	On	Shows the strength of the connection of 3G mobile network.	
» <mark>.</mark>	Flashing	Browsing mobile network.	
Voice Mail	Flashing	Got voice mail message.	
\boxtimes	Off	No message.	
WAN	Flashing	The Broadband Router is establishing an mobile network link.	
	Off	No mobile network link.	
WLAN	On	Wireless LAN (WLAN) link.	
(¶)	Flashing	The Broadband Router is sending or receiving data via WLAN.	
	Off	No WLAN link.	
Internet	On	Internet connection is functioning correctly.	
B	Flashing	The Broadband Router is establishing an Internet link.	
	Off	No Internet link.	
Phone Line	On	Telephone line is off-hook, i.e., call in progress.	
0	Off	Telephone line is on-hook. No call in progress.	

The LAN port LED indicators on the rear panel are illustrated by the following table.

LED	Status	Description
LAN 1~4	On	Ethernet link.
	Flashing	The LAN port is sending or receiving data.
	Off	No Ethernet link.

Network Connectivity

The Broadband Router contains the following ports on the rear panel:





Warning: Using the wrong type of power adapter may cause damage.

The Broadband Router contains the following ports and buttons:

Item	Description
Phone Port	RJ-11 voice interface.

LAN Ports	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, switch or IP set top box).
Reset Button	Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see "Reboot" on page 72.
Power Inlet	Connect the included power adapter to this inlet.
On/Off Button	Press this button to power on/off the device.

SIM Card Slot

The embedde SIM card socket is located on the side panel as shown below. It supports push-in/push-out mechanism. It is easy to insert and to take out your SIM card by pressing the card into the slot.



FIGURE 3. Side View



Warning: Be sure to insert the SIM card into the card socket **before** power on the Broadband Router.

ISP Settings

Please collect the following information from your ISP before setting up the Broadband Router:

- ISP account user name and password
- PIN code and UMTS account information
- Protocol, encapsulation and VPI/VCI circuit numbers
- DNS server address
- IP address, subnet mask and default gateway (for fixed IP users only)

Connect the System

The Broadband Router can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Broadband Router away from any heating devices.
- Do not place the Broadband Router in a dusty or wet environment.
- You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Broadband Router.



FIGURE 4. Application Diagram

Connect the Phone Line

Connect the phone line (RJ-11) cable from the port labelled Phone on the Broadband Router to your telephone. When inserting the plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Attach to Your Network Using Ethernet Cabling

The four LAN ports on the Broadband Router auto-negotiate the connection speed to 10 Mbps or 100 Mbps, as well as the transmission mode to half duplex or full duplex.



Warning: Do not plug a phone jack connector into an RJ-45 port. This may damage the Router.

Use RJ-45 cables to connect any of the four LAN ports on the Broadband Router to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Router to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Category 5 cable is recommended. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).

Connect the Power Adapter

Plug the power adapter into the power socket on the rear of the Broadband Router, and the other end into a power outlet.

In case of a power input failure, the Broadband Router will

Warning: keep your hands dry when vou install the Broadband Router.

automatically restart and begin to operate once the input power is restored.

Software Installation

Configuring Client PC

After completing the hardware setup by connecting all your network devices, you need to configure your computer to connect to the Router.

Depending on your operating system, see:

"Window XP" on page 14,

"Window Vista" on page 14

"Macintosh Computer" on page 17

To access the Internet through the Router, you must configure the network settings of the computers in your LAN to use the same IP subnet as the Router. The default IP settings for the Router are:

IP address: 192.168.2.1

Subnet mask: 255.255.255.0

Window XP

- 1. On the Windows desktop, click Start/Control Panel.
- 2. In the Control Panel window, click Network and Internet Connections.
- **3.** The Network Connections window will open. Double-click the connection for this device.
- 4. On the connection status screen, click Properties.
- 5. Double-click Internet Protocol (TCP/IP).
- 6. If Obtain an IP address automatically and Obtain DNS server address automatically are already selected, your computer is already configured for DHCP. If not, select this option.

🖉 😵 Connect to a network	
This computer is connected to arcadyan.com.tw	
	49
Windows cannot find any additional networks.	
View network computers and devices	
Diagnose why Windows cannot find any additional networks Set up a connection or network	
Open Network and Sharing Center	

Advanced...

Obtain an IP address auto Use the following IP address

Obtain DNS server address automatics
 Use the following DNS server addresse

Window Vista

- 1. On the Windows desktop, click Start/Connet To.
- 2. The Connect to a network window will open. Click **Open Network and Sharing Center**.
- 3. Click Manage network connections on the left menu bar of the screen.



- **4.** The LAN or High-Speed Internet window will open. Double-click the connection for this device.
- 5. On the connection status screen, click Properties.
- 6. Double-click Internet Protocol (TCP/IP).
- 7. If Obtain an IPv6 address automatically and Obtain DNS server address automatically are already selected, your computer is already configured for DHCP. If not, select the options.

Obtain IP Settings From Your Wireless Broadband Router

Now that you have configured your computer to connect to your Router, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Router, you can verify that you have configured your computer correctly.

- 1. On the Windows desktop, click **Start/Programs/Accessories/ Command Prompt**.
- 2. In the Command Prompt window, type **ipconfig** /**release** and press the Enter key.
- **3.** Type **ipconfig** /**renew** and press the Enter key. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Wireless Broadband Router is functioning correctly.
- **4.** Type **exit** and press the Enter key to close the Command Prompt window.

Your computer is now configured to connect to the Router.

Manual TCP/IP Settings

- 1. Follow steps 1-5 in "Window XP" on page 14.
- 2. Select Use the following IP Address.
- Enter an IP address based on the default network 192.168.2.x (where x is between 2 and 254), and use 255.255.255.0 for the subnet mask. Use 192.168.2.1 for the Default gateway field.

hanced

- 4. Select Use the following DNS server addresses.
- 5. Enter the IP address for the Wireless Broadband Router in the Preferred DNS server field. This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add a specific DNS server into the Alternate DNS Server field and click OK to close the dialog boxes.

Record the configured information in the following table.

TCP/IP Configuration Setting

IP Address____.___.

Subnet Mask____.___.

Preferred DNS Server___.

Alternate DNS Server____.___.

Default Gateway____.___.

Macintosh Computer

You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

- 1. Pull down the Apple Menu . Click System Preferences.
- 2. Double-click the Network icon in the Systems Preferences window.
- **3.** If Using DHCP Server is already selected in the Configure field, your computer is already configured for DHCP. If not, select this option.
- 4. Your new settings are shown in the TCP/IP tab. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Wireless Broadband Router is functioning.
- 5. Close the Network window.

Now your computer is configured to connect to the Wireless Broadband Router.

Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Router's HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

- 1. Open Internet Explorer and click the Stop button. Click **Explorer**/ **Preferences**.
- 2. In the Internet Explorer Preferences window, under Network, select **Proxies**.
- 3. Uncheck all check boxes and click OK.

0	Netwo	rk	
	Location: Automatio	:	
Show: Built-in Ethen	net 📑		
	TCP/IP PPPoE Ap	pleTalk Proxies	
Configure:	Using DHCP	•	
		DNS Servers	(Optional
IP Address:	(Beneficial In: DMCB Course)		
Subnet Mask:	(nowned by brick server)		
Router:		Search Domains	(Optional
DHCP Client ID:			
	(Optional)		
Ethernet Address:	00:50:e4:00:2c:06	Example: apple.com earthlink.net	
Click the lock to r	revent further changes	Report	Canaly
	enanges.	Neven	white

снартег з Web Management

After you have configured TCP/IP on a client computer, you can configure the Broadband Router using your web browser.

To access the Broadband Router's management interface, enter the default IP address in your web browser: <u>http://192.168.2.1</u>. Enter the user name and password, then click **Login**.



Navigating the Web Browser Interface

The Broadband Router's management interface contains four main sections:

- Start (on page 20)
- Data (on page 35)
- Extras (on page 61)
- Logout click this to log out of the management interface.

🙆 http://192.168.2.1/index.stm - V	Vindows Internet Explorer			- 2 -
🕒 🗢 🖉 http://192.168.2.	1/index.stm		🗕 😽 🗙 🚼 Google	+ م
File Edit View Favorites T	ools Help			
× Google 192.168.2.1	👻 🚼 Search 🔹	🖓 🔹 📲 🔹 👰 🔹 🔲 Sidewiki 🔹 🗳 Ch	eck + 🍗 AutoFill + 🌛 强 192.168.2.1	🔌 🔹 🧼 Sign In 🔹
🙀 Favorites 🛛 😸 🔹 🏀 http://	/192.168.2.1/inde 🗴 🌈 Internet Exp	lorer cannot di		
START	DATA EXT	RAS		LOGOUT
WLAN	Status			Â
LAN	You can use the Status screen to to access your network, as well as Current Time: 23.07.2010 (Eri)	see the connection status for the router's W. information on all DHCP client PCs current	AN/LAN interfaces, firmware and hardware version number: y connected to your network.	s, any illegal attempts
	UNTERNET UMTS: CONNECTED Operator: Chunghwa Telecom Operator: Chunghwa Telecom Uploat: 63K (Mps. WAN IP: 116:510:231 Subnet Mask: 255:255:255 Generaty: 116:310:231 Secondary DNS: 168:95:192:1 → Reconnect	GATEWAY IP Address: 192 169 2.1 Subret Mark: 255 255 0 Di/CP Server: Enabled UPAP: Enabled Wireless: Enabled	INFORMATION Numbers of DMCP clears: 0 Runtime of DMCP clears: 0 Boot Code Version: v1 05 00 LAN MAC Address: 88-52-04-FC-69 Wireless MAC Address: 88-52-04-FC-69 Wireless MAC Address: 08-52-04-FC-69 Wireless MAC Address: 08-52-04-FC-69 Ward MAC Address: 08-52-04-FC-69 Wireless MAC Address: 08-52-04-FC-69 Wireless MAC Address: 0-04 Steint Num. Jd25030011 UMTS-Stick UMTS-Stick: DataCand Device Firmware Version: 100611_GKRCCL M0 13 1 11 20101 Ld2:4202[Reless=-1un 1:2010 06:00 MEI: 353918030002162 MMS1: 465023301704607	0 17:08:01) E compilation=Jun 00]
	DHCP Client Log View information on LAN DHCP cl	ents recorded on the router.		
Firmware Version:20.03.30212			*	

Making Configuration Changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a screen, click the **Apply** or **Save Settings** or **Next** button at the bottom of the screen to enable the new setting.

To ensure proper screen refresh after a command entry, be sure that Internet Explorer is configured as follows: Under the menu Tools/ Internet Options/General/Temporary Internet Files/Settings, the setting for Check for newer versions of stored pages should be Every visit to the page.

Start

On the left-hand side of the screen, the first menu item is Start. Click on the **Start** menu, and the **Status** screen appears.

Status

The Status screen displays WAN/LAN connection status, firmware and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients. The security log may be saved to a file by clicking **Save** and choosing a location.



6 http://192.168.2.1/index.stm - 1	Windows Internet Explorer		- 5 💌
🔾 🗢 🖉 http://192.168.2	1.1/index.stm	👻 🐓 🗙 🚰 Google	+ م
File Edit View Favorites	Fools Help		
× Google 192.168.2.1	💽 🛂 Search + 🖓 🧔 + 🚽 🖓 + 🔲 Sidewiki + 🥙 Check + 🕈	🗟 AutoFill 🔹 🌽 🕵 192.168.2.1	🔩 🔹 🥚 Sign In 🔹
🚖 Favorites 🛛 😢 🔹 🏀 http:/	//192.168.2.1/inde × 🍘 Internet Explorer cannot di		
START	DATA EXTRAS		LOGOUT
			*
WLAN		*	
LAN			
	€	тарана и страна и стр	
	View any attempts that have been made to gain access to your network.		
	07/23/2010 11:00:55 192.168.2.100 login success 07/23/2010 11:00:52 If(COM1) start PPP	<u>^</u>	
	07/23/2010 11:00:51 Modem start to dial up 07/23/2010 11:00:51 UMTS Media Up !		
	07/23/2010 11:00:51 UMTS Date/Time updated.		
		-	E
	4	ь	
	A Save A Clear A Defrech		
		?	
Firmware version:20.03.302t2			-

WLAN

The Broadband Router operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, you need to enable the wireless function, define the SSID and the security options.

6 http://192.168.2.1/index.stm - W	/indows Internet Explorer				- 4
🕒 🗢 🖉 http://192.168.2.1	1/index.stm			🝷 👍 🗙 🚼 Google	ۍ م
File Edit View Favorites To	ools Help				
× Google	- 2	Search • 🕂 🌮 📲 • 🛛 👰 • 🔲 Side	ewiki • 🏻 🍄 Check • 🦌 AutoFill • 💡	<i>§</i>	🔦 🔹 🧼 Sign In 🔹
🔆 Favorites 🏾 🌈 http://192.168	.2.1/index.stm				
START	DATA	EXTRAS			LOGOUT
WIAN	WLAN				
» Settings	The Arcadvan-JAD suppo	ts WI AN Standards with transmission	rates up to 300 Mbit/s (802 11b/o/r	a) Devices can connect to th	e Arcadvan JAD wirelessly -
» Security	without the need for cable	15.		,	,,
LAN	WI AN Eurotion	0.0+ 0.0F			
	VIEAN I direction.				
	SSID	WLAN	(WLAN)		
		WPA2 Only PSK			
	Network Security	 Passphrase (min 8 cl 	naracters) 💿 Hex (64 digits)		
		1			
			→ Ap	ply → Cancel ?	
Firmware Version:20.03.302t2					

Parameter	Description
SSID	Specify a radio SSID (Service Set ID) to be used by the Broadband Router and all of its wireless clients.
	<i>Note:</i> Configure all of its clients to the same values.
Network Security	• Pre-shared key type: Select the key type to Passphrase or Hex.
	• Pre-shared Key: Enter the key here.

Settings

Specify a common radio channel and SSID (Service Set ID) for the Broadband Router, and all of its wireless clients. Be sure to configure all of its clients to the same values.

🕞 🗢 🙋 http://192.168	21/index.stm	- 😽 🗙 🚱 Google	
Edit View Favorites	Tools Help		
Google	💽 🚼 Search 🔹 🧒 🔹 🛖 •	🔊 • 🔲 Sidewiki • 🏾 🍄 Check • 🣔 AutoFill • 🌽	🔌 🔹 🥥 Sign
Favorites 🏾 🏀 http://192.	68.2.1/index.stm		
START	DATA EXTRAS		LOGOUT
VLAN	WLAN - Settings		
Settings	You can change the following parameters of the	wireless network.	
Security Timer			
AN	SSID Broadcast		
	Wireless Mode	Mixed 802.11n, 802.11g and 802.11b	
	Bandwidth	20/40MHz • (2010/40)	
	Channel	6 V (Auto)	
	Extension Channel	(read)	
	Protected Made		
	Separated ID Addresses		
	for LAN and WLAN	OFF - (OFF)	
		→ Apply → Cancel ?	
irmware Version:20.03.302t2			

Parameter	Description
SSID Broadcast	Enable or disable the broadcasting of the SSID. Disabling SSID broadcast will provide increased security by hiding the SSID of your wireless network.
Wireless Mode	This device supports 11n, 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. We recommend using "Mixed (11n+11g+11b) mode" to provide compatibility with 11n, 11b and 11g wireless clients.
Bandwidth	Set the bandwidth to 20 MHz, or 20/40 MHz.

Parameter	Description
Channel	The radio channel used by the wireless Router and its clients to communicate with each other. This channel must be the same on the Router and all of its wireless clients. The Router will automatically assign itself a radio channel, or you may select one manually.
Extension Channe	Select the extension channel, if the bandwidth is set to $20/40$ MHz.
Protected Mode	Enabling this function to ensure the best performance of your 11n throughput in case there is a lot of interference from the 11g and 11b devices in the wireless network.
802.11e/WMM QoS	Enable or disable the use of QoS. The QoS (Quality of Service) function allows you to differentiate WMM (Wi-Fi Multimedia) traffic and provide it with high- priority forwarding service
Separated IP Addresses for LAN and WLAN	Enabling this function for automatically separating the IP addresses for LAN and WLAN connections.

Security

To make your wireless network safe, you should turn on the security function. The Broadband Router supports WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 security mechanisms. This Router also supports WPS (Wi-Fi Protected Setup).

6 http://192.168.2.1/index.stm - V	Vindows Internet Explorer			- 6
🕒 🗢 🖉 http://192.168.2	1/index.stm		🔹 👍 🗙 🚼 Google	۰ م
File Edit View Favorites T	ools Help			
× Google	💽 🚼 Search 🔹 🛷 🦛 -	🛛 🔊 • 🔲 Sidewiki • 🛛 🍄 Check • 🧏 AutoFill •	3	🔌 🔹 🥥 Sign In 🔹
🚖 Favorites 🛛 🏀 http://192.16	8.2.1/index.stm			
START	DATA EXTRAS			LOGOUT
WLAN	WLAN - Security			
» Settings » Security » Timer	The Arcadyan-IAD can transmit your data secu devices. You can choose the allowed security r	ely over the wireless network. Matching security m nechanisms in this page and configure them in the	nechanisms must be setup on y sub-pages.	your router and wireless client
LAN	Enable WPS Function (
	WPS-PIN	→ Start		
	WPS-PIN for External Registrar	78149434 → Generate → Default		
	Allowed Client Type: WPA/WPA2 WF	A2 Only 💿 WPA Only 💿 WEP 💿 Disable	ed (Disabled)	
	Authentication:	0 802.1X • PSK (PSK)		
		(∌Au	pjy → Cancel ?	
Firmware Version:20.03.302t2				

Enable WPS Function: check this box to enable WPS. Enter the PIN in the **WPS-PIN** field, and click **Start** to establish WPS.

WPS-PIN for External Registrar: click Generate to create a new PIN.

Or you can click **Default** to restore the default PIN. Take this PIN you see on the screen, and enter it on the client side.

The following security options are available:

- WPA/WPA2
- WPA2 Only
- WPA Only
- WEP
- Disabled



Disabled option will turn off the wireless security function. We suggest that you turn on the security function to protect your wireless communication. Authentication: this is the authentication method used by clients.

If the **Allowed Client Type** is set to WPA/WPA2 or WPA2 Only or WPA Only, then you should set the authentication to 802.1X or PSK.

WPA/WPA2, WPA2 Only, WPA Only (PSK)

Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service.

Wi-Fi Protected Access 2 (WPA2) is a product certification that is available through the Wi-Fi Alliance. WPA2 certifies that wireless equipment is compatible with the IEEE 802.11i standard. The WPA2 product certification formally replaces Wired Equivalent Privacy (WEP) and the other security features of the original IEEE 802.11 standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA.

Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method.
	802.1X: for the enterprise network with a RADIUS server.
	Pre-shared key (PSK): for the SOHO network environment without an authentication server.

WPA/WPA2, WPA2 Only, WPA Only with 802.1X

If 802.1X is used in your network, you can configure the settings in this screen.



Parameter	Description
Authentication	Choose 802.1X authentication option.
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re- Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the Router will wait between failed authentications.
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.

Parameter	Description
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

WEP-Dynamic

If you want to use WEP to protect your wireless network, you need to set the same parameters for the Router and all your wireless clients.

🖉 http://192.168.2.1/index.stm - V	Vindows Internet Explorer		- ÷ 🐱
🕒 🗢 🖉 http://192.168.2.	1/index.stm	🗕 😽 🗙 🚱 Google	۰ م
File Edit View Favorites T	ools Help		
× Google	💽 🚼 Search 🔹 🛷 🐲 📲 💡	🔯 • 🔲 Sidewiki • 👹 Check • 🦉 AutoFill • 🌽	🔦 🔹 🧼 Sign In 🔹
👷 Favorites 🏾 🌈 http://192.168	3.2.1/index.stm		
START	DATA EXTRAS		LOGOUT
WLAN	WLAN - Security		Â
» Settings	The Arcadvan-IAD can transmit your data securely	over the wireless network. Matching security mechanisms must be setup on	your router and wireless client
» Security	devices. You can choose the allowed security mec	hanisms in this page and configure them in the sub-pages.	
LAN	Enable WPS Function ()		
	WPS-PIN	→ Start	
	WPS-PIN for External Registrar	78149434 Generate	
		- Detaur	
	Allowed Client Type: WPA/WPA2 WPA2	Only ONLY WEP Disabled (Disabled)	1
	WEP Mode:	64 bit 128 bit	
	Key Provisioning:	O Static Dynamic	
	Session Idle Timeout:	300 Seconds (0 for no timeout checking)	
	Re-Authentication Period:	3600 Seconds (0 for no re-authentication)	
	Quiet Period:	60 Seconds after authentication failed	
	Server-IP:	192 . 168 . 2 . 1	
	Server-Port:	1812	
	Secret Key:		
Firmware Version:20.03.302t2	NAS-ID:		
			-

Parameter	Description
WEP Mode	Select 64-bit or 128-bit key to use for encryption.
Key Provisioning	Select Dynamic to enable 802.1X function.

Parameter	Description
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re- Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the Router will wait between failed authentications.
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

WEP-Static

6 http://192.168.2.1/index.stm - 1	Windows Internet Explorer		- 4 -			
🚱 🕞 🔻 🙋 http://192.168.2.1/index.stm		- 4 🗙 🚼 Google 🖉 🖓				
File Edit View Favorites	Tools Help					
× Google	💽 😽 Search 🔹 🛷 🖉 📲 🔹	🔊 • 💚 Sidewiki • 🍼 Check • 🎦 AutoFill • 🌽	🖏 🔹 🥌 Sign In 🔹			
START	DATA EXTRAS		LOGOUT			
WE AN	WLAN - Security					
» Settings » Security » Timer	The Arcadyan-IAD can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages.					
LAN	Enable WPS Function (
	WPS-PIN	→ Start				
	WPS-PIN for External Registrar	78149434 → Generate → Default				
	Allowed Client Type: O WPAWPA2 O WPA2 Only O WPA Only O WPA Only O Disabled Constant					
	WEP Mode:	64 bit 128 bit				
	Key Provisioning:	Static Dynamic				
		⇒Apply →Cancel (2)				
Firmware Version:20.03.302t2						

Parameter	Description
WEP Mode	Select 64-bit or 128-bit key to use for encryption.
Key Provisioning	Select Static if there is only one fixed key for encryption.

Timer

You can also control the wireless function of the Broadband Router based on a time schedule.



Check the day of the week, and enter the start/end time, and click on **Add/Configure** icon to set the schedule.

For the existing entry, you can edit the parameters, or delete that entry.

During the above times the wireless function will be:

- If you set this to **activated**, the wireless function will be on in the configured time schedule.
- If you select **deactivated**, the wireless function will then be off in that configured time period.

LAN

The LAN settings screen allows you to change the default IP address of the Router and modify the DHCP server settings.

http://192.168.2.1/index.stn	n - Windows Internet Explorer			
🖉 🕞 🔻 🙋 http://192.10	58.2.1/index.stm		 	
ile Edit View Favorites Google Favorites Attp://19	Tools Help Clife.2.1/index.stm	- 💠 - 🔯 • 🔍 Sidewiki • 🛛 🍄 Check • 🐚 AutoFill •	🌛 🔌 🛶 Sign Iz	
START	DATA EXTRAS		LOGOUT	
WLAN	LAN Settings			
EM	You can enable DHCP to dynamically all to that you can assign static addresses f	ocate IP addresses to your client PCs, or configure filter or certain clients. The DSL-Easy Box must have an IP a	ng functions based on specific clients or protocols. In addition ddress for the local network.	
	IP Address	192 . 168 . 2 . 1 (192.168.2		
	IP Subnet Mask	255.255.255. 0 (255.255.0)		
	Host Name	easy.box (easy.box)		
	DHCP Server			
	DHCP Server Parameters	102 168 2 100 100 100	1401	
	Address Pool End IP	192 168 2 199 199 199		
	Lesse Time	Forever		
	Domain Name	(Contras)		
	Static DHCP			
	ID IP	MAC Address		
Firmware Version:20.03.302t2	1 0 0 0 0	00 : 00 : 00 : 00 : 00	: 00	
orites 🌈 http://1	02.168.2.1/index.stm	∑ 🚼 Search • 🖓 🛷 • 👘 • 💈	🕽 • 🔲 Sidewiki • 🛛 🍄 Check • 🧏 AutoFill •	ا الحج الحج الحج الحج الحج الحج الحج الح
-------------------	----------------------	--------------------------	---	--
START	DATA	EXTRAS		LOGOUT
AN	Domain Name			
	Static DHCP			
	ID IP		MAC Address	
	1 0 0	.0 .0	00 : 00 : 00 : 00 : 00	: 00
	2 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	3 0 0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	4 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	5 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	6 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	7 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	8 0 .0	, 0 , 0	00 : 00 : 00 : 00 : 00	: 00
	9 0 .0	.0.0	00 : 00 : 00 : 00 : 00	: 00
	10 0 0	0 0	00 : 00 : 00 : 00 : 00	: 00

Parameter	Description
LAN IP:	
IP Address	The IP address of the Router.
IP Subnet Mask	The subnet mask of the Router.
Host Name	Enter the name of the Router.
DHCP Server	Check this option to enable the DHCP server function on this Router.

Parameter	Description							
DHCP Server Parameters:								
Address Pool Start IP	Specify the start IP address of the DHCP pool. Do not include the gateway address of the Router in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.							
Address Pool End IP	Specify the end IP address of the DHCP pool.							
Lease Time	Allows you to select a pre-defined lease time for IP addresses assigned using DHCP. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.							
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.							
Static DHCP	You can assign a static IP to a certain MAC address within your network. You can enter up to 10 entries here in this table.							

Data

The Advanced configuration section, on the left-hand side displays the main menu and the right-hand side shows descriptive information.



The Data section contains the following menu items as described in the following table.

Parameter	Description
WAN	Specifies the Internet connection settings.
Firewall	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection and DMZ.
SNMP	Community string and trap server settings.
DNS & DDNS	Configures the DNS and DDNS function.

Parameter	Description
NAT	Configures address mapping, virtual server and special applications.
Wireless	Configures the radio frequency, SSID, and security for wireless communications.

Firewall



Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network. The firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks. Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

6 http://192.168.2.1/index1.stm	 Windows Internet Expl 	orer			- ÷ ×
😋 🔵 🗢 🙋 http://192.168.	2.1/index1.stm			🝷 😽 🗙 🚼 Google	- م
File Edit View Favorites	Tools Help				
× Google		💌 🚰 Search 🔹 🕫 🖉 📲 🔹	🔊 • 🔲 Sidewiki • 🏾 🖑 Check • 🍾	🔄 AutoFill 🔹 🌽	🔦 🔹 🥚 Sign In 🔹
🚖 Favorites 🛛 🌈 http://192.10	68.2.1/index1.stm				
		· · · · ·			
START	DATA	EXTRAS			LOGOUT
FIREWALL	Security Settin	ngs (Firewall)			
» Access Control » MAC Filter	The Device provide common attacks.	s extensive firewall protection by	y restricting connection parameters	to limit the risk of hacker attack, and defer	nding against a wide array of
Schedule Rule Intrusion Detection	Enable Firew	all features (🗹)			
DNS & DDNS					
NAT					
WIRELESS				→ Apply → Cancel ?	
Firmware Version:20.03.302t2					

It also protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan and TCP SYN flooding.

The firewall function is enabled by default. This feature does not significantly affect system performance, so we advise leaving this function enabled to protect your network.

Access Control

6 http://192.168.2.1/index1.stm -	Windows Internet Explorer					- 🗟 🎫
🕒 🗢 🖉 http://192.168.2.	1/index1.stm			- 4;	🗙 🚼 Google	ۍ م
File Edit View Favorites T	ools Help					
× Google	- 3	Search • 🖗 • 🐥 • 🔯 • 🔲 !	iidewiki • 🍄 Check •	📔 AutoFill 🔹 🌛		🔌 🔹 🧼 Sign In 🔹
🚖 Favorites 🏾 🏀 http://192.168	3.2.1/index1.stm					
START	DATA	EXTRAS				LOGOUT
FIREWALL	Access Control					
» Access Control » MAC Filter » URL Blocking	Access Control allows use filtering.	s to define the traffic type permitt	ed or not-permitted to W	'AN port service. This pa	ge includes IP address fi	itering and MAC address
» Schedule Rule » Intrusion Detection	Enable Filtering Funct	on (🗹)				
» DMZ DNS & DDNS	Normal Filtering Table (up t	o 10 computers):				
NAT	Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure	
WIRELESS	No Valid Filtering Rule	11				
					- Changer and Chan	
					Add PC	
				→ Apply	→ Cancel ?	
Firmware Version:20.03.302t2						

The following items are displayed on the Access Control screen.

Parameter	Description
Enable Filtering Function	Enables or disables the filtering function.
Normal Filtering Table	Displays the IP address (or an IP address range) filtering table.

Click Add PC on the Access Control screen to view the following screen.

Access Control/Add PC

To create a new access control rule:

- 1. Click Add PC on the Access Control screen. The Access Control Add PC screen will appear.
- 2. Define the appropriate settings for client PC services.
- 3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

6 http://192.168.2.1/index1.stm	- Windows Internet Explorer			- 6 🗷						
😋 🔾 🗢 🙋 http://192.168.3	21/index1.stm		🛨 😽 🗙 🚼 Google	Q						
File Edit View Favorites	Tools Help									
× Google	👻 🚰 Search 🕶	🔊 🛷 🔹 🕌 Sidewiki 🔹 🐡 Check 🔹 🦉 AutoFill 🔹	<i>§</i>	🖏 🔹 🥚 Sign In						
🔆 Favorites 🌈 http://192.16	58.2.1/index1.stm									
START	DATA EXTR	AS		LOGOUT						
	Access Control Add PC									
* Access Control										
» MAC Filter	This page allows users to define ser you need to configure the URL addre	vice limitations of client PCs, including IP address, service typ ess first on the "URL Blocking Site" page. For the scheduling fi	e and scheduling rule criteria. Fo unction, you also need to configu	or the URL blocking function, ure the schedule rule first on						
» URL Blocking » Schedule Rule	the "Schedule Rule" page.									
» Intrusion Detection	Client PC Description									
DNS & DDNS	Client PC IP Address	192.168.2. ~								
NAT	Scheduling Rule (Ref. Schedule Rulo Page)									
WIRELESS	rune i øgej									
	Client PC Service:									
	Service Name	Detailed description	Blocking							
	www	HTTP, TCP Port 80, 3128, 8000, 8001, 8080								
	WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)								
	Sending email	SMTP, TCP Port 25								
	News Forums	NNTP, TCP Port 119								
	Receiving email	POP3, TCP Port 110								
	Secure HTTP	HTTPS, TCP Port 443								
	File Transfer	FTP, TCP Port 21								
	Telnet Service	TCP Port 23								
	NetMeeting	H.323, TCP Port 1720, 1503	R							
Firmware Version:20.03.302t2	DNS	UDP Port 53								

MAC Filter

The MAC Filter allows you to define what client PC's can access the Internet. When enabled only the MAC addresses defined in the MAC Filtering table will have access to the Internet. All other client devices will be denied access.

http://192.168.2.1/index1.stm	Windows	Internet E	xplorer					
🕞 🗢 🙋 http://192.168.	2.1/index1.s	itm						- 44 🗙 Google
Edit View Favorites	Tools He	lp						
Google			-	Search	• • 🛷 •	• * •	S- 🗏	iidewiki • 🏽 🍄 Check • 🧏 AutoFill • 🌽 🛛 🔍 🔍 🔍
Favorites 6 http://192.10	58.2.1/inde	d.stm						
START	D	ATA		EX	TRAS			LOGOUT
	MAC	Filterin	g Tabl	е				
Access Control MAC Filter URL Blocking Schedule Rule	This se will get	ction hel denied a AC Addre	ps provid access.	de MAC F This secu trol ()	Filter con unity featu	figuration ire can si	. When er	abled, only MAC addresses configured will have access to your network. All other client device o 32 devices and applies to clients.
Intrusion Detection DMZ	MAC F	iltering T	able (up	to 32 co	mputers)			
DNS & DDNS								
TAN	DHCP	Client Lis	st: ip=19	2.168.2.1	100 name	=A04002	5-PC2 🔻	→ Copy to 1 -
WIRELESS	ID	MAC	Address	3				
	1	00	: 19	: 21	: 43	: BE	: DD	
	2		:	1	:	1	1	
	3		:	1	:	1	1	
	4		:	1	:	1	1	
	5		:	1	:	1	1	
	6		1	1	1	1	1	
	7		:	1	:	1	1	
	8		:	1	:	1	1	
	9		1	1	1	1	1	
	10		:	1	:	1	1	
	11		:	1	:	1	1	
Firmware Version:20.03.302t2	12		1	1	:	1	1	

You can enter up to 32 MAC addresses in this table.

URL Blocking

The VoIP Router allows the user to block access to web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.

6 http://192.168.2.1/index1.stm -	Windows Internet Ex	plorer	- 6 💌
🕒 🗢 🖉 http://192.168.2	1/index1.stm	- 👍 🗙 🚼 Google	+ م
File Edit View Favorites 1	ools Help		
× Google		🔽 🔧 Search 🕂 🛷 * 🐥 * 🔯 * 🔍 Sidewiki * 🥙 Check * 🤤 AutoFill * 🌽	🔌 🔹 🥥 Sign In 🔹
👷 Favorites 🏾 🌈 http://192.16	8.2.1/index1.stm		
START	DATA	EXTRAS	LOGOUT
FIREWALL	URL Blockin	g	- Ĥ
» Access Control	Disallowed Web	Sites and Keywords.	
» URL Blocking	You can block a	ccess to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.	
» Schedule Rule » Intrusion Detection	The following LID	La and knowned are blacked	
» DMZ	The following OK	blocked	-
DNS & DDNS	Rule Number	URL / Keyword allowed	-
MIDELESS	Site 1		
WINCLE 33	Site 2		
	Site 3		
	Site 4		
	Site 5		
	Site 6		
	Site 7		
	Site 8		
	Site 9		
	Site 10		
	Site 11		
	Site 12		
	Site 13		
Firmware Version:20.03.302t2	Site 14		-

To configure the URL Blocking feature, use the table below to specify the web sites (www.somesite.com) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in "Access Control" on page 37. From the Access Control, Add PC section, check the option for **WWW with URL Blocking** in the Client PC Service table to filter out the web sites and keywords selected.

You can define up to 30 sites here.

Schedule Rule

6 http://192.168.2.1/index1.stm -	Windows Internet Explorer				- 2 -
🕒 🔾 🗢 🖻 http://192.168.2	21/index1.stm			🝷 😽 🗙 🚼 Google	+ م
File Edit View Favorites	Tools Help				
X Google		Search • 🖓 🌍 • 👘 • 🛓	🔋 • 💚 Sidewiki • 🍞 Check • 🎦 AutoFill •	· 🌽	🖏 🔹 🥥 Sign In 🔹
ravontes // http://192.10	x8.2.1/index1.stm				
START	DATA	EXTRAS			LOGOUT
FIREWALL	Schedule Rule				
» Access Control » MAC Filter	This page defines sched	ule rule names and activates	s the schedule for use in the "Access Control	" page.	
» URL Blocking » Schedule Rule	Schedule Rule Table (up	to 10 rules):			
» Intrusion Detection	Rule Name	Rule Comment		Configure	
DNS & DDNS	No Valid Schedule Rule				
NAT				9	
WIRELESS				Add Schedule Rule	
			÷1	Apply → Cancel ?	
Firmware Version:20.03.302t2					

You may filter Internet access for local clients based on rules.

Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule screen, and apply the rule on the Access Control screen.

Edit Schedule Rule

You can create and edit schedule rules on this screen.

6 http://192.168.2.1/index1.stm	- Windows Internet Expla	rer		- 2 🔀
🕒 🗢 🖉 http://192.168.	2.1/index1.stm		🗸 🍫 🗙 🚱 Google	+ ٩
File Edit View Favorites	Tools Help			
× Google		💽 🛃 Search 🔹 🧔 🐑 👘 🔹 🧕 🐑 💭	Sidewiki 🔹 🍄 Check 🔹 🧏 AutoFill 👻 🌽	🔦 🔹 🥥 Sign In 🔹
🔆 Favorites 🌈 http://192.1	68.2.1/index1.stm			
START	DATA	EXTRAS		LOGOUT
FIREWALL	Edit Schedule	Rule		
» MAC Filter	Name			
» URL Blocking	Comment			
» Intrusion Detection » DMZ	Activate Time Perio	d:		
DNS & DDNS	Week Day	Start Time (hh:mm)	End Time (hh:mm)	
NAT	Every Day		:	
WIRELESS	Monday		:	
	Tuesday			
	Wednesday		:	
	Thursday		:	
	Friday			
	Saturday		:	
	Sunday		:	
			→ Apply → Cancel ?	
Firmware Version:20.03.302t2				

- 1. Click Add Schedule Rule icon on the Schedule Rule screen. The Edit Schedule Rule screen will appear.
- 2. Define the appropriate settings for a schedule rule.
- 3. Click Apply to save your settings.

Intrusion Detection

The Broadband Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as Denial-of-Service (DoS) attacks.

6 http://192.168.2.1/index1.stm	Windows Internet Explorer		- 4 🐱
🕒 🗢 🖉 http://192.168.2	2.1/index1.stm	- 😽 🗙 🚱 Google	ۍ م
File Edit View Favorites	Tools Help		
× Google	💌 🔧 Search 🔹 🧒 🐑 🚽 😨 Shar	re 🔹 🗣 🔍 Sidewiki 🔹 🍄 Check 🔹 🔚 Translate 🔹 📔 AutoFill 🔹 🌽	🔦 🔹 🥚 Sign In 🔹
🚖 Favorites 🛛 🌈 http://192.10	38.2.1/inded.stm		
START	DATA EXTRAS		LOGOUT
WAN	Intrusion Detection		Â
FIREWALL	When the SPI (Stateful Packet Inspection) firewall feature	is enabled, all packets can be blocked. Stateful Packet Inspection (SPI)	allows full support of
» Access Control	different application types that are using dynamic port nun from the local LAN.	nbers. For the applications checked in the list below, the Device will supp	ort full operation as initiated
» URL Blocking	The Device formall and black common backet effects in	Indian ID Constant Land Attack, Disc of Darah, ID with over langth, Count	
» Schedule Rule	loopback, Snork Attack, TCP null scan, and TCP SYN flor	oding. Populing, Land Attack, Ping of Death, IP with Zero length, Smun oding.	E
» DMZ	Intrusion Detection Feature:		
SNMP			
DNS & DDNS	SPI and Anti-DoS firewall protection		
NAT	RIP defect		
WIRELESS	Discard Ping To WAN Interface		
	Stateful Packet Inspection:		
	Packet Fragmentation		
	TCP Connection		
	UDP Session		
	FTP Service		
	H.323 Service		
	TFTP Service		
	When backers attempt to enter your network, we can aler	t you by e-mail-	
Firmware Version:20.03.302	when nations accomplies oncer your network, we can also	you by o mail.	
_	Your F-mail Address	0	٣

http://192.168.2.1/index1.stm -	Windows Internet Explorer		
→ → 100 mttp://192.168.2	:1/index1.stm	- 4 X Google	. م
File Edit View Favorites	fools Help	an Albert Statement A	
A Enumiter	Search The State of the State o	ewiki * Viceck * 🚪 Autorill * 🌽	n 🧠 🔍 Sign In
ravontes enttp://192.10	s.2.1/indexi.stm		
START	DATA EXTRAS		LOGOUT
FIREWALL	When backers attempt to enter your network we can alert you	by e-mail:	
» Access Control			
» MAC Filter » URL Blocking	Your E-mail Address		
» Schedule Rule	SMTP Server Address		
» DMZ	POP3 Server Address		
DNS & DDNS	User name		
NAT	Password		
WIRELESS	Connection Policy:		
	Fragmentation half-open wait	10 Secs (10)	
	TCP SYN wait	30 secs (30)	
	TCP FIN wait	5 Secs (8)	
	TCP connection idle timeout	3600 secs (3000)	
	UDP session idle timeout	120 secs (120)	
	H.323 data channel idle timeout	180 Secs (180)	
	DoS Detection Criteria:		
	Total incomplete TCP/UDP sessions HIGH	300 session (300)	
	Total incomplete TCP/UDP sessions LOW	250 session (250)	
Firmware Version:20.03.302t2	Incomplete TCP/UDP sessions (per min) HIGH	250 session (250)	
	Incomplete TCP/UDP sessions (per min) LOW	200 session (200)	

Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Broadband Router protects against DoS attacks including: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, $\rm IP$ with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack.

6 http://192.168.2.1/index1.stm	- Windows Internet Explorer			- \$ ×
😋 🔾 🗢 🙋 http://192.168	.2.1/inded.stm		- 🦘 🗙 Google	- م
File Edit View Favorites × Google	Tools Help	ki • 🏾 🏇 Check • 🧏 AutoF	ill • 🌽	🖏 • 🥥 Sign In •
START	DATA EXTRAS			LOGOUT
FIREWALL	TCP connection idle timeout	3600	SECS (3000)	· · · · · · · · · · · · · · · · · · ·
» Access Control	UDP session idle timeout	120	Secs (120)	
» URL Blocking	H.323 data channel idle timeout	180	SECS (180)	
» Schedule Rule » Intrusion Detection » DMZ	DoS Detection Criteria:			
DNS & DDNS	Total incomplete TCP/UDP sessions HIGH	300	session (300)	
NAT	Total incomplete TCP/UDP sessions LOW	250	session (250)	
WIRELESS	Incomplete TCP/UDP sessions (per min) HIGH	250	session (250)	
	Incomplete TCP/UDP sessions (per min) LOW	200	session (200)	
	Maximum incomplete TCP/UDP sessions number from same host	60	(60)	
	Incomplete TCP/UDP sessions detect sensitive time period	1000	msec. (1000)	
	Maximum half-open fragmentation packet number from same host	30	(30)	
	Half-open fragmentation detect sensitive time period	10000	msec. (10000)	
	Flooding cracker block time	300	SOCS (300)	
				E
		ĺ	→ Apply → Cancel ?	
Firmware Version:20.03.302t2				-

Parameter	Defaults	Description
Enable SPI and Anti-DoS firewall protection	Yes	The Intrusion Detection feature of the Router limits the access of incoming traffic at the WAN port. When the Stateful Packet Inspection (SPI) feature is turned on, all incoming packets are blocked except those types marked with a check in the Stateful Packet Inspection section at the top of the screen.

Parameter	Defaults	Description
Stateful Packet Inspection		This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, and TFTP Service.
		It is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communication; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until a connection to the specific port is requested.
		When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks FTP Service in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Parameter	Defaults	Description			
Hacker Preventi	on Feature				
Discard Ping from WAN	Discard	Prevents a ping on the Router's WAN port from being routed to the network.			
RIP Defect Enabled		If the router does not reply to an IPX R request packet, it will stay in the input queue and not be released. Accumulate packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature preven the packets accumulating.			
When hackers a email	ttempt to er	nter your network, we can alert you by			
Your E-mail Address		Enter your email address.			
SMTP Server Address		Enter your SMTP server address (usually the part of the email address following the "@" sign).			
POP3 Server Address		Enter your POP3 server address (usually the part of the email address following the "@" sign).			
User Name		Enter your email account user name.			
Password		Enter your email account password.			
Connection Polic	сy				
Fragmentation half-open wait	10 secs	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.			

Parameter	Defaults	Description
TCP SYN wait	30 secs	Defines how long the software will wait for a TCP session to reach an established state before dropping the session.
TCP FIN wait	5 secs	Specifies how long a TCP session will be managed after the firewall detects a FIN- exchange.
TCP connection idle timeout	3600 secs (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 secs	The length of time for which a UDP session will be managed if there is no activity.
H.323 data channel idle timeout	180 secs	The length of time for which an H.323 session will be managed if there is no activity.
DoS Detect Crite	ria	
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>stop</i> deleting half-open sessions.
Incomplete TCP/ UDP sessions (per min.) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/ UDP sessions (per min.) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.

Parameter	Defaults	Description
Maximum incomplete TCP/ UDP sessions number from same host	30	Maximum number of incomplete TCP/ UDP sessions from the same host.
Incomplete TCP/ UDP sessions detect sensitive time period	900 msecs	Length of time before an incomplete TCP/ UDP session is detected as incomplete.
Maximum half- open fragmentation packet number from same host	20	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	10000 msecs	Length of time before a half-open fragmentation session is detected as half- open.
Flooding cracker block time	300 secs	Length of time from detecting a flood attack to blocking the attack.

DMZ

Contraction in the second second	68.2.1/index1.stm							- 47 🗙 🚦	Google	
Edit View Favorites	Tools Help									
Google		-	Search •	• 🛷 • 🚽	📲 🛛 🔊 🔹 🔲 Sidewiki -	Check • 1	🗧 AutoFill 🔹	3		🔌 • 🔘 Sig
avorites 🏾 🏉 http://19	2.168.2.1/index1.s	tm								
START	DAT	A	EXT	RAS						LOGOUT
REWALL	DMZ(De	emilitarize	d Zone)							
Access Control	If you have	e a local clie	nt PC that c	annot run a	an Internet application pr	operly from behir	nd the NAT fi	rewall, then you	can open the cl	lient up to unrestricted two-
MAC Filter	way Intern	iet access b	y defining a	Virtual DM	IZ Host.					
Schedule Rule	🗔 Enab	le DMZ Fun	ction (🔲)							
Intrusion Detection	13									
DMZ NS & DDNS	Multiple P must set a	'Cs can be e a static IP a	xposed to the ddress for the	e Internet 1 at PC.	for two-way communicat	ions e.g. Interne	t gaming, vid	eo conferencing,	or VPN connect	ctions. To use the DMZ, you
AT										
VIRELESS	F	Public IP Add	iress			Client PC IP Add	dress			
	1. 0	.0.0.0				192.168.2.0				
	2. 0	0.0	. 0	. 0		192.168.2.0				
	3. 0	0.0	. 0	. 0		192.168.2.0				
	4. 0	. 0	. 0	0		192.168.2.0				
	5. 0	0	. 0	. 0		192.168.2.0				
	6. 0	0	. 0	0		192.168.2.0				
				0		192 168 2 0				
	7. 0	. 0	. 0			102.100.2.0				
	7. 0	.0	. 0	. 0		192.168.2.0				
	7. 0 8. 0	.0	. 0	. 0		192.168.2.0				
	7. 0 8. 0	. 0	. 0	. 0		192.168.2.0				
	7. 0 8. 0	.0	. 0	. 0		192.168.2.0		onlu 🕽 🗘 Ca	neat 2	

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted twoway Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

DNS & DDNS

DNS

A Domain Name Server (DNS) is an index of IP addresses and web site addresses. If you type a web site address into your browser, such as www.abc.de, a DNS server will find that name in its index and find the matching IP address: 111.222.333.444. Most ISP's provide a DNS server for speed and convenience. Since your ISP may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

http://192.168.2.1/index1.stm -	- Windows Internet Explorer						
🕞 🗢 🙋 http://192.168.3	2.1/index1.stm					🝷 🍫 🗙 🛃 Goo	ogle 🖇
Edit View Favorites	Tools Help						
Google	- 🔧	Search • 🕂 🤝 • 👘 • 📓	🔹 💷 Sidewiki 🔹	🍄 Check -	📔 Auto	Fill • 🌛	🔩 🔹 🧼 Sign
Favorites 🏾 🏀 http://192.16	68.2.1/index1.stm						
START	DATA	EXTRAS					LOGOUT
	DNS						
	A Domain Name Server (Df	IS) is an index of IP addre	sses and Web ad	dresses. Wi	ien you ty	pe a Web address into you	r browser, such as www.arcadyan.com,
1AT	a DNS server will find that r Since your Senice Provider	ame in its index and find	the matching IP a	ddress:xxx. Reattings in	COX XXX X	xx. Most ISPs provide a DN	IS server for speed and convenience.
MIRELESS	there is a DNS server that	you would rather use, you	need to specify th	e IP address	here.	and the bits series if s are	and provided dynamically. However, if
	Domain Namo Sonor (DN	S) Addross	0 0	0	0	(0.0.0.0)	
	Domain Name Server (DIV	a di an					
	Secondary DNS Address	(optional)	0.0	. 0	. 0	(0.0.0)	
	DDNS (Dynamic DNS Dynamic DNS provides use address automatically by h This DNS feature is powere own location even if you ha Dynamic DNS	B) Settings rs on the Internet a method awing your DNS records c d by an external service p ve a dynamic IP address.	d to tie their domi nanged when your rovider. With a DC	ain name(s) I IP address INS connect	o comput changes. on you ca	ers or servers. DDNS allow: In host your own web site, (s your domain name to follow your IP amail server, FTP site and more at your
	Provider	DynDNS.org -					
	Domain Name						
	Account / E-mail						
	Password / Key						
irmware Version:20.03.302t2							

DDNS

Dynamic Domain Name Service (DDNS) provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

This DNS feature is powered by DynDNS.org or TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

Web Management

NAT



Network Address Translation allows multiple users to access the Internet sharing one public IP.

• Enable NAT function : click on the checkbox to enable this function.

Address Mapping

Address mapping allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security.

Edit View Favorites	Tools Help						• ++ × Google	
Google	-	Search • 🕂 🤝 • 👍 •	🔯 • 🔲 Sidewiki • 🕇	🤣 Check	- 19 A	utoFill • 🤞	1	🔩 + 🥥 Sig
avorites 🏾 🏀 http://19	2.168.2.1/index1.stm							
START	DATA	EXTRAS						LOGOUT
IREWALL	Address Mapping							
NS&DDNS IAT Address Mapping Port Mapping	Network Address Transla Internet. This feature limit one or more than one pul	tion (NAT) allows IP ac s the number of public lic IP address to be m	ddresses used in a private IP addresses required fro apped to a pool of local a	local ne om the IS ddresse	twork to iP and a s.	be mappeo Iso maintair	I to one or more addresses used in the privacy and security of the I	i the public, global ocal network. We allow
Special Application	Address Mapping							
NAT Mapping Table	1 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
WIRELESS	2 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
	3 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
	4 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	0	.0	0		
	5 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
	6 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
	7 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	0	.0	0		
	8 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
	9 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	0	.0	.0		
	10 from 192.168.2.0	~ 192.168.2.0	map to global IP 0	.0	.0	.0		
						→ Арр	ly ƏCancel ?	

Enter a range of internal IPs that will share the global IP, and then enter the Public IP address you wish to share into the global IP field.

Port Mapping

You can configure the Router as a virtual server so that remote users accessing services such as the web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports and combinations of the two. For example:

- Port Ranges: e.g. 100-150
- Multiple Ports: e.g. 25,110,80
- Combination: e.g. 25-100,80

Click Configure/add icon to add a new entry.

6 http://192.168.2.1/index1.stm -	Windows Internet Explorer					- 4
🕒 🗢 🖉 http://192.168.2	1/index1.stm				🝷 😽 🗙 🚼 Google	+ م
File Edit View Favorites T	fools Help					
× Google	•	🚼 Search 🔹 🕫 🐔 🚽	💌 🔊 • 🔲 Sidewiki	Check • 🦌 AutoFill •	<i>9</i>	🔦 🔹 🧼 Sign In 🔹
🚖 Favorites 🛛 🏀 http://192.16	8.2.1/index1.stm					
START	DATA	EXTRAS				LOGOUT
FIREWALL	Port Mapping					
DNS & DDNS NAT > Address Mapping > Port Mapping > Special Application > NAT Mapping Table WiRELESS	You can configure the be automatically redire the router redirects the multiple ports, and cor For example: Port Ranges: ex. 100- Multiple Ports: ex. 25, Combination: ex. 25-11	router as a virtual servy cted to local servers c external service reque nbinations of the two. 150 110,80 10,80	er so that remote users onfigured with private IP est to the appropriate se	accessing services such as th addresses. In other words, de ver (located at another interna	e Web or FTP at your local pending on the requested se Il IP address). This tool can	site via public IP addresses can rvice (TCP/UDP port number), support both port ranges.
	No. LAN IP	Protocol Type	LAN Port	Public Port	Enable Configure	
					D.	
					Add	
					→ Cancel ?	1
Firmware Version:20.03.302t2						



Special Applications

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use the following screen to specify the additional public ports to be opened for each application.

6 http://192.168.2.1/index1.stm -	Windows Internet Explorer						- # X
🕒 💬 🗢 🙋 http://192.168.2.	1/index1.stm				- + × *	Google	, م
File Edit View Favorites T × Google	ools Help] 🚼 Search • 🕂 🧔 • 🛁	🕨 🔊 • 💷 Sidewiki •	🍄 Check • 🦹 AutoFill • 🍐			🔩 🔹 🥚 Sign In 🔹
👷 Favorites 🏾 🌈 http://192.168	8.2.1/index1.stm						
START	DATA	EXTRAS					LOGOUT
FIREWALL DNS & DDNS NAT > Address Mapping > Port Mapping > Special Application	Special Applications recovered when Network Address an application in the "inbound traffic. Note: The range of the	ons uire multiple connectio s Translation (NAT) is e Trigger Port" field, selec Trigger Ports is from 1	ns, such as Internet gami mabled. If you need to rur t the protocol type as TC to 65535.	ng, video conferencing, Interne applications that require multi P or UDP, then enter the publi	t telephony ar ple connection c ports associ	nd others. The ns, specify th iated with the	ese applications cannot work the port normally associated with trigger port to open them for
» NAT Mapping Table	Popular applications	- select one -	- Copy to -				
WIRELESS		- select one - Battle.net	2				
	Trigger Port	Dialpad ICU II	Public Port	Public	Туре	Enabled	
	1.	MSN Gaming Zone PC-to-Phone		TCI	POUDP		
	2.	Quick Time 4 eMule(TCP)		TCI	P O UDP		
	3.	eMule(UDP) Bittorrent(BT)		TCI	P 🔿 UDP		
	4.	● TCP ○ UDP		 TCI 	P O UDP		
	5.	● TCP ○ UDP		 TCI 	P O UDP		
	6.	● TCP ○ UDP		 TCI 	P O UDP		
	7.	● TCP ○ UDP		 TCI 	P () UDP		
	8.	● TCP ○ UDP		TCI	POUDP		
	9.	● TCP ○ UDP		TCI	POUDP		
	10.	● TCP ○ UDP		TCI			
Firmware Version:20.03.302t2							-

Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, then enter the ports that the application requires.

Popular applications requiring multiple ports are listed in the **Popular applications** field. From the drop-down list, choose the application and then choose a row number to copy this data into.

NAT Mapping Table

NAT Mapping Table displays the current NAPT (Network Address Port Translation) address mappings. As the NAT mapping is dynamic, a **Refresh** button is provided to refresh the NAT Mapping Table with the most up-to-date values.



The content of the NAT Mapping Table is described as follows:

- Protocol protocol of the flow.
- Local IP local (LAN) host's IP address for the flow.
- Local Port local (LAN) host's port number for the flow.
- Pseudo IP translated IP address for the flow.
- Pseudo Port translated port number for the flow.
- Peer IP remote (WAN) host's IP address for the flow.
- Peer Port remote (WAN) host's port number for the flow.

Wireless

WLAN

The Router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the SSID, and the security options.

6 http://192.168.2.1/index1.stm -	Windows Internet Explorer			- 2 -
🕒 🗢 💌 🙋 http://192.168.2	1/index1.stm		- 47 🗙 🚼	Google 🔎 🗸
File Edit View Favorites 1	fools Help			
× Google	•	🚼 Search 🔹 🛷 🔹 📲 🔹 🧕 🐑 🔲 Si	dewiki 🔹 🍄 Check 🔹 🦉 AutoFill 🔹 🌽	🔩 🔹 🧼 Sign In 🔹
🔆 Favorites 🏾 🌈 http://192.16	8.2.1/index1.stm			
START	DATA	EXTRAS		LOGOUT
FIREWALL	WLAN			
DNS & DDNS NAT	The Arcadyan-IAD sup without the need for ca	ports WLAN Standards with transmissi bles.	on rates up to 300 Mbit/s (802.11b/g/n). Devices can co	nnect to the Arcadyan-IAD wirelessly -
WIRELESS » Access Control	WLAN Function:	● On ○ Off (On)		
	SSID	WLAN		
		WPA2 Only PSK		
	Network Security	Passphrase (min 8	characters) O Hex (64 digits)	
			∂Apply ∂Canc	a 2
Firmware Version:20.03.302t2				

- WLAN Function: select to enable or to disable the wireless function, or you can use this function based on a time schedule.
- SSID: Service Set ID, this is the name of your wireless network. Specify the SSID to be used by the Router and all of its wireless clients. Be sure you configure all of its clients to the same values.
- Network Security: if WPA/WPA2 and PSK is used as your wireless security method, select **Passphrase** or **HEX** to use as your key entry method. Refer to "Security" on page 25 for more details.



WLAN button located on the device, you can set to activate or deactivate this button.

Access Control

Using the Access Control functionality, you can restrict access based on MAC address. Each PC has an unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, the computers whose MAC address you have listed in the filtering table will be able to connect (or will be denied access) to the Broadband Router.

6 http://192.168.2.1/index1.stm	- Windows I	Internet B	xplorer											
🔾 🗢 🗢 http://192.168.	2.1/index1.s	tm									- + ;	🗙 😽 Google		+ م
File Edit View Favorites	Tools He	lp												
× Google			-	Search	•• 🛷 •	+ • {	🔕 • 🔲 s	dewiki •	> Check	📔 AutoFill 🔸	• 🥖			🔩 🔹 🧼 Sign In 🔹
🙀 Favorites 🏾 🏀 http://192.10	68.2.1/index	d.stm												
						_								
START	D	ATA		EX	TRAS									LOGOUT
FIREWALL	Wirele	ess Ac	cess C	ontrol										
DNS & DDNS NAT	For a m to the N	nore sec AAC Filt	ure Wire ering Tat	less netw ble. Wher	ork you o enabled	an speci , all regis	fy that onl tered MAC	/ certain Wi addresses	reless PCs are controll	can connect ed by the Ad	t to the Acce ccess Rule.	ess Point. Up t	o 32 MAC add	resses can be added
WIRELESS » Access Control	En 🖓	able MA	C Filteri	ng (🔲)										
	Access	Rule fo	r register	ed MAC	address:	Allow	/	(Allow)						E
	MAC F	iltering T	able (up	to 32 sta	tions):									
	ID	MAC	Address	5										
	1	00	: 00	: 00	: 00	: 00	: 00							
	2	00	: 00	: 00	: 00	: 00	: 00							
	3	00	: 00	: 00	: 00	: 00	: 00							
	4	00	: 00	: 00	: 00	: 00	: 00							
	5	00	: 00	: 00	: 00	: 00	: 00							
	6	00	: 00	: 00	: 00	: 00	: 00							
	7	00	: 00	: 00	: 00	: 00	: 00							
	8	00	: 00	: 00	: 00	: 00	: 00							
	9	00	: 00	: 00	: 00	: 00	: 00							
	10	00	: 00	: 00	: 00	: 00	: 00							
	11	00	: 00	: 00	: 00	: 00	: 00							
Firmware Version:20.03.302t2	12	00	: 00	: 00	: 00	: 00	: 00							
-														•

	30	00	: 00	: 00	: 00	: 00	: 00		Π
	31	00	: 00	: 00	: 00	: 00	: 00		
	32	00	: 00	: 00	: 00	: 00	: 00		
	Add curre	ently a	ssociated	I MAC st	ations?	→ Ente	~		н
								→ Apply → Cancel ?	
Firmware Version:20.03.302t2									Ļ

- Enable MAC Filtering: select to enable or disable this function.
- Access Rule for registered MAC address: select to allow/deny access for the registered MAC addresses. Selecting **Allow** means only MAC addresses registered here will be able to connect to the Broadband Router.

- Selecting **Deny** means only the MAC addresses registered here will be denied access to the Broadband Router.
- MAC Filtering Table: you can enter up to 32 addresses here in the table. Click **Enter** for the Add currently associated MAC stations option to quickly copy the entry to the MAC Filtering table.

WDS

The Wireless Distribution System (WDS) provides means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and to allow stations to roam freely within the area covered by the WDS.

6 http://192.168.2.1/index1.stm -	Windows Internet Explo	rer			- # ×
🔾 🗢 🖉 http://192.168.2	1/index1.stm			👻 44 🗙 🚼 Google	+ م
File Edit View Favorites 1	fools Help				
× Google		🝷 🚼 Search 🔹 🕫 🍏	• 👘 • 🛃 Share • 🔯 • 🔲 Sidewiki •	🍄 Check 🔹 🔠 Translate 🍨 📔 AutoFill 👻 🍐	🔰 🛛 🔌 • 🥥 Sign In •
🔆 Favorites 🏾 🏀 http://192.16	8.2.1/inded.stm				
START	DATA	EXTRAS			LOGOUT
WAN	WDS				
FIREWALL	The Wireless Distri	bution System (WDS)	provides a means to extend the range of	a Wireless Local Area Network (WLAN). WD	S allows an Access Point (AP)
SNMP	to establish a direc	t link to other APs and	I to allow stations to roam freely within the	e area covered by the WDS.	
DNS & DDNS	Enable WDS F	Function (🔲)			
NAT	AP MAC Address	Table (up to 4 APs);			
WIRELESS					
» WDS		SSID	MAC Address	Mode	
		ALICE-WLAN03	00 : 1C : 28 : 24 : 64 : 0	06 11n	
		Belkin_159B0B	00 : 22 : 75 : 15 : 9B : 0	0B 11g	
			00 : 22 : 75 : 15 : 9A : A	F 11n	
		HomeNet727884838b	00 : 04 : E2 : C2 : 65 : E	38 11g	
		HIWLAN	00 : 04 : E2 : 4C : 7B : 9	96 11g	
	→ Rescan				
				→ Apply → Cancel ?	
Eirmeare Version 20 03 202					
Commone version:20.03.302					

- Enable WDS function: check this box to enable this function.
- Rescan: click this button to refresh the list of available access points.

Available access points will show up on the AP MAC Address Table, check the box to add that particular access point to the WDS.

Extras

The Broadband Router supports the following extra functions described in the table below:

http://19216821/indev3stm	Windows Internet Evolorer				
	21/index3.stm			- + × Google	ــــــــــــــــــــــــــــــــــــــ
ila Edit View Eavoriter	Tools Help			V N N	
Google	- 1005 Hop	🖥 Search • 🖟 ൽ • 斗 🛛 🐼 • 🔲 S	dewiki - 🏷 Check - 😒 AutoFill -	4	🐁 🔹 🦳 Sian In 🔹
Eavorites Abtto://1921	68.21/index2.ctm		•		Q
6 (10)/1024	00.2.17 110000.3011				
CTADT	DATA	EVTRAC			
START	DATA	EATRAS			LOGOUT
HSPA Modem	System Settings				
Password Settings	This page includes all th	e basic configuration tools for the rou	er, such as time zone, password se	ttings, and remote management.	
Time Settings					
Remote Management					
Firmware Upgrade					
Diagnostic Utility					
Reboot					
UPnP					

Menu	Description
HSPA Modem	The high-speed packet access (HSPA) delivers 5.8 Mbps of the uplink and 14 Mpbs in the downlink.
Password Settings	Sets the password for administrator access.
Time Settings	Sets the local time zone, etc.
Remote Management	Enables/disables remote management of the Router.
Firmware Upgrade	Allows you to upgrade your firmware version.
Diagnostic Utility	Allows you to test network connection status.
Reboot	Performs system reboot if the Router stops responding.
UPnP	Enables/disables the Universal Plug and Play function.

HSPA Modem

UMTS-Stick

Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) mobile telecommunications technologies. It combines three different air interfaces, GSM's Mobile Application Part (MAP) core, and the GSM family of speech codecs.

6 http://192.168.2.1/index3.stm -	Windows	Internet Explorer								x
🔾 🔾 🗢 🙋 http://192.168.2	1/index3.s	tm					- 47 ×	Soogle 🚼	,	, -
File Edit View Favorites 1	Fools He	lp								
🗴 Google 192.168.2.1 💽 🚼 Search + 🖉 + 👘 - 💭 Sidewiki - 🏷 Check - 🧏 AutoFill - 🥖 💽 192.168.2.1								🔩 🔹 🧼 Sign	In •	
👷 Favorites 🛛 😸 🔹 🏀 http:/	//192.168.2	.1/inde × 🌈 Inte	rnet Explo	rer cannot di						
START	D	ATA	EXTR	AS					LOGOUT	
HSPA Modem	UMTS	S-Stick								Â
Password Settings	The dev	vice enables a conn	ection with	n a UMTS for Intern	et and Voice over the UN	VITS mobile netv	vork. Please ins	ert the SIM card	I into the device before power on.	
Time Settings	Once d	lone, please enter th	e PIN coo	le of the SIM card I	here.					
Remote Management	PIN C				Store PIN (7)	Change PIN (ode			
Firmware Upgrade	_									
Diagnostic Utility	Sept	Status	Service F	mylder	() 1 min 21 ann	Max Rate	Lasvas	1 es visa		
HEDOOT		Available (Data)	Chunghy	a Telecom GSM	- 1 mill. 21 dec.	Act Bate	1 24 Khon	220 hos		E
UP IIP					= 20.40 NDyles.		• 1.54 Rups.	• 000 0pa.		
	UMTS	connection								
	Backu	in-connection		Only UMTS con	nection					
				No UMTS backup fo	ip or Data					
	APN			UMTS backup fo	or Voice (met)					
	Phone	Number		Only UMTS conr	nection					
	Idle Ti	me (Minutes)		5 (5)						
	User N	Vame								
	Passv	vord								
	Confirm	m Password								
Firmware Version:20.03.302t2						•	Apply 👌	Cancel ?		
										-

The Broadband Router enables a connection with a UMTS-Stick for Internet and Voice over the UMTS mobile network. Please insert the SIM card into the UMTS jack of the Router. Then, enter the PIN code of the SIM card on the screen.

Enter the PIN code of your SIM card on the screen. Check the **Store PIN** box to store the PIN. Thus, this Router will remember the PIN code.

Click on **Change PIN Code** if required by your ISP. The following screen will appear. Click **Apply** to save your setting.

🙆 http://192.168.2.1/index3.stm -	Windows Internet Explo	rer						
🔾 🗢 🗢 🙋 http://192.168.2.	1/index3.stm		🝷 😽 🗙 🚼 Google	۰ م				
File Edit View Favorites T	ools Help							
× Google		🖌 🔧 Search 🔹 🖗 🛪 👘 🖉 🧟 🔹 💷 Sidewiki 🔹 🦃 Check 🍷 🧏 AutoF	Fill • 🌽	🔌 🔹 🥚 Sign In 🔹				
🔆 Favorites 🌈 http://192.168	8.2.1/index3.stm							
START	DATA	EXTRAS		LOGOUT				
HSPA Modem	UMTS-Stick			Â.				
Password Settings	The DSL EasyBox	enables a connection with a UMTS-Stick for Internet and Voice over the UM	WTS mobile network. Please insert the	SIM card into the device				
Time Settings	before power on. Or	ce done, please enter the PIN code of the SIM card here.						
Remote Management	PIN Code (for SIM	card)	N Code					
Firmware Upgrade	1	Change PIN Code - Windows Internet Explorer						
Diagnostic Utility	See Chatra	http://192.168.2.1/usb_setpin.stm						
Reboot	2 Status	Change PIN Code						
UPNP	adding Available (V	onango i ni oodo						
	UMTS connectio	You change the PIN code for your SIM-card						
	D	Please enter current PIN code						
	Backup-connection	Please enter new PIN code						
	APN	Double check new PIN code						
	Phone Number							
	Idle Time (Minute	→ Apply → Cancel						
	User Name							
	Password							
	Confirm Passwor	Contract Destantial Marks On	- @ 100% -					
		Themes Protected Mode: On Va						
		(→ Apply → Cancel ?					
Printware version:20.03.302t2				-				

See the following table for additional parameters that needs to be configured.

Parameter	Description
Backup connection	This sets how the UMTS connection is used primarily.
APN	Access Point Name, this is the name used to identify a general packet radio service (GPRS) bearer service in the GSM mobile network. The APN defines the type of service that is provided in the packet data connection. This information should be provided by your ISP.
Phone Number	This is the number to dial to connect to your ISP. This information should be provided by your ISP.

Parameter	Description
Idle Time (Minutes)	This is the time period in which there is no Internet connection activity before the mobile connection goes to automatic termination.
User Name/ Password	Enter user name and password.
Confirm Password	Enter your password again.

The service information is displayed in the **Network Operator** section on the screen. Click **Rescan/Refresh** to update the information.

6 http://192.168.2.1/index3.stm -	Windows Int	ernet Explorer			- 2 -
Solution = 2 http://192.168.2.1/index3.stm				🕶 😽 🗙 🚼 Google	+ م
File Edit View Favorites	Tools Help				
× Google		💽 🔧 Search 🔹 🛷 🖉 📲 📲	🕸 • 🔲 Sidewiki • 🏾 🖑 Check • 🧏 AutoFill •	• 🤌	🔩 🔹 🧼 Sign In 🔹
🚖 Favorites 🏾 🏉 http://192.16	58.2.1/index3.:	stm			
START	DAT	TA EXTRAS			LOGOUT
HSPA Modem				Apply Cancel ?	
Password Settings					
Time Settings					
Remote Management					
Diagnostic Utility	Networ	k Operator			
Reboot	Select	Network Operator	Status	Service	
UPnP	۲	Automatic (UMTS preferred)	-	-	
	\odot	Chunghwa Telecom(46692)	current	UMTS	
	\odot	Chunghwa Telecom(46692)	available	GSM	
		Far EasTone(46601)	forbidden	UMTS	
	0	TW Mobile(46697)	available	GSM	
		Far EasTone(46601)	forbidden	GSM	
	\odot	TW Mobile(46697)	available	UMTS	
	0	VIBO(46689)	available	UMTS	-
	→ Resc	an			
			→ Refresh	→ Apply → Cancel	
Einneren Version 20.03.30212					
					-

Select your telecommunications service and click $\ensuremath{\mathbf{Apply}}$ for the HSPA connection.

Password Settings

6 http://192.168.2.1/index3.stm -	Windows Internet Explorer		- \$ *			
🕒 🕞 🗢 🙋 http://192.168.2.	ۍ م					
File Edit View Favorites T	ools Help					
× Google 192.168.2.1	💽 🚼 Search 🔹 🛷 🔹 🛖 🔹	🔊 • 🔲 Sidewiki • 🛛 🍄 Check • 📔 AutoFill • 🌛 💽 192.168.2.1	🔌 🔹 🧼 Sign In 🔹			
👷 Favorites 🛛 😪 🔹 🏉 http://	/192.168.2.1/inde 🗙 🌈 Internet Explorer cannot di					
START	DATA EXTRAS		LOGOUT			
HSPA Modem	Login Settings					
Password Settings Time Settings	Set a username/password to restrict management access to the router. If you want to manage the router from a remote location (outside of the local network), you must also specify the IP address of the remote PC. You can do this in the Remote Management menu.					
Remote Management	Login Account (Leave this table empty if you don't	t wish to change anything)				
Diagnostic Utility	Current Username					
Reboot	New Usemame					
UPnP	Current Password					
	New Password					
	Re-Enter Password for Verification					
	Login Parameter					
	Idle Time Out	10 Min (Idle Time =0 : NO Time Out) (10)				
		• Apply • Cancer				
Firmware Version:20.03.302t2						



>> Note: If you lost the password, or you cannot gain access to the user interface, press the reset button on the rear panel, holding it down for at least 10 seconds to restore the factory defaults. The default user name is **root**, and password is 123456.

Use this screen to change the password for accessing the management interface. Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

Time Settings

6 http://192.168.2.1/index3.stm	 Windows Internet Explore 	r				
🔾 🗢 🖉 http://192.168.	2.1/index3.stm			🗝 🔩 🗙 🚼 Google	. م	
File Edit View Favorites	Tools Help					
× Google 192.168.2.1	-	🛾 🚼 Search 🔹 🖗 🍏 🔹 🛖	🔹 📓 • 🔲 Sidewiki • 🍄 Check • 🧏 A	utoFill 🔹 🌽 🔩 192.168.2.1	🔩 🔹 🧼 Sign In 🔹	
👷 Favorites 🛛 😸 🔹 🏉 http	://192.168.2.1/inde × 👔	🧉 Internet Explorer cannot o	i			
START	DATA	EXTRAS			LOGOUT	
HSPA Modem	Time Settings					
Password Settings	Set Time Zone:					
Time Settings	Lico this setting to in	sure the time based client	filtering feature and sustem leg optrios are	baced on the correct localized time		
Remote Management	Use this setting to m	sure the time-based client	intening reactive and system log entries are	based on the conect localized time.		
Firmware Upgrade	(GMT+01:00)Amsterd	am, Berlin, Bern, Rome, St	ockholm, Vienna 👻 ((GMT+01:00)Amsterdam. B	erlin, Bern, Rome, Stockholm, Vienna)		
Diagnostic Utility						
Reboot	Configure Time Serve	Configure Time Server (NTP):				
UPnP	You can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet.					
	Enable Automation	: Time Server Maintenanc	e ([V])			
				Annlu ACancel 2		
				Abbit Acaucal :		
Firmware Version:20.03.302t2						

Select your local time zone from the drop down list. This information is used for log entries and client filtering.

For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down list.

If you want to automatically synchronize the Broadband Router with a public time server, check the **Enable Automatic Time Server Maintenance** box.

Click Apply.

Remote Management

By default, management access is only available to users on your local area network. However, you can also manage the Broadband Router from a remote host by entering the IP address of a remote computer on this screen.



Note: If you check Enabled and specify an IP address of 0.0.0.0, any remote host can manage the Broadband Router. Check the **Enabled** box, and enter the IP address of the **Host Address** and **Port Number**, then click **Apply**.

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by: 8080, for example, 211.20.16.1:8080.



Firmware Upgrade

6 http://192.168.2.1/index3.stm -	Windows Internet Explorer		- 6 💌		
🕒 🗢 🔻 🙋 http://192.168.2.	1/index3.stm	🗸 😽 🗙 Google	+ ۹		
File Edit View Favorites T	ools Help				
× Google 192.168.2.1	💌 🚼 Search 🔹 🛷 🐲 📲 🔹 🧕	🕽 = 🔲 Sidewiki = 🛛 🖑 Check = 🧏 AutoFill = 🌽 🗔 192.168.2.1	🔩 🔹 🥥 Sign In 🔹		
👷 Favorites 🛛 😸 🔹 🏀 http://	/192.168.2.1/inde × 🎉 Internet Explorer cannot di				
START	DATA EXTRAS	LO	GOUT		
USDA Markan	Firmware Upgrade		*		
HSPA Modem					
Password Settings	This tool allows you to upgrade the router firmware u	sing a file provided by us. You can download the latest firmware from http://www.arcadyan.co	<u>ш</u>		
Time Setungs	Enter the path and name, or browse to the location,	of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade	to complete		
Remote Management	the process.				
Ciananatia Utility	Firmware File	Browse			
Diagnosuc ounty					
Hebool		→ Apply → Cancel ?			
OPHP					
	Backup Configuration of Arcadyan-IAD				
	Selecting "Backup" allows you to create and care a	backup conv of this Arcadvan IAD's configuration on your local bard drive			
	Selecting Dackup allows you to create and save a	backup copy of this Arcadyan-Ab a complication on your local hard only.			
		→ Backup ?			
	Restore Configuration of Arcadvan-JAD				
	Restore Conniguration of ArCadyan-IAD Choose the path and name of the backup file, then click the "Apply" button. You will be prompted to confirm the backup restoration.				
	Restore from saved Configuration file	Browse			
	Notoro nom sarea comgaration me				
		→ Apply → Cancel ?			
Einmutate Vertice: 20.03.30212	Restore to Factory Defaults				
			-		


• Firmware Upgrade: this allows you to upgrade to the latest firmware.

To update the firmware:

- 1. Download the upgrade file from company web site, and save it to your hard drive.
- 2. Then click **Browse...** to look for the downloaded file. Click **Apply** to begin the upgrade.
- HSPA Modem Firmware Upgrade:

To update the HSPA firmware:

- 1. Remove the SIM card from the jack slot.
- **2.** Download the upgrade file from company web site, and save it to your hard drive.
- **3.** Then click **Browse...** to look for the downloaded file. Click **Apply** to begin the upgrade.
- Check the **Status** screen **Information** section to confirm that the upgrade process was successful.
- Backup Configuration of Broadband Router: this allows you to save the system configuration to a file. To backup the configuration file, just click the **Backup** button on the screen.
- Restore Configuration of Broadband Router: this function is used to restore the previously saved backup configuration file. To restore the configuration file: click **Browse...** to locate the previously saved file.
- Restore to Factory Defaults: this resets the Broadband Router back to the original default settings. Click the **Restore** button to restore the default factory settings. Note that all of the user configurations and settings will be lost.



>> Note: Be sure to remove the mobile SIM card from the slot before click on the Restore button.

Diagnostic Utility

This tool allows you to test network connection status. You can specify a domain name or a valid IP address of the remote host for ping test.

6 http://192.168.2.1/index3.stm - 1	Windows Internet Explorer				
🔾 🗢 🖉 http://192.168.2.	1/index3.stm		- + × 猪	Google	. م
File Edit View Favorites To	ools Help				
× Google	•	🛃 Search • 🕂 🛷 • 👘 • 🔯 • 🔲 Sidewiki • 🛛 🍄 Check • 🧏 AutoFill •	· 🤌		🔌 🔹 🥚 Sign In 🤊
👷 Favorites 🏾 🌈 http://192.168	3.2.1/index3.stm				
START	DATA	EVTRAC			LOCOUT
START	DAIA	EATRAS			200001
HSPA Modem	Diagnostic Utility				
Password Settings	This tool allows you to test.	capture and/or test your network's connection status. You can specify a d	lomain name or a val	lid IP addres	s of the remote host for ping
Remote Management	WAN Desket Centure				
Firmware Upgrade	White Packet Capture				
Diagnostic Utility	Target Interface	UMTS-Stick			
Reboot	Ping Test				
UPnP	i nig root				
	Destination Address	→ Execute			
	Execution Result		Destination IP Address 192.	168.2.100	
	Test Result	Reply from 192.168.2 100; bytes=32 time=11ms Reply from 192.168.2 100; bytes=32 time=10ms Reply from 192.168.2 100; bytes=32 time=10ms Reply from 192.168.2 100; bytes=32 time=10ms Ping statistics for 192.168.2 100; bytes=32 time=10ms Approximate round trip times in milli-seconds: Mamimum = 10ms, Maximum = 11ms, Newlige = 10ms			
				?	
Firmware Version:20.03.302t2					

• WAN Packet Capture: select the interface, start/stop capturing, then download the file.

http://192.168.2.1/index3.stm -	Windows Internet Explore	r			- 2 -				
G V • E http://192.168.2	▼ 🌴 🗙 🚰 Google	، م							
File Edit View Favorites 1	fools Help								
x Google		Search • 🕈 🍏	🕽 • 👘 • 🔯 • 🔍 Sidewiki • 🍼 Check • 🍗 AutoFil	d • 🌽	🖏 🔹 🥌 Sign In 🔹				
👷 Favorites 🏾 🌈 http://192.16	8.2.1/index3.stm								
START	DATA	EXTRAS			LOGOUT				
HSPA Modem	Diagnostic Utility	/							
Password Settings	This tool allows you to	o capture and/or te	est your network's connection status. You can specify a	a domain name or a valid IP address of the	remote host for ping				
Time Settings	test.								
Remote Management	WAN Packet Capture								
Firmware Upgrade	Target Interface	UMTS-Stick	→ Start → Stop →						
Reboot	-	File Drawload							
UPnP	Ping Test		Designed to see the state of the o						
	Destination Address		bo you want to open or save this me :						
			Name: pktDump.cap Type: HTML Document	tion					
	Execution Result		From: 192.168.2.1	ess 192.168.2.100					
		Reply from 19 Reply from 19	Open Save C	Cancel					
	Test Result	Reply from 19							
		Ping statistics	While files from the Internet can be useful, some files can	octentially					
		Packets: Sen Approximate r	ham your computer. If you do not trust the source, do not save this file. What's the risk?	open or					
		Minimum = 10							
				_					
				?					
Firmware Version:20.03.302t2									

• Ping Test: enter the destination address, then click the execute button. The result will be displayed on the Execution Result field.

Reboot

Click **Reboot Router** to reboot the Router, if the device becomes unresponsive. The reboot will be completed when the power LED stops blinking.



UPnP



The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.

UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the office, home and everywhere within your network.

Product Specifications

IEEE Standards

IEEE 802.3 10 BASE-T Ethernet IEEE 802.3u 100 BASE-TX Fast Ethernet IEEE 802.3, 802.3u, 802.11g, 802.1D

Mobile Standards

GSM 850, 900, 1800,1900 WCDMA 850, 900,1900, 2100 AWS Band HSDPA 7.2: Category 7 HSUPA 5.76 : Category 6

LAN Interface

4 RJ-45 10 BASE-T/100 BASE-TX ports: Auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half-duplex or full-duplex

WAN Interface

One RJ-11 FXS port

ADSL Features

Supports DMT line modulation

Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 &T1.413, Issue 2) and ADSL2 (G.992.3) and ADSl2+ (G.992.5) Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream

Dying GASP support

ATM Features

RFC1483 Encapsulation (IP, Bridging and encapsulated routing) PPP over ATM (LLC &VC multiplexing) (RFC2364) Classical IP (RFC1577) Traffic shaping (UBR, CBR) OAM F4/F5 support PPP over Ethernet Client

Indicator Panel

Voice mail, Mobile, WLAN, Internet, Phone, LAN 1~4 (on the rear panel)

Dimensions

188 x 185 x 33 mm (7.40 x 7.28 x 1.30 in)

Weight

0.285 kg (0.764 lbs)

Input Power

 $9 \mathrm{V} 1 \mathrm{A}$

Power Consumption

8 Watts maximum

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS Firewall – Client privileges, hacker prevention and logging, Stateful Packet Inspection Virtual Private Network – PPTP, L2TP, IPSec pass-through, VPN pass-through

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 783 TFTP, RFC 1661 PPP, RFC 1866 HTML, RFC 2068 HTTP

Radio Features

Wireless RF module Frequency Band

- 802.11n Radio: 2.4GHz
- 802.11g Radio: 2.4GHz
- 802.11b Radio: 2.4GHz
- USA FCC: 2412~2462MHz (Ch1~Ch11)
- Canada IC: 2412~2462MHz (Ch1~Ch11)
- Europe ETSI: 2412~2472MHz (Ch1~Ch13)
- Japan STD-T66/STD-33: 2412~2484MHz (Ch1~Ch14)

Modulation Type

OFDM, CCK

Operating Channels IEEE 802.11n Compliant:

11 channels (US, Canada, Europe, Japan)

Operating Channels IEEE 802.11g Compliant:

11 channels (US, Canada) 13 channels (Europe, Japan)

Operating Channels IEEE 802.11b Compliant:

11 channels (US, Canada)13 channels (Europe)14 channels (Japan)

Standards Compliance

Safety: LVD

Environmental

CE Mark

Temperature

Operating 0 to 40 °C (32 to 104 °F) Storage -40 to 70 °C (-40 to 158 °F)

Humidity

5% to 95% (non-condensing)

Vibration

IEC 68-2-36, IEC 68-2-6

Shock

IEC 68-2-29

Drop

IEC 68-2-32

Compliance

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

Technical Support Information

Taiwan Headquarter Address: 4F, No.9 Park Avenue II, Science Park, Hsinchu, Taiwan TEL: +886 3 5787000 FAX: +886 3 5637326 Sales : sales_hq@arcadyan.com Press contact : press_hq@arcadyan.com Employment : hr_hq@arcadyan.com EU Sales Office Address: Hauptstrasse 30, 65760 Eschborn, Germany TEL: +49 (0)6196 - 7693133 FAX: +49 (0)6196 - 8871870 Sales: sales_eu@arcadyan.com

US Sales Office

Address: Suite 110, 2160 Lundy Ave., San Jose, CA 95131

TEL: +1 408 548 9950

FAX: +1 408 747 1091

Sales: sales_us@arcadyan.com