Router 3G Ethernet

- Router with **built-in 3G HSUPA** embedded module
- Router with **WAN Ethernet** interface
- WAN/3G automatic **BackUP**
- Wireless LAN 11N up to 300Mps



3G Router AM11

User's Guide rev. 1.1 03/2014

3G embedded module

INFORMATION ABOUT THE USE OF THIS WIRELESS DEVICE (Radio LAN)

This equipment complies with the essential requirements and other principles according to 1999/5/CE Directive.

As per art. 6.3 of D.Lgs. 9.5.01 n. 269 we inform that the use of this device is regulated by:

- D.Lgs 1.8.2003, n.259, art.104 (activities subject to general authorization) and art.105 (free use) for private use.
- D.M. 28/5/03 for the public supply of R-LAN access to the networks and telecommunication services.

REGULATORY DOMAIN SETTING (usable channels)

The products are supplied with the setting of Regulatory Domain for the European Community (ETSI). The Regulatory Domain defines which channels can be used in that specific local context (country or list of countries).

For the devices that allow the modification of such a setting, the user must make sure of not to break the limitations on the use of channels (and relative powers) applicable in the country.

DECLARATION CE OF CONFORMITY

We, Digicom S.p.A., with registered office at Cardano al Campo (VA - Italy) - Via Volta 39, declare under our sole responsibility, that the products named **3G Router AM11** to which this declaration refers to, satisfy the essential requirements of following Directive:

- 1999/5/CE 9th March 1999, R&TTE (concerning radio equipment and telecommunication terminal equipment and the acknowledgment of their conformity) Law Decree 9th May 2001, n.269, (G.U. n. 156 of 7-7-2001).

As indicated in conformity with the requirements of following Reference Standards or of other regulations documents:

EN 301 489-1	EN 301 489-17	EN 301 489-7	EN 301 489-24	
EN 301 908-1	EN 50385	EN 301 511	EN 300 328	EN 60950-1

CE

INDEX

RES FR	TRICTION OF USE OF WIRELESS RADIO EQUIPMENT USIN REQUENCY BAND	IG THE 2.4GHZ ISM 2
DEC		2
1.0	INTRODUCTION	4
1.1	PACKAGE LIST	4
1.2	HARDWARE INSTALLATION	5
2.0	CONFIGURATION	10
	2.1 Wizard	
	2.2 Advanced Setting	
	2.2.1 Basic Setting	
	2.2.2 Forwarding Rules	
	2.2.3 Security Setting	
	2.2.4 Advanced Settings	
	2.2.6 SMS	
	2.2.7 Tool Box	54

1.0 Introduction

Congratulations on your purchase of this outstanding **3G Router 11 AM**. The device is a HSPA router with built-in HSUPA embedded module. It supports NAT, routing, firewall, VPN pass-through, auto-3G-dial-up backup connection, DHCP server, and so on. And is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Package List

items	Description	Quantity
1	WiFi Mobile Broadband	1
	Gateway	
2	Power adapter 12V 2A	1
3	CD	1

1.2 Hardware Installation

Hardware configuration



* Not Supported on 3G Router 11AM



LED indicators

	LED status	Description	
Status	Green in flash	Device status is working.	
	Red in flash	Disconnected. No SIM card / signal or unverified PIN code	
	Amber in flash	Connecting.	
	Red	Connected. Signal strength in level one (weak)	
	Red in quick flash	Roaming alert, and 3G signal is weak	
3G Signal Strength LED	Amber	Connected. Signal strength in level two or three (middle)	
	Amber in quick flash	Roaming alert, and 3G signal is middle	
	Green	Connected. Signal strength in level four or five (strong)	
	Green in quick flash	Roaming alert, and 3G signal is strong	

2G/2.5G LED	Green	EDGE or GPRS connection is established		
	Green in flash	Data packet transferred via 2G/2.5G		
3G/3.5G LED	Green	UMTS/HSDPA/HSUPA connection is established		
	Green in flash	Data packet transferred via 3G/3.5G		
SMS LED	Green	SMS storage is full		
	Green in flash	There is any unread SMS in the storage		
WAN LED	Green	RJ45 cable is plugged		
	Green in flash	Data access		
	Green	RJ45 cable is plugged		
	Green in flash	Data access		
	Green	WLAN is on		
WiFi LED	Green in flash	Data access		
	Green in fast flash	Device is in WPS PBC mode		

How to operate

Step 1. Attach the antenna.

1.1. Remove the antenna from its plastic wrapper.

1.2. Screw the antenna in a clockwise direction to the back panel of the unit.1.3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.

1.4. And rip the "USIM/SIM & PWR" sign label from "Pull" tag.



1.Turn off the Power Switch first.

2.DO NOT connect WiFi HSPA IAD to power before performing the installation steps below.

Step 2. Insert SIM/USIM to IAD.

NOTE: 2.1. The WiFi HSPA IAD builds in a HSUPA 3G modem card. Please refer to your service provider for detailed feature information.

2.2. A 3G SIM/USIM Card with services is MUST, the Data service and the Voice service.





Step 3. Insert the RJ11 cable for a Phone:

.You can make and receive 3G phone calls by a RJ-11 Phone.

* RJ-11 Port is not supported on 3G Router 11AM.

Step 4 Insert the Ethernet cable into LAN Port:

Insert the Ethernet patch cable into LAN port on the back panel of the WiFi HSPA IAD, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.

Step 5 Insert the Ethernet patch cable into Wired WAN port:

Insert the Ethernet patch cable into Wired WAN port on the back panel of the WiFi HSPA IAD.

NOTE: The step does not need if you select the 3G Wireless WAN.

Step 6. Power on the IAD:

6.1. Connect the power adapter to the receptor on the back panel of your WiFi HSPA IAD.

6.2. Then plug the other end of the power adapter into a wall outlet or power strip.6.3. Turn on the Power Switch.



Step 7. Complete the setup.

7.1. All LEDs will transient illumination to indicate power has been applied.
7.2. And then LEDs will flash ON and OFF as the Wifi HSPA IAD performs initialization and Internet connection processes. This will take a few minutes.
7.3. When complete, the Status LED will flash.



2.0 Configuration

2.1 Wizard

Type in the IP Address (<u>http://192.168.123.254</u>)

Type password, the default is "admin" and click 'login' button.

	WiFi HSPA I	AD (R0.03a1)	
D USER'S MAIN MENU	-1 Status		_
	System Password :	(default: admin) Login	

Select your language.

	WIFTHS	SPA IAD (R0.0	3a1)	English .
- ADMINISTRATOR'S MAIN MEMU	-fi Status	W Wittend	CIII Advanced	English 変種中文 第後中文 English Desbich
G Please Select the Operation	s []			
		Winterd		
	0	Advance Setup		
.,	hin screen reminds yo	Enter	he Wizard is finished.	

Press "Wizard" for basic settings with simple way.

	WIEI HS	SPA IAD (R0.0	(3a1)	English
DMINISTRATOR'S MAIN MENU	-fit Status	W Weard	NB Advanced	+ Lopou
Please Select the Operation	6			
		Wizard		
	e	Advance Setup		
	his screen reminds yo	e to configure until	the Witzard is finished.	

Press "Next" to start wizard.



wizard

Step 1: Set up your system password.

	WIFI HSPA IAD (R0.03a1)			English	
ACHINISTRATOR'S MAIN HEND	- Status	W Witzerd	11 Advanced	+ Lopo	
💷 Setup Waxed - Setup Login Pa	ssword			(EXIT)	
	OldPassward				
	New Password				
	Poeconam				
Start =	Password > Time >	LAROWAR > WIG	loss'> Summary > Finisht]	Nad +	

Step 2: Select Time Zone.

		or rear freedo		
CORRESTRATOR'S MADE BEING	-A Status	W Witserd	Will Advanced	+ Lo
[
D Setup Wixerd - Setup Time Zoo	w :			[ENIL]
104/7	08-00 Toisai		21	
(Gain	roe.co) raper			
	23	Talast Casta		
	8	Detect Agen		

Step 3: Select Wan Type.

Auto Detecting or Setup Manually.



Setup the LAN IP and WAN Type.

WIFI HSPA IAD (R0.03a1)			3a1)	English	
ADMINISTRATOR'S HAIN MENU.	-1 Status	W Witterd	becrevbå IIC?	> Loga	
😅 Setup Wizard - Select WAII Typ	0).			(EuT)	
+ LAN IP Address	19	2 168 123 254			
 WWW Interface 	10	roless WWN +			
WAN TIDE	34				
<back [="" start=""> P</back>	assword > Time >	LAN/WAN > Wire	iess > Semmary > Fisical)	Ned>	
Rummerfactorization	0.00033420000000			-	

Example:

Step 4: Please fill in 3G service information which is provided by your ISP.

Step 5: Set up your Wireless.

	WIFI HSPA IAD (R0.03a1)	English
DMINISTRATOR's MAIN MEAU	-A Status W Wound 100 Advanced	+ Log
G Selap Woard - Wroless sellings		(EXIT)
• Wireless Bodale	Enable Disable	
 Network ID(SSID) 	clofault	
Channel	11 -	
* Back Starl * Pas	secord > time > LANIWAN > Wireless > Sommary > to	Not -



🛛 Setup Waard - Wreless settings		_				t meri
Authentication	A480			•		
 Encryption 	WEP	٠				
WEP Kay 1	HEX	٠	1234567890			
C WEP Kay 2	HEK	•	1234567890			
C WEP Key 3	HEG	٠	1234567890			
C WEP Kay 4	HEX	٠	1234567890			

Step 6: Then click Apply Setting. And then the device will reboot.

ADMINISTRATOR'S HAIN MERU	-B Sizian	W Winard	(B Advanced	> Logo
😂 Setup Wizard - Summary				(ENT)
75	Please confi	rm the information	tion below	
6	WAN Setting [
V	WN Type	36		
	PN	internet		
8	W Code			
0	saled Number	199#		
U.	sename	guest		
9	browese			
t	Whekas Setting]			
v	fireless	Enable		
5	50	default		
0	hannel	11		
,	athentication	Auto (Open	(Shared)	
E	acryption	WEP		
v	VEP Key	123456785	90	
	Do you want	to proceed the nets	rork testing?	

Step 7: Click Finish to complete it.

ADMINISTRATOR'S MAIN NEW	WFIHSPAIAD (R0.03a1) - Hi Status VV What 1 18 Advanced	English • • Logos
😂 Setup Wicard - Apply settings		112011
	Configuration is Completed. Please clor: 'Finish' to sack to Status sage.	

2.2 Advanced Setting

2.2.1 Basic Setting



1. Network Setup

		WIFI HSPA IAD	(R0.03a1)		English 🔻
D ADMINISTRATOR'S MAIN ME	NU - 1 1	Status 💔 Wiza	rd 🕅 Advanced		► Logout
	ORWARDING RULES	SECURITY SETTING		🕜 Voice 🖂 S	MS
Network Setup	LAN Setup			an atu	
DHCP Server		Item		Setting	
Wireless	LAN IP Addres	SS 1	92. <mark>1</mark> 68.123.254		
Change Password	Subnet Mask	2	55.255.255.0		
	Internet Setu	ıp			[HELP]
	WAN Interface	E	Ethernet WAN 👻		
	• WAN Type	V	Vireless WAN		

- 1. **LAP IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
- 2. Subnet Mask: insert 255.255.255.0
- 3. WAN Interface: Select Ethernet WAN or Wireless WAN to continue.

WAN Type	Static IP Address 💌
Activate WWAN for Auto-Failover	Static IP Address Dynamic IP Address PPP over Ethernet ve: PPTP
WAN IP Address	L2TP

4. **WAN Type**: WAN connection type of your ISP. You can click WAN Type Combo button to choose a correct one from the following options:

A. Static IP Address:

	WiFi HSPA	IAD (R0.03a1)	English 😽
O ADMINISTRATOR'S MAIN MEN	U 🚽 A Status 💔	Wizard Cill Advanced	+ Logout
	RWARDING RULES 🐵 SECURITY SET	TING 🏠 ADVANCED SETTING 🌈 Voice 🖂 SMS	TOOLBOX
- Network Setup	LAN Setup		-
· DHCP Server	llem	Setting	
• Wireless	LAN IP Address	192.168.123.254	
Change Password	Subnet Mask	255 255 255 0	
	Internet Setup		[HELP]
	WAN Interface	Ethernet WAN 🐱	
	WAN Type	Static IP Address	
	Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:	
	VIAN IP Address		
	• WAN Subnet Mask		
	WAN Gateway		
	Primary DNS		
	Secondary DNS		
	NAT disable	Enable	
		Save Undo	

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

B. Dynamic IP Address:

	WiFi HSPA	IAD (R0.03a1)	English 💊
O ADMINISTRATOR'S MAIN M	ENU 🚽 Status 🖤	Wizard 🔨 🕅 Advanced	+ Logour
De Basic Setting	FORWARDING RULES SECURITY SET	ING 1 ADVANCED SETTING 1 Voice SM	s (2) TOOLBOX
Network Setup	LAN Setup		
DHCP Server	Item	Setting	
+ Wireless	LAN IP Address	192.168.123.254	
Change Password	Subnet Mask	255.255.255.0	
	U Internet Setup		[HELP]
	+ WAN Interface	Ethernet WAN	
	• WAN Type	Dynamic IP Address 💌	
	Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:	
	+ Host Name	(optional)	
	ISP registered MAC Address	Cione	
	Connection Control	Connect-on-Demand	
	+ NAT disable	Enable	
		[Save] Undo	

- 1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
- 2. Host Name: optional, required by some ISPs, for example, @Home.
- 3. ISP register MAC address: You can change the WAN port MAC address, it is your ISP assigned to you.
- 4. Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

5. NAT disable: the option bridges data form WAN port to LAN port.

C. PPP over Ethernet

	WiFi HSPA	IAD (R0.03a1) English
BASIC SETTING	WARDING RULES SECURITY SETT	ING M ADVANCED SETTING C Voice SMS 1
Network Setup	LAN Setup	
DHCP Server	Item	Setting
• Wireless	LAN IP Address	192.168.123.254
Change Password	Subnet Mask	255.255.255.0
	Internet Setup	[HELP]
	► WAN Interface	Ethernet WAN 👻
	► WAN Type	PPP over Ethernet
	Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:
	PPPoE Account	
	PPPoE Password	
	Primary DNS	
	Secondary DNS	
	Connection Control	Connect-on-Demand -
	Maximum Idle Time	600 seconds
	PPPoE Service Name	(optional)
	Assigned IP Address	(optional)
	▶ MTU	0 (0 is auto)
	NAT disable	Enable
		Save Undo

- 1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
- PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
- 3. Primary DNS/ Secondary DNS: This feature allows you to assign a Primary/Secondary DNS Server, contact to your ISP to get it.
- 4. Connection Control: There are 3 modes to select:
 - **Connect-on-demand**: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

- 5. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.
- 6. PPPoE Service Name: optional. Input the service name if your ISP requires it.

Otherwise, leave it blank.

- 7. Assigned IP address: Optional, Input the IP address you want. Usually, leave it blank.
- 8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).
- 9. NAT disable: the option bridges data form WAN port to LAN port

	WiFi HSPA	IAD (R0.03a1)		English 👻
D ADMINISTRATOR'S MAIN MENU	🚽 Status 💔 V	Vizard 🕅 Advance	ed	► Logout
BASIC SETTING 🥺 FOR	WARDING RULES 🥝 SECURITY SETTI	ING 🌀 ADVANCED SETT	ING 🌈 Voice 🖂 SMS	TOOLBOX
Network Setup	LAN Setup			
DHCP Server	Item		Setting	
• Wireless	LAN IP Address	192.168.123.254		
Change Password	 Subnet Mask 	255.255.255.0		
	Internet Setup			[HELP]
	WAN Interface	Ethernet WAN 👻		
	WAN Type	PPTP 🔻		
	Activate WWAN for Auto-Failover	Enable Remote Host for keep a	live:	
	▶ IP Mode	Dynamic IP Address 👻	-	
	My IP Address			2
	My Subnet Mask			
	Gateway IP			
	Server IP Address/Name			2
	PPTP Account]	
	PPTP Password	••••]	
	Connection ID		(optional)	
	Maximum Idle Time	600 seconds		
	Connection Control	Connect-on-Demand	•	
	▶ MTU	0 (0 is auto)		
		Save Undo		

D. PPTP

First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

- 1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
- 2. My IP Address, My Subnet Mask and WAN Gateway IP: the private IP address, subnet mask and Gateway IP your ISP assigned to you.
- 3. Server IP Address/Name: the IP address or URL of the PPTP server.
- 4. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
- 5. Connection ID: optional. Input the connection ID if your ISP requires it.

 Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable "Auto-reconnect" to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

E. L2TP

	WiFi HSPA	IAD (R0.03a1)	English 🔻
D ADMINISTRATOR'S MAIN M	IENU 📲 Status 💔 I	Vizard M Advanced	► Logout
BASIC SETTING	FORWARDING RULES SECURITY SETT	ING 🍿 ADVANCED SETTING 🌈 Voice 🗵	sms 🔂 Toolbox
Network Setup	LAN Setup		
DHCP Server	Item	Setting	
• Wireless	LAN IP Address	192.168.123.254	
Change Password	Subnet Mask	255.255.255.0	
	Internet Setup		[HELP]
	WAN Interface	Ethernet WAN 👻	
	▶ WAN Type	L2TP •	
	Activate WWAN for Auto-Failover	Enable Remote Host for keep alive:	
	▶ IP Mode	Dynamic IP Address 👻	
	▶ IP Address		
	Subnet Mask		
	WAN Gateway IP		
	Server IP Address/Name		
	L2TP Account		
	L2TP Password	•••••	
	Maximum Idle Time	600 seconds	
	Connection Control	Connect-on-Demand 🔻	
	▶ MTU	0 (0 is auto)	
		Save Undo	

First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

- Activate WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
- 2. IP Address, Subnet Mask and WAN Gateway IP: the private IP address, subnet mask and Gateway IP your ISP assigned to you.
- 3. Server IP Address/Name: the IP address or URL of the PPTP server.
- 4. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
- Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable "Auto-reconnect" to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.
- Connection Control: There are 3 modes to select: Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

Or select Wireless WAN for 3G Setting.

		WIFI HSPA IAD	0 (R0.03a1)			English
D ADMINISTRATOR'S MAIN I	AENU 🥠	Status 💔 Wiza	rd M Advanced			► Logou
BASIC SETTING	FORWARDING RULES	SECURITY SETTING	M ADVANCED SETTING	C Voice	🖂 SMS	TOOLBO
Network Setup	LAN Setup					
DHCP Server		Item		Setting		
• Wireless	LAN IP Addres	ss 1	92.168.123.254			
Change Password	Subnet Mask	2	255.255.255.0			
	Internet Set	up				[HELP]
	WAN Interface		Wireless WAN 🔻			
	► WAN Type	N E	Vireless WAN Ethernet WAN			

F. 30

ADMINISTRATOR'S MAIN MEN	IU 📲 Status 🕅	Wizard Witanced + Logo
BASIC SETTING	DRWARDING RULES 🚱 SECURITY SE	TTING M ADVANCED SETTING C Voice SMS 🔂 TOOLBO
Network Setup	LAN Setup	
DHCP Server	Item	Setting
Wireless	LAN IP Address	192.168.123.254
Change Password	Subnet Mask	255.255.255.0
	Internet Setup	[HELP]
	► WAN Interface	Wireless WAN 🔻
	WAN Type	3G -
	▶ Dial-Up Profile	C Auto-Detection Manual
	▶ Country	Taiwan
	▶ Telecom	Chunghwa Telecom 👻
	▶ 3G Network	WCDMA/HSPA -
	► APN	internet (optional)
	PIN Code	(optional)
	Dialed Number	*99#
	► Account	(optional)
	▶ Password	••••• (optional)
	Authentication	Auto PAP CHAP
	Primary DNS	(optional)
	Secondary DNS	(optional)
	Prefer Service Mode	Auto Mode 🔻
	Connection Control	Auto Reconnect (always-on) 🔻
	Allowed Connection Time	Always By Schedule
	▶ Keep Alive	 Disable LCP Echo Request Interval Max. Failure Time Times Ping Remote Host Host IP Interval Seconds

For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect with the 3G network.

Please refer to your documentation or service provider for additional information.

- 1. Dial-Up Profile: select auto or manual to continue.
- 2. Country: select your country.
- 3. Telecom: select your telecom.
- 4. 3G Network: select the 3G Network.

- 5. APN: Enter the APN for your PC card here.(Optional)
- 6. Pin Code: Enter the Pin Code for your SIM card(Optional)
- 7. Dial-Number: This field should not be altered except when required by your service provider.
- 8. Account: Enter the new User Name for your PC card here, you can contact to your ISP to get it.
- 9. Password: Enter the new Password for your PC card here, you can contact to your ISP to get it.
- 10. Authentication: Choose your authentication.
- 11. Primary DNS: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it.
- 12. Secondary DNS: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it.
- 13. Connection Control: select your connection control
- 14. Keep Alive: you can diagnose your connection by it.

2. DHCP Server

		WiFil	HSPA IAD	(R0	.03a1)			English 🛩
C. ADMINISTRATOR'S MAIN MENU	-11	Status	W Wizar	d	Cill Advanced			Logout
BASIC SETTING 🛞 FOR	WARDING RULES	🙁 SECURI	TY SETTING	16	ADVANCED SETTING	C Voice	🖂 SMS	TOOLBOX
+ Network Setup	DHCP Serve	ar			ý1-			[HELP]
* DHCP Server	Item			Setting				
+ Wireless	► DHCP Server				O Disable 🖲 Enable			
Change Password	IP Pool Starting Address			100				
	IP Pool Endir	ng Address			200			
	▶ Lease Time				86400 Seconds			
	Domain Nan	18						
		Save	Undo More		Clients List.	Fixed Mapping	i	

Press "More>>",

- 1. DHCP Server: Choose either Disable or Enable
- 2. Lease Time: DHCP lease time to the DHCP client
- 3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
- 4. Domain Name: Optional, this information will be passed to the client
- Primary DNS/Secondary DNS: Optional, This feature allows you to assign a DNS Servers
- Primary WINS/Secondary WINS: Optional, this feature allows you to assign a WINS Servers
- 7. **Gateway:** Optional, Gateway Address would be the IP address of an alternate Gateway.

This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

DHCP Clients List

The list of DHCP clients shows here.

			W	IFI HSPA IAD	(R0	.03a1)				English
ADMINISTRATOR'S	MAIN MENU	-ii	Status	W Wizard	4	Cill Advanced				⊁ Logo
BASIC SETTING	S FOR	WARDING RULES	(©) 5F	CURITY SETTING	10	ADVANCED SETTING	0	/olce	🖂 sms	TOOLBO
Network Setup		DHCP Client	s List		_			_		
DHCP Server Wireless		IP Address	5	Host Name		MAC Address	5	Тура	Lease Time	Select
Change Password		192.168.123.100	my	chat-437abf9b		00-13-49-AA-03-17	1	Wired	23:58:13	
				Delete B:	ack (Refresh Fixed k	lapping	2		

DHCP Fixed Mapping The DHCP Server will reserve the special IP for special MAC address, shows below.

		WIFI HSPA IAD	(R0.03a1)		English -
D ADMINISTRATOR'S MAIN MENU		📲 Status 😽 Wiza	rd 🕅 Advanced		► Logout
	NARDING RULE	s 🕲 Security Setting	ADVANCED SETTING	🖌 Voice 🖂 S	MS 💽 TOOLBOX
Network Setup	Fixed M	apping			[HELP]
• DHCP Server		DHCP clients sele	ct one 👻 🕻	Copy to ID 👻	
• Wireless	ID	MAC Address		IP Address	Enable
Change Password	1	00:1F:16:B0:73:67	192	.168.123.100	
	2	2			
	3	2			
	4	2			
	5	[]		J	
	6]	
	7]	
	8	[
	9	[
	10				
		<pre><< Previo</pre>	us Next >> Save Und	Jo Back	

3. Wireless Settings

	WiFi HSPA IAD (R0.03a1) English -									
D ADMINISTRATOR'S MAIN MEN	🗅 ADMINISTRATOR'S MAIN MENU 🚽 👘 Status 🖤 Wizard 🕼 Advanced > Logo									
BASIC SETTING 😵 FO	RWARDING RULES 🛞 SECURITY SETTIN	G C ADVANCED SETTING	C Voice	🖂 sms	TOOLBOX					
Network Setup	Uireless Setting				[HELP]					
DHCP Server	Item	works works works	Setting							
• Wireless	Wireless Module	enable Disable								
Change Password	Network ID(SSID)	default								
	SSID Broadcast	Enable Disable								
	▶ Channel	11 •								
	▶ Wireless Mode	B/G/N mixed 🔻								
	► Authentication Auto ▼									
	► Encryption None ▼									
	U WPS S	ave Undo WDS Setting etup Wireless Client	 List							

Wireless settings allow you to set the wireless configuration items.

- 1. Wireless Module: The user can enable or disable wireless function
- Network ID(SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is "default")
- 3. **SSID Broadcast:** The router will broadcast beacons that have some information, including ssid so that wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.
- Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is channel 11.

The factory setting is channel 11.

- 5. Wireless Mode: Choose B/G Mixed, B only, G only, N only, G/N Mixed or B/G/N mixed. The factory default setting is B/G/N mixed.
- Authentication mode: You may select from nine kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, WPA /WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client's request automatically.

WPA-PSK

Select Encryption and Pre-share Key Mode If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits. If you select ASCII, the length of pre-share key is from 8 to 63. Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name. Select Encryption and RADIUS Shared Key If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits If you select ASCII, the length of pre-share key is from 8 to 63. Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

WPA-PSK/WPA-PSK2

Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

WDS(Wireless Distribution System) Setting WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

		WIFI HSPA IAD	(R0.03a1)			English 💌	
D ADMINISTRATOR'S MAI	N MENU 🦂	Status 💔 Wiza	rd 🔨 🕅 Advanced			Logout	
Desic Setting	FORWARDING RULES	SECURITY SETTING	C ADVANCED SETTING	C Voice	🖂 SMS	🔞 тоолвох	
* Network Setup	D WDS Set	ting				[HELP]	
* DHCP Server		ltem	Setting				
* Wireless	 Wireless 8 	Bridging	C Enable Disable				
 Change Password 	Remote Al	P MAC 1					
	Remote Al	P MAC 2	-				
	Remote A	P MAC 3					
	Remote A	P MAC 4					
	Encryption	type N	None 💌				
		din .	Save Undo Back				
	· · · · · · · · · · · · · · · · · · ·						

WPS (Wi-Fi Protection Setup)

WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

	WiFi	HSPA IAD (R0.03a1) English				
D ADMINISTRATOR'S MAIN MEN	U 🚽 Status	W Wizard 🕅 Advanced > Logout				
	RVIARDING RULLS 🕲 SECUR	STY SETTING 🌀 ADVANCED SETTING 🌈 VOICE 🖂 SMS 🔃 TOOLBOX				
 Network Setup 	WI-FI Protected Setup					
 DHCP Server 	Item Setting					
+ Wireless	• WPS					
Change Password	+ AP PIN	22458582 Generale New PIN				
	Config Mode	Registrar 🛩				
	Config Status	CONFIGURED Release				
	► Config Method	Push Button 👻				
	• WPS status	NOUSED				
		Save Trigger Cancel				

Wireless Client List

The list of wireless client is shows here.

		WiFi HSPA	(R0.03a1)			English 🗸
ADMINISTRATOR'S M	AIN MENU - 👘	Status 💔	Wizard Mil Advanced			+ Logout
BASIC SETTING	E FORWARDING RULES	SECURITY SET	TING TIN ADVANCED SETTING	C Voice	🖂 SMS	C TOOLBOX
Network Setup	D Wirele	ess Clients List				
DHCP Server		ID	ID MAC Address			
Wireless		1	1 00-0C-43-27-70-00			
Change Password			Back Refresh			

4. Change Password

				WIFI HSPA IAD	(R	0.03a1)				E	nglish 💌
O ADMINISTRATOR'S	MAIN	VENU -1	Statu	is 💔 Wiza	rd	Kill Advanced	_	_		_	+ Logout
(C) BASIC SETTING	Ś	FORWARDING RULES	0	SECURITY SETTING	16	ADVANCED SETTING	6	Voice	SW S	150	TOOLBOX
 Network Setup 		📮 Change	Passw	rord	_		_			_	
DHCP Server			Item		Setting						
* Wireless		Old Pass	word	E							
Change Password		New Pas	sword								
		Reconfirm	untima and a second sec								
					1	Save Undo					

You can change Password here. We **strongly** recommend you to change the system password for security reason.

2.2.2 Forwarding Rules

		WIFI HSPA IAD	(R0.03a1)		English 💌
D ADMINISTRATOR'S MAIN	MENU - 1 i	Status 💔 Wiza	rd 🕅 Advanced		Logout
🕷 BASIC SETTING 🥺	FORWARDING RULES	SECURITY SETTING	I ADVANCED SETTING	🕜 Voice 🖂 SMS	TOOLBOX
- Virtual Server	🗟 Forwardi	ng Rules			
 Special AP 					
Miscellaneous	• Vin -/ • Spa -1 • Mis -1 -1 -1	tual Server Allows others to access WM Incial Application This configuration allows so cellaneous P Address of DMZ Host Allo Immunication. Note that, thi JPnP Setting: If you enable I	W, FTP, and other services o me applications to connect, a was a computer to be expose s feature should be used only JPnP function, the router will	n your LAN. and work with the NAT route d to unrestricted 2-way y when needed. work with UPnP devices/so	r. Awares.

Virtual Server

ADMINISTRATOR'S MAIN N	NENU -III	Status 💔 Wiza	rd Oil Advanced		→ Logo
🔊 BASIC SETTING 🥝	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	C Voice	SMS 🔂 TOOLB
Virtual Server	Urtual Serv	vər			[HELP]
Special AP		Well known servic	es - select one - 👻 Cop	in -	*
Miscellaneous	ID	Service Ports	Server IP	Enable	Use Rule#
	1				(0) Ahways 💌
	2				(0) Always 🐱
	3				(0) Always 😒
	4				(0) Always 🔽
	5				(0) Always 🐱
	6				(0) Always 🐱
	7				(0) Always 🔽
	8				(0) Always 🐱
	9				(0) Always 🐱
	10				(0) Abways 💌
			Save Lindo		

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.12 3.1	V
80	192.168.12 3.2	V
1723	192.168.12 3.6	V

Click on "Save" to store your setting or "Undo" to give up

Special AP

		WIFIHSPA	IAD (R0.03a1)	English 💌
O ADMINISTRATOR'S MAIN ME	NU	-fil Status 🖤 V	Vizard 🕅 Advanced	Logout
💓 BASIC SETTING 😵 P	ORWARDING RULE	s 🕲 SECURITY SETTI	NG 🍿 ADVANCED SETTING 🌈 VO	ice 🖂 SMS 🔃 TOOLBOX
Virtual Server	D Special	Applications		[HELP]
 Special AP 		Popular applica	itions – select one – 🛛 🔽 Copy to 🛛 🗤	
* Miscellaneoux	ID	Trigger	Incoming Ports	Enable
	1			
	2			
	3			
	4			
	5			
	6			
	7			
	8			
			Save Undo	

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

- 1. Trigger: the outbound port number issued by the application.
- Incoming Ports: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall. This product provides some predefined settings.

Select your application and Click "Copy to" to add the predefined setting to your list.

Click on "Save" to store your setting or" Undo" to give up

Miscellaneous

			WiFi	HSPA IAD	(R0.	03a1)			English
ADMINISTRATOR'S	MAIN MEN	u -ni	Status	W Wiza	rd	VII Advanced			+ Logou
BASIC SETTING	S 101	RWARDING RULES	(C) SECU	RITY SETTING	۳D	ADVANCED SETTING	C Voice	🖂 sms	(道) TOOLBO
 Virtual Server 		Miscellane	ous Items						[HELP]
 Special AP 			Item			Se	etting		Enable
 Miscellaneous 		• IP Address (of DMZ Host						
		UPnP setting	0						2
					8	iave Undo			

1. IP Address of DMZ Host

DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

2. UPnP Setting

The device also supports this function. If the OS supports this function enable it, like Windows XP. When the user gets IP from Device and will see icon as below:

2.2.3 Security Setting

	WiFi HSPA IAD (R0.03a1)	English 👻
ADMINISTRATOR'S MAIN MENU	🔺 Status 🖤 Wizard 🕥 Advanced	Logout
C BASIC SETTING S FORWA	ARDING RULES 😒 SECURITY SETTING 🏠 ADVANCED SETTING 🌈 Voice 🖂 SM	s 🕡 TOOLBOX
Status Packet Filters URL Blocking MAC Control Miscellaneous	 Packet Filters Packet Filters Allows you to control access to a network by analyzing the incoming and outgoing pa and letting them pass or halting them based on the IP address of the source and des Domain Filters Let you prevent users under this device from accessing specific URLs. URL Blocking	ackets tination.
	 Close the Administrator session. Set this to zero to disable it. Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot the Device. 	iot ping

Packet Filters

		WIFI HSPA IAD	(R0.03a	1)			English
ADMINISTRATOR'S MAIN MENU	-1	Status 💔 Wiza	rd 🔨	III Advanced			Elogos
💓 BASIC SETTING 😪 FOR	WARDING RULES	SECURITY SETTING	TO ADV	ANCED SETTING	6 Voice	SM:	TOOLBO
Status	D Outbound	Packet Filter		12			[HELP]
Packet Filters		Item			Setti	ng	
Domain Filters	OutboundPa	acket Filter		Enable			
URL Blocking	() All	ow all to pass except those	match the fol	lowing rules.			
MAC Control	ODe	ny all to pass except those i	match the foll	lowing rules.			
Miscellaneous	ID	Source IP	0	lestination IP : Pe	orts	Enable	Use rule#
	1						(O) Ahways 💌
	2 [1			(O) Always 💌
	3			1			(0) Always 🐱
	4 []{			(0) Ahways 💌
	5			1			(0) Always 💌
	6			1			(0) Ahways 🔽
	7 [1			(0) Ahways 🔽
	8						(0) Ahways 💉
		Save Undo) hbound	I Filter) MA	AC Level	Y	

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting.

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

- 1. Allow all to pass except those match the specified rules
- 2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

Each rule can be enabled or disabled individually.

Domain Filters

D ADMINISTRATOR'S MAIN	AENU 🦂	l Status 💔 Wiza	d 🕅 Advanced			> Logou
💓 BASIC SETTING 🙁	FORWARDING RULES		\mathcal{T}_{T} advanced setting	C Voice	🖂 sms	(@) TOOLBO
- Status	Domain Fi	lter				[HELP]
Packet Filters		Item		Setting		
Domain Filters	Domain Fill	er	Enable			
URL Blocking	Log DNS Q	uery	Enable			
MAC Control	Privilege IP	Addresses Range	From To			
Miscellaneous	ID	Domain Suffix		Action		Enable
	1			Drop Log		
	2			Drop Log		
	3			Drop Log		
	4					
	5					
	6			Drop Log		
	7					
	8					
	9					
	10	* (all others)			2	-
		(an onlers)	Save Undo			

1. Domain Filter

Let you prevent users under this device from accessing specific URLs.

2. Domain Filter Enable

Check if you want to enable Domain Filter.

3. Log DNS Query Check if you want to log the action when someone accesses the specific URLs.

4. Privilege IP Address Range

Setting a group of hosts and privilege these hosts to access network without restriction.

5. Domain Suffix

A suffix of URL can be restricted, for example, ".com", "xxx.com".

6. Action

When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check drop to block the access. Check "log" to log these access.

7. Enable

Check to enable each rule.

URL Blocking

		WIFI HSPA IAD	(R0.03a1)			English
D ADMINISTRATOR'S MAIN MENU	-11	Status 😾 Wiza	rd Cill Advanced			► Logou
💓 BASIC SETTING 😪 FORM	WARDING RULES	SECURITY SETTING	C ADVANCED SETTING	C Voice	🖂 SMS	100LB0
- Status	URL Blocki	ng				[HELP]
Packet Filters		Item		Setting		
Domain Filters	VRL Blockin	g	Enable			
URL Blocking	ID		URL			Enable
MAC Control	1					
Miscellaneous	2					
	3	[1		
	4	Ê		1		
	5					
	6				111	
	7					
	8					
	9					
	10					
			Save Undo			

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between "Domain filter" and "URL Blocking" is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

1. URL Blocking Enable

Check if you want to enable URL Blocking.

2. URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. Enable

Check to enable each rule.

MAC Control

		N	IFI HSPA IAD) (R0.03a1)			English N
O ADMINISTRATOR'S MAIN MENU	-ni	Status	W Wiza	rd 🖑 🕷 Advanced			F Logout
🕼 BASIC SETTING 😵 FOR	WARDING RULES	() s	ECURITY SETTING	M ADVANCED SETTING	C Voice	🖂 SM S	TOOLBOX
- Status	MAC Addres	s Contro					[HELP]
Packet Filters	Item			Setter	lg		
Domain Filters	MAC Address	Control	🔲 Enable				
URL Blocking MAC Control	Connection	control	Wireless and wir unspecified MAC	ed clients with C checked car addresses to connect.	i connect to this	s device; and	allow 🛩
Miscellaneous	Association of	control	Wireless clients allow wunspe	with A checked can associate cified MAC addresses to asso	to the wireless	s LAN; and	
		DHCP	clients - select o	ne 👌	Copy to	D - V	
	ID		MAC	Address		с	A
	1						
	2						
	3			1			
	4						
	5						
			<< P)	evious Next >> Save	Undo		

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

1. MAC Address Control

Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

2. Connection control

Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.

3. Association control

Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

Miscellaneous

		WiFil	HSPA IAD	(R0.03a1)			English 🗸
D ADMINISTRATOR'S MAIN ME	w -ii	Status	W Wizar	d Mil Advanced			+ Logout
🕅 BASIC SETTING 😵 FO	ORWARDING RULES	SECURI	TY SETTING	CD ADVANCED SETTIN	G 🌈 Voice	🖂 SMS	TOOLBOX
- Status	D Miscellaneo	us Items					[HELP]
Packet Filters		Item			Setting		Enable
Domain Filters	Administrator	Time-out		300 second	s (0 to disable)		
URL Blocking	Remote Admi	inistrator Host	: Port		1		
MAC Control	Discard PING	from WAN sid	le	00			
Miscellaneous	> DoS Attack De	staction					
				Save Undo			

1. Administrator Time-out

The time of no activity to logout automatically, you may set it to zero to disable this feature.

2. Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24". NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

3. Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

4. DoS Attack Detection

When this feature is enabled, the router will detect and log the DoS attack comes from the

Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke,

Port Scan, Ping of Death, Land Attack etc.

2.2.4 Advanced Settings

	WIFI HSPA IAD (R0.03a1) Englis	sh 💌
D ADMINISTRATOR'S MAIN ME	IENU 📲 Status 🖤 Wizard 🕬 Advanced 🔸 L	ogout
😥 BASIC SETTING 😪 F	FORWARDING RULES 🐵 SECURITY SETTING 🌾 ADVANCED SETTING 🌾 Voice 🖾 SMS 🍓 TOO	LBOX
 Status System Log Dynamic DKS QoS SMMP Routing System Time Scheduling 		

System Log

		WIFI HSPA IAI) (R0.03a1)			English 🐱		
D ADMINISTRATOR'S MAIN MENU	-11	Status 💔 Wiza	ard CIII Advanced			+ Logout		
💓 BASIC SETTING 😪 FORM	ARDING RULES	SECURITY SETTING	The Advanced Setting	6 Voice	🖂 sms	100LBOX		
+ Stotus	System Log	1	10.5 C			[HELP]		
System Log		Item	Setti	ng		Enable		
 Dynamic DNS 	FIP address for	or syslogd			2			
+ QoS	Setting of En	nali alert						
* SNMP	SMTP Ser	ver : port		1				
* Routing	SMTP Use	ername		7				
* System Time	SMTP Pas	sword		_	-			
* Scheduling	• E-mail ad	riresses						
	- E man ea							
	. ·			2				
	• E-mail sul	bject						
		Vie	(Save) (Undo) w Log) Email Log Nov	v				

This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Sys log

Host IP of destination where sys log will be sent to.

Check **Enable** to enable this function.

Setting of E-mail Alert

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

SMTP Username and Password

Input a user account and password for the SMTP server.

E-mail address

The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert, this setting is optional.

View Log...

Reference the section Toolbox/System Info.

Dynamic DNS

	WiFi	HSPA IAD (R0.03a1)			English N
ADMINISTRATOR'S MAIN MENU	🐴 Status	W Wizard M Advanced		_	> Logou
💓 BASIC SETTING 🤗 FORM	VARDING RULES 🛞 SECU		6 Voice	🖂 sms	100LB0
+ Status	Dynamic DNS				[HELP]
+ System Log	llem	S	etting		
+ Dynamic DNS	> DDNS	⊙ Disable ○ Enable			
* QoS	Provider	DynDNS.org(Dynamic) 🔽			
* SHMP	+ Host Name				
* Routing	Username / E-mail		1		
 System Time 	Password / Key		1		
Scheduling		Save Undo			
	1				

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable Dynamic DNS click the check box next to Enable in the DDNS field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

QOS

- ADMINISTRATOR- MAIN MEN		WiFi HSPA IAD	(R0.03a1)			English
BASIC SETTING	IN IN THE RUL	ES (C) SECURITY SETTING		C Voice	🖂 SM	s 12 TOOLBO
• Status	QoS Ru	le .	40			
System Log		Item		Setting		
Dynamic DNS	• QoS Con	trol	Enable			
QoS	Bandwid	th of Upstream	kbps	(Kilobits per sec	cond)	
SNMP	ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
Routing	1			High 💌		(0) Always 👻
System Time	2			High 🐱		(0) Always 🐱
Scheduling	3			High 🗸		(0) Always 🗸
	4			High 💌		(0) Always 🔽
	5			High 💌		(0) Always 🔽
	6			High 💌		(0) Always 💌
	7			High 💌		(0) Always 💌
	8			High 💌		(0) Always 💌
			Save Undo			

Provide different priority to different users or data flows, or guarantee a certain level of performance.

Enable

This Item enables QoS function or not.

Bandwidth of Upstream

Set the limitation of upstream speed.

Local: IP

Define the Local IP address of packets here.

Local: Ports

Define the Local port of the packets in this field.

Remote: IP

Define the Remote IP address of packets here.

Remote: Ports

Define the Remote port of the packets in this field.

QoS Priority

This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

User Rule#

The QoS item can work with Scheduling Rule number#. Please reference the section Advanced setting/schedule Rule.

SNMP

D ADMINISTRATOR'S	MAIN MENU	-	WiFi H	ISPA IAD	(R0.	.03a1)				English
BASIC SETTING	S FORM	ARDING RULES	Status	TY SETTING	1	ADVANCED SETTING	C V	xice 🖂	SMS	TOOLBO
• Status		D SNMP Set	ing							[HELP]
 System Log 		ł	lem			5	Setting			
 Dynamic DNS 		Enable SNN	IP	Loca		mote				
- QoS		Get Commu	inity							
- SNMP		Set Commu	nity	1						
 Routing 		• IP 1				1				
 System Time 		• IP 2								
Scheduling		+ IP 3								
		• IP 4		1						
		SNMP Versi	on		V2c					
		· WAN Acces	s IP Address							
						Save Undo				

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports.

WAN Access IP Address

If the user wants to limit to specific the IP address to access, please input in the item. The default 0.0.0.0 and means every IP of Internet can get some information of device with SNMP protocol.

Routing

		WIFI H	SPA IAD (F	R0.03a1)			English
ADMINISTRATOR'S MAIN MEN	U	-fil Status	W Wizard	Will Advanced			⊁ Logo
🔞 BASIC SETTING 🥝 FO	RWARDING RU	LES 🧐 SECURIT	Y SETTING) ADVANCED SETTING	C Voice	🖂 SMS	TOOLBC
- Status	Routir	g Table					[HELP]
 System Log 		Item			Setting		
 Dynamic DNS 	+ Dynam	ic Routing	Oisable (RIPv1 O RIPv2			
⇒ Qo\$	 Static F 	louting	Oisable	Enable			
= SNMP	ID	Destination	Subne	t Mask	Gateway	Нор	Enable
- Routing	1						
 System Time 	2 [
 Scheduling 	3						
	4 [
	5 [
	6 [
	7 [
	8 [
				Save Undo			

Routing Tables

Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static and dynamic routing.

Dynamic Routing

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

System Time

			w	IFI HSPA IAC	(R0.03a1)			English 🗸
D ADMINISTRATOR'S	MAIN MEN	u -1	Status	💔 Wiza	rd 🕅 Advanced			Logout
BASIC SETTING	S 10	RWARDING RULES	(2) SL	CURITY SETTING		C Voice	🖂 sms	100LBOX
+ Status		System Time	,					[HELP]
 System Log 		Item			Sett	ing		
+ Dynamic DNS		Time Zone		* Not yet confi	gured! The default is GMT+00	0.00		~
* QoS		Auto-Synchron	ization	Enable	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1			
* SNMP				Time Server (R	(FC-868) Auto	~		
* Routing				_	Save Undo	_		
+ System Time		6		Change welling and EV	Sync with Time Server	000 00:40:433		
 Scheduling 				Sync with my PV	c (underlined November 26, 2	009 22.18.43)		

Time Zone

Select a time zone where this device locates.

Auto-Synchronization

Select the "Enable" item to enable this function.

Time Server

Select a NTP time server to consult UTC time

Sync with Time Server

Select if you want to set Date and Time by NTP Protocol.

Sync with my PC

Select if you want to set Date and Time using PC's Date and Time

Scheduling

				141	1						
ADMINISTRATOR'S	MAIN MENU	-11	Status	W Wizar	d	KIII Advanced	_		_	> Logo	
BASIC SETTING	S FORM	ARDING RULES	(2) SLC	JRITY SETTING	16	ADVANCED SETTING	C V0	ice 🗵] sms	TOOLBO	
Status		D Schedule F	tule							[HELP]	
System Log			Item				Setting	1			
Dynamic DNS		• Schedule				Enable					
QoS		Rule#			Rule	Name			A	ction	
SMMP		1							New Add		
Routing		2							New Add		
System Time		3							New Add		
Scheduling		4							Ne	w Add	
		5							Ne	w Add	
		6							Ne	w Add	
		7							Ne	w Add	
		8							Ne	w Add	
		9	New Add							w Add	
		10							Ne	w Add	
			1	<< Previous	Nex	t >> Save Add N	lew Rule				

You can set the schedule time to decide which service will be turned on or off.

Select the "Enable" item. Press "Add New Rule" You can write a rule name and set which day and what time to schedule from "Start Time" to "End Time". The following example configure "ftp time" as everyday 14:10 to 16:20

		WIFI HSPA IAD	(R0.03a1)			English 💌
D ADMINISTRATOR'S	MAIN MENU	-fil Status 💔 Wizar	d 🕅 Advanced			Logout
(2) BASIC SETTING		RULES 🕼 SECURITY SETTING	C ADVANCED SETTING	C Voice	🖂 SMS	TOOLBOX
• Status	📮 Edit Sc	hedule Rule				[HELP]
 System Log 		Item		Setting		
 Dynamic DNS 	Name of the second s	f Rule 1				
- QoS	+ Policy		Inactivate 👻 except the se	elected days ar	nd hours belo	w.
* SNMP	ID	Week Day	Start Time (hh:mm)		End Time (hh:mm)
- Routing	1	- choose one - 💌				
 System Time 	2	- choose one - 💌				
 Scheduling 	3	- choose one - 💌				
	4	– choose one – 💌				
	5	- choose one - 🐱				
	6	choose one 💙				
	7	choose one 🐱				
	0	choose one 😪				
			Save Undo Back			

Click on "Save" to store your setting.

2.2.6 SMS

		WiFi	HSPA IAD	(R0.	03a1)				English
ADMINISTRATOR'S MAIN MENU	-11	Status	W Wizard		Cill Advanced	_			+ Logo
📆 BASIC SETTING 🛞 FORW	ARDING RULES	🛞 SECUR	RITY SETTING	Ś	ADVANCED SETTING	C	Voice	🖂 SMS	TOOLBO
Create Message	D SMS								
inbox	• Cre -/ • Inb -/	ate Message diow you to ci ox diow you to re	e reate and send ead new SMS m	new Si essag	MS message. e, and delete/forward	existe	ed messa	age.	

Create Message

		WIFI HSPA IAD	(R0.03a1)			English 💌
D ADMINISTRATOR'S MAIN M	ENU -1	Status 💔 Wiza	rd 🔨 🥅 Advanced			+ Logout
🔊 BASIC SETTING 🛞	ORWARDING RULES	SECURITY SETTING	C ADVANCED SETTING	C Voice	🖂 SMS	🔃 тоосвох
Create Message	Create Mess	sage				
* Inbox	Item		Sett	ing		
	▶ Text message			0		
	_	The max. leng	th of a message is 160 char.	acters for pure	alphabetical	or numeric.
	Receiver:	Add '+' for inte	ernational format of the phon	e number.		
			Send Cancel			
			Contra Contra			

You can create a new SMS message on this page. After finishing content of message, and filling with phone number of receiver(s), pressing send button to send this message out. You can see "Send OK" if the new message has been sent successfully.

Inbox

in arrivo			
	Da	Data e Ora 🔺	Testo
		uð uð	
é.			
	SMS Rice	vuti(0) ;SMS Nuovi(0) ;Capacită Totale(50)
D SMS			
			-

You can read, delete, reply, and forward messages. Just click on one from the SMS lists, then you can view the whole content of it in the SMS window below.

Refresh:

You can press "Refresh" button to renew SMS lists.

Delete, Reply, Forward Messages:

After reading message, you can check the checkbox on the left of each message to delete, reply, or forward this message.

2.2.7 Tool Box



System Info

ADMINISTRATOR'S MAIN MENU	-1in st	tatus	W Wiza	rd ^K	III Advanced	_	_		> Logo		
💓 BASIC SETTING 😪 FOR	WARDING RULES	3 ×	CURITY SETTING	MD ADV	ANCED SETTING	C	Voice	🖂 sms	TOOLBO		
System Info	System Infoma	tion									
Firmware Upgrade	Item				Sett	ing					
Backup Setting	WAN Type		3G								
Reset to Default	► Display time		Thu, 26 Nov 20	009 14:37:22	+0000						
Reboot	System Log										
Miscellaneous	Time				Lo	q					
	Nov 26 14:32:	55	kernel: klogd started: BusyBox v1.3.2 (2009-11-05 20:12:35 CST)								
	Nov 26 14:33:	01	O3G/hotplug: 3	G modern V	endorID=0408 P	roductil	D=ea05				
	Nov 26 14:33:	02	udhcpd[1438];	udhcpd (v0.§	9.9-pre) started						
	Nov 26 14:333	02	udhcpd[1438]	Unable to pp	en Mar/run/udho	pdleas	es for r	eading			
	Nov 26 14:33:	02	commander: 3	G phone sup	oported						
	Nov 26 14:33:	02	init: Starting pi	d 1472, cons	ole /devityS1: 7b	in/ash'					
	Nov 26 14:33:	03	commander: STOP WANTYPE 3G								
	Nov 26 14:33:	10	udhcpd[1440]	sending OFI	FER of 192.168.1	123.100					
	Nov 26 14:33:	10	udhcpd[1440]	sending ACI	K to 192.168.123	.100					
	Nov 26 14:33:	11	03G/3g_notity	d: 3G Notity S	erver started						
	Nov 26 14:33:	12	commander: S	TART WANT	YPE 3G						
	Nov 26 14:33:	15	pppd[1745]; pp	pd 2.4.4 sta	rted by root, uid 0)					
	Page: 1/7 (Log Nur	mber:	96) Cerevious Refres	Next >>	First Page	Last	Page	I			

You can view the System Information and System log, and download/clear the System log, in this page.

Firmware Upgrade

		WIFI HSPA IAD	0 (R0.03a1)		English 🝷			
D ADMINISTRATOR'S MAIN MENU	-ii	Status 💔 Wiza	rd 🕅 Advanced		▶ Logout			
BASIC SETTING 🛞 FORM	WARDING RULES	SECURITY SETTING	ADVANCED SETTING	🌈 Voice 🖂 SMS	TOOLBOX			
System Info	Firmware Up	grade						
Firmware Upgrade			Firmware Filename					
Backup Setting				》覽 …				
Reset to Default		Curr	ent firmware version is R0.03	3a1.				
Reboot								
Miscellaneous	1	lote! Do not interrupt the p When the process is don	process or power off the unit w e successfully, the unit will be	vhen it is being upgraded. e restarted automatically.				
		I	Accept unofficial firmware	.				
	Upgrade Cancel							

You can upgrade firmware by clicking "Upgrade" button.

Backup Setting



You can backup your settings by clicking the "**Backup Setting**" button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

Reset to Default

		WiF	HSPA IAD	(R0.	.03a1)				E	nglish 🝷
O ADMINISTRATOR'S MAIN MENU	-11	Status	W Wiza	d	MII Advanced	_	_		_	Logout
	WARDING RULES	(S) 800	RETY SETTING	16	ADVANCED SETTING	C	Voice	SM15	碰	TOOLBOX
 System Into 	U Toolbox									
 Firmware Upgrade 	5	_	-	_	L. 72.					
+ Backup Setting	• •									
 Reset to Default 		0								
+ Reboot	• FI	1	eset all setting	s to fac	tory default?					
+ Miscellaneous						evice.				
	• 8		Y	88	Cancel					
	• Res	et to Defaul								
	- R	eset the set	tings of this de	vice to fi	he default values.					
	 Reb 	loci								

You can also reset this product to factory default by clicking the **Reset to default** button.

Reboot

	WiFi HSPA IAD (R0.03a1) English
D ADMINISTRATOR'S MAIN MENU	📲 Status 💔 Wizard 🖓 Advanced 🛛 Elogo
💓 BASIC SETTING 🥺 FORW	ARDING RULES 🐵 SECURITY SETTING 🎲 ADVANCED SETTING 🌈 Voice 🖂 SMS 🙀 TOOLBO
 System Info Firmware Upgrade Backup Setting Reset to Default Reboot Miscellaneous 	Toolbox View L ·View ·Vie
	Reboot Reboot this device

You can also reboot this it by clicking the **Reboot** button.

Miscellaneous

WiFi HSPA IAD (R0.03a1)						English 🗸	
📮 ADMINISTRATOR'S MAIN MENU 🛛 🔺		Status 🖙 Wiza	rd 🔨 M Advanced	Logout			
🏹 BASIC SETTING 🔗	FORWARDING RULES	SECURITY SETTING	ADVANCED SETTING	C Voice	🖂 SM S	100LBOX	
System Info	Miscellaneous items					[HELP]	
Firmware Upgrade	Item			Setting			
Backup Setting	MAC Address		Wake up				
Reset to Default	Domain Name or IP address for Pir		est	Ping			
Reboot		Save Undo					
Miscellaneous							

Domain Name or IP address for Ping Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.



