# User Manual

# BandLuxe

# R300 Series HSPA+ WLAN Router R200 Series HSPA WLAN Router





# Table of Contents

1

Table of Contents	1
Package Contents	3
Package Contents	3
Features	3
Hardware Overview	4
Installation	6
Wizard Setup	9
Internet Setup	11
Basic Setting	11
DDNS	15
Optional	16
Router Setup	18
Network Setting	
Advanced Routing	20
WiFi Setup	22
Basic WiFi Network	22
WiFi Security	23
Advanced WiFi Setting	27
WiFi Clients Filter	29
3.5G HSPA Setup	30
PIN Verification	
PIN Management	30
Preferred Network	31
Security Setup	32
Firewall	32
Internet Access Policy	35
Single Port Forward	37
Port Range Forward	38
Port Range Trigger	39
QoS	40



Admin Setup	. 42
Management	. 42
Diagnosis	. 44
Recover & Renewal	. 45
Status	. 47
3.5G HSPA & Internet	. 47
Router	. 48
Appendix A: FAQ	. 50
Appendix B: Specification	. 57
Appendix C: Important Safety Information and Glossary.	. 60
Europe – EU Declaration of Conformity	. 60
Federal Communication Commission Interference Statement	. 61
Glossary	. 63



# Package Contents

Thank you for your purchase of this HSPA+/HSPA WLAN Router. This product is designed to access the Internet via 3.75G technology and share the bandwidth through a WiFi network. It is easy to configure and operate even for non-technical users. This manual contains instructions for installing and configuring the product. Read the manual carefully before you use the product, so that you can fully exploit the product functions.

## **Package Contents**



## **Features**

- HSPA+/HSPA WLAN Router
- Uplink up to 5.7 Mbps Downlink up to -- R300 Series: 21/ 28.8 Mbps R200 Series: 7.2 Mbps
- Support WiFi 802.11 b/g/Pre-n
- R300 -- UMTS: 850/900/1900/2100 MHz

GSM: 850/900/1800/1900 MHz

- R302 -- UMTS: 2100 MHz
- R305 -- UMTS: AWS Band
- R307 -- UMTS: 850/1900 MHz

GSM: 850/900/1800/1900 MHz



- R250 -- UMTS: 850/1900/2100 MHz GSM: 850/900/1800/1900 MHz
- Support WAN/LAN Ethernet Port
- Optional External 3G Antenna Port Ready
- Sleek Design and Easy to Use

## **Hardware Overview**



1 Reset Button	To reset the Router, press the reset button briefly.
	To restore the Router's factory settings, press the reset button for longer than 5 sec.
2 3G External Antenna Port	To connect to the 3G External Antenna if needed.
3 SIM Slot	Insert SIM/USIM. Push-push type.
4 WAN Port	Connect a DSL or Cable modem.
5 LAN Port	Connect Ethernet devices such as computers, switches, and hubs.
6 Power Switch	To switch on/off the router.



7 Power Receptor	Receptor for the Power Adaptor.
8 UMTS LED	Reference below table.
9 Roaming LED	Solid light shows the Router is connecting to Roaming network.
10 WLAN LED	Solid light indicates that the wireless segment is ready. Flashing light shows that data is being transmitted via WLAN.
11 Ethernet LED	Solid light shows that an Ethernet-enabled computer is connected via the LAN port but no data is being transmitted. Flashing light shows that data is being transmitted via LAN.
12 DIAG LED	Reference below table.
13 Power LED	Solid light indicates that the power supply is connected properly.
14 3G Radio On/Off & Signal Strength Button	Short press – Enable Signal Strength indication for 3 sec. Long press (>5 sec) – 3G radio on/off
15 3G Radio Signal Strength Indicator	Indicates the 3G signal strength when 3G Radio button is in short press.

#### Table for UMTS and DIAG LED:

Operation status	UMTS	DIAG
Error in Router	OFF	Solid
Fail to boot module	Solid Red	Flashing
No SIM exist	Flashing Red	OFF
Waiting for PIN entering	Flashing Red	OFF
No network/Searching for network	Flashing Red	OFF
3G camped	Flashing Green/Pink	OFF
3G connected	Solid Blue/Green/Pink	OFF

Note: Pink for UMTS LED is available by product if 2G is available.



# Installation



**1.** Connect the power adaptor to the Router and connect it to an outlet.



- **2.** Insert your SIM card into the slot on the Router, making sure the SIM card orientation matches the SIM card slot, as shown in the picture.
- **3.** Turn on the Power switch.



**4.** One of the following two methods can be chosen to link your Router with PC.



 A. To link the Router with your PC via WiFi, in Microsoft Windows, go to *Control Panel* > *Network Connections*, right-click on Wireless Network Connection, and choose View Available Wireless Networks. Select the HSPA\_ROUTER wireless network, and click Connect.



**B.** To link the Router with your PC via Ethernet cable, connect one end of the cable to the LAN port on the Router, and the other end of the cable to the Ethernet port on your computer.

**Note:** If you choose to access the Internet via Ethernet, connect one end of the cable to the WAN port of Router, and the other end to your xDSL/Cable Modem.

The Router uses a web-based configuration utility. To access the configuration utility, open a browser (for example Internet Explorer) and enter the IP address (http://192.168.1.1) or the URL



(http://R300.ROUTER) for the Router in your browser's address bar.



Enter the Router User name (admin) and Password (hsparouter).

Connect to 192.1	68.1.1 ? 🔀
	GP
The server 192,168, username and passw Warning: This server password be sent in without a secure cor	1.1 at 3.5G WiFi Router requires a word. r is requesting that your username and an insecure manner (basic authentication unection).
<u>U</u> ser name:	2
Password:	
	Remember my password
	OK Cancel



# Wizard Setup

User can set preferred settings step by step via Wizard. If the router is in Factory default settings, the GUI will always open Wizard. User can set the Wizard via Basic Setting> Network Setting > Basic WiFi Network > WiFi Security.

Basic Setting					
Dasic Setting	Wizard Interne	et Router	WiFi 3.5G HS	SPA Security	Admin Status
	Basic Setting /	Network Setting	/ Basic WiFi Netv	vork / WiFi S	ecurity
• Wizard					
	Welc	ome to Se	etup Wizard		
			Sta	rt	
Basic Setting					
Dasic Setting	Wizard Intern	et Router	WiFi 3.5G HS	SPA Security	Admin Status
	Basic Setting /	Network Setting	/ Basic WiFi Netv	vork / WiFi	Security
• 3.5G HSPA Setting				н	elp
		Get Latest APN I	Database		
	Roaming Connection:	Enabled	Oisabled		
	APN Setting.	internet	Maliual		
	User Name:				
	Password:				
	Authentication Type:	◎ PAP	CHAP		
	Connection:	On Demand, r	nax idle time 3 min		
		Keep Alive			
Ethernet Setting				_	
	Connection Type: All	omatic Configuration -	DHCP -		
	connection Type.	,,			
			Next>	ancel	
	Connection Type: Aut	iomatic Configuration -	DHCP ¥		
			Next > C	ancel	



Network Setting	Waard	et Router WiFi 3,5G HSPA	Security Admin Status
	Basic Setting /	Hetwork Setting / Basic WiFi Network	/ WiFi Security
• Router IP	Local IP Address:	192 , 168 , 1 , 1	Help
	Subnet Mask: URL Address:	255.255.255.0	
DHCP Service			-
	DHCP Server: Start IP Address: Maximum Number of	Enabled Disabled DHCP Reservation	
	Users: IP Address Range:	50 192 . 168 . 1 . 100 - 149	
	Client Lease Time: Static DNS 1:	0         minutes (0 means one day)           0         .           0         .	
	Static DNS 2: Static DNS 3:		
	WINS		
		< Back Ilext > Cancel	
Basic WiFi Network	Warned Intern	net Router WiFi 3.5G HSPA	Security Admin Status
	Basic Setting /	Network Setting / Basic WiFi Hetwork	/ WiFi Security
• Basic Wifi Setting	Network Mode: Network Name(SSID): Standard Channel: SSID Broadcast:	Mixed HSPA_ROUTER 7 - 2.442GHz	Help
		< Back Hext > Cancel	
WiFi Security	Waxard Intern	net Router WiFi 3.5G HSPA	Security Admin Status
- WiEi Security Setting	Basic Setting	Hetwork Setting / Basic Wirl Hetwork	Halp
	Security Mode:	Disabled	
	Save	<back   sais=""> Cancel</back>	-



# Internet Setup

## **Basic Setting**

Basic Setting	Wizard	et R	outer	WiFi	3.5G HSPA	Security	Admin	Status
	Basic Setting	/ DDNS /	Optional					
<ul> <li>Connection Type</li> </ul>	Connection Priority:	3.5G	HSPA First	O	Ethernet First	He	<u>lp</u>	
• 3.5G HSPA Setting		Get La	test APN Databa	se				
	Roaming Connection:	Enal	bled	۲	Disabled			
	APN Setting:	Auto	D	$\bigcirc$	Manual			
	APN:	internet						
	User Name:							
	Password:							
	Authentication Type:	PAP		۲	CHAP			
	Connection:	On	Demand, max idl	e time	3 min			
		Kee	p Alive					
• Ethernet Setting	Connection Type: Aut	omatic Confi	guration - DHCP	•		_		
			Save Se	ttings	Cancel Chan	ges		

## **Connection Type**

The Router can link to the internet via 3.5G HSPA or Ethernet. Select the connection type you prefer.

## 3.5G HSPA Setting

#### **Get Latest APN Database**

Get the latest Profile Name, Number, User Name, Password, and APN from the web site automatically.

#### **Roaming Connection**

To allow roaming network connection, select **Enabled**. To block roaming connection, select **Disabled**.



**Note:** Charges for roaming connection may be high. Contact your mobile network operator for more information.

#### **APN Setting**

The APN (Access Point Name) is provided by your mobile network operator. You can choose to set the APN automatically or manually. In most cases, the Router works properly when the APN is set to Auto.

To set the APN manually, contact your mobile network operator for the APN, User Name and Password of the data service.

#### **Authentication Type Setting**

To allow user to set PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

#### Connection

**On Demand:** You can set the idle time for the 3.5G HSPA connection. When the Router is idle, the connection will be disconnected automatically after the idle time expires.

**Keep Alive:** The connection is always kept on. If the HSPA connection is disconnected, the Router tries to reconnect.

## **Ethernet Setting**

#### **Automatic Configuration - DHCP**

Choose **Dynamic IP Address** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services.



### Static IP

Ethernet Setting	Connection Type:	Static IP	_			_	*	
	IP Address:	192		168	. 2		210	
	Subnet Mask:	255	].	255	. 255		0	
	Default Gateway:	192	].	168	. 2		254	
	DNS 1:	192	].	168	. 1		202	
	DNS 2:	0	].	0	. 0		0	
	DNS 3:	0	].	0	. 0		0	

Select **Static IP** if all WAN IP information is provided to you by your ISP. You will need to enter the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP.

#### PPPoE

Connect on Demand:Max kile Time      minutes     Keep Alive: Redial Period 30 seconds			User name: Password: Service Name (Optio Connect on Den & Keep Alive: Red	nal): nand:Max Idle Time iial Period 30	5 minutes seconds	
---	--	--	---	---	----------------------	--

Choose **PPPoE** (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

Service Name: Enter the ISP Service Name (optional).

**Connect on Demand:** Enter a maximum idle time during which the Internet connection is maintained during inactivity.

**Keep Alive:** If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router automatically tries to re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, specify how often you want the Router to check the Internet connection.



#### PPTP

		_					
•	Ethernet Setting	Connection Type: PPT	TP	1	1	~	
		Internet IP Address:	0	. 0	. 0	. 0	
		Subnet Mask:	0	. 0	. 0	. 0	
		Server IP Address:	0	. 0	. 0	. 0	
		User name:					
		Password:					
		O Connect on Deman	d:Max Idle	Time 5	m	ninutes	
		Keep Alive:Redial P	Period 30	se	conds		
					Save	Settings	Cancel Changes

Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password.

Internet IP Address: Enter the IP address

**Subnet Mask:** This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Server IP Address: Enter the Server IP provided by your ISP (optional).

#### L2TP

•	Ethernet Setting	Connection Type: L2TP Internet IP Address: 0 . 0 . 0 . 0 . 0 User name: Password: Connect on Demand:Max Idle Time 5 minutes Keep Alive:Redial Period 30 seconds
	1	Save Settings Cancel Changes

Choose **L2TP** (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.

Internet IP Address: Enter the IP address provided by your ISP.

**Connect on Demand:** Enter a maximum idle time during which the Internet connection is maintained during inactivity.

**Keep Alive:** Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, the Router automatically tries to re-establish your connection. To use this option, select **Keep Alive**. In the **Redial Period** field, you specify how often you want the Router to check the Internet connection.



## DDNS

DDNS	Wizard Inte Basic Setting	rmet Router / DUIS / Optio	WiFi	3.5G HSPA	Security	Admin	Status
• DDNS DDNS Service	Service Type: User name: Password: Host Name: WildCard: Internet IP Address: Status: Update	DynDNS.org	abled		<u>He</u>	p	
		Sa	ve Settings	Cancel Chang	es		

DDNS (Dynamic DNS Service) is a system which allows the domain name data held in a name server to be updated in real time. It allows an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com.

Service Type: From the drop-down list, select your DDNS service type.

**User name:** Enter the user name for your DDNS account.

**Password:** Enter the password for your DDNS account.

**Host name:** The Host Name is optional but may be required by some ISPs.

**WildCard:** Some DDNS servers support the wildcard alias feature which points \*.yourhost.dyndns.org to your computers automatically. All aliases for your domain such as www.yourhost.dyndns.org will point to your computer by default due to Wildcard Alias. This allows users to access your computer using all types of derivatives of your domain name.

**Internet IP Address:** The Router's Internet IP address is displayed here. Because it is dynamic, it changes.

Status: This shows whether the DDNS service is enabled or disabled.



## Optional

	Optional	Wizard	Internet	Router	WiFi	3.5G HSPA	Security	Admin	Status
		Basic Se	tting / D	DNS / Optio	nal				
•	Host Setting	-					He	<u>sip</u>	
		Host Name:							
		Domain Name:							
		MTU:	А	uto 🚩 Size:	1500				
•	MAC Address Clone				<u> </u>				
		Service:		) Enabled		isabled			
		MAC Address							
				CIONE My PCS I	nac.				
	Time Setting								
		(GMT-08:00)	) Pacific Time (l	JSA & Canada)	*				
		🗹 Automatio	cally adjust cloo	ck for daylight sav	ing changes.				
			_						
				Sa	ive Settings	Cancel Char	nges		

## Host Setting

### Host Name and Domain Name

These fields allow you to assign a host and domain name for the Router. Some ISPs require these names as identification. In most cases, leaving the fields blank will work.

#### MTU

MTU (Maximum Transmission Unit) specifics the largest packet size permitted for Internet transmission. To have the Router select the best MTU for your Internet connection, keep the default setting, Auto.

## MAC Address Clone

Some ISPs will require you to register a MAC address in order to access the Internet. If you do not want to re-register the MAC address with your ISP, you can assign the MAC address you have currently registered with your ISP to the Router by clicking the **Clone My PCs MAC** button.



## **Time Setting**

Select the Time Zone from the drop-down menu according to your current location.

Automatically adjust clock for daylight saving changes: Select the checkbox to enable Daylight Saving time.



# **Router Setup**

## **Network Setting**

Network Setting	Witter	at Builer	MiEi	2.5C HCDA	Coourity	Admin	Status
_	Hetwork Setting	/ Advanced Routi	ng	3.30 H3FA	Security	Admin	Status
Router IP					He	<u>lp</u>	
	Local IP Address:	192 . 168 . 1	. 1				
	Subnet Mask:	255.255.255.0	]				
	URL Address:	http://R300.ROUTE	ER				
		L .			_		
• DHCP Service							
	DHCP Server:	💿 Enabled 🔵 Dis	abled DHCF	Reservation			
	Start IP Address:	192.168.1.100					
	Maximum Number of Users:	50					
	IP Address Range:	192 . 168 . 1 . 100 - 1	49				
	Client Lease Time:	0 minutes (0 m	eans one day)				
	Static DNS 1:	0.0.0	. 0				
	Static DNS 2:	0.0.0	. 0				
	Static DNS 3:	0.0.0	. 0				
	WINS	0.0.0	. 0				
		Sav	ve Settings	Cancel Chan	ges		

## Router IP

This is the Router's IP address and subnet mask which is seen in your local network. The default IP address is 192.168.1.1, and the default Subnet Mask is 255.255.255.0. Keeping the default values will work.

## **DHCP Service**

DHCP stands for Dynamic Host Control Protocol. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. If the Router's DHCP server option is enabled, make sure there is no other DHCP server on your network.



### **DHCP** Reservation

To assign the same IP address to a PC every time it reboots, click the **DHCP Reservation** button.

DHCP Table	Client Name	Interface	IP Ad	dress	MAC Address	Select
	eta-007-xp-tc	LAN	192.168.	.101.100	00:0F:EA:37:DE:52	
	eta-90ac1fec7a6	LAN	192.168.	101.101	00:0C:29:59:CD:B5	
Manually Add Client	Enter Client Name	Assign IP A	ddress	To This	MAC Address	
Manually Add Client	Enter Client Name	Assign IP A	ddress	To This	MAC Address	
Manually Add Client	Enter Client Name	Assign IP A 192.168.101	ddress	<b>To This</b>	<b>MAC Address</b>	Add
Manually Add Client DHCP Reservation	Enter Client Name	Assign IP A 192.168.101	ddress 0	To This	MAC Address	Add

A list of DHCP clients is displayed with the following information: Client Name, Interface, IP Address, and MAC Address. Select a checkbox to reserve a client's IP address. To add clients, click **Add Clients**. To manually assign an IP address, enter the client's name in the **Enter Client Name** field. Enter an IP address in the **Assign IP Address** field. Enter a MAC Address in the **To This MAC Address** field. Click **Add**. A list of DHCP clients and their fixed local IP addresses is displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**. To view the most up-to-date information, click **Refresh**.

**Start IP Address:** Enter a starting IP address for the DHCP server's IP assignment.

**Maximum Number of Users:** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to.

**DHCP Lease Time:** The length of time for the IP address lease. Enter the lease time in minutes.

**Static DNS (1-3):** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS:** The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.



## **Advanced Routing**

Advanced Routing	Wizard Interne	Reuter WiFi	3.5G HSPA Secu	rity Admin Status
	Network Setting	Advanced Routing		
• NAT	Service:	Enabled (	) Disabled	Help
• RIP	Service:	C Enabled	) Disabled	
Static Routing				
	Route Entry: Enter Route Name: Destination LAN IP: Subnet Mask: Gateway: Interface: Show Routing Table	1 V Delete Th	is Entry	
<ul> <li>VPN Passthrough</li> </ul>	IPSec Passthrough PPTP Passthrough L2TP Passthrough	<ul> <li>Enabled</li> <li>Enabled</li> <li>Enabled</li> <li>Enabled</li> </ul>	) Disabled ) Disabled ) Disabled	
		Save Setting	s Cancel Changes	

## NAT Setup

The Network Address Translation (NAT) service is a standard that allows multiple computers on a private network to share a single IP address.

## RIP

The **Routing Information Protocol (RIP)** helps the Router dynamically adapt to changes of network connections by communicating information about which networks each Router can reach and how far away those networks are.

## Static Routing

This section allows you to define fixed routes to defined destinations.

**Route Entry:** To set up a static route, select a number from the drop-down list.



Enter Route Name: Enter a name for the route here.

**Destination LAN IP:** Enter the Destination IP address that will be assigned to a specific network or host.

Subnet Mask: Enter the subnet mask associated with the Destination IP.

**Gateway:** This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

**Interface:** This interface tells you whether the Destination IP Address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet).

**Show Routing Table:** Click **Show Routing Table** to open a screen displaying how data is routed through your local network. Click **Refresh** to update the information.

## VPN Passthrough

A **Virtual Private Network (VPN)** is a type of secured private network connection, built upon publicly-accessible infrastructure such as the Internet. They usually provide connectivity to various devices behind a gateway or firewall.

### **IPSec Passthrough**

IP Security (IPSec) provides authentication and encryption. Since it is mainly a Layer 3 technology, it can secure all data on the network. To allow IPSec tunnels to pass through the Router, click **Enabled**.

### **PPTP Passthrough**

Point-to-Point Tunneling Protocol (PPTP) allows you to establish a connection to an enterprise network. To allow PPTP tunnels to pass through the Router, click **Enabled**.

### L2TP Passthrough

Layer 2 Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks. To allow L2TP tunnels to pass through the Router, click **Enabled**.



# WiFi Setup

## **Basic WiFi Network**

Basic WiFi Network	Wizard Interne	t Router	MIFI 3.5G HSPA	Security Admin	Status
• Basic WiFi Setting	Network Mode: Network Name(SSID): Standard Channel: SSID Broadcast:	Mixed V HSPA_ROUTER 7 - 2.442GHZ V © Enabled O Disabled Save St	ettings Cancel Chang	Help	

## Basic WiFi Setting

**Network Mode:** From this drop-down menu, you can select the wireless standards running on your network. If you have 802.11g, 802.11b, 802.11n devices in your network, keep the default setting, Mixed. If you have only 802.11g devices, select **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-B Only**. If you do not want to use any WiFi network, select **Disabled**.

**Network Name (SSID):** Network Name is used for identifying the Wireless LAN (WLAN).

**Standard Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain (e.g in the USA, it is 1 to 11).

**SSID Broadcast:** Disable this function will let your SSID setting not be exposed to view in the air. For security purposes, you may choose to hide your network's SSID by selecting **Disable** from the drop-down list. This will prevent computers scanning for the presence of wireless networks to detect your network name.



## WiFi Security

WiFi Security	Wizard Internet Basic WiFi Network	Router	Advanced WiFi Set	A Security A ting / WiFi Clients	.dmin Status s Filter
WiFi Security Setting	Security Mode:	Disabled V WEP WPA-Personal WPA-Personal WPA2-Enterprise RADIUS Disabled Save Se	ettings Cancel C	Help	

## WiFi Security Setting

Router provides several different levels of security to protect your WiFi network. Select a level in the Security Mode drop-down menu.

#### WEP

Security Mode:	WEP
Encryption:	104 / 128-bit (26 hex digits) 💙
Passphrase:	Generate
Key 1:	
Key 2:	
Key 3:	
Key 4:	
TX Key:	1 💌

The Router supports two WEP (Wired Equivalent Privacy) standards: 64-bit and 128-bit. Select a standard from the drop-down list. The 64-bits encryption requires 10 hexadecimal digits (letters a-f and numbers 0-9 are valid). The 128-bits encryption requires 26 hexadecimal digits (letters a-f and numbers 0-9 are valid). You can set up to four different keys.

**Passphrase:** Strings of hexadecimal characters are not easy to remember. This conversion utility converts a simple word or phrase into hex, so that you can easily remember and regenerate the pass-phrase.

TX Key: You can specify which key you want to use for the WiFi network.

WPA, or WiFi Protected Access, is a WiFi standard that was designed to improve the security features of WEP. WPA uses two encryption methods, TKIP and AES, with dynamic keys.



#### **WPA-Personal**

Encryption: TKIP V Passphrase:	
Passphrase:	
Key Renewal: 3600 seconds	

**Encryption:** Choose **TKIP** or **AES** from the drop down list. (AES is a stronger encryption method than TKIP.)

**Passphrase:** Enter a passphrase between 8-63 characters.

**Key Renewal:** Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

#### WPA2-Personal

Security Mode:	WPA2-Personal
Encryption:	AES 🗸
Passphrase:	
Key Renewal:	3600 seconds

WPA2 is a more advanced, more secure version of WPA.

Encryption: Choose AES, or WPA-TKIP, or WPA2-AES from the drop down list.

Passphrase: Enter a passphrase between 8-63 characters.

**Key Renewal:** Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.



#### **WPA-Enterprise**

WiFi Security Setting	-		
	Security Mode:	WPA-Enterprise	
	Encryption:		
	RADIUS Server:	0.0.0	
	RADIUS Port:	1812	
	Shared Key:		
	Key Renewal:	3600 seconds	
		Save Settings	Cancel Changes

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

**Encryption:** Choose **TKIP** or **AES** from the drop down list. (AES is a stronger encryption method than TKIP.)

RADIUS Server: Enter the IP Address of the RADIUS server.

**RADIUS Port:** Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

**Key Renewal:** Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

#### **WPA2-Enterprise**

	The entry to the
Encryption:	AES
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
Shared Key:	
Key Renewal:	3600 seconds

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose AES or WPA-TKIP or WPA2-AES from the drop down list.



**RADIUS Server:** Enter the IP Address of the RADIUS server.

**RADIUS Port:** Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

**Key Renewal:** Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

### RADIUS

Security Mode:	RADIUS
RADIUS Server:	0.0.0.0
RADIUS Port:	1812
Shared Key:	
Encryption:	104 / 128-bit (26 hex digits)
Passphrase:	Generate
Key 1:	32229D322935BD5290118980
Key 2:	
Key 3:	
Key 4:	
TX Key:	1 💌

RADIUS stands for Remote Authentication Dial-In User Service. It is a networking protocol that uses access servers to provide centralized management of access to large networks.

**RADIUS Server:** Enter the IP Address of the RADIUS server.

**RADIUS Port:** Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

**Encryption:** Select either 64-bits or 128-bits from the drop-down list The 64-bits encryption requires 10 hexadecimal digits. The 128-bits encryption requires 26 hexadecimal digits .You can set up to four different keys.

**Passphrase:** Strings of hexadecimal characters are not easy to remember. This conversion utility converts a simple word or phrase into hex, so that you can easily remember and regenerate the pass-phrase.

**TX Key:** You can specify which key you want to use for the WiFi network.



### Disabled

If you do not want to use any security method for your wireless network, choose **Disabled**.

## **Advanced WiFi Setting**

Advanced WiFi Setting	Wizard Internet	: Router VIII 3.5G HSPA Se	ecurity Admin Status
	Basic WiFi Network	/ WiFi Security / Advanced WiFi Setting	/ WiFi Clients Filter
<ul> <li>Advanced WiFi Setting</li> </ul>	-		Help
	AP Isolation:	Enabled Image: Disabled (Default: Disabled)	
	Frame Burst:	💿 Enabled 🔘 Disabled ( Default: Enabled)	
	Authentication Type:	Auto (Default: Auto)	
	Basic Rate:	Default V (Default: Default)	
	Transmission Rate:	Auto 💙 (Default: Auto)	
	Transmission Power:	High 🕑 (Default: High)	
	CTS Protection Mode:	Auto 💙 (Default: Auto)	
	Beacon Interval:	100 (Default: 100, milliseconds, Range: 20~1000)	
	DTIM Interval:	3 (Default: 3, Range: 3 - 255)	
	Fragmentation Threshold:	2346 (Default: 2346, Range: 256 - 2346)	
	RTS Threshold:	2347 (Default: 2347, Range: 256 - 2347)	
		Save Settings Cancel Changes	

**AP Isolation:** This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other.

**Frame Burst:** Enabling this option may provide your network with greater performance.

**Authentication Type:** The default is Open System authentication, where the sender and the recipient do not use a WEP key for authentication. To use a WEP key for authentication, select Shared Key.

**Basic Rate:** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router advertises its Basic Rate to the other wireless devices in your network, so they know which rates are used. The Router also advertises that automatically selects the best rate for transmission. The default setting is **Auto**, where the Router can transmit at all standard wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the **Transmission Rate** setting.



**Transmission Rate:** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds.

**CTS Protection Mode:** CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). The default setting is **Auto** and the Router automatically uses CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy traffic. This function boosts the Router's ability to catch all Wireless-B and Wireless-G transmissions, but it severely decreases performance.

**Beacon interval:** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting.

**DTIM Interval:** The default setting for DTIM (Delivery Traffic Indication Message) is 3. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

**Fragmentation Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the setting value will be fragmented before transmission. 2346 is the default setting.

**RTS Threshold:** This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.



## **WiFi Clients Filter**

WiFi Clients Filter	Wizard	Internet Rout	ter Wil	3.5G HSPA	Security	Admin	Status
	Basic WiFi	Network / WiFi S	ecurity /	Advanced WiFi Setting	/ WiFi C	lients Filter	
WiFi Clients Filter	Cominan	C Enchlad	<ul> <li>Disable</li> </ul>	4	Help	<u>o</u>	
	Service.	U Enabled		u			
	Filtering By:	Prevent PCs listed	below from acc	essing the wireless netwo	ark		
		O Permit PCs listed t	pelow access to	the wireless network			
<ul> <li>Filtered Client List</li> </ul>	Wireless	Client List	Reset				
	MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00			
	MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00			
	MAC 03:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:00			
	MAC 04:	00:00:00:00:00:00	MAC 20:	00:00:00:00:00:00			
	MAC 05:	00:00:00:00:00:00	MAC 21:	00:00:00:00:00:00			
	MAC 06:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00			
	MAC 07:	00:00:00:00:00:00	MAC 23:	00:00:00:00:00:00			
	MAC 08:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00			
	MAC 09:	00:00:00:00:00:00	MAC 25:	00:00:00:00:00:00			
	MAC 10:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00			
	MAC 11:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00			
	MAC 12:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00			
	MAC 13:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00			
	MAC 14:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00			
	MAC 15:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00			
	MAC 16:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00			
			Save Settin	as Cancel Chan			
			Save Setun	cancer chang			

## WiFi Clients Filter

You can allow or deny specific users to access your wireless network by using the WiFi Clients Filter.

**Service:** To use the WiFi Clients Filter, select Enabled. To disable it, select **Disabled**.

**Filtering By:** You can filter users by two methods: **Prevent** the listed PCs from accessing the wireless network, or **Permit** the listed PCs to access the wireless network. Select the method you want.

## Filtered Client List

Enter MAC addresses in the Filtered Client List section, and click **Save Settings**.

To display a list of network users, click Wireless Client List.



# 3.5G HSPA Setup

## **PIN Verification**

PIN Verification	Wizard         Internet         Router         WiFi         1.5C (ISPA)           Fill Wernication         /         PIII Management         /         Preferred lietwork	Security Admin Status
<ul> <li>U/SIM's PIN Verification</li> </ul>		Help
	SIM Status: PIN Disabled	
	PIN Code: (4 ~ 8 digits)	
	Verify	

If your SIM card PIN protection is enabled, you must enter the PIN code for verification. Enter the code in the PIN Code field, and click **Verify**.

## **PIN Management**

PIN Management	Wizard Interne PIII Verification /	et Router PIII Management	WiFi / Prefei	3.5G HSPA Ted Network	Security	Admin	Status
• U/SIM's PIN Management	SIM Status: PIN Protectio	PIN Disabled n: 🔿 Enabled 💿	Disabled		He	<u>p</u>	
• U/SIM's Change PIN	PIN Code: Old PIN Code: New PIN Code:	Apply	(4 ~	8 digits) 8 digits)			
		Change			1		

## U/SIM's PIN Management

After your SIM card is verified, you can enable or disable the PIN protection on your SIM card. Select **Enabled** or **Disabled**, and click **Apply**.



## U/SIM's Change PIN

You can change the PIN code on the SIM card. Enter your original PIN code in the **Old PIN Code** field, enter the new PIN code in the **New PIN Code** field and the **New PIN Confirm** field, and click **Change**.

## **Preferred Network**

Preferred Network	Wizard Internet Router WiFi 1.66 JISVA	Security Admin Status
Preferred Network	PIII Verification         PIII Management         Preferred lifetxeat           Network Type:         Auto         V	Help
Network Selection	Select Network:   Auto  Manual	
	Rescan	
	Select	
	Save Settings Cancel Chan	ges

### **Preferred Network**

**Network Type:** In the drop-down menu, select the network type your SIM card supports. If you do not know the network type, select **Auto**.

## **Network Selection**

To select the mobile network operator automatically, in the **Select Network** field, select **Auto**. To select the operator from a list, select **Manual** and click **Rescan**. The list is displayed below. Select the mobile network operator you are currently using on your SIM card.



# Security Setup

## Firewall

Firewall	Wizard	Internet	Router	WiFi	3.5G HSPA	Security	Admin	Status
	Firewall / In	ternet Access	s Policy / Sing	gle Port Forwa	rd / Port Rang	e Forward /	Port Range Tri	igger /QoS
• Firewall	6					He	alp	
	SPI Firewall P	rotection:	⊙ Enabled (	) Disabled				
	Internet filter	services:	Filter Anony	nous Internet Re	quests			
			Eitter Multica	st				
			Eitter Internet	t NAT Redirection	ı			
			Filter IDENT (	Port 113)				
	Web filter se	rvices:	Proxy J	ava 🗌 ActiveX	Cookies	_		
	DMZ service:		🔿 Enabled (	) Disabled				
	Source IP Ad	dress:	Any IP Addre	355				
	Destination:		D     Address:	192 169 1 0	0			
	D South Multim		O MAC Address.	ss: 00:00:00:00:	00:00			
		_	Sa	ve Settings	Cancel Chan	iges		

## Firewall

This tab is used to configure a firewall that filters out various types of unwanted traffic on the Router's local network.

### **SPI Firewall Protection**

The SPI (stateful packet inspection) firewall is programmed to recognize legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

#### Internet filter services

Filter Anonymous Internet Requests: This feature makes it more difficult for outside users to work their way into your network.

**Filter Multicast:** Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, the Router allows



IP multicast packets to be forwarded to the appropriate computers.



Filter Internet NAT Redirection: To use port forwarding to block access to local servers from local networked computers, select Filter Internet NAT Redirection.

Filter IDENT (Port 113): This feature keeps port 113 from being scanned by devices outside of your local network.

#### Web filter services

Using the Web Filters feature, you may enable up to four specific filtering methods.

**Proxy:** Use of WAN proxy servers may compromise the Router's security. Select this option to disable access to any WAN proxy servers.

**Java:** Java is a programming language for websites. Select this option to disable Java. If you disable Java, you run the risk of not having access to Internet sites created using this programming language.

**ActiveX:** ActiveX is a programming language for websites. Select this option to disable ActiveX. If you disable ActiveX, you run the risk of not having access to Internet sites created using this programming language.

**Cookies:** A cookie is data stored on your PC and used by Internet sites when you interact with them. Select this option to disable cookies.

#### **DMZ** service

When a firewall is used, it is sometimes necessary to place some clients (for example Internet games, video conferencing, or VPN connections) outside of the firewall while leaving the others protected. You can do this using a Demilitarized Zone. This feature allows you to specify the IP address of the computers that are placed outside the firewall of your network.

#### **Source IP Address**

If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

### Destination

Enter the IP address or MAC address of the computer you want to expose.



## **Internet Access Policy**

Internet Access Policy	Wizard Internet	Router	WiFi	3.5G HSPA	Security	Admin	Status
	Firewall / Internet Access	Policy / Singl	le Port Forward	/ Port Range	e Forward	/ Port Range Tr	igger /QoS
<ul> <li>Internet Access Policy</li> </ul>	Access Policy: 10	Delete This	s Policy Si	ummary		<u>Help</u>	
	Enter Policy Name: Status:	⊖Enabled ⊙D	Disabled				
Applied PCs	Edit List (This policy a	oplies only to PC	s on the list.)				
Access Restriction	● Deny Internet ar ○ Allow	ccess during selec	ted days and hou	NS.			
Schedule	Days: ✓Everyday [ Times: ④ 24 Hours (	Sun Mon .	Tue 🗌 Wed 📃 🖌 - 00 💙; 00	Thu 🗌 Fri 📃	Sat		
Website Blocking by URL Address	URL 1:	UR	1L 2: 1L 4:				
Website Blocking by Keyword	Keyword 1:	Ki	eyword 2:				
Blocked Applications	Note: You can only add up to	o 3 applications into	o the blocked list.	_			
	Appreations PNS (53-53) HTTP (80-80) HTTPS (443-443) FTP (21-21) POP3 (110-110) IMAP (143-143) SMTP (25-25) NNTP (119-119) SNMP (161-161)	>>>					
	Application Name C Port Range 53	INS					
	Protocol	UDP 💌					
	Add Modify	Delete					
		Sav	e Settings	Cancel Chang	ges		

Access can be managed by a policy. Use the settings on this screen to establish and access policies. To display a policy's settings, select the policy from the drop-down menu. To delete a policy, select the policy's number and click **Delete This Policy**. To view all the policies, click **Summary**. To delete multiple policies, in the Summary screen, selecting the policies and click **Delete**).



To create an Internet access policy:

- 1. Select a number from the Access Policy dropdown menu.
- 2. Enter a policy name in the field provided.
- 3. To enable the policy, select Enabled.

MAC Address	01	00:00:00:00:00:00	06	00:00:00:00:00
	02	00:00:00:00:00:00	07	00:00:00:00:00:00
	03	00:00:00:00:00:00	08	00:00:00:00:00:00
	04	00:00:00:00:00:00	09	00:00:00:00:00
	05	00:00:00:00:00	10	00:00:00:00:00
IP Address	01	192. 168. 101. 0	04	192. 168. 101. 0
	02	192. 168. 101. 0	05	192. 168. 101. 0
	03	192. 168. 101. 0	06	192. 168. 101. 0
Address Range	01 1	92. 168. 101. 0 ~ 0	03 19	92. 168. 101. 0 ~ 0
	02 1	92. 168. 101. 0 ~ 0	04 19	92. 168. 101. 0 ~ 0

- 4. To select which PCs are affected by the policy, click Edit List. The List of PCs screen appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want the policy to affect a group of PCs. After making your changes, click Save Settings to apply your changes or Cancel Changes to cancel your changes. Then click Close.
- **5.** Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.
- 6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. To set times for the policy, select 24 Hours, and enter the times you want.
- To filter websites by URL, enter URLs in the Website Blocking by URL Address fields. To filter websites by keywords, enter keywords in the Website Blocking by Keyword fields.
- 8. To filter access to various services accessed over the Internet, such as FTP or telnet, select services in the Applications column, and click Add to add them to the Blocked List. (You can only add up to 3 applications.) You can also add an application into the Applications column. Enter the information in the Application Name, Port Range



and Protocol fileds, and click Add.

## **Single Port Forward**

Single Port Forward	Wizard	Internet	Router	WiFi	3.5G H	SPA	Security	Admin	Status
	Firewall / Inte	ernet Access P	olicy / Si	igle Port Forwar	d / Poi	rt Range F	orward /	Port Range T	rigger /QoS
Single Port Forwarding	<u> </u>						He	łn	
Application Name	External Port	Internal Port	Protocol	To IP addre	ss	Enabled			
None 💌				192.168.1.	0				
None 💌				192.168.1.	0				
None 💌				192 . 168 . 1 .	0				
None 💌				192.168.1.	0				
None 💌				192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			TCP 🔽	192 . 168 . 1 .	0				
			TCP 🔽	192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			TCP 🔽	192 . 168 . 1 .	0				
			TCP 💌	192 . 168 . 1 .	0				
			ТСР 🚩	192 . 168 . 1 .	0				
			s	ave Settings	Cance	el Change:			

## Single Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications. To forward a port, enter the information in each field.

**Application Name:** You can select an application from the 10 preset applications in the drop-down menu. For custom applications, enter the name of your application in one of the available fields.

**External Port:** Enter the port number of external ports used by the server or Internet application.

**Internal Port:** Enter the port number of internal ports used by the server or Internet application.

**Protocol:** Select the protocol used for this application: TCP, UDP, or Both.

**To IP address:** For each application, enter the IP address of the PC running the specific application.

**Enabled:** To enable port forwarding for the application, select **Enabled**.

To apply the changes, click **Save Settings**.



Port Range Forward	Wizard	Internet	Router	WiFi	3.5G HS	PA S	ecurity	Admin	Status
	Firewall / Ir	nternet Access	Policy / Sing	gle Port Forwar	d / Port	l Range Fo	rward /	Port Range Tr	igger /QoS
Port Range Forwarding	6						Не	alp	
Application Name	Start	~ End Port	Protocol	To IP addre	ess	Enabled			
		-	TCP 💌	192.168.1.	0				
		-	TCP 💌	192.168.1.	0				
		-	TCP 💌	192.168.1.	0				
		-	TCP 💌	192.168.1.	0				
		-	TCP 💌	192 . 168 . 1 .	0				
			TCP 💌	192.168.1.	0				
			TCP 💌	192.168.1.	0				
			TCP 🔽	192.168.1.	0				
			TCP 💌	192.168.1.	0				
			TCP 💌	192.168.1.	0				
			TCP 💌	192.168.1.	0				
			TCP 💌	192.168.1.	0				
				192.168.1.	0				
				192.168.1.	0				
				192.168.1.	•				
			Sa	ve Settings	Cancel	Changes			

## Port Range Forwarding

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

Application Name: Enter the name of your application.

**Start - End Port:** Enter the number that starts the port range in the left field and the number that ends the range in the right field.

**Protocol:** Select the protocol used for this application: **TCP**, **UDP**, or **Both**.

**To IP address:** For each application, enter the IP address of the PC running the specific application.

**Enabled:** To enable port forwarding for the application, click the **Enabled** checkbox to enable port forwarding for the relevant application.

To apply the changes, click **Save Settings**.



## Port Range Trigger

Port Range Trigger	Wizard Inter	net Router	WiFi 3.5G	HSPA Se	eurily Admin	Status
	Firewall / Internet /	Access Policy / Sing	gle Port Forward 🥖 F	Port Range For	ward / Port Range 1	rigger /QoS
<ul> <li>Port Range Triggering</li> </ul>	6				Help	
	Application Name	Triggered Range	Forwarded Range	Enabled		
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		-	-			
		Sa	ve Settings Car	icel Changes		

## Port Range Triggering

This feature allows the Router to watch outgoing data for specific port numbers. The Router remembers the IP address of the computer that sends the matching data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Application Name: Enter the application name of the trigger.

**Triggered Range:** For each application, enter the triggered port number range. Check with the Internet application documentation for the port number needed. Enter the starting port number of the Triggered Range in the left field. Enter the ending port number of the Triggered Range in the right field.

**Forwarded Range:** For each application, enter the forwarded port number range. Check with the Internet application documentation for the port number needed. Enter the ending port number of the Triggered Range in the right field.

Enabled: To enable port triggering for the application, select Enabled.



## QoS

005				_				_
400	Wizard Firewall / I	Internet Internet Access	Router Policy / Sing	WiFi le Port Forwa	3.5G HSP. rd / Port F	A Secur Range Forwa	ny Admin rd / Port Range	Status • Trigger / 005
QoS Control	F						Help	
Wireless	VVMM Suppo	ort: (	⊙ Enabled ○	Disabled (Det	fault: Enabled	)		
	No Acknow	ledgement: (	🔘 Enabled 💿	Disabled (Det	fault: Disablec	D)		
nternet Access Priority	O Enable	d 💿 Disabled						
Category	Application	$\sim$						
	Application	n MSN Mes	senger	$\sim$				
	Priority	Medium (	Recommended)	~				
		Add						
Summary								

## **QoS** Control

Quality of service is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

#### Wireless

**WMM Support:** If no devices on your network support WMM, select **Disabled**. Otherwise, keep the default, **Enabled**.

**No Acknowledgement:** If the Router's Acknowledgement feature is disabled, the Router will not re-send data if an error occurs, then keep the default, **Disabled**. Otherwise, select **Enabled**.

#### **Internet Access Priority**

You can set the Internet bandwidth priority for a variety of applications and devices. There are four levels priority: **High**, **Medium**, **Normal**, and **Low**. To use the Internet Access policies you set, select **Enabled**.

### Category

There are four categories available. Select one of the categories and proceed to the instructions for your selection.



#### To add an online games or applications:

- 1. Select the appropriate online games or applications.
- 2. Select the appropriate priority: High, Medium, Normal, or Low.
- 3. Click Add to save your changes.

#### To add a new online games or applications:

- 1. Select Add a New Game/Application.
- 2. Enter any name to indicate the name of the entry.
- **3.** Enter the port range that the application will be using. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535.
- 4. Select the protocol TCP or UDP, or select Both.
- 5. Select the appropriate priority: High, Medium, Normal, or Low.
- 6. Click Add to save your changes.

#### To add an MAC address:

- 1. Enter a name for your device.
- 2. Enter the MAC address of your device.
- 3. Select the appropriate priority: High, Medium, Normal, or Low.
- 4. Click Add to save your changes.

#### To add a Voice Device:

- 1. Enter a name for your voice device.
- 2. Enter the MAC address of your voice device.
- 3. Select the appropriate priority: High, Medium, Normal, or Low.
- 4. Click Add to save your changes.

#### Summary

This lists the QoS entries you have created for your applications and devices. Select **Edit** to edit an item or **Remove** to remove the item. Preset items cannot be edited.



# Admin Setup

## Management

Management	Wizard	Internet	Router	WiFi	3.5G HSPA	Security	Admin	Status
	Manageme	nt / Dia	gnosis /	Recover & R	enewal			
Router Access	<u> </u>					Hel	p	
	Router Passwo	ird:	•••••	•				
	Re-Enter to cor	ıfirm:	•••••	•				
Web Access								
	Web Utility Acc	ess:	💿 нттр (	HTTPs				
	Web Utility Acc Wireless:	ess via	Enabled	🔘 Disabled				
Remote Access								
	Remote Manage	ement:	O Enabled	💿 Disabled				
	Web Utility Acc	ess:	• НТТР	HTTPs				
	Remote Upgrad	e:	Enabled	O Disabled				
	Allow Remote I	P Address:	Any IP Add	iress				
	Remote Manage	ement Port:	0 0. 8080	• . • . ]	00			
• UPnP						-		
	UPnP:		📀 Enabled (	O Disabled				
	Allow Users to	Configure:	📀 Enabled (	🔿 Disabled				
	Allow Users to Internet Access	Disable s:	C Enabled	⊙ Disabled				
			Si	ave Settings	Cancel Chan	iges		

## **Router Access**

You can change the Router's password here. Enter the password you want to set in the **Router Password** field, and re-enter it in the **Re-Enter to confirm** field. Then click **Save Settings**.

## Web Access

**Web Utility Access: HTTP** (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. **HTTPs** uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security.

**Web Utility Access via Wireless:** If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. The wireless



access to the Router web-based utility can be disabled. If you disable the setting, you are only able to access the web-based utility via a wired connection.

## **Remote Access**

**Remote Management:** To access the Router remotely, from outside the network, select **Enabled**.

Web Utility Access: Choose to access the Router via HTTP or HTTPs.

**Remote Upgrade:** To enable remote upgrade of the Router, select **Enabled**.

Allow Remote IP Address: To allow any IP address to access to access the Router, select Any IP Address. To allow a specific range of IP addresses to access the Router, enter IP addresses.

**Remote Management Port:** Enter the port number that will be open to outside access.

## UPnP

**UPnP:** Universal Plug and Play (UPnP) is a set of computer network protocols that allows compatible devices to be ready to work without any configuration once they are connected to the network.

Allow Users to Configure: To enable manual changes to the Router while using the UPnP feature, keep the default setting, **Enabled**. To disable manual changes, select **Disabled**.

Allow Users to Disable Internet Access: To prohibit users from accessing the Router web-based utilities, keep the default setting, **Disabled**. Otherwise, select **Enabled**.



## Diagnosis

Diagnosis	Wizard Interne	et Router	WiFi	3.5G HSPA	Security	Admin	Status
	Management /	Diagnosis /	Recover & Re	newal			
• Log	6				Help		
• Ping Test	Service: Logviewer IP Address: View Log	<b>Enabled</b> (	Disabled (0 means di	sabled)			
	IP or URL Address: Packet Size: Number of Pings:	32 bytes ( 5 V Start Test	(32~65500)				
• Traceroute Test	IP or URL Address:	Start Test					
		Sa	ive Settings	Cancel Change	es		

## Log

The Router can keep logs of all traffic for your Internet connection. To monitor the network, select **Enabled**.

You can view logs by clicking **View Log**. If you want to view logs in a browser, enter an IP address in the **Logviewer IP Address** field. You can enter this IP in a browser to view logs.

## Ping Test

To check the status of a connection, enter the IP address or URL that you want to ping in the **IP or URL Address** field, define the packet size you want to use in the **Packet Size** field, And select the number of times you wish to ping: **5**, **10**, **15**, or **Unlimited**. Click **Start Test** to begin the ping test. A new screen displays the test results.

## Traceroute Test

To test the performance of a connection, enter a URL or IP address in the **IP or URL Address** field, and click **Start Test**. A new screen displays the test results.



Recover & F	Renewal			
Recover & Renewal	Wizard         Internet         Router         WiFi         3.5G HSPA         Securit           Management         /         Diagnosis         /         Recover & Renewal	y Admin Status		
Backup and Restore	Backup Configurations Restore Configurations	Backup and Restore You can click the Backup Configurations button or Restore Configuration button to backup or restore your Router settings		
Factory Defaults     APN Update	Restore Factory Defaults	Restore Factory Defaults Restore Factory Default allows you to reset all of the Router's configuration settings to the default values.		
Router Upgrade	Get Latest APN Database         Please Select a File to Upgrade:	Get Latest APN Database You can press the button to get the latest Profile Name, Number, User Name, Password, and APN from the BandRich web site automatically.		
	Start Upgrade Warning: Upgrading firmware may take a few minutes; please don't turn off the power or press the Reset button.	Router Upgrade Router Firmware can be upgraded by clicking the Start Upgrade button after browsing for the firmware. The latest Firmware version can be downloaded from the menufacturer website		
	0% Upgrade must NOT be interrupted !!			

## **Backup and Restore**

### **Backup Configurations**

Click **Backup Configurations** to back up your Router's current configuration. In the file dialog box, select a location and file name for the configuration file.

#### **Restore Configurations**

Click the Restore Configurations. In the file dialog box, click Browse to locate the configuration file, and click Restore.

### Factory Defaults

To reset the Router's configuration settings to the default values, click **Restore Factory Default.** 

### APN Update

To update the APN database, click Get Latest APN Database. In the



dialog box, click Start.

## Router Upgrade

To upgrade the Router's firmware, click **Browse** and locate the latest firmware upgrade file. After the file is located, click **Start Upgrade**. The upgrade progress is displayed.



**Warning:** Upgrading firmware may take a few minutes; do not turn off the power or press the Reset button during upgrade.



# Status

## 3.5G HSPA & Internet

3.5G HSPA & Internet	Wizard Inter	net Router	WiFi 3.5G HSPA	Security	Admin	Sintus
	3.56 HSPA & Intern	iet / Router				
<ul> <li>Single Quality</li> </ul>	Rx Signal Strength:	a -	Refresh	Help		
● U/SIM Status	SIM Status:	PIN Disabled	PIN unlock	]		
Register Network	Network Name: Network Technology: Home/Roaming:	FET Taiwan 3G(VVCDMA) Home	Select network	)		
<ul> <li>Internet Connection</li> </ul>	Connection Type:	3.5G HSPA APN: fetims	Change APN	)		
	Internet IP Address: Subnet Mask: Default Gateway: DNS 1:	114.140.54.146 255.255.255.255 10.64.64.64 210.241.192.201				
	DNS 2: DNS 3:	168.95.1.1 0.0.0.0				
		_	_			

## Signal Quality

When you access the Internet via 2G or 3G, click **Refresh** to show the signal strength.

### **U/SIM Status**

Your SIM card verification status is shown in this area. Clicking **Pin unlock** displays the **PIN Verification** tab.

### **Register Network**

Network Name: This shows the name of your network operator.

Network Technology: This shows the network technology you are



currently using.

**Home/Roaming:** This indicates whether the Router is in Home or Roaming status.

## Internet Connection

**Connection Type:** This indicates the type of Internet connection you are using.

**Internet IP Address:** This is the Router's IP Address, as seen on your local network.

**Subnet Mask** and **Default Gateway:** The Router's Subnet Mask and Default Gateway address are displayed here for DHCP and static IP connections.

**DNS1-3:** The DNS (Domain Name System) IP addresses currently used by the Router are shown here.

## Router

Router	Wizard Intern 3.5G HSPA & Interne	et Router	WiFi	3.5G HSPA	Security	Admin	Sistus
					_		
<ul> <li>Firmware Information</li> </ul>					Help	<u></u>	
	Firmware Version:	1.03.000.001_200906	15				
	Modern Version:	120085_001_012					
	APN Version:	1.00					
	Current Time:	Thu Jan 1 00:02:02 1	1970 (GMT -08:0	0)			
<ul> <li>Local Network</li> </ul>							
	Local MAC Address:	00:21:00:F0:08:C7					
	Router IP Address:	192.168.1.1					
	Subnet Mask:	255.255.255.0					
					-		
	DHCP Server:	Enabled	C	hange			
	Start IP Address:	192.168.1.100					
	End IP Address:	192.168.1.149					
	DHCP Client Table						
• WiFi Network		_					
	MAC Address:	00:21:00:F0:08:C7					
	Mode:	Mixed					
	Network Name (SSID):	HSPA_ROUTER	0	hange			
	Standard Channel:	7		_			



## Firmware Information

Firmware Version: This is the Router's current firmware.

Modem Version: This is the 3G Module's current firmware.

APN Version: This is the APN's current version.

Current Time: This shows the time, as you set on the Optional tab.

## Local Network

Local MAC Address: This is the Router's MAC Address, as seen by your ISP

**Router IP Address:** The Router's IP Address that appears on your local network.

**Subnet Mask:** This shows the current subnet mask being configured for your local network.

**DHCP Server:** The status of the DHCP server function is displayed here.

**Start IP Address:** This shows the beginning of the range of IP Addresses used by devices on your local Ethernet network.

**End IP Address:** The end of the range of IP Addresses used by devices on your local Ethernet network is shown here.

**DHCP Client Table:** Click this button to open a screen showing you which PCs are utilizing the Router as a DHCP server.

## WiFi Network

**MAC Address:** This is the Router's MAC Address, as seen on your local wireless network.

**Mode:** This displays the wireless mode (Mixed, Wireless-G Only, Wireless-B Only, or Disabled) used by the network.

**Network Name (SSID):** This displays the wireless network name or SSID.

**Standard Channel:** This displays the channel on which your wireless network is broadcasting.

Security: This shows the security method you are using.

**SSID Broadcast:** This shows whether the Router's SSID Broadcast function is on or off.



# Appendix A: FAQ

Q: What should I know and how long does it take when I upgrade the firmware of router or modem?

- A: 1. While upgrade the firmware, it must take some time to do the job. During that, you ARE NOT ALLOWED to turn off the power or interrupt the progress.
  - 2. You may use Ethernet cable or Wireless to upgrade the firmware. It is suggested to use Ethernet cable.
  - 3. It may take 2 minutes to upgrade the firmware of the router and 5 minutes to upgrade the firmware of the modem.
  - 4. When the firmware of the modem is upgrading, the UMTS LED will flash among Blue-Green-Red. You should wait until the LED is in single color (about 4~5 minutes).
- Q: How to connect to Router?
- A: 1. Connect Ethernet cable between PC/NB and Router.2. Use WiFi to connect.
- Q: What's the default "User name" and "Password" for the Router?
- A: User name: admin Password: hsparouter
- Q: How to enter GUI?
- A: 1. Connect PC/NB to Router.
  - 2. Open Internet Explorer or other Web browser.
  - 3. Input "http://192.168.1.1" (default) or "http://R300.ROUTER".
  - 4. Input User name and Password.
- Q: How to setup the configuration for the Router?
- A: 1. Enter Wizard page to setup.
  - 2. Enter each GUI page to setup.
- Q: Why can't I connect to the network via built-in 3G module?
- A: 1. Check the SIM/USIM if it is inserted well.
  - 2. Check the UMTS LED on Router if it is Solid.
  - 3. Check the Status on GUI if the SIM/USIM detected well.
  - 4. Check the Status on GUI if the APN it is correct.
  - 5. Check the Internet on GUI if the Connection is "Keep Alive" or not.
- Q: Why the Roaming LED on Router is light?
- A: Because the SIM/USIM is in roaming network.



If you want to connect to the network while roaming:

- 1. Ask the operator of SIM to turn on the roaming service allowed to connect to the network.
- 2. Set the Internet on GUI with Roaming Connection Enabled.

Q: Why can't I link on the GUI?

A: If you have changed your WiFi security, SSID, Local IP address, you have to repair your network to get a new IP that you can link the GUI. **XP:** 

If you are a WiFi user, click Network Connections and right click on Wireless Network Connection, click Repair.



If you use Local Area Connection to connect the Router, click Network Connections and right click on Local Area Connection, click Repair.



Edit View, Favorites T	iools 4	Advanced He	lp	
) Back - 🕥 - 🏂 🔒	¥ 🕻		•	
iress 🔕 Network Connections	10000			
Network Tasks	<u>^</u> _	LAN or High-	Speed Internet	
<ul> <li>Create a new connection</li> <li>Set up a home or small office network</li> <li>Change Windows Firewall settings</li> <li>Disable this network device</li> <li>Repair this connection</li> </ul>		Wireless Network	Local Area Connection 2	Local Are Connection Disable Status Repair Bridge Connections Create Shortcut
Rename this connection				Delete
View status of this connection				Properties
Change settings of this				

Vista:

1. If you are a WiFi user, please click Network and Sharing Center > Manage network connections > Wireless Network Connection > Diagnose

eneral		
Connection		
IPv4 Connectivi	ty:	Local
IPv6 Connectivi	ty:	Limited
Media State:		Enabled
SSID:		Stelera
Duration:		03:31:07
Speed:		54.0 Mbps
Signal Quality:		lite
D <u>e</u> tails	Wireless Properties	3
Activity		
	Sent —	Received
Bytes:	146,376	1,061,581
Properties	🛞 <u>D</u> isable Dia	agnose
		Class

2. Please click Reset the network adapter "Wireless Network Connection" and it will began to repair.





- If you use Local Area Connection to connect the Router, please click Network and Sharing Center > Manage network connections > Local Area Connection > Diagnose, do the step 1 and following the message to repair it.
- Q: How to setup my WiFi settings from GUI?
- A: Entering the GUI first then click WiFi > Basic WiFi Network, you can setup your basic WiFi settings here.

If you want to set your WiFi Security please click "WiFi Security". There are six wireless security mode options supported by the Router: WEP, WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, RADIUS.

WiFi Security	Wizard	Internet	Router	WIFI	3.5G HSPA	Security	Admin	Status
	Basic WiF	i Network	/ WiFi Security	/ Advan	ced WiFi Setting	j / WiFi (	Clients Filter	
WiFi Security Setting						He	<u>elp</u>	
	Security Mod	de:	Disabled WEP WPA-Personal WPA-Enterprise RADIUS Disabled	ve Settings	Cancel Char	nges		

- Q: How can I have a long-time link?
- A: Please set the internet > Basic Setting > 3.5G HSPA Setting > Connection to Keep Alive.
- Q: Why can't I use the Router in the office?
- A: Your Router's IP address might be conflict with the office default settings.
- Q: Why my internet speed is so slow with Router?
- A: 1. You can check the GUI Status > Single Quality, the Rx Signal Strength. If the footstep is too low it means the signal is too weak.



3.5G HSPA & Internet	Wizard II 3.56 HSPA & Im	nternet Route lennet / Router	r WiFi	3.5G HSPA	Security	Admin	Status
<ul> <li>Single Quality</li> </ul>	Rx Signal Strength	a.		Refresh		p	
U/SIM Status	SIM Status:	PIN Disabled		PIN unlock			

2. You can go to the GUI WiFi > Basic WiFi Network, change the Standard Channel to others then save.

Basic WiFi Network	Wizard         Internet         Router         Will         3.5G HSPA         Security         Admin         Status           basic Will Hetwork         /         WiFi Security         /         Advanced WiFi Setting         /         WiFi Clients Filter	J
• Basic WiFi Setting	Network Mode:       Mixed       Help         Network Name(SSID):       HSPA_ROUTER         Standard Channel:       7 - 2.442GHz         SSID Broadcast:       Image: Cancel Changes	

- Q: Why can't I use VPN via Router?
- A: You may check your office IP settings, the IP settings must not conflict with each other.
- Q: How do I do the settings when I use xDSL to link the Router?
- A: 1. PPPoE: Go to the GUI Internet > Basic Setting > Ethernet Setting. Change Connection Type to PPPoE Fill information in the blank of Username and Password which provide by your ISP. Remember to connect your xDSL or Modem to the WAN Port on your Router.
  - Static IP: Go to the GUI Internet > Basic Setting > Ethernet Setting. Change Connection Type to Static IP. Fill information in the blank provide by your ISP. Remember to connect your xDSL or Modem to the WAN Port on your Router.
- Q: Can I prevent others from using my Router?
- A: Yes, there are some ways to prevent others from using your ROUTER.
  - 1. Enable your WiFi client filter.
  - 2. Disabled your SSID Broadcast.
  - 3. Setting your WiFi security.



Q: My PIN code is enabled and where can I input the PIN code to use my Router?

A: Enter GUI > 3.5G HSPA > PIN Verification and input your PIN Code.

PIN Verification	Wizard PIN Verifi	Internet cation / P	Router IN Management	WiFi / Prefer	3.5G HSPA rred Network	Security	Admin	Status
U/SIM's PIN Verification		SIM Status: PIN PIN Code:	Enabled(PIN Incor • Verify	rect - Retry: 3 tir (4 ^	nes remain) · 8 digits)	He	<u>lp</u>	

Q: Why does my SIM status display "No Device" or "SIM Error", what can I do?

A: You can check the SIM card is inserted correctly in your router.

- Q: Where can I change the password of Router?
- A: Enter GUI > Admin > Management

Management	Wizard	Internet	Router	WiFi	3.5G HSPA	Security	Admin	Status
	Managen	nent / Dia	gnosis /	Recover & Re	enewal			
De la trans								
<ul> <li>Router Access</li> </ul>						He	<u>up</u>	
	Router Pass	word:	•••••	•				
	Re-Enter to o	confirm:	•••••	•				

- Q: Can I backup all my settings of Router?
- A: Enter GUI > Admin > Recover & Renewal, Select "Backup Configuration".
- Q: How to use the Reset button on the Router?
- A: 1. Short press the Reset can restart the Router.
  - 2. Long press the Reset for more than 5 sec can reset the Router to factory default.

Q: Where can I reset Router to factory default?

- A: 1. Long press the Reset button on the Router for more than 5 sec.
  - 2. Enter GUI > Admin > Recover & Renewal, Select "Restore Factory Defaults".



Q: If I remove the SIM when 3G is connected, why can't I see the SIM status change?

A: You have to restart the router to see the status.



# **Appendix B: Specification**

Form Factor					
Weight (g)	170g				
Interface					
LAN port	RJ45, 1 port				
WAN port	RJ45, 1 port, can be configured to be 2 <sup>nd</sup> LAN port				
Power supply plug	Yes				
Reset button	Yes				
SIM slot	Yes, Push-push type				
Connectivity and Data Speed					
UMTS Band	By built-in module				
HSPA/WCDMA Data Rate	Uplink up to 5.7 Mbps Downlink up to R300 Series: 21/ 28.8 Mbps R200 Series: 7.2 Mbps				
WCDMA power class	Power Class 3				
WLAN	802.11b/g with Pre-n 2.4 GHz band				
LAN	Ethernet 10/100 Mbps				
Antenna					
GSM/WCDMA Main Antenna	Embedded				
WCDMA RX Diversity Antenna	Embedded				
3G External Antenna Port	Yes				
WiFi Antenna	Embedded				



Protocol				
Default connection	"3.5G HSPA First" or "Ethernet First" customizable			
Automatic WAN connection fail-over	Supported			
WME Traffic Prioritization / Traffic Shaping	Supported			
Fixed WAN connection	DHCP, Static IP, PPPoE, PPTP, L2TP			
UMTS/HSPA connection	Connection On Demand, Keep Alive, Auto APN matching with USIM			
Security	Multiple VPN passthrough (IPsec, PPTP, L2TP), Internet access restriction, Firewall, DoS Prevention, Traffic and Event Logging			
NAT-NAPT	Port forwarding, Port triggering, DMZ,Multicast Pass-Through, Static Routing, Dynamic Routing (RIP 1, RIP2), QoS			
DNS	DNS Agent, DDNS			
ALG Support	Yahoo messenger, AOL messenger, MSN messenger, ICQ, RealAudio, NetMeeting, Telnet, FTP, Microsoft Traceroute, Quake, IRC, Microsoft PPTP Client			
Browser-based Admin GUI	Setup Wizard in GUI. Browser supported: IE, Firefox, Safari			
Browser-based Admin GUI Multi-Language Supported	English, Traditional Chinese,			
Other Features	IPv4, TCP, UDP, ICMPv4, ARP, DHCP Server/Client, HTTPs, NTP, TFTP server, MAC Clone			
Wireless LAN				
802.11b data rate	1/2/5.5/11 Mbps, Auto or Fixed Rate			
802.11g data rate	6/9/12/18/24/36/48/54 Mbps, Auto or Fixed Rate			
802.11n data rate	65Mbps/135Mbps (No MIMO)			
Security	WPA2/WPA/AES/TKIP, WPA/WPA2 PSK mode, 802.1x (identify all EAP types supported), 64/128 bits WEP Encryption, MAC address filtering, open system and shared key authentication, SSID Broadcast Disable			
Other Features	Support up to 32 simultaneous wireless users, WME			
<b>Status Indication</b>				



LED	LED location from top to bottom: UMTS, Roaming, WLAN, Ethernet, DIAG and Power. UMTS, Roaming, WLAN, Ethernet, DIAG LED will be multiplexed for signal strength when 3G button short pushed			
Accessories				
Power adaptor	Supported, Input 100~240V AC, 50~60GHz Output 12V DC, 1A (targeted)			
Power Consumption	on			
Voltage	12V DC			
Data mode	4.0V Peak: 2.5A, Average: 1A / 1.5V average: 0.5A			
Environment				
Operation Temperature	0°C to 40°C (32°F to 104°F)			
Storage Temperature	-20°C to 60°C (-4°F to 140°F)			
Operating Humidity	10% to 80% Non-Condensing			
Storage Humidity	5% to 90% Non-Condensing			
Conformance				
	FCC			
	RoHS			



# Appendix C: Important Safety Information and Glossary

## **Europe – EU Declaration of Conformity**

# CE

#### **European Union Notice**

Products with CE marking comply with the R&TTE Directive (99/5/EC), the EMC Directive (2004/108/EC), and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards).

#### EN 60950-1 (IEC 60950-1)

Safety of Information Technology Equipment.

#### EN 300 328

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques.

#### EN 301 489-24

Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA direct spread (UTRA) for mobile and portable (UE) radio and ancillary equipment.

#### ETSI EN 301 511

Global system for mobile communications (GSM); Harmonised EN for mobile stations in the GSM 900 and GSM 1800 bands, covering essential requirements of article 3.2 of the R&TTE directive (1995/5/EC).

#### ETSI EN 301 489-1

Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements.

#### ETSI EN 301 489-7

Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS).



#### ETSI EN 301 489-17

Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems.

#### ETSI EN 301 908-1 & -2

Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third Generation cellular networks; Part 1: Harmonised EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive.

#### EN 50385

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz - 40 GHz) - General public.

## Federal Communication Commission Interference Statement

#### 15.21

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

15.105(b)

#### Federal Communications Commission (FCC) 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 or more 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 of the device.

#### FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.



## Glossary

- **2G:** Second-generation mobile networking technology. Represents a switchover from analog to digital; most 2G networks use GSM.
- **3G:** Third-generation mobile networking technology that enables simultaneous transfer of voice and non-voice data; most 3G networks use WCDMA.
- **3.5G:** A more recent standard of mobile networking technology; generally uses HSDPA.
- **3.75G:** A more recent standard of mobile networking technology; generally uses HSUPA.
- APN (Access Point Name/Network): Provides GPRS routing information. Consists of:

Network ID: Identifies the external service requested by a GPRS user.

Mobile network operator ID: Specifies routing information.

- ARFCN (Absolute Radio Frequency Channel Number): The specific ID numbers for all radio channels used in cellular mobile communications.
- bps (bits per second): How data flow is measured.
- CHAP (Challenge Handshake Authentication Protocol): CHAP identifiers are changed frequently and authentication can be requested by the server at any time.
- **DNS (Domain Name System):** Helps route network traffic by making the addressing process more user-friendly.
- **DHCP (Dynamic Host Configuration Protocol):** How devices obtain IP addresses from a server.
- **DUN (Dial-Up Network):** Windows component that enables online access via a modem.
- EDGE (Enhanced Data GSM Environment/Enhanced Data for Global Evolution): Advanced GPRS that delivers multimedia and other data needing greater bandwidth at up to 237 kbps.
- GPRS (General Packet Radio Service): Delivers data in packets at up to 86 kbps.
- **GSM (Global System for Mobile Communications):** The most popular cellular network, mostly operates in 850-900 or 1800-1900 MHz; the primary 2G system.
- **HSDPA (High Speed Downlink Packet Access):** Advanced WCDMA that delivers downlink bandwidth intensive data at up to 7.2Mbps; typically associated with 3.5G.
- **HSUPA (High Speed Uplink Packet Access):** Advanced WCDMA that delivers uplink bandwidth intensive data at up to 5.76Mbps; typically associated with 3.75G.
- HSPA+ (High Speed Packet Access +): This is also known as HSPA Evolved, is the next step and is more focused on delivering data services enabling speeds of up



to 42Mbps in the downlink and 11Mbps in the uplink.

- IMEI (International Mobile Equipment Identity): A number unique to each GSM/UMTS device that can be used block network access by a stolen mobile device.
- **IP (Internet Protocol):** Routes packets over a network.
- Kbps (Kilobits per second): A data flow measure; 1024 bits/second.
- LAN (Local Area Network): A data network with limited range but good bandwidth.
- Mbps (Megabits per second): A data flow measure; 1,048,576 bits/second.
- **PAP (Password Authentication Protocol):** The difference between PAP authentication and a manual or scripted login, is that PAP is not interactive. The username and password are entered in the client's dialing software and sent as one data package as soon as the modems have established a connection, rather than the server sending a login prompt and waiting for a response.
- PPP (Point-to-Point Protocol): An internet connection method.
- **PIN (Personal Identity Number):** Four to eight digital numbers SIM card security code; allows access to the carrier's network.
- **Rx:** Shorthand for Reception.
- **SIM (Subscriber Identity Module):** A small card that contains key mobile device identification, subscription and contact information.
- **Tx:** Shorthand for Transmission.
- WCDMA (Wideband Code Division Multiple Access): Advanced EDGE that supports 384kbps data flow. Most 3G networks use this standard, the same as UMTS.

