



### Preface

The purpose of this manual is to provide you with detailed information on the installation, operation and application of your HSPA WiFi Router with Voice Important Notice and Safety Precaution

- Before servicing or disassembling this equipment, always disconnect power from the device.
- Use an appropriate power supply, preferably the supplied power adapter, with an output of DC 12V 1.5A.
- Do not operate the device near flammable gas or fumes. Turn off the device when you are near a petrol station, fuel depot or chemical plant/depot. Operation of such equipment in potentially explosive atmospheres can represent a safety hazard.
- The device and antenna shall be used only with a minimum of 20 cm from the human body.
- The operation of this device may affect medical electronic devices, such as hearing aids and pacemakers.
- The Antennas must be connected to this product prior to connecting the telephone cord.
- The telephone cord must be disconnected prior to disconnecting the Antennas.

# Thank You

# Chapter-1

1 - Introduction	5
1.1 Features	6
1.2 Package Contents	6
1.3 LED Indicators	7
1.4 Rear Panel	7
3 - Web user Interface	
3.1 Default Settings	9
3.2 Transmission Control Protocol/Internet Protocol (TCP/IP) Settings	9
3.3 Login Procedure	12
3.4 Web User Interface Homepage	
4 - Etisalat Settings	
4.1 Etisalat Service Setup	
4.1.1 Profile Setup	
4.2 PIN Configuration	
4.2.1 PIN Code Protection	
4.2.2 PIN Code Change	
5 - Wireless	
5.1 Setup	
5.2 Security	
5.3 Configuration	21
5.4 Media Access Control (MAC) Filter	23
5.5 Wireless Bridge	23
5.6 Station Info	
<mark>6</mark> - Management	
6.1 Device Settings	
6.1.1 Backup Settings	
6.1.2 Update Settings	
6.1.3 Restore Default	
6.1.4 Update Firmware	
6.2 Access Control	27
6.2.1 Services	27
6.2.2 IP Addresses	
6.2.3 Passwords	

6.3 Configure SNMP agent on 3G10WVE	29
6.4 Simple Network Time Protocol (SNTP)	
6.5 Save and Reboot	
7. Other and active	71
7 - Advanced setup	
7.1 Local Area Network (LAN)	
7.2 Network Address Translation (NAT)	
7.2.1 Port Forwarding	
7.2.2 Port Triggering	
7.2.3 Demilitarized Zone (DMZ) Host	
7.3 Security	
7.3.1 IP Filtering	
7.4 Routing	
7.4.1 Default Router	
7.4.2 Static Route	
7.4.3 Dynamic Route	
7.5 Domain Name System (DNS)	
7.5.1 Domain Name System (DNS) Server	
7.5.2 Dynamic Domain Name System (Dynamic DNS)	
8 - Voice	20
8.1 Configuring your 3G10WVE for placing Voice Calls	
8.1 Configuring your serowve for placing voice cans	
9 - Status	
9.1 Diagnostics	
9.2 System Log	
9.3 Etisalat Status	
9.4 Statistics	
9.4.1 LAN Statistics	
9.4.2 Etisalat Statistics	
9.5 Route	
9.6 Address Resolution Protocol (ARP)	
9.7 Dynamic Host Configuration Protocol (DHCP)	
9.7 PING	
Appendix A: Print Server	
Appendix B: USB Storage	

# Table of Contents



With the increasing popularity of the 3G standard worldwide, the Etisalat HSPA WiFi Router with Voice provides you with triple-band coverage through expanding cellular networks throughout the world.

Integrating a Sierra Wireless HSPA module, this Router is capable of performing at typical downlink speeds of 550Kbps to 3Mbps, bursting up to 6Mbps and typical uplink speeds of 300Kbps to 1Mbps, bursting to 1.3Mbps in most places in the CBD, metro and other areas.

The Router also provides state-of-the-art security features such as WiFi Protected Access (WPA) data encryption, Firewall and Virtual Private Networks (VPN) pass through.



# Introduction

Introduction



### 1.1 Features

- The Etisalat HSPA WiFi Router with Voice allows you to share your Etisalat connection with multiple wireless or wired devices
- Provides you with worldwide coverage through triple-band HSUPA/HSDPA/UMTS (850/ 1900 / 2100MHz), quad-band EDGE/GSM (850/ 900 / 1800 MHz)
- Embedded multi-mode HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM module
- 1 x RJ11 port for voice calling over the Etisalat network via a connected standard Analogue Telephone (not included).
- Built-in USB 2.0 Print Server functionality
- Support for USB 2.0 Mass Storage device (NTFS, FAT 32)
- Integrated 802.11g/54Mbps AP (backward compatible with 802.11b)
- WiFi Protected Access (WPA)/ WiFi Protected Access 2 (WPA2) and 802.1x wireless encryption
- Static route/ Routing Information Protocol (RIP)/RIP v2 routing functions
- Media Access Control (MAC) address and IP filtering
- Network Address Translation (NAT) / Port Address Translation (PAT)
- Supports Universal Plug and Play (UPnP) and Internet Group Management Protocol (IGMP) snooping
- Supports Virtual Private Network (VPN) Pass-Through
- Dynamic Host Configuration Protocol (DHCP) Server/Relay/Client
- Domain Name System (DNS) Proxy and Dynamic Domain Name System (DDNS)
- Web-based Management
- Command Line Interface (CLI) via Telnet
- Configuration backup and restoration
- Remote configuration
- Router and Etisalat module firmware upgrade
- Supports half-bridging mode
- Supports Simple Network Management Protocol (SNMP)

## 1.2 Package Contents

Your package contains the following:

- Etisalat HSPA WiFi Router with Voice
- Printed Quick Start Guide
- CD (Containing User Guide)
- Ethernet Cable
- Security Card
- 2 x 3G Antennas
- 1 x WiFi Antenna
- Power Supply

# Introduction

## 1.3 LED Indicators

The LED indicators are shown in this illustration and followed by detailed explanations in the table below.

etisalat 🔈	اتصالات		H	SPA Wi-Fi Router u	
0 sut	<sup>0</sup> 1400 <sup>1</sup> 1400 <sup>1</sup> 1400 <sup>1</sup>	O str. O sterre	0* 0*	Signal Strengt	

LED	Color	Mode	Description
POWER	Green	On	Power on
		Off	Power off
Phone	Green	On	Phone line active
		Off	Phone line inactive or not connected
LAN 1~2	Green	On	Powered device connected to the associated port (includes devices with wake- on-LAN capability where a slight voltage is supplied to an Ethernet connection)
		Off	No activity, modem powered off, no cable or no powered device connected to the associated port
		Blink	LAN activity present (traffic in either direction)
WiFi	Green	On	Local WiFi access to the Router is enabled and working
		Off	Local WiFi access to the Router is disabled
		Blink	Data being transmitted or received over WiFi.
Internet	Green	Blink	Data is transmitted through Internet connection
		Off	No connection to the internet or Router powered off
		On	Internet connection established
ЗG	Green	On	Connection established with 3G network
		Blink	Connecting with 3G network
		Off	No connection with UMTS cellular station, no activity, Router powered off.
2G	Green	On	Connection established with 2G network
		Blink	Connecting to an EDGE, GPRS or GSM cellular station
		Off	No connection with EDGE, GPRS or GSM cellular station, no activity or Router powered off.
Low	Green	On	Low signal strength
		Off	No activity, Router powered off or on other signal strength
Med	Green	On	Medium signal strength
		Off	No activity, Router powered off or on other signal strength
High	Green	On	High signal strength
		Off	No activity, Router powered off or on other signal strength

NOTE: The six LEDs on the left side of the top panel display (Low, Med, High, Internet, 3G, 2G) will cycle on and off if PIN code protection is activated. In this case, you should consult section 3.2.1 PIN Code Protection (page 16) for further instructions.

### 1.4 Rear Panel

The rear panel contains the ports for data and power connections.



- (1) Power jack for DC power input (12VDC / 1.5A)/Power button
- (2) USIM card slot
- (3) USB Port (For connecting a USB Printer or USB Storage Device)
- (4) Reset button
- (5) Phone Port (for Voice calls over the Etisalat Network)
- (6) 2 RJ-45 Ethernet LAN ports





# Interface

This section describes how to access the device via the web user interface using a web browser such as Microsoft Internet Explorer (version 5.0 or later). Mozilla Firefox or Safari

# Chapter-2

### 2.1 Default Settings

The following are the default settings for the Router

- Local (LAN) access (username: admin, password: admin)
- Remote (WAN) access (username: support, password: support)
- User access (username: user, password: user)
- LAN IP address: 192.168.1.1
- Remote WAN access: disabled
- NAT and firewall: enabled
- Dynamic Host Configuration Protocol (DHCP) server on LAN interface: enabled

#### Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power LED blinks or by clicking the Restore Default Configuration option in the Restore Default Settings screen (see section 5.1.3).

## 2.2 TCP/IP Settings

It is likely that your computer will automatically obtain an IP Address and join the network. This is because the Dynamic Host Configuration Protocol (DHCP) server (on the device) will start automatically when your Router powers up.

This automatic assignment requires that DHCP is configured on your computers. It is likely that this is already the case, but should you be required to configure this, please see the instructions below.

### Windows XP

#### DHCP Mode

To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

eneral	Alternate Configuration				
this cap	n get IP settings assigned au ability. Otherwise, you need appropriate IP settings.				
0	otain an IP address automati	cally			
O Us	e the following IP address:				
IP ac	idress:				
Subr	iet mask:				
Defa	ult gateway:			3	
0 Ot	tain DNS server address au	tomatically			
O Us	e the following DNS server a	addresses:			
Prefe	erred DNS server:				
Alter	nate DNS server:				
Bros					
				Advi	anced
		-	OK		Cano

#### STATIC IP Mode

The following steps show how to configure your PC IP address using subnet 192.168.1.x. The following assumes you are running Windows XP.

- 1: From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the Properties button.
- 2: Select Internet Protocol (TCP/IP) and click the Properties button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x. (1<x<254) with subnet mask of 255.255.255.0. Set the default Router and DNS server to the Router's IP address.
- NOTE: The IP address of the Router is 192.168.1.1. (default), so the PC must be set with a different IP. In the case below, the PC's IP address is set as 192.168.1.2



3: Click OK to submit the settings.

### MAC OSX 10.4

#### DHCP Mode

To set your Apple Mac for DHCP mode, browse to the Apple menu and select System Preferences. In the System Preferences menu, click on the Network icon and select Ethernet. Next select Using DHCP from the Configure drop down list. After clicking Apply, your Mac's IP Address will now be automatically assigned from the Router.

	Location:	Automatic	
Ethernet 2 Connected     FreWire Not Connected     Orf     Bioetooth PAN Not Connected     USB Etet (en3) Not Connected     USB Etet (en3)			Connected Ethernet 2 is currently active and has the IP address (92)(83,12) Using DHCP with manual address Using BootP Manually Off Create PPPoE Service
+ - 0.			(Advanced)

### STATIC Mode

If you do not wish to use automatic assignment of IP Addresses and wish to configure your Router manually, your computer must have a static IP address within the Router's subnet. The following steps show how to configure your computer's IP address within the subnet 192.168.1.x

- 1. Browse to the Apple menu and select System Preferences. From the System Preferences, click the Network icon and select the Ethernet connection.
- 2. From the Configure drop down list, you can set your computer to Static IP mode by selecting the Manually option.



- 3. Choose an IP address between 192.168.1.2 192.168.1.254 (Do not choose the Router IP of 192.168.1.1). Enter this IP address into the field marked IP Address, and enter a Subnet Mask of 255.255.255.0
- 4. Set the Router and DNS server field to 192.168.1.1 (The Router's IP address).
- NOTE: The IP address of the Router is 192.168.1.1. (default), so the computer must be set with a different IP to the Router.In the case below, the PC's IP address is set as 192.168.1.2

Location	Automatic	•	
Connected     Connected     Connected     Lettophere		Connected Ethernet is currently active and has the address 192.568.25.102.	
Kat Connected     Mat Connected     Set Connected     Set Connected	Subnet Mask: Router: DNS Server Search Domains	192,998,1.1 192,998,1.1	
USB Rtet (enS)     Stat Connected     USB Rtet (en2)     Stat Connected     + - 0-	Search Libratins	Advance	rd.

5. Click Apply to submit the settings.

#### Windows Vista

#### DHCP Mode

To set your PC for DHCP mode, click properties of your Local Area Connection. You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

	Alternate Configuration				
this cap	n get IP settings assigned au pability. Otherwise, you nee appropriate IP settings.				
0	btain an IP address automat	ically			
O U	se the following IP address:				
IP a	ddress:	1	14	4	
Subr	net mask;				
Defa	ult gateway:	61	38.7		
00	btain DNS server address au	Itomatically			
© U:	se the following DNS server	addresses:			
Pref	erred DNS server:	Î, ki	34	5	
	nate DNS server:				

#### STATIC IP Mode

To configure your Router manually, your PC must have a static IP address within the Router's subnet. The following steps show how to configure your PC IP address using subnet 192.168.1.x. The following assumes you are running Windows Vista.

- 1: From Control panel select the Network and sharing center, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the Properties button.
- 2: Select Internet Protocol (TCP/IPv4) and click the Properties button. The screen should now display as below. Choose an IP address between 192.168.1.2 – 192.168.1.254
- NOTE: The IP address of the Router is 192.168.1.1. (default), so the PC must be set with a different IP. In the case below, the PC's IP address is set as 192.168.1.2
- 3: Set the Router and DNS server field to 192.168.1.1 (The Router's IP address).

General				
	ned automatically if your network supports u need to ask your network administrator s.			
Obtain an IP address au	tomatically			
O Use the following IP add	ress:			
IP address:	192.168.1.2			
Subnet mask:	255 . 255 . 255 . 0			
Default gateway:	192.168.1.1			
<ul> <li>Obtain DNS server address</li> <li>Obtain DNS server address</li> </ul>				
Preferred DNS server:	192.168.1.1			

3. Click OK to apply the settings.

### 2.3 Login Procedure

To login to the web interface, follow the steps below:

#### NOTE: The default settings can be found in 3.1 Default Settings.

- 1: Open a web browser and enter the default IP address for the Router in the Web address field. In this case http://192.168.1.1
- NOTE: For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.
- 2: A dialog box will appear, as illustrated below. Enter the default username and password, as defined in section 2.1 Default Settings.

Click OK to continue.

Connect to 192.1	68.1.1	? 🗙
Voice requires a user Warning: This server	is requesting that your u an insecure manner (basi	isername and
User name:	🖸 admin	~
Password:	•••••	
	Remember my passv	/ord
	ОК	Cancel

#### NOTE: The login password can be changed later (see 6.2.3 Passwords)

3: After successfully logging in for the first time, you will reach this screen.



## 2.4 Web User Interface Homepage

The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, HSPA/3G Settings, WIFI, Management, Advanced Settings and Status.

Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

### BASIC

The Basic screen is the WUI homepage and the first selection on the main menu. It provides information regarding the firmware, 3G, and IP configuration.

10	HSPR/3G SET	TINGS WI-FI	MANAGEMENT	ADVANCED SETTINGS
asic > Home				
Hardware Ver	rsiorc	96358G-133V8		
Software Ver	sion	N3G10WV-L101-S306NCM	T01_R02	
Bootloader (C	FE) Versiore	1.0.37-6.8		
Wireless Driv	er Version:	3.131.35.4.cpe2.0		
evice Info for:	3G			
Network	1			
Link:	WAN : C	onnected		
Mode:	HSDPAN	ISUPA		
Signal Streng	the Y			
SIM Info:	SEM inus	erted		
his informatio	n reflects the	current status of your coni	nection.	
	-			
LAN IP Addre		192.168.1.1		
WAN IP Addre	15.85	WAN :120.16.52.38		
Default Gatew	ray:	10.64.64.64		
Primary DNS 1	Server	202.81.67.132		
Secondary DN	IS Server:	203.2.193.67		
account of the				

The following table provides further details.

Fields	Description
Software version	The software version of the device.
Hardware version	The Hardware version of the device
Bootloader version	The bootloader version of the device.
Wireless driver	The wireless driver version of the wireless module.
version	
Network	The name of or other reference to the mobile network operator.
Link	Shows the connection status of the current Etisalat connection.
Mode	The radio access technique currently used to enable internet access. It can be HSUPA, HSDPA, UMTS, EDGE, GPRS or Disconnected.
Signal strength	The mobile network (UMTS or GSM) signal quality available at the device location. This signal quality affects the performance of the unit. If two or more bars are green, the connection is usually acceptable.
SIM info	Shows the SIM card status on the device.
LAN IP Address	Shows the IP address for LAN interface.
WAN IP Address	Shows the IP address for WAN interface.
Default Router	Shows the IP address of the default Router for the WAN interface.
Primary DNS	Shows the IP address of the primary DNS server.
Server	
Secondary DNS	Shows the IP address of the secondary DNS server.
server	
Date/Time	The time according to the device's internal clock



# Settings

This menu includes HSPA/30 Settings and PIN Configuration

# Chapter-3

#### NOTE: Sections 8.3 and 8.4.2 also provide information about the Etisalat service.

### 3.1 HSPA/3G Settings

Select your HSPA/3G settings according to predefined or custom profiles. Setup instructions are provided in the following sections for your assistance.

Basic	HSPA/3G	SETTINGS WI-FI	MANAGEME	NT ADVANCED SETTI	INGS STATUS
	3G Settings > Setup > D	ata APN			
	Profile:	Custom APN 👻			
	Authentication Method:	AUTO V			
	APN:	etisalat.ae			
	Username:				
	Password:				
	IP Compression: Off	*			
	Data Compression: Off	*			
	<ul> <li>All Bands/Automatic</li> </ul>	3G-2100 only	<b>3</b> G-2100/2G-900/180	0 3G-ALL 2G-ALL	
	Save Connect Dis	sonnest			

#### 3.1.1 Profile Setup

Etisalat will provide the information required to complete the first time setup instructions below. Only complete those steps for which you have information and skip the others.

- 1. If your SIM card is not inserted into the Router, please turn the Router off. Then insert the SIM and turn the Router on.
- To connect to Etisalat's 3G network, please select the Etisalat profile with Etisalat's APN as
  etisalat.ae. Authentication Method should be provided by Etisalat; or just leave it AUTO if not
  acquired. If you have not received the username and password, leave these fields empty.

ic HSPA/3	CSETTINGS UHFI	REPAREMENT	ROWNICED SETTINGS STRTUS
3G Settings > Setup >	Onta APTI		
Paste	Cution APN		
Authentication Method			
APN.	sticulation of		
Usumanu			
Passaced			
P Companyon 0 Data Compression 0	6 w. 7 w.		
EA1 Descalation at a	1 9G-2100 uniy 🖾 S	0-2109/23-960/1600	35ALL 223AL
San Covat	1. C. M. C. M. C.		

- 3. Select IP compression and Data compression to be ON or Off. By default they are set to off.
- 4. Click the Save button to save the new settings.
- 5. Press the Connect button to connect to Internet. The Device Info for 3G network box in the WUI Basic screen should indicate an active connection, as shown below. The 3G and Internet LEDs on the front

panel of the Router should also be blinking.

HSP	N353ET	TINGS UILPI	RIVEROEMENT	REVANCED SETTINGS STATUS
Basic > Home				
Hardmane Versio	'n	BUILDE KITAR		
Software Version		80048/19 4 101-10105-08	79(,842	
Buildinger CPD.	WEIGHTE.	143548		
Werness Driver V	ersiest.	3333.38.47242.8		
Device anto for 3G				
Includes.	1. Sector			
Link:	(148-5)	minimum family .		
Madel	HIDEAN	EUPA		
lignal Urangth:	Y.			
Sea or other	Are sur	met.		
1848 estimation re	fierts the	current atomics of your contr	ection	
LAS IF ADDRESS.	3	NU WALLS		
WARD? Address	-	148 (ER. 16.82.5E		
Default Catowryl	2 1 9	4443434		
Printery DHS Serv	41. 1	02.01.07.032		
Second States	actant 1	RELATEDAY.		
Data Gimer		Lar less 47 hz (2:10 2000		

If the LEDs are off, then either your profile settings are incorrect, the SIM card is not working or the service network is unavailable. In either case, contact Technical Support for further instructions.

NOTE: If the LEDs light in an on/off pattern moving from left to right this indicates that your SIM is PIN Locked, please see PIN Lock Off on page 16 for instruction on how to fix this

### 3.2 PIN Configuration

This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call Etisalat for assistance.

#### 3.2.1 PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G internet service with this Router however, the PIN code protection must be disabled. If the SIM card inserted into the Router is locked with a PIN code, the web user interface will display the following screen after login.

ensic	ish	BE SETTINGS	uiri	HMM60H017	NOVINCED SETTINGS	STRTUS
361	settings >P18 Cor	Iguration				
0202 ID 2202	PTD Cube Change I PRI Cube with Obles intervite Cube maining times 2 PTD code protection lack. Code of m PTN Cube : member PTS code maining times	or w				
			1	*		

### PIN Lock On

After you are finished using your SIM card for Internet service, you may wish to lock it again. In this case, first go to the 3G Settings - PIN Configuration screen, as shown below. Select PIN lock ON, enter the PIN code twice. You can select Remember PIN code to Yes so you don't need to input the PIN code every time when the Router turns on. Then click Apply.

BRSIC	HSPR/3G SET	TINGS UP	IFI	MANACEMENT	ROVANCED SETTING	s   stritus
0.223						
30 Sel	tings > PIN Configurat	son				
[]m	Code Change					
OR P	N Code					
	Pfu Code:					
	m PN Code					
10.000	ning times: 3					
1 P	code protection					
PTL 10	On M	1				
PN C						
	m PN Code	-				
	mber PNI code: No r	~				
2017	and make the					
				Audy		
				1000		

After you do so, the following dialog box should appear.

1	You have enabled PIN code protection.
	OK

You can now return your SIM card to your cellular phone or other mobile device.

### PIN Lock Off

If you wish to connect to the Internet using a PIN locked SIM card, you must first turn PIN code protection Off. Select PIN lock Off, enter the PIN Code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Etisalat if you require assistance. You can select Remember PIN Code to ON so you don't need to input the PIN code every time when the Router turns on. Afterwards, click Apply. The following dialog box should now appear.



# Settings

### 3.2.2 PIN Code Change

If you wish to change your PIN code for greater security, enable the PIN Code protection. Go to the previous section and follow the procedure listed under PIN Lock On.

After locking the SIM card, select PIN Code Change and enter your Old and New PIN codes in the fields provided. Keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Etisalat if you require assistance. Afterwards, click Apply to activate the change.

HSF	R/3G SETTINGS WI-FI	MANACEMENT	ROVRACED SETTINGS STRTUS
3G Settings > PN C			
PRI Code Change			
Diz Ptv Code:			
New PN Code:			
Confirm PN Code: Remaining times:			
Pli code protect	и		
PN look:	On 💌		
PN Code:			
Confirm PN Code	and the second sec		
Remember PN code Demaining times	No w		
		Awate	

NOTE: If you forget to change the PIN Code without first turning on PIN lock protection, you will see this dialog box as a helpful reminder.



NOTE: If your PIN Code change request was successful the following dialog box will display.

Window	5 Internet Explorer	×
	You have successfully changed t	he PIN code
	ОК	





# Uireless

The WIFI submenu provides access to Wireless Loca Area Network (LAN) configuration settings

# Chapter-4

## 4.1 Setup

This screen allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.

BRSIC		HSPR/3G SETTINGS	WIFE	MANAGEMENT	ADVANCED SETTINGS STATUS
	Wireless >	Setup			
	hide the net	work from active scans, se	it the wireless re	wreiess LAN interface. You c nuołk name (also ksowa as S	an enable or disable the wireless LAN interface, GD) and restrict the channel set based on country
	P Ena	ble Wireless			
	E Hide	Access Point			
	\$50	ETISALATI234	1		
	8010	00114291148610			
	Courters	UNITED AIVAB BARATES		~	
	🕅 Era Guest SSI	tle Wireless Guest Networ D <b>Duest</b>	k	Serve Appry	

Option	Description
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, BSSID and Country settings.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open Network Connections from the start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings.
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish. NOTE: Remote wireless hosts cannot scan Guest SSIDs.



### 4.2 Security

This Router includes a number of options to help provide a secure connection to the Etisalat Network.

Security features include:

- WEP / WPA / WPA2 data encryption
- SPI Firewall
- VPN Pass-Through
- MAC address IP filtering
- Authentication protocols PAP / CHAP

You can authenticate or encrypt your service on the WiFi Protected Access algorithm, which provides protection against unauthorized access such as eavesdropping.

The following screen appears when Security is selected. The Security page allows you to configure security features of your Router's wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Wireless > Security           This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption           Click "Apply" to configure the wireless security options.           Select SSID:         ETISALAT1234 w           Network Authentication:         Mixed WPA2/WPA-PSK w           WPA Pre-Shared Key:         Click here to display           WPA Group Rokey Interval.         TKP+AES w	HSPA/3G SET	TINGS WI-FI	MANAGEMENT	ADVANCED SETTINGS   STATUS
selecting data encryption, speicify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply" to configure the wireless security options. Select SSID. ETISALAT1234 Network Authentication: WPA Pre-Shared Key: WPA Group Rekey Interval: Description: Click here to display: WPA Group Rekey Interval:	Wireless > Security			
Network Authentication: Moved WPA2/WPA-PSK x WPA Pre-Shared Key: WPA Group Rekey Internal: 0 Click here to display	selecting data encryption, sp strength.	ecify whether a network	key is required to authenticate t	
WPA Pre-Shared Key: Click here to display WPA Group Rekey Internal:	Select SSID.	ETISALAT1234		
WPA Group Rekey Interval: 0	Network Authentication	Mixed WPA2/WPA -	PSK 💌	
	WPA Pre-Shared Key:		Click here to display	
WPA Encryption: TKIP+AES V	WPA Group Rekey Interval:	0		
	WPA Encryption:	TKIP+AES M		
WEP Encryption: Disabled V	WEP Encryption:	Disabled ~		
			Save/Apply	
		Wireless > Security This page allows you to confi- salecting date encryption, sp atrength. Click "Apply" to configure the Select SSID: Network Authentication: WPA Pre-Shared Key: WPA Group Rekey Interval: WPA Encryption:	Wireless > Security           This page allows you to configure security features o selecting data encryption, specify whether a network atrength.           Click "Apply" to configure the wireless security option           Select SSID.           ETISALATI234 w           Network Authentication:           WPA Pre-Shared Key           WPA Group Rekey Interval.           WPA Factorphon.	Wireless > Security         This page allows you to configure security features of the wireless LAN interface. You selecting data encryption, specify whether a network key is required to authenticate to strength.         Click "Apply" to configure the wireless security options.         Select SBID:       ETISALAT1234 w         Network Authentication:       Mixed WPA2/WPA-PSK w         WPA Pre-Shared Key:       Click here to display         WPA Encryption:       TKIP-AES w         WPA Encryption:       Disabled w

Click Save/Apply to configure the wireless security options.

	Option	Description
	Select SSID	Your Service Set Identifier (SSID), sets your Wireless Network Name. You can connect multiple devices including Laptops, Desktop PCs and PDAs to your HSPA WiFi Router with Voice. To get additional devices connected, scan for a network, and locate the SSID shown on your Wireless Security Card. If the SSID does not match, access is denied.
	Network Authentication	This option is used for authentication to the wireless network. Each authentication type has its own settings as illustrated below. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields.
1		WEP Encryption will also be enabled.
		The settings for WPA authentication are shown below.
	WPA-Pre- Shared Key	It is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.

# Wireless

WPA Encryption:	Select the data encryption method for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES.
	TKIP (Temporary Key Integrity Protocol) takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. Then it regularly changes and rotates the encryption keys so that the same encryption key will never be used twice.
	AES (Advanced Encryption Standard) provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.
	TKIP+AES combine the features and functions of TKIP and AES.

### 4.3 Configuration

The following screen appears when you select Configuration. This screen allows you to control the following advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set Xpress mode
- Program short or long preambles

Click Save/Apply to set the advanced wireless configuration.

BASIC	HSPR/3G SETT	INGS WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS
	Wireless > Configuration			
	operate, force the transmission	rate to a particular speed, a mode, set the beacon inte	set the fragmentation thresho	can select a particular channel on which to Id, set the RTS threshold, set the wakeup XPress mode and set whether short or long
	AP Isolation:	Off 🖌		
	Band:	2.4GHz 💌		
	Channel:	Auto 🛩	Current: 6	
	Auto Channel Timer(min)	0		
	54g™ Rate:	Auto 🗸		
	Multicast Rate:	Auto 🗸		
	Basic Rate:	Default	~	
	Fragmentation Threshold:	2346		
	RTS Threshold:	2347		
	DTIM Interval:	1		
	Beacon Interval:	100		
	XPress™ Technology:	Disabled 💌		
	54g™ Mode:	54g Auto 💌		
	54g™ Protection:	Auto 💌		
	Preamble Type:	long 💌		
	Transmit Power:	100% 💌		
			Save/Apply	



Option	Description
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point can be linked.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel	The Auto Channel times the length it takes to scan in minutes.
Timer (min)	
54g Rate	In Auto (default) mode, your Router uses the maximum data rate and lowers the data rate dependent on the signal strength. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.
Multicast Rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Sets basic transmission rate.
Fragmentation Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented.
	Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Option	Description
Beacon Interval	The amount of time between beacon transmissions in is milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Xpress Technology	Broadcom's Xpress Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. Default is disabled.
54g Mode	Select Auto mode for greatest compatibility. Select Performance mode for the fastest performance among 54g certified equipment. Select LRS mode if you are experiencing difficulty with legacy 802.11b equipment. If this does not work, you may also try 802.11b only mode.
54g Protection	In Auto mode, the Router will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turning protection Off will maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for applications where maximum throughput is desired but it does not work with legacy equipment. Long preamble works with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	Set the power output (by percentage) as desired.

# Wireless

## 4.4 MAC Filter

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address.

To add a MAC Address filter, click the Add button shown below.

To delete a filter, select it from the table below and click the Remove button.

BASIC	HSPA/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
		Setup			
	Wireless > MAC Filter	Security Configuration			
		Wireless Bridge	Disabled 🖸 Allow	U Deny	
		Station Info			
		MAC Ad	dress Remove		
		Add	Remove		

Option	Description				
MAC Restrict Mode	Disabled – Disables MAC filtering				
	Allow - Permits access for the specified MAC addresses.				
	NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the Router's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address.				
	Deny - Rejects access for the specified MAC addresses				
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.				

Enter the MAC address on the screen below and click Save/Apply.



### 4.5 Wireless Bridge

The following screen appears when selecting Wireless Bridge, and goes into a detailed explanation of how to configure wireless bridge features of the wireless LAN interface.

Click Save/Apply to implement new configuration settings.

Areless Distribution Sy less bridge functionalit rict which disables wir les wireless bridge res "Refresh" to update to	striction. Only those brid	Moge nutry, Salecting Acess Pont enables access port function on strong will be able to associate to the AP. Salect Disability may uneverse bridge will be granted access. Salecting Enabled or Enabled ges salected in Remote Bridges will be granted access. for few seconds to update.
Under	Access Date	
woue.	Access Poin	× ×
ge Restrict:	Disabled	M

Feature	Options
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled in Bridge Restrict disables Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) allows wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.



### 4.6 Station Info

The following screen appears when you select Station Info, and shows authenticated wireless stations and their status.

Click the Refresh button to update the list of stations in the WLAN.

BASIC	HSPA/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
		Setup			
	Wireless > Station Info	Security			
	Wheless > Station into	Configuration			
	This page shows authenticated wireless	MAC Filter	5.		
		Wireless Bridge			
	BSSID Associated Authorized	Station Info			
	D351D A550Clated Authorized				
		_			
			Refresh		

	BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
	Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
	Authorized	Lists those devices with authorized access.

# Wireless



# Management

The management menu controls the maintenance Functions of your router



The Management menu has the following maintenance functions and processes:

- 5.1 Device Settings
- 5.2 Access Control
- 5.3 Simple Network Management Protocol (SNMP)
- 5.4 Simple Network Time Protocol (SNTP)
- 5.5 Save and Reboot

### 5.1 Device Settings

The Device Settings screens allow you to backup, retrieve and restore the default settings of your Router. It also provides a function for you to update your Router's settings.

#### 5.1.1 Backup Settings

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings.

You will be prompted to define the location of a backup file to save to your PC.

BASIC	HSPA/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
		Backup	Device Settings		
	Management > Device Settings > Ba	Update	SNMP		
	Management > Device Settings > Da	Restore Default	SNTP		
	Backup Gateway configurations. You m	Update Firmware	Access Control	our PC.	
			Save/Reboot		
		Bac	kup Settings		

#### 5.1.2 Update Settings

The following screen appears when selecting Update from the submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings to load it.

BASIC		HSPA/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
			Backup	Device Settings		
	Managamant	nt > Device Settings > Up	Update	SNMP		
	Management	- Device Settings - Of	Restore Default	SNTP		
	Update Gateway settings. You may up		Update Firmware	Access Control		
				Save/Reboot		
	Settings File N	ame:	Browse			
			Upd	late Settings		

#### 5.1.3 Restore Default

The following screen appears when selecting Restore Default. By clicking on the Restore Default Settings button, you can restore your Gateways default firmware settings. To restore system settings, reboot your Router.

BASIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
		Backup	Device Settings		
	Management > Device Settings > Re	Update	SNMP		
	management > Device Settings > Re	Restore Default	SNTP		
	Restore Gateway settings to the factory	Update Firmware	Access Control		
			Save/Reboot		
		Restore	Default Settings		

#### NOTE: The default settings can be found in section 2.1 Default Settings.

Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your computer's IP address to match your new configuration (see section 2.2 TCP/IP Settings for details).

#### Gateway Restore

The Gateway configuration has been restored to default settings and the Gateway is rebooting.

Close the Gateway Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

NOTE: The Restore Default function has the same effect as the reset button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

# Management

#### 5.1.4 Update Firmware

The following screen appears when selecting Update Firmware. By following the steps on this screen, you can update your Router's firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

BASIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS
		Backup	Device Settings	
	Anagement > Device Settings > Up	Update	SNMP	
· ·	vanagement > Device Settings > of	Restore Default	SNTP	
5	tep 1: Obtain an updated software im:	Update Firmware	Access Control	
9	Step 2: Enter the path to the image file	location in the box bel	Save/Reboot ow or click the "Browse" bi	utton to locate the image file.
5	Step 3: Click the "Update Software" but	ton once to upload the	new image file.	
				the 3G modem takes about 10 minutes, he webpage during the update process.
\$	Software File Name:	Browse		
		u	pdate Software	

- 1: Obtain an updated software image file
- 2: Enter the path and filename of the firmware image file in the Software File Name field or click the Browse button to locate the image file.
- 3: Click the Update Software button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The Router will reboot and the browser window will refresh to the default screen upon successful installation.

It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

### 5.2 Access Control

The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

- Services
- IP Addresses
- Passwords

Access Control is used to control local and remote management settings for your Router.

Management > Access Control > Services Service State A Service Control (SLT) while Service Services Services Service State P Advecses Service Service Services Serv	HSPR/3G SETTINGS	WHE		MANAGEMENT	ROVRNCED SETTINGS STATUS
Management > Access Control > Services Strr Service Centrol (TSC); anales PAddresses Centrol = Services PAddresses Centrol = Services PAddress Centrol = Services PAddresses Centrol = Services PAddresses PAddresses Centrol = Services PAddre					
A Speec Corrol Lot ("SCL") vaables Services Access Corbot Services of the biology goal and in the biology goal and intervention of the services of 2.2.2.2.00.1092.101, 10116) TET Corbot Services LAN WAM FTP Enable Enable HTTP Enable Enable State Enable State Enable State Enable State Enable TETNET Enable Enable TETNET TETNET Enable Enable TETNET	Management > Access Control > Ser	rvices			
The following ports are not recommende <u>PrAdverses</u> management purpose in some paticular <u>Preswords</u> <u>2 23 250, 00 0900 (bit, 16116)</u> <u>Services LAM</u> <u>FTP</u> <u>Cable</u> <u>Trable</u> <u>Trable</u> <u>SMM</u> <u>Cable</u> <u>Cable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u> <u>Trable</u>		Processing.	_		
enangement purpose in some paticular generators FTP CLAR VAAN FTP Enable Enable por CLAP Enable Enable por CLAP Enable Enable SMBP Canbo Enable SMBP Enable Enable SMBP Enable Enable SMBP Enable Enable	The following north are not recommended	THE RECEIPTORY	ine .		with them for other
Services     LAN     WAM       FTP     Enable     Enable     Enable       HTTP:     Enable     Enable     port       ICMP     Enable     Enable     port       SMMP     Enable     Enable     port       SSM     Enable     Enable     port       YEINET     Enable     Enable     port	management purpose in some particula	Pasmword	1	2, 23, 2323, 69, 6969.	
FTP Fibes for Enable prove HTTP Enable for Enable prove ICMP Enable for Enable SMMP Enable for Enable SSM For Enable for Enable SSM For Enable for Enable					
FTP Enable Enable port KTTP Enable Enable port KLMP Enable Enable 55MM Enable Enable SSM Enable Enable SSM Enable Enable SSM Enable Enable		-	-	P. CO. CO.	
HTTP C Enable E Enable por ICLEP Enable E Enable SMAP C Enable E Enable SMAP E Enable E Enable SST E Enable E Enable		Services	LAN	WAN	
ICMP Enable Enable SMMP Enable Enable SSH Enable Enable TELNET Enable Enable		FTP	Enable	Enable	
SMBP     Image: Constraints     Image: Constraints       SSH     Image: Constraints     Image: Constraints       TELNET     Image: Constraints     Image: Constraints		HTTP	Enable	Enable 20	part
SSH 🖉 Enable 🕅 Enable TELNET 🐱 Enable 🖉 Enable		ICMP	Enable	Enable	
TELNET 🦉 Enable		SNMP	👻 Enable	Enable	
		SSH	Frable	Enable	
TETP Finable Finable		TELNET	🖓 Enable	Enable	
		TETP	Enable	Enable	
P. Company P. Company		TETP	C Enable	Enable	

#### 5.2.1 Services

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. These access services are available: FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Click Save/Apply to continue.

¢.	HSPA/3G SETTINGS WI-FI		Management ad	WANCED SETTINGS   STATUS
	Management > Access Control > Services			
	A Service Control List ("SCL") enables or disat The following ports are not recommended for H management purpose in some particular case	TP remote mana	gement in case conflict with t	them for other (6116)
	Servi	es LAN	WAN	1
	FTP	Enable	Enable	1
	HTTP	Enable	Enable 77 por	
	ICMP	Enable	Enable	1
	SNAM	Enable	Enable	1
	SSH	Enable	Enable	1
	TELN	T 👻 Enable	Enable	1
	TETP	To contra	Enable	1

# Management

### 5.2.2 IP Address

The IP Address option limits local access by IP address. When the Access Control Mode is enabled, only the IP addresses listed here can access the device. Before enabling Access Control Mode, add IP addresses with the Add button.

RSIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS	
Man	agement > Access Control > IP	Address			
Acce	ss Control List. If the Access Cor	de, if enabled, permits access to local management services from IP addresses containe Control mode is disabled, the system will not validate IP addresses for incoming packets is listed in the Service Control List Access Control Mode. C Disable C Enable			
		IP Address	Subnet Mask Interface Re	emove	
			Add Remove		

On this screen, enter the IP address Subnet Mask and the different interface for which you wish to allow permission. Click Save/Apply to continue.

HSPR/	3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS
ccess Control				
nter the IP address o	f the manageme	ent station perm	itted to access the local man	agement services, and click 'Save/Apply.'
IP Address	Su	ibnet Mask	Interface	

### 5.2.3 Passwords

The Passwords option configures your account access password for your Router. Access to the device is limited to the following three user accounts:

- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click Save/Apply to continue.

	HSPR/3G SETTINGS	WI-FI	MRINAGEMENT	ADVANCED SETTINGS STATUS
			Device Settings	
	and a second a first		SNMP	
Manageme	nt > Access Control > Pas	sswords	SNTP	
Access to y	our Gateway is controlled t	Services	Access Control	ser.
		IP Addresses	Save/Reboot	
The user nar	ne "admin" has unrestricte	Pasawords	new contiguration of y	our Gateway
The user nar	ne "support" is used to allo	w an ISP technicia	n to access your Gateway	or maintenance and to run diagnostics.
The user nar	ne "user" can access the G	Sateway, view confi	guration settings and statis	tics, as well as, update the Gateway's software
				tics, as well as, update the Gateway's softwar a passwords. Note: Password cannot contain a
Use the field				
Use the field space.	s below to enter up to 16 cl	haracters and click		
Use the field space. Usemame	s below to enter up to 16 cl	haracters and click		

# Management

### 5.3 Configure SNMP agent on the 3G10WVE

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the 3G10WVE (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

By default, SNMP agent is enabled on the Router.

#### Setting up SNMP agent

- Open a web browser (IE/Firefox/Safari), type in LAN address of the Router (http://192.168.1.1 by default) to log into the web interface.
- The login username and password by default is admin/admin.
- Go to Advanced Settings > SNMP. Enable SNMP agent and set up all options according to the screenshot below.
- Click Save/Apply to activate these settings.

BASIC	HSPA	/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS
				Device Settings	
	Management > Acc	ess Control > Pa	esworde	SNMP	
	management + Acc	concontrol - 1 a	3500103	SNTP	
	Access to your Gatev	way is controlled t	Services	Access Control	ser.
	<b>T</b> I		IP Addresses	Save/Reboot	
	The user name "admi	n nas unrestricte	Passwords	new configuration of your	Gateway.
	The user name "supp	ort" is used to allo	ow an ISP technician to a	access your Gateway for	maintenance and to run diagnostics.
	The user name "user"	can access the (	Gateway, view configurat	ion settings and statistics	s, as well as, update the Gateway's software.
	Use the fields below t space.	o enter up to 16 c	haracters and click "App	oly" to change or create p	asswords. Note: Password cannot contain a
	Username:		~		
	Old Password:				
	New Password:				
	Confirm Password:				
			2	Save/Apply	

### 5.4 Simple Network Time Protocol (SNTP)

This screen allows you to configure the time settings of your Router. To automatically synchronize with Internet time servers, tick the box as illustrated below.

BASIC	HSPR/3G	SETTINGS	WI-FI	MRORGEMENT	ADVANCED SETTINGS STATUS
			- C-2	Device Settings	
	Management > SNTP			SNMP	
	management > SHTP			SNTP	
	This page allows you to the	ne modem's	time configuration.	Access Control	
	Automatically synchronize wit	onize with In			
	First NTP time server:	Other	~	0.netcomm.pool.ntp.org	
	Second NTP time server:	Other	×	1.netcomm.pool.ntp.org	
	Time zone offset.	(GMT+04:0	0) Abu Dhabi, Mu	scat Seve/Apply	×

The following options should now appear (see screenshot below):

First NTP time server:	Select the required server.
Second NTP time server:	Select second time server, if required.
Time zone offset:	Select the local time zone.

Configure these options and then click Save/Apply to activate.

This page allows you to the modem's time configuration.							
Automatically synchronize with Internet time servers							
First NTP time server:	Other	~	0.netcomm.pool.ntp.org				
Second NTP time server: Other							
Time zone offset: (GMT+04:00) Abu Dhabi, Muscat							



### 5.5 Save and Reboot

This function saves the current configuration settings and reboots your Router.

BASIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS		
			Device Settings				
Man	agement > Save/Reboot		SNMP				
Widthe	agement > SaverReboot		SNTP				
			Access Control				
	CI	ick the button below to	Save/Reboot	ateway.			
Save/Reboot							

NOTE1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

NOTE2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings.

# management



# Advanced

This chapter explains advanced setting for your Router:



## 6.1 Local Area Network (LAN)

This screen allows you to configure the Local Area Network (LAN) interface on your Router.

BASIC	HSPA/3	G SETTINGS WI-FI	MA	nagement	ADVANCED SETTING	55 STATUS
	Advanced > Local Area	Network (LAN) Setup				
		P Address and Subnet Mas es the LAN configuration d				
	IP Address	192.168.1.1				
	Subnet Mask	255.255.255.0				
	Enable UPnP					
	Enable Half-Bridge Enable NAT					
	Enable IGMP Snoo	ping				
	C Blocking Mode					
	Disable DHCP Serve	er				
	Enable DHCP Serve	Er	_			
	Start IP Address	192.168.1.2				
	End IP Address	192.168.1.254				
	Leased Time (hour)	24				
	OPTION 42:					
	OPTION 66:					
	OPTION 150:					
	OPTION 160:					
	configured)	Please click on Save/Rebo IP Address Remove Remove Grbies	ot button to make t	he new configuratio	n effective. (A maximu	m 32 entries can be
1	Configure the second I	P Address and Subnet Mas	k for LAN interface			
			Save Save/R	stoot		

See the field descriptions below for more details.

Note: If you change your Router's IP address (first option on the chart), the installation software/connection manager may not be able to communicate with the Router. Please reset the Router's IP address to 192.168.1.1 if this occurs.

Option	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable UPnP	Tick the box to enable Universal Plug and Play
Enable Half-Bridge	The Etisalat HSPA WiFi Router with Voice can be set up as a half- transparent bridge to cope with some special applications such as VPN pass- through. By default half-bridge is off. Please refer to Appendix B for more information.
Enable Internet Group	Enable by ticking the box
Management Protocol	Standard Mode: In standard mode, multicast traffic will flood to all bridge ports
(IGMP) Snooping	when no client subscribes to a multicast group.
(Idmr) shooping	Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.
Dynamic Host	Select Enable DHCP server and enter your starting and ending IP addresses
Configuration Protocol	and the lease time. This setting configures the Router to automatically assign IP, default Router and DNS server addresses to every DHCP client on your LAN
(DHCP) Server	
ENADIE INHT	To enable/disable Network Address Translation (NAT, please refer to 7.2 for NAT setting). By default NAT is enabled.
Option 42, 66,150,160	These options are used for special DHCP set up.
Static IP Lease List	To specify the IP address assigned through DHCP according to the MAC address of the hosts connected to the Router.
Enable DHCP	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP
Server Relay	server on other subnets. DHCP Server Relay is disabled by default. To access enable DHCP relay, please un-tick NAT enable first, that means to disable NAT first, and then press save button. The Enable DHCP server Relay option will then show up on the same page as below:

C Enable DHCP Server Relay

DHCP Server IP Address:

# Advanced

IP Address:	Enter the secondary IP address for the LAN interface.
Subnet Mask:	Enter the secondary subnet mask for the LAN interface.
	[2] Configure the second IP Address and Subnet Mask for LAN interface     IP Address:     Subnet Mask:

Configure a second IP address by ticking the checkbox shown below and enter the following information:

NOTE: The Save button saves new settings to allow continued configuration, while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

### 6.2 Network Address Translation (NAT)



### 6.2.1 Port Forwarding

Port Forwarding allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Advanced > NAT > Port Forwarding  Vitual Server allows yours direct incoming traffic from VIAN side (denotified by Protocol and External port) to the Internal server with provide P address on the LAS set. The Internal Cost are accurated by Protocol and External port to the Internal server with provide P address on the LAS set. A maximum 22 direct accurate set of the Cost and Set of the Internal Cost accurate set of the Internal Cost and Set of the Internal Cost accurate set of the Internal Co		HSPA/3G SETTI	NGS WI-FI		MANAGEMENT	ADVRI	NCED SETTINGS	STATUS	
private P address on the LLA add. The Internal point required day if the extransition to the converted to a offerent point number used by the server on the LLA add. A maximum 22 effects data the concepts of the converted to a offerent point If the server is the server of the serve	Advance	d > NAT > Port Forwar	ding						
number used by the server on the LAN ade. A maximum 32 entries can be configured. All Tensor Benner External Port External Port External Port Internal Port Internal Port Internal Port Internal Port	Virtual S	rver allows you to direct i	ncoming traffic from	WAN side (dr	entified by Protoco	and External port)	to the internal ser	ver with	
				remulted ash-	if the external part	needs to be needed	start in a different	nert	
	private P number v	address on the LAN side sed by the server on the l	The Internal port is				rted to a different	port	
	private P number v	address on the LAN side sed by the server on the l	The Internal port is				rted to a different	port	

To add a Virtual Server, click the Add button. The following screen will display.

NAT Virtual Server						
					rard IP packets for this ser al Port End" normally ar	
same as the "Internal	Port Start" or "Ext	emai Port I	ind" if either or	e is modified.		
Remaining number of	fentries that can b	e configure	et 32			
Server Name						
Select a Service	Select One			~		
Custom Server	6					
Server IP Address		_				
Server IP Address	192.106.1					
			Served	ut for		
-			and an an an array of the			
	External Port End	Protoce		irt Start, Internal	(Part End)	
ACCOUNT OF A COUNTY OF A COUNT						
		TCP	*			
		TCP	~			
		TCP TCP	• •			
		TCP TCP TCP	> > >			
		TCP TCP	> > >			
		TCP TCP TCP	• •			
		TCP TCP TCP TCP	2 2 2 2			
		TCP TCP TCP TCP TCP				
		TCP TCP TCP TCP TCP TCP				
		TCP TCP TCP TCP TCP TCP TCP TCP				
		TCP TCP TCP TCP TCP TCP TCP TCP TCP				
		TCP TCP TCP TCP TCP TCP TCP TCP				

Options	Description
Select a Service	User should select the service from the list.
Or	Or
Custom Server	Create a custom server and enter a name for the server
Server IP Address	Enter the IP address for the server.
External Port	Enter the starting external port number (when you select Custom Server). When a
Start	service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.



### 6.2.2 Port Triggering

Some applications require specific ports in the Router's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Adva	nced > NAT > Port Trigg	pering Setu						
dynar	applications require that a nically opens up the 'Open the Transmiss Posts' The	Ports' in the	frewall wi	hen an applica	tion on the	LAN initiates		tion to a remote pa
	ation on the LAN side usin							IS DALK TO THE
	ation on the LAN side usin		Ports'. A n		ntries can l enove		Remove	IS DALK ID THE
	ation on the LAN side usin	ng the 'Open	Ports'. A n Tr	naximum 32 e	ntries can l move	e configured. Ipen		IS DALE. ID UNP

To add a Trigger Port, simply click the Add button. The following will be displayed.

NAT -	Port Triggering					
Gatew	ay/s firewall be opened	for access by the ng your own (Custor	applications m applicatio	ote access applications . You can configure the p njand click "Save/Apply" 2	ort settings from this s	
	ation Name: Select an application:	Select One		-		
Election of the second se	Custom application:	Delect One	12	24		
	1990 (1995 <b>1</b> 997 (1997)					
				Save/Apply		
The second			1101-0-000	And the second se		1
Trig	ger Port Start Trigge		Protocol O	pen Port Start Open Po		0
Trig	ger Port Start Trigge	r Port End Tripger TCP	Protocol O	pen Port Start Open Po	rt End Open Protocol TCP	
Trig	ger Port Start Trigge		and the owner where the party of	pen Port. Start Open Po		
Trig	ger Port Start Trigge	TCP	~	pen Port Start Open Po	TCP 💌	
Trig	ger Port Start Trigger	TCP TCP TCP	~	pen Port Start Open Po	TCP V TCP V TCP V	
Trig	ger Port Start Trigge	TCP TCP TCP TCP	> > >	pen Port Start Open Po	TCP V TCP V TCP V TCP V	
Trig	ger Port Start Trigge	TCP TCP TCP TCP TCP	> > > >	pen Port Start Open Po	TCP V TCP V TCP V TCP V TCP V	
Trig	ger Port Start Trigge	TCP TCP TCP TCP	> > >	pen Port Start Open Po	TCP V TCP V TCP V TCP V	
	ger Port Start Trigge	TCP TCP TCP TCP TCP	> > > >	pen Port Start Open Po	TCP V TCP V TCP V TCP V TCP V	
	per Port Start Trigge	TCP TCP TCP TCP TCP TCP	2 2 2 2	pen Port Start Open Po	TCP V TCP V TCP V TCP V TCP V TCP V	

Options	Description
Select an Application	User should select the application from the list.
ог	or
	User can enter the name of their choice.
Custom Application	
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When
	an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an
	application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an
	application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP or UDP.

### 7.2.3 Demilitarized (DMZ) Host

Your Router will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click Save/Apply to activate the DMZ host.

Clear the IP address field and click Save/Apply to deactivate the DMZ host.

BASIC	HSPA/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
	Advanced > NAT > DMZ Host				
	The Gateway will forward IP packets fr to the DMZ host computer.	om the WAN that do not I	pelong to any of the app	lications configured in the V	/irtual Servers table
	Enter the computer's IP address and o	lick "Apply" to activate th	e DMZ host.		
	Clear the IP address field and click "A	pply" to deactivate the DN	IZ host.		
	DMZ Host IP Address:				
		s	ave/Apply		

# Advanced

### 6.3 Security

Your Router can be secured with IP Filtering or Parental Control functions.



### 6.3.1 IP Filtering

The IP Filtering screen sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled to allow individual IP packets to pass through the filter.

### **Outgoing IP Filter**

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.

BASIC	HSPA/3G	SETTINGS	WI-FI	MANAGEME		D SETTINGS	STATUS
Adv	vanced > Security >	IP Filtering	> Outaoina IP Filterina	a Setup			
Ву	default, all outgoing IP	traffic from L	AN is allowed, but some	e IP traffic can t	e BLOCKED by setting	up filters.	
Cho	ose Add or Remove to	o configure ou	utgoing IP filters.				
	Filter Name	Protocol S	ource Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
			Ad	d Remove			

To add a filtering rule, click the Add button. The following screen will display.

Add IP Filter Outgoing			
			g a new filter name and at least one condition take effect. Click 'Save/Apply' to save and activate
Filter Name:			
Protocol	~	1	
Source IP address			
Source Subnet Mask:			
Source Port (port or port port):		8	
Destination IP address:			
Destination Subnet Mask:		1	
Destination Port (port or port port)			

Options	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address
Source Subnet Mask	Enter source subnet mask
Source Port	Enter source port number or port range
(port or port:port)	
Destination IP address	Enter destination IP address
Destination Subnet Mask	Enter destination subnet mask
Destination port	Enter destination port number or range
(port or port:port)	

Click Save/Apply to save and activate the filter.



### Incoming IP Filter

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

Adv	anced > Secur	ity > IP F	iltering > I	ncoming IP Filtering Se	tup			
	Sefault, all incon ing up filters.	ning IP trat	fic from the	WAN is blocked when the	e firewall is ena	bled. However, some IP	traffic can be	ACCEPTED
			5 57	10122				
Cho	ose Add or Rem	ove to con	ifigure inco	ming IP filters.				
		No.	Destruct	Source Address / Black	Source Port	Dest, Address / Mask	Dest Port	Remove
	Filter Name	VPI/VCI	Protocol	COULDS MORNING I INCLUS	Contraction of the	The second s	and the second	and the second second

To add a filtering rule, click the Add button. The following screen will display.

ISIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ROVANCED SETTINGS STATUS
	Add IP Filter Incoming			
				g a new filter name and at least one condition lake effect. Click 'Save/Apply' to save and activate
	Filter Name			
	Protocol:			
	Source IP address:			
	Source Subnet Mask:			
	Source Port (port or port port):			
	Destination IP address:			
	Destination Subnet Mask:			
	Destination Port (port or port port)			
	WAN Interfaces (Configured in Rou Select at least one or multiple WAN in			
	Select All     ppp0/ppp0     ppp1/ppp1			

Please refer to the Outgoing IP Filter table for field descriptions.

Click Save/Apply to save and activate the filter.

### 6.4 Routing

Default Router, Static Route and Dynamic Route settings can be found in the Routing link as illustrated below.



### 6.4.1 Default Router

If the Enable Automatic Assigned Default Router checkbox is selected, this device will accept a default Router assignment. If the checkbox is not selected, a field will appear allowing you to enter the static default Router and/or WAN interface, then click Save/Apply.

BASIC	HSPR/3G SETTINGS WI-FI MANRGEMENT	ADVANCED SETTINGS STATUS
Ad	ivanced > Routing > Default Gateway	
395	Enable Automatic Assigned Default Gateway checkbox is selected, this Gateway v signment from WAN connection. If the checkbox is not selected, enter the static d ne/Apply' button to save it.	
	TE: If changing the Automatic Assigned Default Gateway from unselected to selec tomatic assigned default Gateway	cted. You must reboot the Gateway to get the
9	Enable Automatic Assigned Default Gateway	
	Save/Apply	

NOTE: After enabling the Automatic Assigned Default Router, you must re-boot the Router to activate the assigned default Router.

# Advanced
#### 6.4.2 Static Route

The Static Route screen displays the configured static routes.

#### Click the Add or Remove buttons to change settings.

BA	SIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
	Advanced >	Routing > Static Route				
	Autonova -	- State Roate				
		De	stination Subnet Mask	Gateway Interface	Remove	
			Add	Remove		

Click the Add button to display the following screen.

HSPR/3G SETT	INGS WI-FI	MRNAGEMENT	ADVANCED SETTINGS STATUS
outing Static Route Add			
	iddress, subnet mask, (	Gateway AND/OR available W	AN interface then click "Save/Apply" to add the
Use Interface	ppp0/ppp0 💌		
		Save/Apply	
	outing Static Route Add	buting – Static Route Add ter the destination network address, subnet mask, try to the routing table. Instination Network, Address. Use Gateway IP Address	butting – Static Route Add ter the destination network address, subnet mask. Gateway AND/OR available W rstination Network Address: ibnet Mask: Use Gateway IP Address Use Interface ppp0/ppp0 m

Enter Destination Network Address, Subnet Mask, Router IP Address and/or WAN Interface. Then click Save/ Apply to add the entry to the routing table.

#### 6.4.3 Dynamic Route

To activate this option, select the Enabled radio button for Global RIP Mode.

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for that interface. Click Save/Apply to save the configuration and to start or stop dynamic routing.

vanced :							
			oynann	¢ NO	210		
ired RIP	version	n and	operation	, follo	wed by plac	ing a check in the 'Enabled' cl	teckbox for the interface. Click the 'Save/Apply' butt
bal RIP	Mode	(•	Disabled	0	Enabled		
terface	Versl	on	Operat	ion	Enabled		
br0	2	*	Active	۲	F		
ppp0	2	Y	Passiv	0 4			
		v	Passi		Contract of the local division of the local		
	ired RIP ave the o bal RIP iterface	terface Veral br0 2	terface Version br0 2 Y	ired RIP version and operation save the configuration, and to to obtail RIP Mode	ired RIP version and operation, follo ave the configuration, and to start or obtal RIP Mode C Disabled C iterface Version Operation br0 2 V Active V	ind RP version and operation. followed by plas ave the configuration, and to start or stop RP b obal RIP Mode  Doabled  Enabled torface Version Operation Enabled br0 2  Version Control Con	terface Version Operation Enabled br0 2 v Active v

#### 6.5 Domain Name Servers (DNS)

#### 6.5.1 DNS Server Configuration

If the Enable Automatic Assigned DNS checkbox is selected, this device will accept the first received DNS assignment from the Wide Area Network (WAN) interface during the connection process. If the checkbox is not selected, a field will appear allowing you to enter the primary and optional secondary DNS server IP addresses. Click on Save to apply.

BASIC	HSPR/3C SETTINGS WI-FI	MANAGEMENT	ADVANCED SETTINGS STATUS
Adva	aced > DNS > DNS Server Configuration		
conne IP add	Iresses. Click 'Save' button to save the new co	he checkbox is not selected, ent	the first received DNS assignment from Wan er the primary and optional secondary DNS serve Gateway to make the new configuration effective.
<b>P</b>	Inable Automatic Assigned DNS		
		Sava	

NOTE: Click the Save button to save the new configuration. To make the new configuration effective, reboot your Router.



### 6.5.2 Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the Router to be more easily accessed from various locations on the internet.

HSPR/3G SETTINGS	WI-FI		MANAGE	MENT	ADVANCED SETTINGS STATUS
Advanced > DNS > Dynamic DNS					
					ame in any of the many domains, allowing your
Choose Add or Remove to configure 0	lynamic DNS				
	Hostname	Username	Service	Interface	Remove
		Add	Remove		
	Advanced > DNS > Dynamic DNS The Dynamic DNS service allows you Gateway to be more easily accessed	The Dynamic DNS senice allows you to alias a dyn Gateway to be more easily accessed from various Choope Add or Remove to configure Dynamic DNS	Advanced > DNS > Dynamic DNS The Dynamic DNS sence ablow you to alias a dynamic IP add Gateway to be more easily accessed form various locations on to Choose Add or Remove to configue Dynamic DNS.	Advanced > DNS > Dynamic DNS The Dynamic DNS service allows you to alias a dynamic IP address to a r darway to be more easily accessed from various locations on the interem Choose Add or Remove to configure Dynamic DNS. Hostname Username Service	Advanced > DNS > Dynamic DNS The Dynamic CNS service allows you to alias a dynamic IP address to a static hosts Gateway to be more easily accessed from various locations on the internet.

Note: The Add/Remove buttons will be displayed only if the Router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and this screen will display.

BASIC	HSPR/3	G SETTINGS   WI-FI	MANAGEMENT	ROVANCED SETTINGS STATUS	
	Add dynamic DDNS				
	This page allows you to	add a Dynamic DNS address fit	em DynDNS org er TZO.		
	D-DNS provider	DynDNS.org			
	Hostname		i		
	Interface	ppp0/ppp0			
	DynDNS Settings		-		
	Username Password				
	Password				
			Seve/Apply		
			manuf which h		

Options	Descriptions
D-DNS provider	Select a dynamic DNS provider from the list.
Hostname Enter the name for the dynamic DNS server.	
Interface Select the interface from the list.	
Username	Enter the username for the dynamic DNS server.
Password	Enter the password for the dynamic DNS server.

### Advanced



## Voice

Using a standard telephone, you can make calls using your router over the 3G Network



The 3G10WVE Etisalat HSPA WiFi Router with Voice allows you to make telephone calls over the 3G Mobile/ Cellular Telephone network using a standard Analogue Telephone via the built in RJ-11 Phone port.

Please refer to the documentation provided by the manufacturer for operating your Analogue Telephone.

Note that your SIM card and Mobile service needs to be provisioned for Voice Calling. Please consult with your Network Provider for verification.

Note that any telephone calls placed using the may incur call usage charges determined by your Network Provider. Please consult with your Network Provider for verification.

### 7.1 Configuring your 3G10WVE for placing Voice Calls

Once your has been correctly configured to access the mobile networ you can make and receive telephone calls after connecting your Analogue Telephone to the socket labeled Voice on the back of your HSPA WiFi Router with Voice.

### Voice



## Status

The status menu alllows you to monitor your connection and diagnose common issues



### The Status menu has the following submenus:

- Diagnostics
- System Log
- 3G network
- Statistics
- Route
- ARP
- DHCP
- PING

С	HSPA/3G SETTINGS	WI-FI		MANAGEMENT	ADVANCED SETTINGS	STATUS
					· ·	Diagnostics
6	status > DATA APN Diagnostics					System log
3	status > DATA APN Diagnostics					3G network
Your Gateway is capable of testing your WAN connection. The individual tests are listed below. If a test displays a						
"Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues						
a	nd follow the troubleshooting procedur	es.				ARP
т	est the connection to your local ne	the second s				DHCP
- ŝ	est the connection to your local he					PING
	Test your ENET1 Connection:	FAIL	Help			
	Test your ENET2 Connection:	PASS	Help			
	Test your Wireless Connection:	PASS	Help			
T	est the connection to your Internet					
	Test DATA APN assigned IP addre	ss: FAIL He	<u>dp</u>			
	Ping primary Domain Name Serve	er: PASS He	dn			

### 8.1 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

- 1: Click on the Help link
- 2: Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error
- 3: If the test continues to fail, follow the troubleshooting procedures in the Help screen.

1	Status > DATA APN Diagnostics					
	Your Gateway is capable of testing yo Rerun Diagnostic Tests" at the botton and follow the troubleshooting procedu Test the connection to your local m	of this page to res.				
	Test your ENET1 Connection:	FAIL	Help			
	Test your ENET2 Connection:	PASS	Help			
	Test your Wireless Connection:	PASS	Help			

### Status

	Description			
ENET Connection	<b>Pass:</b> Indicates that the Ethernet interface from your computer is connected to the LAN port of this Router.			
	Fail: Indicates that the Router does not detect the Ethernet interface on your computer.			
Wireless connection	Pass: Indicates that the wireless card is ON.			
	Down: Indicates that the wireless card is OFF.			
Ping Default Router	<b>Pass:</b> Indicates that the Router can communicate with the first entry point to the network. It is usually the IP address of the ISP's local Router.			
	<b>Fail:</b> Indicates that the Router was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.			
Ping Primary Domain Name Server	<b>Pass:</b> Indicates that the Router can communicate with the primary Domain Name Server (DNS).			
	<b>Fail:</b> Indicates that the Router was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.			

### 8.2 System Log

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

• 1: Click Configure System Log to continue.



• 2: Select the system log options (see table below) and click Save/Apply.

BASIC		HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS STRTUS
	System Log	- Configuration			
	selected level selected mode	will be logged. For the D	isplay Level, all logged ents will be sent to the	events above or equal to specified IP address an	e Log Level, all events above or equal to the the selected level will be displayed. If the d UDP port of the remote syslog server. If the
	Select the der	sired values and click 'Sa	ve/Apply' to configure	the system log options.	
	Log:	Disable			
	Log Level:	Debugging M			
	Display Level:	Error 💌			
	Mode:	Local M			
			1	Save/Apply	

Option	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the Router's SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows:
	Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, be sent to a remote syslog server, or to both simultaneously.
	If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the you to enter the Server IP address and Server UDP port.

3: Click View System Log. The results are displayed as follows.



### 8.3 Etisalat Status

Select this option for detailed status information on your Gateways 3G connection.



Consult the table on the next page for detailed field descriptions.

### Status

Status	Description	Status	Description							
Manufacturer	The manufacturer of the embedded 3G module.	Signal Strength	The 3G/2G service signal strength in dBm.							
Model	The model name of the embedded 3G module.		Signal	-109 ~	-101 ~ -93	91 ~	-87 -8	85 ~ ₋79	-77 ~ -52	
FW Rev.	The firmware version of the 3G module.		level in	-103	-101 -5.	-51			-77 -52	
IMEI	The IMEI (International Mobile Equipment Identity) is a 15 digit number that is used to identify a mobile device on a network.		dBm	-105						
FSN	Factory Serial Number of the 3G module.		5 Signal							
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15-digit number used to identify an individual user on a GSM or UMTS network.		bars							
HW Rev.	The hardware version of the 3G module.									
Temperature	The temperature of the 3G module in degrees Celsius.									
System Mode	WCDMA/Europe		LED	Low		Medi	UM		High	
	CDMA 2000 / America									
WCDMA band	The 3G radio frequency band which supports tri-band UTMS/HSDPA/HSUPA	Signal Level (RSSI)	3G Radio Signal Strength Index							
	frequencies (850/1900/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850 MHz, WCDMA1900 is 1900 MHz.		Value	2 ~ 5	6 ~ 10	11 ~ 13	14 ~ 17	18 ~ 31	99	
GSM band	The 2G radio frequency band which supports Quad-band GSM/GRPS frequencies,		Signal	-109 ~	-101 ~	-91 ~	-85 ~	-77 ~	unknow	
	including GSM850, GSM900, DCS1800, PCS1900 with each number representing the respective frequency in MHz.		level in	-103	-93	-87	-79	-52		
WCDMA channel	The 3G channel.		dBm							
GSM channel	The 2G channel.		5 Signal							
GSM (PS) state	Packet Switching state		bars							
ጠጠ (CS) state	Circuit Switching state									
~ /										
			LED	Low		Medium		High		

Quality (Ec/lo)

strongest cells.

The total energy per chip per power density (Ec/lo) value of the active set's three

Status	Description
Network	Should display as registered with a valid unlocked SIM card.
Registration Status	
Network Name	The 3G internet Service Provider.
Country & Network	Each country and network has a unique code.
Codes	
Cell ID	The network information for the "serving" cell ID.
Primary Scrambling	The PSC of the reference WCDMA cell
Code (PSC)	
Data Session Status	Connected or Disconnected
HSUPA/HSDPA	The HSUPA/HSDPA categories correspond to different data transmission rates with
Categories	higher numbers generally indicating faster rates
Received Signal	The RSCP of the active set's three strongest cells
Code Power (RSCP)	
Battery Connection	BCS of the MT (Mobile Termination)
Status (BCS)	
Battery Charge Level	BCL of the MT (Mobile Termination)
(BCL)	

### 8.4 Statistics

These screens provide detailed information for:

- Local Area Network (LAN) and Wireless Local Area Network (WLAN)
- 3G Interfaces

#### NOTE: These statistics page refresh every 15 seconds.



#### 8.4.1 LAN Statistics

This screen displays statistics for the Ethernet and Wireless LAN interfaces.

Interface		Recei	ived		Т	ransn	nitteo	ł			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops			
Ethernet eth1	473478	3152	0	0	936120	2571	0	0			
Ethernet eth0	0	0	0	0	8848	78	0	0			
Wireless	0	0	0	0	23521	169	71	0			

Interface	Shows connection interfaces						
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes					
	Pkts	Rx/TX (receive/transmit) packets					
	Errs	Rx/TX (receive/transmit) packets with errors					
	Drops	Rx/TX (receive/transmit) packets dropped					

### Status

### 8.4.2 Etisalat Statistics

Click Etisalat network in the Statistics submenu to display the screen below.

	HSPR	/3G SETTING	is WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
Status >	Statistics >	3G				
Statist	ics of WAN	Inbound O	utbound			
Octect	S					
Packe	ts					
Drops						
Error						

Service	Shows the service t	type				
Inbound	Octets	Number of received octets over the interface.				
	Packets	Number of received packets over the interface.				
	Drops	Received packets which are dropped.				
	Error	Received packets which are errors.				
Outbound	Octets	Number of Transmitted octets over the interface.				
	Packets	Number of Transmitted packets over the interface.				
	Drops	Transmitted packets which are dropped				
	Error	Transmitted packets which are errors.				

### 8.5 Route

Select Route to display the paths the Router has found.

BRSIC		HSPR/3G S	SETTINGS U	i-fl		м	ANAGEMENT	ADVANCED SETTING	S STATUS
	Status > Route								
	Flags: U - up, 1 - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).								
	-		INCOME AND INCOME.		100000000	INCOMPANY.	No. of Concession, Name		
	Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface		
	192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0		

Field	Description
Destination	Destination network or destination host
Router	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up
	!: reject route
	G: use Router
	H: target is a host
	R: reinstate route for dynamic routing
	D: dynamically installed by daemon or redirect
	M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces



### 8.6 ARP

HW Address

Device

Click ARP to display the ARP information.

	BASIC		HSPR/3G S	ETTINGS WI-FI		MANAGEMENT	ADVANCED SETTING	S   STATUS
		Status > Al	8P					
				HW Address 00:1E:68:AC:0E:94	Device br0			
Field			Descrip	tion				
IP address			Shows II	P address of	host p	IC		
Flags			Complet	e				

### 8.8 PING

The PING menu provides feedback of connection test to an IP address or a host name.

BASIC	HSPR/3G SETTINGS	WI-FI	MANAGEMENT	ADVANCED SETTINGS	STATUS
Host	Name or IP Address:				
	Submit				

Input an IP address or a host name, e.g www.google.com and press Submit. The connection test result will be shown as below.

BASIC	HSPR/3G SETTINGS WI-FI	MANAGEMENT	ROVANCED SETTINGS STRTUS
56 b 56 b 56 b	G www.lgoogle.com (74.125.127.103): 5 tytes from 74.125.127.103: icmp_seq=0 tti ytes from 74.125.127.103: icmp_seq=1 tti ytes from 74.125.127.103: icmp_seq=2 tti ytes from 74.125.127.103: icmp_seq=3 tti	=41 time=270.1 ms =41 time=272.0 ms =41 time=256.8 ms	
4 pa	www.l.google.com ping statistics ickets transmitted, 4 packets received, 09 nd-trip min/avg/max = 256.8/267.7/272.1		

The above screen is not showing successful ping result

### 8.7 Dynamic Host Configuration Protocol (DHCP)

Shows the MAC address of host pc

Shows the connection interface

Incomplete Permanent Publish

Click DHCP to display the DHCP information.



	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

### Status



# Appendix

A: Print Server

49

These steps explain the procedure for enabling the Print Server.

1: Enable Print Server from the Advanced menu in the Web User Interface.

Select Enable on-board print server checkbox and enter Printer name and Make and model

NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

SIC	HSPR/3G SETTINGS WI-FI	MANAGEMENT	RDVRNCED SETTINGS STRTUS
Print Ser	ver settings		
This page	allows you to enable / disable printer support	d.	
🕑 Enab	le on-board print server.		
Printer na Make and			
		Save/Apply	

### For Windows XP:

2: Go to the Printers application in the Control Panel and select the Add a printer function (as located on the side menu below).

Chine O Ch	1	wards 🐑 Politiers 🚦	11-				
Appleton The Press and Party							ie.
Statement of the local division of the local	100	Aaso -	Documents		Commento	Lecation	
Pater Talks	0	Adde POP	0	Ready		My documents	
Add And Add Into		Conference Client		Pilatr Pilatr			- 22
@ Sittle Press				Braty .	1004-1 ten Outereill	100104-1	- 12
Conc. and	PROF	street, which spectra it	B. Contraction	Reals	10194-119a-Outereit	80154-5	1.0
Sec also							
No. of Concession, Name							
Stokenstering							
R og aben hand							
Other Flaces	18						
D- Crostend							
S Scanners and Campus							
E Ph Constantia							
A Ph Patron							
M Ny Caracter							
Details							
Bet and							

3: Click Next to continue, when you see the dialog box below.

This wizard helps you install a printer or make printer connections.
Fyou have a Plug and Play printer that connects through a USB poit (or any other hit pluggable point, auch as IEEE 1394, infrared, and as on h, you do not need to use this viscant. Click Cancel to our source the second to be an end of the second to our source and the printer of the second to computer's infrared poit, and turn the printer on. Windows will automatically install the printer for you. To continue, click Next.

4: Select Network Printer and click Next.

Add Printer Wizard	
Local or Network Printer The wizard needs to know which type of printer to set up.	Ø.
Select the option that describes the printer you want to use:	
O Local printer attached to this computer	
Automatically detect and install my Plug and Play printer	
A network printer, or a printer attached to another computer	
To set up a network printer that is not attached to a print server, use the "Local printer" option.	
< Back Next >	Cancel

- 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. http://192.168.1.1:631/printers/printername) and click Next.
- NOTE: The printer name must be the same name entered in the web user interface "printer server setting" as in step 1.

### Appendix: A

	http://www.com/commencedures.com/commencedures/commencedu commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedures/commencedur
What printe	er do you want to connect to?
O End a p	rinter in the directory
	t to this printer (or to browse for a printer, select this option and click. Next):
Name:	
	Example: \\aerver\printer
<li>Connec</li>	t to a printer on the internet or on a home or office network:
URL:	nttp://192.168.1.1.631/printers/hp3845
	Example : http://server/printers/myprinter/printer

6: Click Have Disk and insert the printer driver CD.

an installatio	anufacturer and mode n disk, click Have Disk nentation for a compat	l of your printer. If your printer c. If your printer is not listed, o ible printer.	r came with consult you
Manufacturer Agfa Alps Apollo Apple APS-PS AST	AGFA	AccuSet v52.3 AccuSetSF v52.3 AccuSet 800 AccuSet 800SF v52.3 AccuSet 800SF v2013.108	(
This driver is digit Tell me why drive	ally signed. : signing is important	ок (	ave Disk Cancel

7: Select driver file directory on CD-ROM and click OK.

L.	Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.	OK Cancel
	Copy manufacturer's files from:	

8: Once the printer name appears, click OK.



9: Choose Yes or No for default printer setting and click Next.

Default Printer Your computer wil always se otherwise.	nd documents to the default pinter unless you specify
Do you want to use this prints	r as the default printer?
Olies	
0 Mg	

10: Click "Finish".





11: Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.

ton Same at two							
and a start	.0	Next - Galantif? Officing Mellow Defining Mellow Defining Mellow Defining Comparison Defining Comparison Defining Comparison	ban.	11113	Deveni Deve Milety	Labler Folkowik	Not Aske KY Converse H Donat Biel Sera H Const Die Source Linear Unie Grow H Const Dies Source Linear Unie Grow Drag May Fill Print Dire
Bee Also B Traditional particle B Total Sector (Sector)							
Other Places							
Contractioned Society Contraction Contractions Society Contraction Society Contraction							

### For Mac OSX:

- 2. Browse to the Apple menu and select System Preferences. In the System Preferences menu click on Print .
- 3. With your Printer driver installed, please add your printer from the Printer menu.



4. Click + to add your printer from the Print menu.

Show All	Print & Fax	
Printers Customer Care a Idle		ner Care e this printer
	Location: Kind: Generic I Status: Idle	PostScript Printer
	Open Print	Queue) Options & Supplies)
+- D	efault Printer: Last Printe	r Used
Default Paper Size	n Page Setup: A4	÷
Click the lock to prevent fur	ther changes.	0

### Appendix: A

5. Select Internet Printing Protocol – IPP from the Protocol drop down list.

	o 🖴 💈 🥏 🖨	9		
	IP Windows Bluetooth AppleTalk More Printers		Search	
Protoco	✓ Internet Printing Protocol – IPP Line Printer Daemon – LPD			
Address	HP Jetdirect - Socket			
	Enter host name or IP address.			
Queue:				
	Leave blank for default queue.			

6. Type into the Address field "GatewaylPAddress:631" where GatewaylPAddress is the IP address of your Router (default: 192.168.1.1). See screenshot below for an example. Also enter into the Queue field "/printers/PrinterName", where PrinterName is the name you gave your printer in the initial step above.

○ <b>○</b> ろ	9 🖴 8 🥏 🚊	9		¢
	IP Windows Bluetooth AppleTalk More Printers		Statin	
Protocol:	Line Printer Daemon - LPD			
Address:	192.168.1.11631			
	Valid and complete address.			
Queue:	/printers/samsung			
	Leave blank for default queue.			

7. Select your printer from the Print Using drop down list.

ocation:	unknown	
nt Using:	Select a driver to use	
	9	
	3300 Series	
	350 Series	
	4300 Series	
	\$200 Series	
	5400 Series	
	6200 Series	

8. Click Add and check the printer status.



Print Server set up is now complete. You will now be able to print from common applications by selecting this printer from the Print dialogue box.



#### For Windows Vista

2. Go to the control panel, and select Printers. Once in the Printers page, click the Add a printer button as shown below.



3. Select Add a network, wireless or bluetooth printer.



- Click on the radio-button labelled Select a shared printer by name, and type "http://192.168.1.1:631/ printers/PrinterName" in the box below. Click Next.
- NOTE: The PrinterName must be the same as the printer name entered in the Web User Interface above.

1	Find a printer by name or TCP/IP address	
1	Browse for a printer	
	Select a shared printer by name	
	http://192.168.1.1.%31/printans/samsung	Bronsern
	Example: \\computername\printername or http://computername/printers/printername/.printer	
- 34	Add a printer using a TCP/IP address or hostname	
1	Add a Bluetooth printer	

5. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.

an installation	n disk, click	and model of your printer. If your printer came with Have Disk. If your printer is not listed, consult your a compatible printer.
Manufacturer Apollo Brother Canon Citizen Dell		Printers Apollo P-1200 ≩ Apollo P-2100/P2300U ≩ Apollo P2200
This driver is digita Tell me why driver		Have Disk OK Cancel

6. Choose whether you want this printer to be the default printer, and then click Next.

### Appendix: A



7. Click Finish. Your device is now configured and ready for use.







# Appendix

B: USB Storage

These steps explain the procedure for enabling the USB Storage.

- 1: Enable Samba Server from Web User Interface.
- Select Enable Samba checkbox and enter Netbios name and Directory Name

Advanc	ed > USB Storage set	tings		
USB St	orage: Down			
This easi	e allows you to enable i	/ disable 1100 stasses		
inis pag	ye allows you to enable i	/ disable USD storage		
🖻 En	able USB storage			
Netbios	Name: 3G10WVE			
Directo	y Name: USB-Storage			
			Save Reboot	

Field	Description
Netbios Name	It is the hostname of the PC
	The default name is "3G10WVE"
Directory Name	The folder name of "root" directory.
	The default name is "USB-Storage"

### For Mac OSX:

- 2. From the Finder, select the Go and then click Connect to Server
- In the address field of the Connect to Server dialog, type in the address: smb:// "NetbiosName"/ "DirectoryName" (eg smb://3G10WVE/USB-Storage)

😣 ⊖ ○	Connect to	Server	
Server Address			
smb:// 3G10	OWVE / USB-Storage		+ 0,
Favorite Server	5:		
🔤 smb://3	G10WVE /USB-Storage		
Remo	ove	Browse	Connect

4. Click the + button to add this server to the list of Favourites and then click Connect

	Col	nnect to Server	
Server Ad	dress:		
smb://	3G10WVE / USB-Stora	ge	+ 0,
Favorite S	ervers:		
🔤 sm	b://3G10WVE /USB-Sto	orage	
0	Remove	Browse	Connect
	Keniove	Browse	Connect

- For Windows XP:
- 2: Open a web-browser (such as Internet Explorer, Firefox or Safari) and type in the address. \\"NetbiosName"\"DirectoryName"\(eg. \\3G10WVE\USB-Storage)
- Note: There is no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.



5. Select the Guest radio button and then click Connect





For Windows Vista

- 1. Open a web-browser (such as Internet Explorer, Firefox or Safari)
- 2. Type in the address "\\NetbiosName\DirectoryName\" (eg \\ntc-cpe\ntc-cpe)

🔾 🔾 💌 🧎 \\ntc-cp#\i	Mc-cpe		• 49 Search	م
File Edit View Tools	Help			
🐚 Organize 🔹 🏢 View	s 🔹 🕐 Bam			e
Favorite Links	Name	Date modified	Туре	
Documents	🍌 usb1_1		File Folder	
Pictures				
Pictures Music				

Note: There is no username and password required to access the USB drive. Any network user will be able to read/write the folder/files in the USB drive.

### Appendix: B