



# DataRoute voice



## Installation and User Manual

Version 4 – October 2011

## Document Control

Date	Doc Version	Change
Dec 2010	1	1 <sup>st</sup> release of document
Dec 2010	2	Added VoIP options
Jan 2011	3	Security Options
Oct 2011	4	Additional features and options

## Notices

### Emergency Calls

This terminal operates using mobile signals, which cannot guarantee connection in all conditions. Therefore, you should never rely solely on the terminal equipment for essential communications such as medical or emergency services.

No responsibility is assumed by TFM for the use or reliability of the DataRoute voice when used in a situation or with other equipment not supplied or specified by TFM.

TelecomFM shall accept no liability for any error or damages of any kind resulting from the use of this document or the equipment it relates to.

The wording in this document may change from time to time. Please refer to the TelecomFM web site [www.telecomfm.co.uk](http://www.telecomfm.co.uk) for the latest release.



# 1. Contents

<b>1. Contents</b> .....	<b>3</b>
<b>2. Overview</b> .....	<b>5</b>
<b>3. Specification</b> .....	<b>5</b>
3.1 Indicators & Interfaces .....	5
3.2 Package Contents .....	7
<b>4. Getting Started</b> .....	<b>8</b>
4.1 Hardware Connection .....	8
4.2 Computer Configuration.....	9
4.3 Log In .....	10
<b>5. Status</b> .....	<b>11</b>
<b>6. Quick Setup</b> .....	<b>12</b>
<b>7. Network</b> .....	<b>19</b>
7.1 3G Configuration (WAN Device/WAN Service).....	19
7.2 ADSL Configuration (WAN Service) .....	21
7.3 SIM PIN (3G Settings) .....	24
7.4 Advanced ADSL Settings .....	25
7.5 DMZ Host .....	25
7.6 Port Forwarding (Virtual Servers) .....	26
7.7 Advanced IP Routing (Static Route) .....	27
7.8 QoS Configuration.....	28
<b>8. Application</b> .....	<b>30</b>
8.1 UPnP Settings.....	30
8.2 Dynamic DNS.....	30
8.3 VPN (IPSec VPN).....	31
8.4 VPN (PPTP Config).....	32
<b>9. Wireless (WLAN)</b> .....	<b>33</b>
9.1 WLAN Basic.....	33
9.2 WLAN Security .....	34
9.3 Advanced Settings .....	34

9.4	WLAN MAC Filters .....	35
9.5	WLAN Bridge .....	36
<b>10.</b>	<b>LAN (DHCP) .....</b>	<b>37</b>
<b>11.</b>	<b>Firewall .....</b>	<b>39</b>
11.1	Firewall Settings .....	39
11.2	IP Filters .....	39
11.3	Domain Filters .....	41
11.4	MAC Filters.....	42
11.5	Access Control (Remote Access).....	43
<b>12.</b>	<b>Voice (VoIP) .....</b>	<b>44</b>
12.1	Voice Configuration .....	44
12.2	Basic Settings.....	44
12.3	Advanced Settings.....	46
<b>13.</b>	<b>Tools .....</b>	<b>48</b>
13.1	Account Settings (Users) .....	48
13.2	Time Settings .....	49
13.3	Backup Settings .....	50
13.4	Update (Restore) Settings .....	50
13.5	Update Software .....	51
13.6	Factory Settings.....	51
13.7	Reboot Router .....	51
13.8	TR-069 Client .....	52
13.9	Ping Reboot.....	53
13.10	3G Link Notice .....	53
<b>14.</b>	<b>Troubleshooting .....</b>	<b>54</b>
14.1	Unable to Access Internet.....	54

## 2. Overview

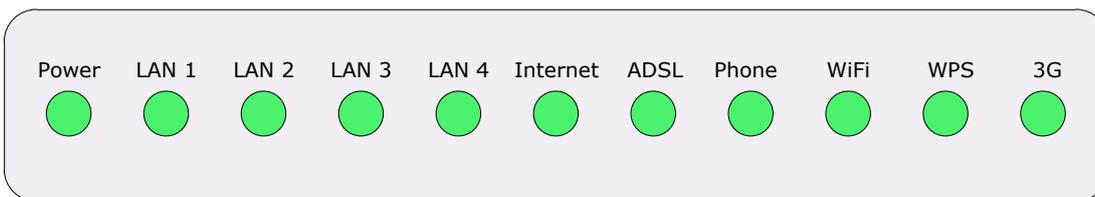
The DataRoute voice is a high-speed gateway with functions including:

- Build-in wireless module with speed up to 7.2Mbps;
- ADSL2/2+ modem for broadband connection;
- Four 10/100M auto-sensing Ethernet ports for wired connections;
- Built-in 802.11n enhanced WLAN complies with IEEE 802.11n draft v2.0 and backward to 802.11b/g specifications. It supports 2x2 MIMO and up to 300Mbps of bandwidth. The throughput of WLAN to LAN is more than 100Mbps;
- Integrated FXS port for voice calls;
- Supports TR-069 remote management;

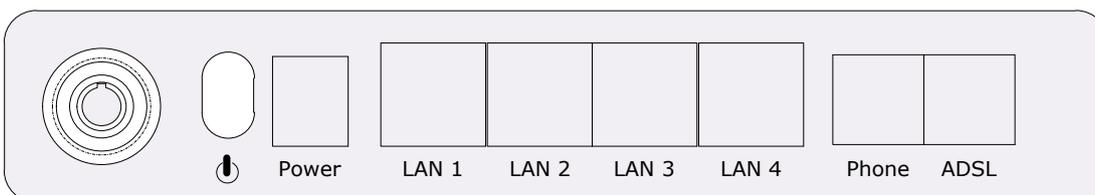
## 3. Specification

### 3.1 Indicators & Interfaces

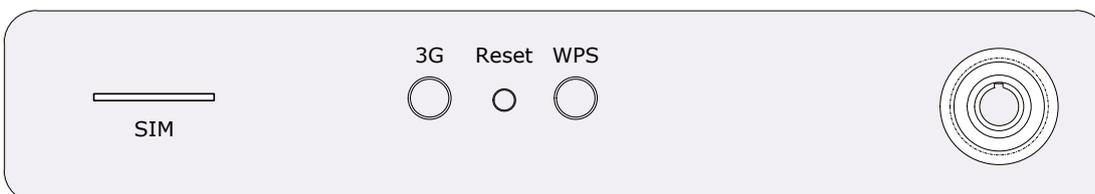
Front Panel Indicators:



Right Side Interfaces:



Left Side Interfaces:



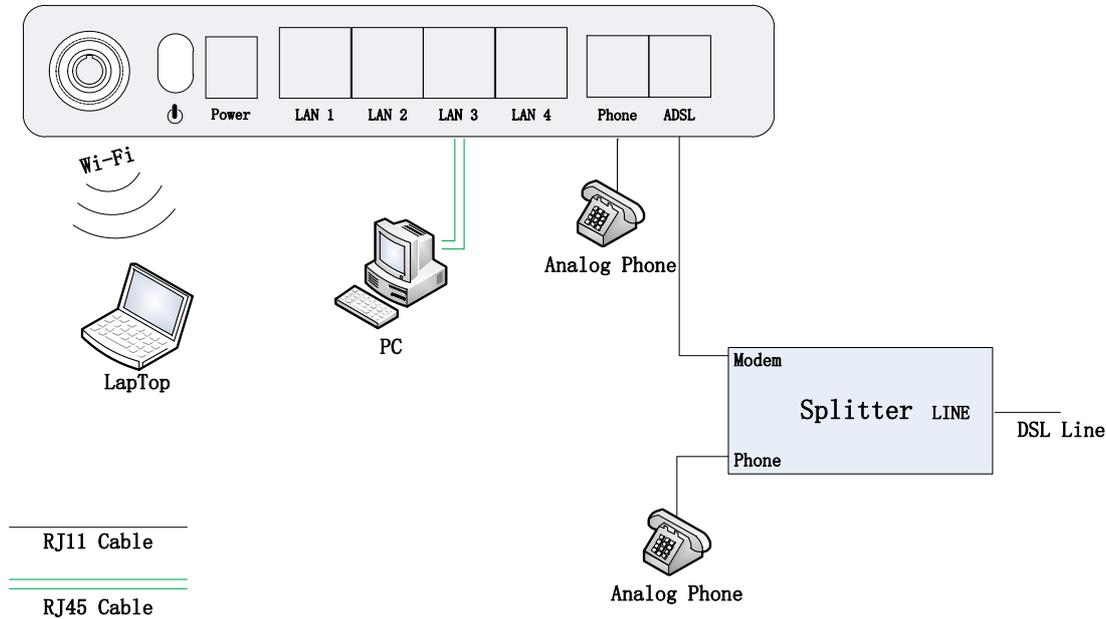
Item	Label	Description
Indicators	Power	Solid green: DataRoute Power on
		Solid red: Firmware update in progress
		Off: DataRoute Power off
	LAN1-4	On: Ethernet is connected
		Blinking green: Ethernet Traffic flows
		Off: Ethernet is disconnected
	Internet	Blinking green: PPP/DHCP negotiation
		Solid green: PPP/DHCP up
		Quick blinking green: Tx/Rx traffic on line
	ADSL	On: Modem synchronized to the DSLAM
		Quick blinking green: Modem training, but not synchronized
		Slow blinking green: Modem Idle
	Phone	On: The analogue phone connected to Phone port off-hook
		Off: The analogue phone connected to Phone port on-hook
	Wi-Fi	On: Wi-Fi connection is available
		Blinking green: Negotiation or traffic on line
		Off: Wi-Fi connection is not available
	WPS	On: WPS connection setup successfully
		Blinking: WPS connection has been activated
		Off: WPS connection is not activated
3G	Blinking green: Negotiation or traffic on line	
	Solid green: Up	
	Quick blinking green: Tx/Rx traffic on line	
	Solid red: Authentication failed	
	Off: Traffic through DSL interface	
Right Side		Power switch
	Power	For 12V DC power adapter
	LAN1-4	LAN interface for connecting to computers
	Phone	Connection for analogue telephones
	ADSL	Connection for ADSL enabled telephone line
Left Side	3G	Manually connect/disconnect 3G data
	WPS	Start Wi-Fi Protected Setup
	Reset	Restore to factory default settings

## 3.2 Package Contents

Item	Quantity
Power Adapter	1
Phone Line	2
RJ-45 Cable	1
DataRoute Voice	1
User Manual	1
ADSL Splitter	1

## 4. Getting Started

### 4.1 Hardware Connection



1. Use a telephone cord to connect the LINE port of the splitter with the phone socket on the wall (only if using ADSL).
2. Use another telephone cord to connect the MODEM port of the splitter with the ADSL port of the DataRoute voice (only if using ADSL).
3. Connect Ethernet port of the DataRoute voice with 10/100BASE-T port of the computer using the network cable that comes with the unit.
4. Plug in the power cord, and turn on the power.

## 4.2 Computer Configuration

The default IP address for DataRoute voice is: **192.168.1.1**

The Subnet Mask is: 255.255.255.0

Devices can be connected via one of the Ethernet ports or via Wi-Fi. The default Wi-Fi settings are:

Wireless SSID: **DATAROUTE**

Wireless Key: **data1234**

Users can configure the DataRoute voice through a web browser. The DataRoute voice can be used as a gateway, DNS server and DHCP server; by default the DataRoute voice will automatically assign an IP address to any devices connecting to it, alternatively users can set the computer's TCP/IP settings manually as follows:

1. Set the computer IP address to the same subnet as the DataRoute voice i.e. set the IP address of the PC to one in the range of 192.168.1.2 - 192.168.1.254" excluding 192.168.1.1.
2. Set the computer's gateway address to the IP address of the DataRoute voice.
3. Set the computer's Primary DNS server to the IP address of the DataRoute voice or to that of an effective DNS server.

## 4.3 Log In

Start the web browser and enter the following in the address bar:

<http://192.168.1.1>

The authentication interface will pop up as below:



The default user name and password is **admin** for web log-on. Press **ENTER** or click on '**OK**' to enter the configuration interface.

**Warning:** Please be sure the IP of the computer network card is in the same IP range as the DataRoute voice LAN port before trying to log on (ex: 192.168.1.2 and 192.168.1.1 are in the same IP range). If the login is not displayed please check in Internet Explorer--Tools---Internet Options---Connection---LAN Setup---Proxy server, disable the function 'Proxy for LAN' and then retry.

If log on successful, the status page will be displayed as follows:

Status	Status	Quick	Network	Application	WLAN
Basic Info	Basic Info				
Network Status	Device Model	DataRoute voice			
WAN Info	Hardware Version	V1.5			
WLAN Status	Software Version	1.1.2			
Connected Devices	System Run Time	48 seconds			
Routing Table	Current Time	Thu Jan 1 00:00:47 1970			
Statistics	MAC Address	00:1a:a9:b3:04:65			
VoIP Status	LAN Subnet IP	192.168.1.1			
	LAN Subnet Mask	255.255.255.0			
	Default Gateway				
	Primary DNS Server				
	Secondary DNS Server				
	Synchronized Time				

## 5. Status

Click on the **Status** menu in the web interface

The following status information is available by clicking the links on the left of the webpage:

### **Basic Info**

Includes hardware and software versions, system time info and basic IP information.

### **Network Status**

Includes basic 3G status (SIM card details, network and signal strength) and basic ADSL status.

### **WAN Info**

Lists the configured WAN (3G and ADSL) interfaces and shows type, connection status and basic IP information.

### **WLAN Status**

Includes basic Wireless information and a list of clients connected wirelessly.

### **Connected Devices**

Shows a full list of connected clients, both wired and wireless.

### **Routing Table**

Displays the current IP routing table

### **Statistics**

Displays a list of configured WAN (3G and ADSL) interfaces and shows the amount of traffic sent and received on each interface.

### **VoIP Status**

Shows the current registration status of a configured VoIP provider.

## 6. Quick Setup

Click on the **Quick** menu in the web interface.

This will show a quick setup wizard that allows the user to configure the most commonly used options:

### Step 1: Access Account

Username:	<input type="text"/>
New Name:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

This sets the username and password to access the web interface.

The default username to access the DataRoute voice is **admin**.

The default password is **admin**.

To change the password:

1. Select **admin** from the **Username** drop-down box
2. Enter the password **admin** in the **Old Password** box
3. Enter a new password in both the **New Password** and **Confirm Password** boxes
4. Click the **Next** button
5. Login with the new password
6. Click on the **Quick** menu to continue the wizard

To continue to the next step without changing the password click the **Skip** button.

## Step 2: Time Settings

Current Time: Thu Jan 1 00:24:29 1970

Set Time Mode:  Time Server  Manual Setting

Time:  year  month  day  
 hour  minute

Time Zone Offset:

From this page the current time can be set manually or the DataRoute voice can be set to obtain the correct time from an internet time server.

**Note:** it is recommended that an internet time server is used when available – if the time is set manually it will be lost in the event of a power cut or if the unit is restarted.

To set the time manually:

1. Select **Manual Setting**
2. Enter the current time
3. Select the correct Time Zone
4. Click **Next**

To use an internet time server:

1. Select **Time Server**
2. Enter the time server domain name e.g **time.nist.gov** or **pool.ntp.org**
3. Select the correct Time Zone
4. Click **Next**

### Step 3: Wireless Settings

Enable WLAN

Disable SSID broadcast

SSID:	<input type="text" value="DATAROUTE"/>
BSSID:	00:1A:A9:B3:04:6E
Country:	<input type="text" value="UNITED KINGDOM"/>
Max client number:	<input type="text" value="16"/>
Channel:	<input type="text" value="1"/>
Auto Channel Timer(min):	<input type="text" value="0"/>

By default the Wireless (Wi-Fi) access point is enabled and the SSID (the name that is displayed when users search for Wi-Fi networks) is set to "DataRoute". To keep the default settings click **Next** to go to the next step.

To change the SSID:

1. Enter the new SSID in the **SSID** box
2. Select the correct Country
3. Click the **Next** button

#### Step 4: Local Area Network Setup

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static DNS Server:

Get DNS Server From WAN

Configure the second IP Address and Subnet Mask for LAN interface

By default the DataRoute voice has an IP Address of 192.168.1.1 and the DHCP server is enabled so that IP addresses will be automatically assigned to clients connecting to either the wired ethernet ports or via Wi-Fi. To keep the default settings click **Next** to go to the next step.

A new IP address can be assigned to the DataRoute voice and the DHCP options can be changed from this screen – for more details on available options refer to section 10.

#### Step 5: 3G Failover

Enable Automatic 3G backup

Time out all dsl linkdown to run 3G(seconds)  seconds

WAN Device Select:

When both ADSL and 3G connections are available the DataRoute voice can failover to the 3G connection when the ADSL connection is unavailable. To use the feature check the **Enable Automatic 3G backup** box and enter the amount of time (in seconds) that the ADSL link must be unavailable before switching to 3G.

Click **Next**

## Step 6: Configure 3G and ADSL connections

To setup the 3G connection:

### 3G Network (WAN) Service Setup

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Connected		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

Click the **Edit** button for the 3G service

### 3G network settings

PPP Connect Mode

PPP author

PPP Username

PPP Password

APN

Dial Number

Auto reconnect interval time

Service Mode

Port Bind  LAN1  LAN2  LAN3  LAN4  SSID1

Enable LAN DHCP [\(?\)](#)

For most networks it is only required to set the correct **APN** value (this should be provided by your network operator)– leave the other settings on default values.

If your network requires login enter the valid **PPP Username** and **PPP Password**.

Fill in the required information and click the **Apply/Save** button.

To setup the ADSL connection:

**ADSL Network (WAN) Service Setup**

Interface	Vpi	Vci	Category	QoS	Description
atm0_1	0	35	UBR	Disabled	2_INTERNET_B_0_35
atm1_1	8	35	UBR	Disabled	3_INTERNET_B_8_35



Click the **Add** button to start the ADSL network wizard.

VPI: [0-255]

VCI: [32-65535]

Enter the values for VPI and VCI supplied by the ADSL Service Provider and click **Next**.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA
- PPPoA
- IPoA

Encapsulation Mode:

Service Category:

Select the DSL link type and Encapsulation Mode supplied by the ADSL service provider; (note: please choose EoA for PPPoE connection) and click **Next**.

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Service Mode:

Port Bind (?):  LAN1  LAN2  LAN3  LAN4  SSID1

Enable LAN DHCP (?)

If EoA link type was selected choose the WAN service type, normally PPP over Ethernet (PPPoE).

Click **Next**.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:  ▼

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

- Enable IGMP Multicast Proxy

Enter the username and password provided by the ADSL service provider; select any other options required and click **Next**.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>PORT / VPI / VCI:</b>	0 / 0 / 35
<b>Connection Type:</b>	PPPoE
<b>Service Name:</b>	pppoe_0_0_35
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Automatically Assigned
<b>Service State:</b>	Enabled
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Enabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Check the Summary screen and then click **Apply/Save** to enable the connection.

The Quick Setup wizard is now complete. Refer to the following sections for a complete description of all of the available options.

## 7. Network

### 7.1 3G Configuration (WAN Device/WAN Service)

**Note:** please power off the Gateway before inserting the SIM card.

Please go to path: **Network** -> **WAN Device** page.

When both ADSL and 3G connections are available the DataRoute voice can failover to the 3G connection when the ADSL connection is unavailable. To use the feature check the **Enable Automatic 3G backup** box and enter the amount of time (in seconds) that the ADSL link must be unavailable before switching to 3G. Then click **Apply/Save**.

#### WAN Device Settings

Please click Apply/Save to save you configure

Enable Automatic 3G backup

Time out all dsl linkdown to run 3G(seconds)  seconds

WAN Device Select:

Then go to path: **Network** -> **WAN Service**

#### WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.  
If Ports Binding is enable,only the binding port can access to the internet.  
If Ports Binding is disable,all of the ports can access to the internet.

Enable Ports Binding

#### 3G Network (WAN) Service Setup

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Connected		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

Click the **Edit** button for the 3G service

**3G network settings**

PPP Connect Mode	Auto Connect
PPP author	AUTO
PPP Username	
PPP Password	
APN	mobile.o2.co.uk
Dial Number	
Auto reconnect interval time	30
Service Mode	VOIP_INTERNET
Port Bind	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input checked="" type="checkbox"/> LAN4 <input type="checkbox"/> SSID1
	<input checked="" type="checkbox"/> Enable LAN DHCP <a href="#">(?)</a>
<input data-bbox="172 790 276 824" type="button" value=" &lt;Back "/> <input data-bbox="288 790 477 824" type="button" value=" Apply/Save "/>	

Fill in the required information and click the **Apply/Save** button. For most networks it is only required to set the correct **APN** value – leave the other settings on default values.

If your network requires login enter the valid **PPP Username** and **PPP Password**.

## 7.2 ADSL Configuration (WAN Service)

Please go to path: **Network** -> **WAN Service** page. Then do the following to setup an ADSL connection:

- 1) Click **Add** button to start the ADSL network wizard;

### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI).

**Notice: If the link type is EoA, it can use the PVC repeatedly though it is existent. But the PPPoA or IPoA can't.**

VPI: [0-255]

VCI: [32-65535]

Enter the values for VPI and VCI supplied by the ADSL Service Provider.

- 2) Click **Next** to select the DSL link type and Encapsulation Mode supplied by the ADSL service provider; (note: please choose EoA for PPPoE connection)

### ATM PVC Configuration

Select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA  
 PPPoA  
 IPoA

Encapsulation Mode:

Service Category:

Enable VLAN

### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

- 3) Click **Next** – if EoA link type was selected choose the WAN service type, normally PPP over Ethernet (PPPoE)

**WAN Service Configuration**

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Port Bind:  LAN1  LAN2  LAN3  LAN4  
 SSID1  SSID2  SSID3  SSID4

- 4) Click **Next** to input the username and password provided by the ADSL service provider; select any other options required.

PPP Username:   
PPP Password:   
PPPoE Service Name:   
Authentication Method:

- Enable Fullcone NAT
- Enable Firewall
- Dial on demand (with idle timeout timer)
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

- Enable IGMP Multicast Proxy

5) Click **Next** to check the Summary of this connection;

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>PORT / VPI / VCI:</b>	0 / 0 / 35
<b>Connection Type:</b>	PPPoE
<b>Service Name:</b>	pppoe_0_0_35
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Automatically Assigned
<b>Service State:</b>	Enabled
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Enabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

6) Click **Apply/Save** to enable the connection.

## 7.3 SIM PIN (3G Settings)

Go to path **Network** -> **3G Settings**

### PIN Settings

#### PIN code operation

Disable--When PIN lock disabled, SIM card can be activated without PIN auth.

Enable--When PIN lock disabled, SIM card should be activated after PIN auth successfully.

Modify--Set PIN code as a new one.

PIN code: 4~8 decimal digits.

PUK code: 8 decimal digits. When SIM card is PIN locked, it should be unlocked with correct PUK code.

Residual allowed try time After these times, SIM card will be locked.

PIN State:	Disabled
PIN code operation:	Enable <input type="button" value="v"/>
PIN code:	<input type="text" value="••••"/>
Residual allowed try time:	3

This page allows the user to enable or disable the SIM pin function.

Select whether the SIM Pin should be enabled or disabled, enter the current SIM pin and click the **Apply/Save** button.

The "PIN State" shows whether the SIM PIN function is currently enabled or disabled.

The "Residual allowed try time" shows how many attempts to enter a correct PIN remain – if the incorrect PIN is entered too many times a PUK code will then be required for the SIM before it can be used again.

## 7.4 Advanced ADSL Settings

Go to page **Network -> ADSL Settings**

### DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Apply/Save

This page allows advanced settings for the ADSL interface to be adjusted. It is recommended that these settings are unchanged from their default values unless instructed by the ISP.

## 7.5 DMZ Host

Go to page **Network -> DMZ Host**

### NAT -- DMZ Host

The DSL router will forward IP packets from the 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 "Apply" to activate the DMZ host.

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

DMZ Host IP Address:

Save/Apply

This page allows an IP Address to be entered where all incoming traffic from the WAN interfaces will be routed.

Note that the "Virtual Servers" options take precedence – all traffic that does not match any application configured in Virtual Servers will be forwarded to the DMZ Host IP Address.

Enter the required IP Address and clickt the **Save/Apply** button.

## 7.6 Port Forwarding (Virtual Servers)

Go to path **Network -> Virtual Servers**

### NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with 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 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

This page allows the user to forward incoming traffic on selected ports on the WAN interfaces to internal hosts. This can be used to make internal applications available to the internet (e.g. a web server).

Click the **Add** button to add a new forward:

### NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".** Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

- Use Interface – select the WAN interface to forward from
- Service Name – either select from the list of predefined services (e.g. Web Server (HTTP)) or enter a name for a custom service.
- Server IP Address – enter the local IP Address to forward network traffic to
- Ports Table – if a predefined service is selected the table will be completed automatically. If a custom service is being entered the table must be filled in manually.
  - Enter the range of IP addresses to match from the external (WAN) interface (start and end ports can be the same to match a single IP Address).
  - Select the Protocol (TCP, UDP or both TCP/UDP)
  - Enter the range of IP addresses to forward to at the internal host. These can be the same as the external ports or the traffic can be forwarded to a different port on the internal host.

Enter the required values and then click the **Apply/Save** button.

## 7.7 Advanced IP Routing (Static Route)

Go to page **Network -> Static Route**

**Routing -- Static Route (A maximum 32 entries can be configured)**

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

This page allows the user to manually edit the routing table and create Static IP Routes. Note that in normal operation this is not required.

Click the **Add** button to add a new static route:

**Routing -- Static Route Add**

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)  
Metric:

- Destination IP address/prefix length – enter the destination in the format IP address/network prefix e.g. 124.80.0.0/16
- Interface – select the network interface to route to
- Gateway IP address – specify the IP address for the gateway (if required)
- Metric (optional) – specify the route metric

Enter the required values and then click the **Apply/Save** button

## 7.8 QoS Configuration

Please go to path: **Network -> QoS Configuration** page to enable Queue Management Configuration. If **Enable QoS** checkbox is selected, a default DSCP mark should be chosen to automatically mark incoming traffic without reference to a particular classifier. Click **Apply/Save** button to save.

**Note:** If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces; The default DSCP mark is used to mark all egress packets that do not match any classification rules.

### QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS

Select Default DSCP Mark

Please click **QoS QUEUE** button to enter the QoS Queue setup page, then click **Add** button. This screen allows you to configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface. Click **Apply/Save** to save and activate the queue.

### QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

**Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others**

Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Please click **QoS Class** button to enter QoS Classification Setup page, then click **Add** button to configure network traffic classes. This screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the rule.

**Add Network Traffic Class Rule**

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

**Specify Classification Criteria**

A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

## 8. Application

### 8.1 UPnP Settings

Go to path **Application** -> **UPnP**

#### UPnP Settings

Enable UPnP.

Apply/Save

Use this page to enable or disable Universal Plug and Play (UPnP) functionality. UPnP allows networked devices to automatically discover each other.

By default UPnP is enabled – it is recommended that this setting be left unchanged.

### 8.2 Dynamic DNS

Go to path **Application** -> **Dynamic DNS**

#### Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
----------	----------	---------	-----------	--------

Add Remove

Dynamic DNS allows a static hostname to be assigned to a connection which is not assigned a static IP address. A subscription to a Dynamic DNS provider is required to maintain the mapping between the hostname and the currently assigned IP address.

DataRoute voice can work with either the DynDNS or TZO dynamic DNS services.

Click the **Add** button and then enter the details provided by the dynamic DNS service provider

## 8.3 VPN (IPSec VPN)

Go to path **Application** -> **IPSec VPN**

### IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove	Edit
<input type="button" value="Add New Connection"/> <input type="button" value="Remove"/>					

A Virtual Private Network (VPN) Tunnel can be established to provide secure communications between 2 points on the internet using the IPSec tunneling protocol.

Click the **Add New Connection** button to display the IPSec Settings:

### IPSec Settings

IPSec Connection Name	<input type="text" value="new connection"/>
Remote IPSec Gateway Address (IP or Domain Name)	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="Auto(IKE)"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="text" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Show Advanced Settings"/>

- IPSec Connection Name – specify a name to identify the tunnel
- Remote IPSec Gateway Address – specify the IP address or FQDN for the remote end of the tunnel, this should be the internet IP address for the remote gateway
- Tunnel access from local IP addresses – specify the IP address or subnet for the local side of the IPSec tunnel
- Tunnel access from remote IP addresses – specify the IP address or subnet for the remote side of the IPSec tunnel
- Key Exchange Method – select Auto to use the standard Internet Key Exchange (IKE) method or Manual to specify the encryption and authentication keys manually
- Authentication Method – only Pre-Shared Key is supported
- Pre-Shared Key – enter the Pre-Shared Key
- Perfect Forward Secrecy – select whether to use the Perfect Forward Secrecy (PFS) method

Fill in the required options and then click the **Apply/Save** button

## 8.4 VPN (PPTP Config)

Go to path **Application -> PPTP Config**

### PPTP Config

Choose Edit to modify information over PPTP WAN Service.

**Note:**If the table below is empty, please add WAN Service first! [Click Here](#)

Tunnel Name	Ip Address/Domain Name	WAN Interface	Enable	Default Gateway	Use Default Gateway	Status	Edit	Action
1_VOIP_INTERNET_R_orangeinternet	(null)	ppptd3g0	NO	(null)	NO	Unconfigured		<a href="#">Connect</a>

A default PPTP tunnel is automatically created for each available WAN interface. Click the Edit button to configure the tunnel:

### PPTP Edit

Tunnel Name:

Ip Address or Domain Name:

WAN Interface:

PNS Username:

PNS Password:

Enable:  ▼

Use Default Gateway On The Remote Network:  ▼

Authentication Method:  ▼

Use Static IP Address

[Apply](#)

- Tunnel Name – specify a name to identify the tunnel
- Ip Address or Domain Name – specify the IP Address or FQDN for the remote PPTP Network Server
- PNS Username - -specify the username required to login to the remote PPTP Network Server
- PNS Password - -specify the password required to login to the remote PPTP Network Server
- Enable – set to use to start using the PPTP tunnel
- Use Default Gateway On the Remote Network – set to yes to forward traffic to the remote gateway
- Authentication Method – select the authentication method required to login to the PNS (PAP/CHAP/MSCHAP) or set to AUTO for the authentication method to be determined automatically.
- Use Static IP Address – select to specify the IP Address manually

Set the required options and then click the **Apply** button

## 9. Wireless (WLAN)

### 9.1 WLAN Basic

Go to path: **WLAN** -> **WLAN Basic**

#### WLAN Basic Settings

Enable WLAN

Disable SSID broadcast

SSID:

BSSID: 00:1A:A9:B3:04:6E

Country:

Max client number:

Channel:

Current channel: 1

Auto Channel Timer(min):

- Enable WLAN – select to enable the built-in Wi-Fi access point
- Disable SSID broadcast – select to prevent the Access Point from being discoverable. Users will need to manually specify the SSID to connect.
- SSID – enter the SSID to identify the Wi-Fi access point, this is the name that will be displayed when users search for Wi-Fi networks.
- Country – select the country where the DataRoute voice is installed
- Max client number – specify the maximum number of Wireless clients that will be allowed. The DataRoute voice supports up to 16 simultaneous Wi-Fi connections.
- Channel – select the Wireless channel to use. The channel number can be changed if interference is experienced.

After entering the required settings click the **Apply/Save** button.

## 9.2 WLAN Security

Go to path: **WLAN** -> **WLAN Security**

The default Wireless Pre-Shared Key is **data1234** – it is strongly recommended that this be changed.

It is recommended that all other security settings be left unchanged to maintain maximum security and compatibility.

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Enable WLAN security

Network Authentication:

WPA Pre-Shared Key:  [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

Enter a new **WPA Pre-Shared Key** and then click **Apply/Save**. This is the key that must be entered whenever connecting a PC or other client to the DataRoute voice via Wi-Fi.

## 9.3 Advanced Settings

Go to path **WLAN** -> **Advanced Settings**

This page contains Advanced parameters for the Wireless LAN interface.

It is strongly recommended that these settings be left unchanged unless there is a specific requirement for different settings in the environment where the DataRoute voice is installed.

Altering these parameters may result in a reduction in Wireless performance.

## 9.4 WLAN MAC Filters

Go to path **WLAN** -> **WLAN MAC Filters**

### Wireless -- MAC Filter

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address	Remove
-------------	--------

This page can be used to restrict the clients that are permitted to connect Wirelessly to the DataRoute voice.

**WARNING:** Changing the mode takes immediate effect and so may disconnect any connected Wireless clients.

MAC Restrict Mode – select from the following:

- Disabled – all MAC Addresses will be allowed to connect
- Allow – only MAC addresses listed below will be allowed to connect
- Deny – all MAC Addresses will be allowed to connect EXCEPT those listed below

Use the **Add** button to add MAC addresses to the list.

## 9.5 WLAN Bridge

Go to path **WLAN** -> **WLAN Bridge**

AP Mode:	<input type="text" value="Access Point"/>	
Bridge Restrict:	<input type="text" value="Enabled"/>	
Remote Bridges MAC Address:	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>

Use this page to configure Wireless Bridging functionality. Wireless Bridging allows a Wi-Fi network to be extended to cover a larger area through the use of multiple Wi-Fi bridge devices.

AP Mode:

- Access Point – DataRoute voice can be used as both a Wireless Access Point and a Wireless Bridge (default)
- Wireless Bridge – DataRoute voice can be used as a Wireless Bridge only

Bridge Restrict:

- Enabled –only Wireless Bridges whose MAC Addresses are entered below may connect
- Disabled – any Wireless Bridge may connect

Remote Bridges MAC Address – enter MAC Addresses for remote bridges which are permitted to connect when “Bridge Restrict” option is enabled.

Enter the required settings and then click the **Apply/Save** button.

## 10. LAN (DHCP)

Configure the DataRoute voice's IP address and DHCP options.

Go to path **DHCP** -> **LAN Setup**

### Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default ▼

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static DNS Server:

Get DNS Server From WAN

Configure the second IP Address and Subnet Mask for LAN interface

Set the required options then click the **Apply/Save** button

Important Note – changes will take effect immediately and if the IP Address of the DataRoute voice is changed the connection to the web interface will be lost. The new IP address will need to be entered into the web browser (The PC must be in the same subnet as the new IP address to view the webpage).

**IP Address** – enter the IP address that the DataRoute voice will be available on. The default IP address is 192.168.1.1.

**Subnet Mask** – enter the Subnet Mask. The default subnet mask is 255.255.255.0.

**Enable IGMP Snooping** – select to have the DataRoute voice monitor all IGMP network traffic for the purpose of reducing the multicast overhead (Advanced option)

**Disable DHCP Server** – turn off the built-in DHCP server. If the DHCP server is disabled all clients will need to have manually assigned IP addresses in order to connect.

**Enable DHCP Server** – turn on the built-in DHCP server

**Start/End IP Address** – enter the range of IP addresses that the DHCP server can assign to clients. These IP addresses must be in the same subnet as the IP address assigned to the DataRoute voice.

**Leased Time** – enter the duration for the lease of DHCP IP addresses (default is 24 hours)

**Static DNS Server** – enter an IP address for a DNS server to pass to DHCP clients. By default this is set to the IP address of the DataRoute voice to use the built-in DNS server (recommended).

**Get DNS Server from WAN** – select to pass the DNS server addresses obtained automatically from the WAN interface to the DHCP clients.

**Configure the second IP address** – select to assign an additional IP address to the DataRoute voice (advanced option).

Notes:

1. When you use the DHCP Server, please make sure you don't have multiple DHCP Servers in one LAN.
2. To view a list of clients that have been assigned addresses by the DHCP server go to the path **DHCP -> Assigned Leases**
3. To reserve an IP address within the DHCP range for a client so that the client always receives the same IP address go to the path **DHCP -> Static Leases**. Click the **Add Static Lease** button and enter the MAC address and required IP Address for the client. Make sure that the IP address chosen is within the range entered on the LAN Setup page.

## 11. Firewall

### 11.1 Firewall Settings

Please go to path: **Firewall** -> **Firewall Settings** page, check **Enable** to activate **Global firewall settings**, then click **Apply/Save**.

**Note:** three Firewall levels are supported in the device, they are:

- Low: enable basic firewall features - prevent port scanning; allow PING from WAN side; allow ICMP redirect messages from WAN side.
- Middle: in addition to Low level, prevent ICMP redirect messages.
- High: in addition to Middle level, prevent SYN Flood attack; against PING from WAN side.

#### Firewall Settings

Global firewall settings:  Enable

Firewall level Low ▼

Apply/Save Low  
Middle  
High

**Note:** by default the Firewall is enabled and set to the “High” setting – it is recommended that to maintain maximum security this setting is not changed,

### 11.2 IP Filters

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Please go to path: **Firewall** -> **IP Filters** -> Incoming IP Filtering Setup.

#### Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	------------	----------	---------------------	---------	---------------------	---------	--------

Click **Add** button to configure incoming IP filters. The following interface allows user to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**  
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

- Select All
- ppptd3g/ppptd3g0
- br0/br0

Apply/Save

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Please go to path: **Firewall -> IP Filters -> Outgoing IP Filtering Setup.**

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Add Remove

Click Add button to configure outgoing IP filters. The following interface allows the user to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

**Add IP Filter -- Outgoing**

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Apply/Save

## 11.3 Domain Filters

Please go to path: **Firewall** -> **Domain Filters** page. Please select the list type first then configure the list entries.

List type:

- Exclude: accept all the DNS except the list;
- Include: drop all the DNS except the list;

**domain Filter** -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

**Exclude:** default accept all the DNS except the list

**Include:** default drop all the DNS except the list

domain List Type:  Exclude  Include

Address	Port	Remove
---------	------	--------

Add	Remove
-----	--------

Click **Add** to do the configuration after choosing a domain list type. Then set the domain address and port number in the next interface. Click **Apply/Save** to add the entry to the domain filter.

**Parental Control** -- **domain Add**

Enter the domain address and port number then click "Apply/Save" to add the entry to the domain filter.

domain Address:

Apply/Save

## 11.4 MAC Filters

Please go to path: **Firewall** -> **MAC Filters** page to setup MAC filtering. All MAC layer frames will be forwarded except those matching with any of the specified rules in the settings.

### MAC Filtering Setup

All MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. Choose Add or Remove to configure MAC filtering rules.

Protocol	MAC address	Remove
----------	-------------	--------

Please click **Add** to create a filter to identify the MAC layer frames by specifying at least one condition. If multiple conditions are specified, all of them will take effect. Click **Apply** to save and activate the filter.

### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Source MAC Address:   
(eg: 00:90:96:01:2A:3B)

## 11.5 Access Control (Remote Access)

The Access Control feature allows ports to be opened to the internet (WAN) connections so that it is possible to connect remotely to the DataRoute voice.

Go to path **Firewall -> Access Control**

### Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used. Only the service of WAN is Enabled, the WAN Port can be configed effectively.

Services	LAN	WAN	WAN Port
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	80
ICMP	Enable	<input type="checkbox"/> Enable	
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	69

Save/Apply

To enable remote access to the DataRoute voice web interface check the Enable box under WAN for the HTTP service. The default port is the standard web port 80 which can be changed by entering a new value under WAN Port.

Once enabled it will be possible to access the web interface by browng to the Internet IP Address assigned to the DataRoute voice. For example, if the IP address assigned by the ISP is 80.70.60.50 and the WAN Port is set to 8080 the following would be entered into the web browser:

<http://80.70.60.50:8080>

**Note: It is strongly recommended that the web interface password be changed (go to path Tools -> Access Control) before enabling the Access Control feature.**

This feature can be used via an ADSL or 3G connection. Note that some 3G networks have internal NAT and Firewall systems which do not allow remote access.

## 12. Voice (VoIP)

### 12.1 Voice Configuration

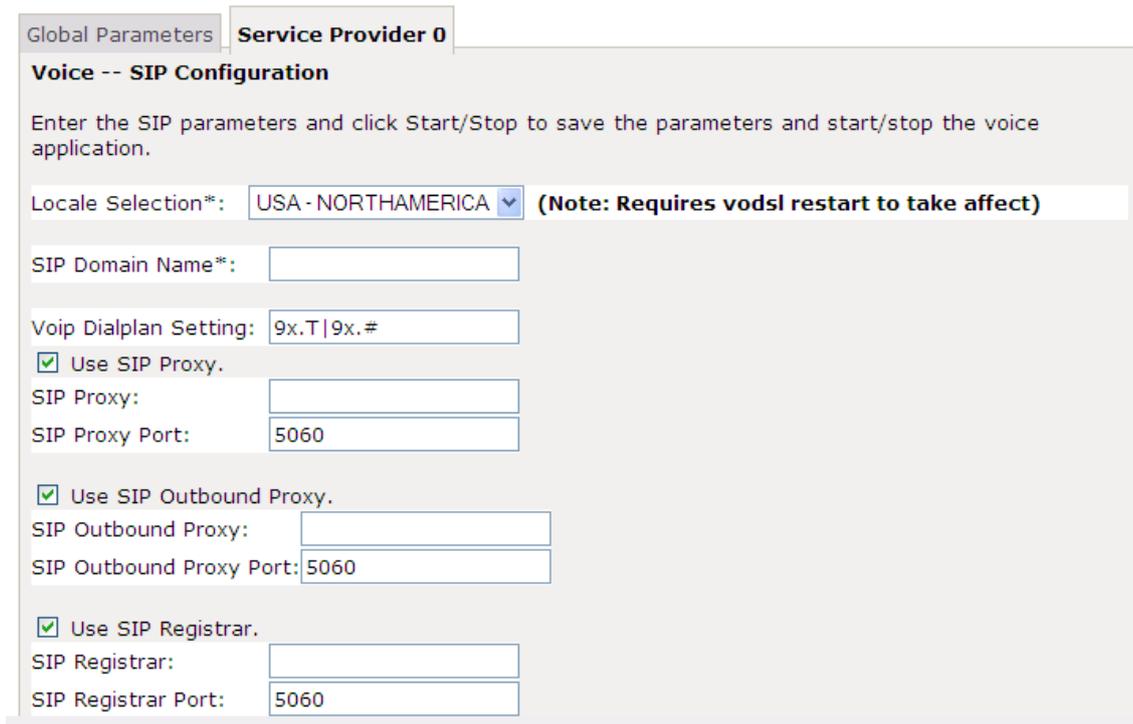
Connect a normal analogue telephone to the Phone port.

Phone calls can be made over the GSM/3G network (when a valid SIM is inserted) and using Voice over IP (when there is an active connection to the internet).

By default, all calls are dialled over the GSM/3G network. To make calls via VoIP (SIP) it is necessary to configure a connection to a SIP Service Provider:

### 12.2 Basic Settings

Go to path: **VoIP** -> **Basic Settings** page, then click on the **Service Provider 0** tab. Enter SIP parameters and click Apply to save the parameters.



The screenshot shows the 'Service Provider 0' configuration page for SIP. The title is 'Voice -- SIP Configuration'. Below the title is a note: 'Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.' The form contains several fields and checkboxes:

- Locale Selection\*:** A dropdown menu set to 'USA - NORTHAMERICA' with a note: '(Note: Requires vodsl restart to take affect)'
- SIP Domain Name\*:** An empty text input field.
- Voip Dialplan Setting:** A text input field containing '9x.T|9x.#'
- Use SIP Proxy.**
  - SIP Proxy:** An empty text input field.
  - SIP Proxy Port:** A text input field containing '5060'.
- Use SIP Outbound Proxy.**
  - SIP Outbound Proxy:** An empty text input field.
  - SIP Outbound Proxy Port:** A text input field containing '5060'.
- Use SIP Registrar.**
  - SIP Registrar:** An empty text input field.
  - SIP Registrar Port:** A text input field containing '5060'.

**Locale selection:** choose the Location – this will set the local tones etc. heard on the phone.

**SIP Domain Name:** enter the SIP Domain provided by the SIP Provider

**Voip Dialplan Setting:** specify the dial strings to be matched for VoIP calls. All numbers dialled which match one of the dial strings will be dialled via the SIP Service Provider; all numbers dialled which do not match any of the dial strings will be dialled via the GSM/3G network.

- Key:
- x = any digit
  - . = 1 or more digits
  - T = dial after timeout
  - # = dial immediately when # terminator dialled
  - | = separator between dial strings

e.g. 9x.T|9x.# = all numbers starting with a 9 will be dialled via SIP (numbers will be dialled after a timeout or after a # is dialled)

012x.T|013x.T = all numbers starting with 012 or 013 will be dialled via SIP (numbers will be dialled after a timeout)

**Use SIP Proxy:** enable to allow using SIP Proxy. Enter the SIP proxy address (IP address or FQDN) and port

**Use SIP Outbound Proxy:** enable to allow using SIP Outbound Proxy. Enter the SIP Outbound Proxy address (IP address or FQDN) and port

**Use SIP Registrar:** enable to register to a SIP server. Enter the SIP Registrar address (IP address or FQDN) and port

<b>SIP Account</b>	0
<b>Account Enabled</b>	<input checked="" type="checkbox"/>
<b>Physical Endpt Id</b>	0
<b>Authentication Name</b>	1001
<b>Password</b>	1001
<b>Preferred Ptime</b>	20
<b>Preferred Codec 1</b>	G.711ALaw
<b>Preferred Codec 2</b>	G.729a
<b>Preferred Codec 3</b>	G.723.1
<b>Preferred Codec 4</b>	G.726_24
<b>Preferred Codec 5</b>	G.726_32
<b>Preferred Codec 6</b>	GSM_AMR_12K

**Authentication Name:** the username which is provided by the SIP provider

**Password:** the password which is provided by the SIP provider

**Preferred codec list:** select the order of the audio codecs to be used

Once the configuration is complete, click the **Apply** button to save changes. Click **Stop SIP client**, and then click **Start SIP client** to enable the configuration.

## 12.3 Advanced Settings

Go to path: **VoIP** -> **Advanced Settings** page, to configure the advanced VoIP features.

Voice -- SIP Advanced Configuration	
Line	1
Echo Cancellation	<input checked="" type="checkbox"/>
Call Waiting	<input type="checkbox"/>
Call Forwarding Number	
Forward Unconditionally	<input type="checkbox"/>
Forward on "Busy"	<input type="checkbox"/>
Forward on "No Answer"	<input type="checkbox"/>
MWI	<input type="checkbox"/>
Call Barring	<input checked="" type="checkbox"/>
Call Barring Pin	9999
Call Barring Digit Map	
Anonymous Call Blocking	<input type="checkbox"/>
Anonymous Calling	<input type="checkbox"/>
DND	<input type="checkbox"/>
Silence Suppression	<input checked="" type="checkbox"/>
CNG	<input checked="" type="checkbox"/>
Ingress Gain	0 ▾
Egress Gain	0 ▾

**Echo Cancellation** – select to enable the built-in echo canceller

**Call forwarding Number:** set a number to use call-forwarding. Select the conditions to use call forwarding by ticking the required boxes.

**MWI** – select to enable MWI (Message Waiting Indicator) support

**Call Barring** – select to enable Call Barring

**Anonymous Call Blocking** – select to disallow incoming calls with no CLI

**Anonymous Calling** – select to withhold CLI on outgoing calls

**DND** – select to enable DND (Do Not Disturb) support

**Silence Suppression** – when selected audio packets will not be transmitted to the network if no audio is detected to reduce bandwidth usage

**CNG** – select to enable detection of CNG (Fax) tones

**Ingress Gain** – used to increase or decrease the volume of the incoming audio

**Egress Gain** – used to increase or decrease the volume of the outgoing audio

<input type="checkbox"/> Enable T38 Support	
<input checked="" type="checkbox"/> Enable V18 Support	
Registration Expire Timeout*	<input type="text" value="0"/>
Registration Retry Interval	<input type="text" value="0"/>
DSCP for SIP*:	<input type="text" value="EF (101110)"/> ▼
DSCP for RTP*:	<input type="text" value="EF (101110)"/> ▼
Dtmf Relay Setting*:	<input type="text" value="InBand"/> ▼
Hook Flash Relay Setting*:	<input type="text" value="None"/> ▼
SIP Transport Protocol*:	<input type="text" value="UDP"/> ▼
<input checked="" type="checkbox"/> Enable SIP Tag Matching* (Uncheck for Vonage Interop).	
<input type="checkbox"/> SIP Prack	
Music Server*:	<input type="text"/>
Music Server Port*:	<input type="text" value="0"/>

**Enable T38 Support** – enable support for T.38 fax compatible devices

**Enable V18 Support** – enable support for V.18 Textphone compatible devices

**Registration Expire Timeout** – enter the timeout length for the registration

**Registration Retry Interval** – enter the retry interval for the registration

**DSCP for SIP/RTP** – select the codepoint to use when connecting via QoS compatible systems

**Dtmf Relay Setting** – select the format to transmit DTMF tones to the network. Tones can be transmitted In-Band or Out-Of-Band (SIP INFO or RFC2833)

**Hook Flash Relay Setting** – select whether local Hook Flash should be ignored or sent as SIP INFO packet

**SIP Transport Protocol** – select the protocol (UDP or TCP) to use for SIP packets. Most systems use UDP.

**Enable SIP Tag Matching** – uncheck when using with Vonage

**SIP Prack** – use the SIP Prack method instead of ACK

**Music Server** – enter an address and port for an external music server to provide music on hold.

## 13. Tools

### 13.1 Account Settings (Users)

When you configure the DataRoute voice through an Internet browser, the system requires user name and password to validate access permission. The factory sets the default username of "admin" and the password of "admin". Go to path **Tools** -> **Account Settings**, you can choose the username and change the password.

#### Access Account

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:	<input type="text"/>
new name:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
<input type="button" value="Apply/Save"/>	

**Attention:** please remember the password after change, otherwise you will need to reset the device and will lose all configuration settings.

## 13.2 Time Settings

Go to path Tools -> Time Settings

From this page the current time can be set manually or the DataRoute voice can be set to obtain the correct time from an internet time server.

**Note:** it is recommended that an internet time server is used when available – if the time is set manually it will be lost in the event of a power cut or if the unit is restarted.

Current Time: Thu Jan 1 10:46:42 1970

Set Time Mode:  Time Server  Manual Setting

Time Server:

Time Zone Offset:

Enter the required options and click the **Apply/Save** button.

## 13.3 Backup Settings

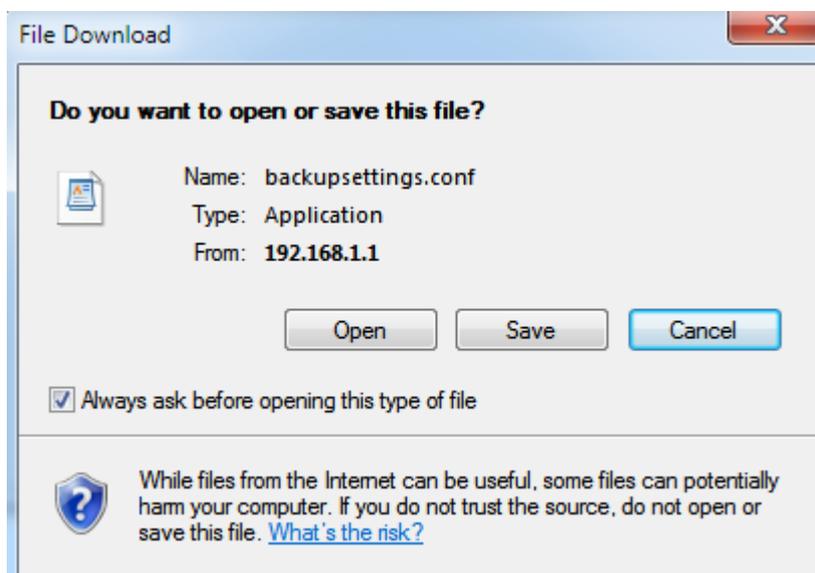
To backup the current configuration to a file:

Please go to path: **Tools** -> **Backup Settings** page. Click Backup Settings button, then a File download window will pop-up. Click **Save** button to download/save current configuration of the device to the PC.

### Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings



## 13.4 Update (Restore) Settings

Please go to path: **Tools** -> **Update Settings** page. Click **Browse** button to choose a configuration file, then click **Update Settings** to restore configuration.

### Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

## 13.5 Update Software

Please go to path: **Tools** -> **Update Software** page. Click **Browse** to choose the right software. Then click **Update Software** to update.

The power LED will go **red** to indicate that the software upgrade is in progress. Once complete the unit will automatically restart with the new software. The current software version can be viewed by going to path **Status** -> **Basic Info**

**Attention:** please make sure the power to the device is not interrupted during the software updating process. Also, the RJ45 cable should be connected tightly between the PC and device during the software uploading process.

Once updated, please press the reset button or go to path: **Tools** -> **Factory Settings** to restore the device to the new factory default settings if necessary.

### Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

## 13.6 Factory Settings

To restore the DataRoute voice to the factory default configuration either press the **Reset** button on the side of the unit or go to path **Tools** -> **Factory Settings** and click the **Restore Default Settings** button.

**Note:** all user entered configuration options will be lost.

## 13.7 Reboot Router

To perform a soft restart of the DataRoute voice go to path **Tools** -> **Reboot Router** and click the **Reboot** button. A restart takes approximately 2 minutes.

## 13.8 TR-069 Client

The DataRoute voice can be provisioned remotely via the use of a TR-069 remote management server.

Please go to path: **Tools** -> **TR-069 Client** page to setup an auto-configuration server to perform auto-configuration, provision, collection and diagnostics to this device. Select the desired values and click **Apply/Save** to configure the TR-069 client options.

**Note:** all the parameters in the screenshot should be matched with the TR-069 Server.

### TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Safe Link:	<input type="button" value="Cert Import"/>
Inform Interval:	<input type="text" value="300"/>
ACS URL:	<input type="text" value="http://200.48.229.23:70"/>
ACS User Name:	<input type="text" value="001aa92e202d"/>
ACS Password:	<input type="password" value="*****"/>
WAN Interface used by TR-069 client:	<input type="text" value="Any_WAN"/>
Display SOAP messages on serial console	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	<input type="text" value="admin"/>
Connection Request Password:	<input type="password" value="*****"/>
Connection Request URL:	<input type="text" value="(null)"/>

## 13.9 Ping Reboot

The "Ping Reboot" feature can be used to monitor the status of the internet connection and to automatically restart the DataRoute voice when the internet connection is unavailable.

Go to path **Tools** -> **Ping Reboot**

### Ping Reboot Settings

Disable Ping Reboot

Enable Ping Reboot

Ping IP Address:

Ping Interval(range: 10min~3600min):

Enter an IP Address to ping in order to test the internet connection and a ping interval for how often to check the connection.

## 13.10 3G Link Notice

The 3G Link Notice feature can be used to send an SMS to inform the user when the 3G data connection is unavailable.

### 3G Link Notice

3G Link UP Notice:  Enable

Mobile Number

Enter the Mobile Number to send the SMS to and click the **Apply/Save** button.

## 14. Troubleshooting

### 14.1 Unable to Access Internet

#### Check the Line and the Device

1. Check the power supply indicator is on - if not, make sure the connection to the power supply is correct; Make sure the power switch is turned on;
2. Check the LAN indicator for the PC is on - if not, check the cable connection between the PC and the DataRoute voice; Make sure that the correct cable is used;
3. Check the ADSL LED to see if it is flashing. If no fast flashing is observed within 3 minutes, please check whether phone line has been correctly connected; check whether ADSL filter is correctly used. If multiple extensions have been installed, make sure that the filter is installed prior to the junction box of the phone line. If the above items are confirmed and still no fast flashing of DSL LED is observed, call the ISP to query whether ADSL service has been provided on your line;
4. Check the ADSL LED to see whether it is unable to change status from fast flashing to always on, or whether it changes status to fast flashing after some time of being always on. If these phenomena occur constantly, please contact your ISP with a request to check lines and signal quality;

If there are no problem in the above items, the line and the device should be working. Problems may be caused by your computer configuration or device configuration.

#### Check Your Configuration

1. Enter the device manager to check if Ethernet adapter is correctly installed. If any problem exists, please re-install it;
2. Check the configuration of Ethernet adapter in PC. Try to manually set IP address that is in band 192.168.1.X without conflict.
3. Try to run command "ping 192.168.1.1" in a command prompt (Start, Programs, Accessories, Command Prompt). If the response returns "time out", please check Ethernet connection and IP settings;
4. If the DataRoute voice is reachable, try to ping a known internet IP, e.g. a DNS server: "ping 4.2.2.2".
  - If ping is reachable, there are no problems in the DataRoute voice. Please go to step 5;
  - If ping is not reachable, see step 6 and check if the configuration is correct.
5. Please try to ping a internet URL, e.g. "ping www.google.com".
  - If ping is reachable, there are problems in the network settings. Please check the settings of the PC terminal, e.g. whether the security level is too high, or whether anti-virus or firewall is installed;
  - If ping is not reachable, check the DNS setting of Ethernet adapter.

Note 1: The precondition is that LAN settings in the DataRoute voice have not been modified.

Note 2: To start a Command Prompt in Windows click on the Start menu, Programs, Accessories, Command Prompt

Note 3: The returned values of ping command in the following format show the standard of "reachable"

```
C:\Users\Pretender>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. If ping of the modem is reachable but ping of the internet fixed IP is unreachable, attention should be concentrated upon device settings. Please enter the web interface following the instructions in this manual.

(1) Check first the number of WAN connections. If more than one connection exists, for troubleshooting, delete unused connections and leave the one connection you are using.

(2) Check the connection to see whether correct "type" is selected. When you use PPPoE/PPPoA to login, the following information should be provided: VPI and VCI, which can be queried from your ISP, user name and password.

(3) Then make sure that "using NAT" and "default gateway" have been selected with a tick. Check whether "Dial on demand" has been selected with a tick. If it is selected, the connection is activated only when traffic to the internet arrives.

Make sure that the above parameters are saved after configuration.