

E200 Series – Cellular / WAN / LAN / Wi-Fi Router

Version 0.5



DATE

Copyright

Copyright© 2015 Maestro Wireless Solutions Limited. All right reserved. This document is for the use of intended recipients only and the contents may not be reproduced, redistributed, or copied in whole or in part for any purpose without Maestro prior express consent.

① Note: This document is subject to change without notice

This manual cover the following products:

- Maestro E205XT02
- Maestro E205XT04
- Maestro E206XT

DOCUMENT VERSION

This manual is written without any warranty.

Maestro Wireless Solutions Ltd. reserves the right to modify or improve the product and its accessories which can also be withdrawn without prior notice.

Our company stresses the fact that the performance of the product and its accessories depends on the proper use conditions as well as the surrounding environment.

Maestro Wireless Solutions Ltd. assumes no liability for damage incurred directly or indirectly from errors, omissions or discrepancies between the router and this manual.

This software, solution or application is provided on an "as is" basis. No warranty whether expressed or implied is given by **Maestro Wireless Solutions Ltd.** in relation to this software, solution or application. User shall assume the entire risk of using or relying on this software, solution, and application.

In no event will **Maestro Wireless Solutions Ltd.** be liable for any loss or damage including without limitation, indirect or consequential loss, damage, or any loss, damage whatsoever arising from loss of data or profit arising out of, or in connection with, the use of this router product. Every effort is made to keep the product and its software up and running smoothly. However, **Maestro Wireless Solutions Ltd.** takes no responsibility for, and will not be liable for, the product or its software being temporarily unavailable due to technical issues beyond our control.

The above terms and conditions are subject to change without prior notice. The present use of this product solution implies that the user approves and understands all the above terms and conditions.

Table of Contents

<u>2</u>	SAFETY PRECAUTIONS	7
2.1	General precautions	7
2.2	USING THE ROUTER IN VEHICLE	7
2.3	PROTECTING YOUR ROUTER	7
<u>3</u>	OVERVIEW	8
3.1	Scope	8
3.2	TARGET AUDIENCE	8
<u>4</u>	PREREQUISITES	8
5	LISER MANUAL CONVENTIONS	Q
<u>J</u>		,
<u>6</u>	PRODUCT OVERVIEW	10
<u> </u>		10
6.2	E205 SERIES AT A GLANCE	10
0. <u>2</u>	EZUO SERIES AT A GLANCE BUNDI E CONTENT	11
0.5	DUNDLE CONTENT	11
7	PRODUCT FEATURES	12
_		
<u>8</u>	PHYSICAL DIMENSIONS AND LED	13
8.1	PHYSICAL DIMENSIONS	13
8.2	LED INDICATORS	14
8.3	ETHERNET PORT LED INDICATORS	15
<u>9</u>	HARDWARE INSTALLATION	16
9.1	INSTALL THE SIM CARD	16
9.2	CONNECT THE CELLULAR (WWAN) ANTENNA(S)	16
9.3	CONNECT THE POWER SUPPLY	17
9.4	CONNECTION TO THE DEVICE	17
9. <mark>4</mark> .	1 CONNECTION WITH THE LAN CABLE	17
9.4.	2 CONNECTION VIA WI-FI	17
<u>10</u>	E205 BASIC CONFIGURATION	18
10.	1 CONNECTING TO THE WEB INTERFACE	18
10.	2 LAN CONFIGURATION	19
10.	3 WAN CONFIGURATION	20
10.3	3.1 Manual	20
10.3	3.2 Automatic	20
10.3	3.3 PPPOE (POINT-TO-POINT PROTOCOL OVER ETHERNET)	20
10.	4 Cellular Setup	21
10.	5 WIRELESS (WI-FI)	22

11 E205 ADVANCED CONFIGURATION	<u>24</u>
11.1 FLASHING FIRMWARE AND UPDATING YOUR DEVICE	24
12 STATUS PAGES EXPLAINED	<u>26</u>
12.1 OVERVIEW:	27
12.1.1 System	27
12.1.2 Cellular	28
12.1.3 Memory	28
12.1.4 Network	29
12.1.5 WIRELESS	29
12.1.6 Associated Stations	29
12.1.7 MWAN INTERFACE LIVE STATUS	30
12.2 FIREWALL	30
12.3 ROUTES	31
12.4 SYSTEM LOG	31
12.5 REALTIME GRAPHS	31
<u>13</u> <u>SYSTEM</u>	<u>32</u>
13.1 SYSTEM PROPERTIES	32
13.1.1 GENERAL SETTING	32
13.1.2 LOGGING	32
13.2 Administration	34
13.2.1 ROUTER PASSWORD	34
13.2.2 SSH ACCESS	34
13.3 Software	35
14 NETWORK	<u>35</u>
14.1 INTERFACES	35
14.2 LAN INTERFACE	37
14.2.1 GENERAL SETUP	37
14.2.2 Advanced Settings	38
14.2.3 Physical Settings	39
14.2.4 Firewall Settings	39
14.2.5 DHCP server	40
14.3 WIRED WAN INTERFACE	42
14.3.1 GENERAL SETUP	42
14.3.2 Advanced Settings	43
14.3.3 Physical Settings	43
14.3.4 FIREWALL SETTINGS	44
14.4 Cellular interface (3G or 4G)	45
14.4.1 GENERAL SETUP	45
14.4.2 Advanced Settings	46
14.4.3 FIREWALL SETTINGS	47
14.5 ADD VPN INTERFACE	47
14.5.1 PPTP	48
14.5.2 OPENVPN	50

<u>15</u>	WI-FI	57
15.1	INTRODUCTION	57
15.2	WI-FI AS ACCESS POINT	57
15.2.2	1 DEVICE CONFIGURATION - GENERAL SETUP	58
15.2.2	2 DEVICE CONFIGURATION - ADVANCED SETTINGS	59
15.2.3	3 INTERFACE CONFIGURATION – GENERAL SETUP	60
15.2.4	4 INTERFACE CONFIGURATION – WIRELESS SECURITY	61
15.2.5	5 INTERFACE CONFIGURATION – MAC-FILTER	61
15.3	WI-FI AS CLIENT	62
15.4	CREATING MULTIPLE SSID	63
<u>16</u>	SETTING UP FAILOVER AND LOAD BALANCING	65
16.1	FAILOVER MODE CONFIGURATION	65
16.1.2	1 SETTING UP LOAD BALANCING FOR FAILOVER	66
16.2	LOAD BALANCING MODE CONFIGURATION	70
<u>17</u>	FIREWALL BASICS	72
<u>18</u>	SERVICES	73
18.1	DYNAMIC DNS	73
18.2	SMS DIAGNOSTIC	75
18.3	DOTA	76
18.4	GPS	77
18.5	Event	78
10		=0
<u>19</u>	APPENDIX	/9
19.1	DEFAULT SETTINGS	79
19.2	RESET TO FACTORY DEFAULT SETTING	79
19.2.2	1 USING THE WEB-BASED USER INTERFACE	79
19.2.2	2 USING THE RESET BUTTON ON THE SIDE OF THE ROUTER	79
19.3	LIST OF ACRONYMS	81
19.4	SUPPORT	83
	2	

maestro))

1 Safety Precautions

1.1 General precautions

- The router generates radio frequency (RF) power. When using the router, care must be taken to ensure safety as well as compliance with all the regulations surrounding the use of RF equipment.
- Do not use the router in aircraft, hospitals and petrol stations or in places where using GSM products or other RF equipment is prohibited.
- Be sure that the router will not be interfering with nearby equipment such as pacemakers or medical equipment. The antenna of the router should be directed away from computers, office equipment, home appliance, etc.
- Always keep the router at a minimally safe distance of 26.6cm or more from a human body.
- M Do not put the antenna inside metallic boxes or other containers

1.2 Using the router in vehicle

- Check for any regulation or law authorizing the use of GSM equipment in vehicles in your country before installing the router.
- Installation of the router should be done by qualified personnel. Consult your vehicle dealer for any possible interference concerns related to the use of the router.
- Be careful when the router is powered by the vehicle's main battery. The battery may be drained after extended period.

1.3 Protecting your router

To ensure error-free usage, please install and operate your router with care and comply with the following:

Do not expose the router to extreme conditions such as high humidity/rain, high temperatures, direct sunlight, caustic/harsh chemicals, dust, or water.

- Do not try to disassemble or modify the router as there are no user serviceable parts inside and the warranty would be void in case of tampering.
- M Do not drop, hit or shake the router.
- M Do not use the router under extreme vibrating conditions.
- Do not pull the power supply cable. Please attach or detach it by holding the connector after switching off the supply.
- Install and connect the router in accordance to the instruction manual. Failure to do so will void the warranty.

2 Overview

2.1 Scope

This document provides you all the information you need to set-up, configure and use the Maestro E200 Series router.

2.2 Target audience

This document is intended for customers and integrators who understand basic telecommunications and information technology terminology and concepts.

3 Prerequisites

Before continuing with the installation of your E200 Series router, make sure you have a computer equipped with the following:

- M A computer with an Ethernet port or Wi-Fi connectivity
- M A web browser such as Google Chrome, Mozilla Firefox or Apple Safari



4 User manual conventions

The following symbols are used throughout the user manual:



The following symbol indicates attention must be paid



The following symbol indicates a **warning**



The following symbol provides information



5 Product overview

5.1 E205 Series at a glance

- M Dual-band HSDPA (E205XT02), tri-band HSDPA (E205XT04
- M GPRS/EDGE auto-fallback
- M Switchable WAN/LAN on RJ45 port
- M Built-in Wi-Fi with an external RP-SMA antenna connector
- M Automatic WAN / 3G failover
- M Built-in GPS supporting active antenna via an external SMA connector
- M External SMA antenna connectors for 3G
- M One digital inputs/outputs
- Six color LED's for displaying for Wi-Fi and network activity, signal, power and alarm
- M Device management and configuration via a web GUI
- DIN rail mountable

maes<mark>t</mark>ro)

5.2 E206 Series at a glance

- M Quad-band HSPA+ & dual-band EV-DO (E206XT)
- ℬ GPRS/EDGE auto-fallback
- M Switchable WAN/LAN on RJ45 port
- M Built-in Wi-Fi with an external RP-SMA antenna connector
- M Automatic WAN / 3G failover
- Built-in concurrent diversity/GPS antenna supporting active antenna via an external SMA connector
- M External SMA antenna connectors for 3G
- M One digital inputs/outputs
- Six color LED's for displaying for Wi-Fi and network activity, signal, power and alarm
- Device management and configuration via a web GUI
- DIN rail mountable

5.3 Bundle content

- M E200 Series router x 1
- 1m Ethernet cable 8P8C x 1
- 3) 2G/3G/4G terminal antenna 90 degree hinged SMA x 1
- M 5 dBi, 2.4/5.1~5.9 GHz dipole antenna RP-SMA (M) hinged 90° x 1
- Industrial grade 1.2 A power supply x 1
-)) DIN clip x 1

If any of these items are missing or damaged, please contact Maestro Support immediately. The Maestro Support website can be found at: <u>http://support.maestro-wireless.com/</u>



6 Product features

With high-speed cellular (3G and beyond), WAN, LAN and Wi-Fi connectivity, the E200 is a highly versatile, reliable and rugged router designed for missioncritical enterprise applications requiring faultless connectivity.

The E200 comes in two models; the cost-effective HSDPA ensures alwayson connectivity for 2G migration or low-latency applications such as energy and sales & payment, while the HSPA+ penta-band is ideal for deployment in vertical markets requiring high-speed data or global roaming, such as security and transportation.

The E200 can be configured through an easy-to-use web interface; quick setup section will facilitate basic router configuration. Advanced configuration setting for functions such as Wi-Fi, failover, load balancing, VPN, firewall are also directly available through the web interface. Once configured, a set of 6 LED's on the top of the aluminum alloy casing will help the user ensure that the device is operating correctly. Users can also remotely manage the router is also available through an HTTPS connection over the LAN or WAN.

12 Maestro E200 Series



7 Physical dimensions and LED

7.1 Physical dimensions



E200 Series dimensions without			
connector			
Lenght	83.9mm		
Depth	60mm		
Height 25mm			
Weight	Weight 90g		



7.2 LED indicators

The E200 Series features 6 LEDs on the front to display critical system information

NAME	COLOUR	STATE	DESCRIPTION
	\bigcirc	OFF	Wi-Fi network is deactivated
WI-FI	*	Flashing	Wi-Fi network connection traffic
	•	ON	Wi-Fi network is activated
Activity	\bigcirc	OFF	Cellular data service is not connected
	۲	ON	Cellular data service is connected
	\bigcirc	OFF	SIM card is not inserted, or device is not registered on the cellular network
Network	÷.	Flashing	Device is registered on the cellular home network
	•	ON	Device is registered on the cellular roaming network
	\bigcirc	OFF	No signal (CSQ=0,99)
Signal	•	ON	Weak signal (CSQ<7)
	0-	Flashing	Strong signal (CSQ>7)
Power	0	OFF	Power off
$\mathbf{\mathcal{O}}$		ON	Power on
Alert	\bigcirc	OFF	No alert, device is running smoothly
	*	Flashing	Software fault (crash, issues)
	•	ON	Hardware fault (high temperature, problem with module or SIM card)



7.3 Ethernet port LED indicators

The E200 Series router features two Ethernet ports, each with with two LED.



LED	STATUS	DESCRIPTION	
	On	There is a valid network link.	
Green	Off	No valid network link detected.	
Amber	Flashing	There is activity on Ethernet port	
	Off	There is not activity on the Ethernet port	

8 Hardware installation

8.1 Install the SIM card

SIM card(s) should be inserted into the SIM tray as illustrated in the image below. SIM card contact should be face up.



8.2 Connect the Cellular (WWAN) Antenna(s)

Connect the cellular antenna to the "Cellular" connector (SMA Female) on the unit. If the unit is equipped with a secondary cellular antenna connector "Div.", it is highly recommended to connect an additional antenna to this connector for diversification. Dual antennas will provide improved signal strength thus better performance.

Note: For most applications, the antenna(s) included with the unit will provide suitable reception, but some circumstances/environments may require a higher quality antenna or one mounted in a different location. If this is the case, Maestro has many antenna options to chose from, please contact us or visit maestro-wireless.com.





8.3 Connect the power supply

Connect the Micro-Fit 4-pin male connector of the power supply to the power connector located on the LAN side of the unit.



Make sure Wi-Fi antenna is connected (see chapter 8.2) and Wi-Fi is ON on your computer, phone or tablette. Scan for network and select SSID "Maestro E200". You will be prompted to enter a WPA/WPS-2 mixed-mode password. Default password is '**W1rele\$\$**'.



9 E205 Basic configuration

9.1 Connecting to the web interface

Connect the LAN interface of your E200 to a computer via the RJ-45 cable and and start your web browser. Enter the device LAN IP address in the browser address field.

http://192.168.1.1



Note: If you change the IP address, remember to reboot the router and enter the new IP address into your browser address bar.

You will be invited to enter the admin username and password:

Authorization Required Please enter your username and password.			
Username	admin		
Password			
Login Reset			

- M Default login admin
- Default password admin

(This is the default username and password for Maestro routers. The admin and read-only user passwords can be changed at **System>Administration**

After successfully login the Quick Setup page will show up

Quick Setup
Thanks for using Maestro Wireless E200 series Cellular Ethernet Router.
Available Hardware options:
E205XT - 3G Ethernet Router
E206XT - Dual Mode 3G and EVDO, Ethernet Router
E228XT - LTE Ethernet Router
Please refer to the label on you router or the status page to confirm your model.
Quick Setup will guide you through the basic configurations of the Router Viz. LAN, WAN, Cellular and Wireless setup. Apart from the above mentioned four interface configurations, all other parameters will be set at their factory default settings. Please refer to the user manual for a list of factory default configuration.
For advanced users, please follow the Network Tab to select and configure various options as you wish.
Next

Figure 1: Quick Setup

If you need to access advanced feature you can navigate directly in the menu.



If you want to follow the quick user guide click on the **Next** button and you will enter quick setup page.

Since E200 has multiple WAN interfaces, the default priority settings for switching between various WAN interfaces is as follows and cannot be changed in Quick setup. To make any changes on the WAN priority settings, please go to the **Network/Interfaces** and **Network/Load Balancing** Tab. By default the router is configured in failover mode with WAN priorities as listed below:

- M Priority 1 Wired WAN
- M Priority 2 Wi-Fi as WAN (WWAN) (Wi-Fi in Client Mode)
- Priority 3 Cellular

In the quick setup page, you can perform basic configuration settings for the **LAN, WAN, Cellular and Wi-Fi** interfaces. All other configurations will be set to the factory default or previously saved values.

9.2 LAN configuration

The LAN configuration page is used to configure the LAN settings of the router

Network Setup	
Local Network	
IPv4-Address	192.168.1.1
IPv4-Netmask	255.255.255.0
IPv4-Gateway	

The modem router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The modem router's default LAN IP configuration is as follows:

- M LAN IP address: 192.168.1.1
- M IPv4 Netmask : 255.255.255.0

These addresses are part of the designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes here and click.



The LAN TCP/IP Setup settings are

-)) IPv4 Address: This is the LAN IP address of the modem router.
- IPv4 Netmask: This is the LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.

Advanced LAN configuration parameters could be found under Network/Interfaces, under LAN parameters click Edit > Advanced Settings.

- WAN manual ✓ automatic Protocol PPPoE 9.3.1 Manual WAN Protocol manual 192.168.0.5 IPv4 Address IPv4 Netmask 255.255.255.0 192.168.0.1 IPv4 Gateway 8.8.8.8 DNS Server

- MIPv4 Address: The IP address to assign to the selected WAN interface.
- IPv4 Netmask: The Subnet mask of the IP address above.
- M IPv4 Gateway: The gateway to assign this WAN interface.
- DNS server: The DNS server for the WAN interface.

9.3.2 Automatic

The WAN will be setup automatically.

9.3.3 PPPoE (Point-to-Point Protocol over Ethernet)

Acquire IP Address automatically from your Provider using the PPPoE protocol.

9.3 WAN configuration

By default the WAN is in **automatic** mode, you can also set it to **Manual** or **PPPoE**

maes<mark>t</mark>ro))

WAN			
	Protocol	PPPoE	*
	Username		
	Password		

Many DSL providers use PPPoE. To acquire an IP Address from the PPPoE server, a username and password are required. Ask your provider for your username and password if you don't know them.

Advanced WAN configuration parameters could be found under Network/Interfaces, under WAN parameters click Edit > Advanced Settings.



Selecting PPPoE in the quick setup will require some advance configurations.

9.4 Cellular Setup

Cellular		
	APN	
	PIN	
	Username	
	Password	

You can enter the cellular settings like APN, SIM PIN for security, Username and Password corresponding to your cellular connection (SIM Card), which you will receive from your Cellular Operator.

- APN: Access Point Name, enter the access point name provided by your network operator
- M PIN: If required please enter your SIM card's PIN code
- Username and Password: If required enter login credentials provided by your network operator

Advanced cellular configuration parameters could be found under Network/Interfaces, under 3G parameters click Edit > Advanced Settings.

9.5 Wireless (Wi-Fi)

WIRELESS		
	SSID	Maestro E200
	Password	W1rele\$\$

By default, the Wi-Fi is in Access Point mode:

- M Default SSID: Maestro E200
- Default Password: W1rele\$\$

The E200 Wi-Fi can be configured either as

- M An Access Point, in which case, the Wi-Fi acts as a LAN or
- M As a Wi-Fi Client in which case, the E200 connects to an external Wi-Fi source which will be the source of Internet or WAN for the E200.

Default security settings used are WPA-PSK, WPA2-PSK Mixed Mode. You can choose your encryption and change your password accordingly. Bring up on boot tick box in Wireless section by default is enabled. Ticking the box will enable the Wi-Fi (Wireless) interface every time the Router Reboots.



Wi-Fi section from this Quick setup page will disappear when

- The default Wi-Fi interface is removed from Network / Wi-Fi page
- When you scan for available Wi-Fi networks and convert the Router to Client Mode.

Wireless Overview	
Generic MAC80211 802.11bgn (radio0) Channel: 11 (2.462 GHz) Bitrate: ? Mbit/s	🔂 Scan 🎦 Add
SSID: Maestro Mode: Master 85SID: A4:AE:9A:00:26:C5 Encryption: None	🔕 Disable 🛛 🗹 Edit 💌 Remove

If you create multiple access point networks (Multiple SSDI's), the additional Wi-Fi networks created will not show up in Quick Setup.

Advanced Wi-Fi configuration parameters could be found under **Network/Wi-Fi**, under Wireless Overview parameters click **Edit** > **Advanced Settings**.

Once the Quick Setup is done, you will have basic LAN connectivity, Internet access over WAN and/or Cellular and Wi-Fi will be configured as Access Point.

To verify that your setup were succefully applied and your router is now running go to **Network/Interfaces**.

10 E205 advanced configuration

10.1 Flashing firmware and updating your device E200 Series can be updated through the web interface. Go to **System/Backup / Flash Firmware.**

	poradione		
Actions	Configuration		
Backup /	Restore		
Click "Gener with squashf	rate archive" to dov fs images).	nload a tar archive of the current configuration files. To reset the firmware to it	s initial state, click "Perform reset" (only possible
D	Download backup:	Generate archive	
I	Reset to defaults:	Perform reset	
To restore co	onfiguration files, ye	u can upload a previously generated backup archive here.	
	Restore backup:	Choose File No file chosen	
Upload a sys compatible fi	supgrade-compatib firmware image).	e image here to replace the running firmware. Check "Keep settings" to retain	the current configuration (requires an OpenWrt
Upload a sys compatible fi	supgrade-compatib firmware image). Keep settings:	e image here to replace the running firmware. Check "Keep settings" to retain ☑	the current configuration (requires an OpenWrt
Upload a sys compatible fi	supgrade-compatib firmware image). Keep settings: Image:	e image here to replace the running firmware. Check "Keep settings" to retain Choose File No file chosen Flash image	the current configuration (requires an OpenWrt
Upload a sys compatible f Unde file c	supgrade-compatib firmware image). Keep settings: Image: er Flash n on your coi	e image here to replace the running firmware. Check "Keep settings" to retain Choose File No file chosen File No file chosen File Mage, click on Choose File nputer.	the current configuration (requires an OpenWrt and locate the .bin
Upload a sys compatible f Unde file c new firm	supgrade-compatib firmware image). Keep settings: Image: er Flash n on your con	e image here to replace the running firmware. Check "Keep settings" to retain Choose File No file chosen File No file chosen File Flash image ew firmware image, click on Choose File nputer.	the current configuration (requires an OpenWrt and locate the .bin
Upload a sys compatible f Unde file c new firm a sysupgrad ible firmware	supgrade-compatible firmware image). Keep settings: Image: er Flash n on your cou nware imag be-compatible im e image).	e image here to replace the running firmware. Check "Keep settings" to retain Choose File No file chosen File Flash image Pew firmware image, click on Choose File nputer. ge here to replace the running firmware. Check "Keep settings" to re	the current configuration (requires an OpenWrt and locate the .bin
Upload a sys compatible f Unde file c new firm a sysupgrad ible firmware Keep	supgrade-compatible firmware image). Keep settings: Image: er Flash n on your cou nware imag de-compatible im e image). p settings:	e image here to replace the running firmware. Check "Keep settings" to retain Choose File No file chosen File Flash image Pew firmware image, click on Choose File nputer. ge here to replace the running firmware. Check "Keep settings" to re	and locate the .bin

Once the file located on the computer click Flash image...

maes<mark>t</mark>ro)

Flash Firmware - Verify The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure. • Checksum: 486476dc0ac5ad1585230391beb10ce2 • Size: 6.50 MB (7.69 MB available) • Configuration files will be kept.

Click Proceed

System - Flashing...

The system is flashing now. DO NOT POWER OFF THE DEVICE!

Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

Waiting for changes to be applied...

The system will now be flashing.

DO NOT POWER OFF THE DEVICE! Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.



11 Status pages explained

- M Open your browser on your computer with the address http://192.168.1.1
- M Enter the default login "admin" and password "admin"

By clicking on Status or Overview the page below will be displayed:

اِھِ 📮 🚛	E200 Series	maestro))			
Maestro Quick Setup Status	System Network Services Logout	AUTO REFRESH ON			
Status					
System					
Hostname	Maestro				
Model	Maestro E205				
Firmware Version	Maestro E205 2.0 RC7				
Kernel Version	3.10.49				
Local Time	Mon May 18 13:10:19 2015	Mon May 18 13:10:19 2015			
Uptime	0h 11m 49s	Oh 11m 49s			
IMEI	NA				
Cellular					
Cellular Data	NA				
Signal Strength	NA				
CPIN	NA				
Registration Status	NA				
Operator name	NA				
Roaming Status	NA				
IMSI	NA				

The Status menu is divided in 5 sub-menus:



- .
- M Real time Graphs



11.1 Overview:

11.1.1 System

The system tabs displays all information related to your device hardware and software version as well as basic settings:

Status	
System	
Hostname	Maestro
Model	Maestro E205
Firmware Version	Maestro E205 2.0 RC7
Kernel Version	3.10.49
Local Time	Mon May 18 13:11:14 2015
Uptime	0h 12m 44s
IMEI	NA

ITEM	DEFINITION
Hostname	The name assigned to your router
Model	Model of your router
	The firmware version that is currently residing and
Filliwale version	controlling the router
Kernel Version	The Linux kernel version on the router
Local time	The date and time set up on the router
Lintimo	The time in HH: MM: SS, for which the router is working
Optime	since last power ON
	The IMEI (International Mobile Equipment Identity) of the
IMEI	router, a unique code for identifying devices on a GSM
	network.



11.1.2 Cellular

The Cellular group provides the status of the SIM card inserted in the router.

Cellular				
Cellular Data	NA			
Signal Strength	NA			
CPIN	NA			
Registration Status	NA			
Operator name	NA			
Roaming Status	NA			
IMSI	NA			

ITEM	DEFINITION		
Signal Strength	Scale from 0 to 32. For a good cellular data connection Signal Strength must be 15 or above.		
Registration Status	Indicates if the device is registered on the cellular network		
Operator Name Name of the cellular service provider			
Roaming Status Indicate if the device is roaming on another network			
Uptime The time in HH: MM: SS, for which the router is work since last power ON			
Imsi	The International Mobile Subscriber Identity or IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.		

11.1.3 Memory

The Memory group provides information on the memory in KB available with the router.

Memory	
Total Available	13508 kB / 29460 kB (45%)
Free	3088 kB / 29460 kB (10%)
Cached	7820 kB / 29460 kB (26%)
Buffered	2600 kB / 29460 kB (8%)

ITEM	DEFINITION
Total available	Total available RAM memory
Free	Free RAM memory
Cached	Memory used to cache internal router data
Buffered	Amount of memory used as an internal router buffer



11.1.4 Network

The Network group gives the status of IPV4 and IPV6 WAN status.

Network					
IPv4 WAN Status		? Not connected			
IPv6 WAN Status		P Not connected			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining		
Matts-MBP-2	192.168.1.149	68:5b:35:af:45:11	11h 47m 39s		
Herterne	ID-R Address	0.00			
Piostname	IPvo-Address	DOID	Leasetime remaining		

DHCP and DHCPV6 leases list out the computers connected to the router through respective DHCP lease. This includes IPV4 as well as IPV6 connections

11.1.5 Wireless

The wireless group gives the status of the Wi-Fi network being used by the router.

Wireless		
Generic 802.11bgn Wireless Controller (radio0)	SSID: Maestro E200 Mode: Client Channel: 11 (0.000 GHz) Bitrate: ? Mbit/s Wireless is disabled or not associated	

11.1.6 Associated Stations

The associated stations group lists out the computers connected to the router.

Associated Stations						
MAC-Address	Network	Signal	Noise	RX Rate	TX Rate	
No information available						



11.1.7 MWAN Interface Live status

MWAN Interface provides a live view of all the available and connected WAN options. In the above screenshot, you can see that the interfaces marked in Green are live and connected while the ones in red are available but offline.

MWAN Interface Live Stat	us			
pptp (opto) Offline	openypn (tunc) Offline	wan (etho.s) Offline	wwan (%) Offline	
3g (1g-3c) Offine				

11.2 Firewall

You can verify parameters related to firewall and its settings here. Status of firewalls for both IPv4 and IPv6 can be seen here.



11.3 Routes

The rules that are currently active on this E205 are shown here.

1		100 (a)	E200 Series	maestro)))
Narstro In Routes To Many da a	na Nyanan Natasak n carantij actor or filo system	Lagar		
ARP				
Co.Address		MIC Address		Interlace
102-102-101		KD>=AB		2-141
Active Prd-R	ules.			
Sec. 1	Target		Col Galaxy	Martin
-	102-168 1 0/24		****	
Active Prd-R	outes			
Active IP-6-R	Ndes Seget		Printerray	Bees
Active 1946 R	Nuters Surger Failer The Contributions	44	P.(Bank DODARI
Active (PAG-R) Normal Sec.	Sudats Tangat POBP THE OPTIC SECTION	46e 140	Pd.Carrey 01000000	Bank 5 2000400 5 2000400
Active Prid-R Manual Manual Manual Manual	Nates Factor The Confidence of Pactor The Confidence of Pactor The Confidence of Excession	44	Pil Gamer 01000000 01000000 01000000	Banka 5 0000440 5 Stevense 6 serense

11.4 System Log

The log of all configured events regarding this E200 is displayed here.

11.5 Realtime graphs

This screen provides real time graphs of:

ITEM	DEFINITION
Load	Load indicates the load on CPU
Traffic	Traffic indicates the WAN side incoming and outgoing traffic
Wireless	Wireless indicates the traffic on Wi-Fi irrespective on whether Wi-Fi is used as an access point (LAN) or Client (WAN)
Connections	This page gives an overview over currently active network connections.





12 System

12.1 System properties

12.1.1 General Setting

This page allows you to configure the basic aspects of your device like its hostname or the time zone.

System Here you can configure the System Properties	e basic aspects of your device i	ke its hostname or the time	szone.
General Settings	ime Fri Apr 17 06:33:48 2015	Sync with browser	
Hostni	ame Maestro		
Timez	UTC	\$	

12.1.2 Logging

Parameters about system log like buffer size and log output level can be set here.

System Here you can configure t	the basic	aspects of your device like its	hostnam	e or the ti	mezone
System Propertie	es				
General Settings	Logging	Language and Style			
System log buffe	er size	16			
External system log :	server	0.0.0.0			
External system log :	server port	514			
Log outpu	t level	Debug	\$		
Cron Log	Level	Normal	¢		

ITEM		DEFINITION
System log buffer size	Size of log dis is 16KiB	splayed under Status page / Logs. Default
External system log server	IP address of time log will b	any external TCP server where the real e posted
External system log server port	Port of any ex will be posted	ternal TCP server where the real time log
Log output level	Debug	Provides Information useful for



	developers for debugging the
	application, not useful during operations.
	Normal operational messages which
Info	provide information which can be used
	for general purposes like reporting.
	Events which are unusual but not an
Notice	error. Used to spot potential problems.
	Immediate action is not necessary.
	Warning messages but not error,
Warning	indicating that error might occur if action
	is not taken
Error	Error conditions which should be relayed
EIIO	to developers or admins for resolution.
	Should be corrected immediately but
Critical	indicates failure in the secondary
	systems.
Alort	Problems which should be corrected
Alen	immediately.
Emergency	System is Unusable.
Dobug	Helps you debug cron process which
Debug	has failed during runtime.
Normal	Normal informational messages
	Indicates some issues can happen or
Warning	error could be generated in Cron
	process.



12.2 Administration

12.2.1 Router Password

On this page you can change the administrator password for accessing the device.

Router Password Changes the administrator passv	vord for accessing the device	
Password		61 당
Confirmation		21 탄

12.2.2 SSH access

The E200 integrate Dropbear which offers SSH network shell access and an integrated SCP server.

pbear Instance								
								Delet
Interface	0	3g:	79					
	0	lanc	22					
	0	wanc	22					
	0	wwan: Ø	interfaces	atteched)				
	۲	unspeci	led					
		O Li	sten only on	the given in	face or, if unspe	cified, on all		
Port	22	3						
		O Se	pecifies the l	stening por	f this Dropbear in	stance		
Password authentication	۲	6	Allow SSH	password a	hentication			
Allow root logins with password	3	6	Allow the r	oot user to	in with password	1		
Gateway ports		6	Allow reme	te hosts to	nnect to local SS	H forwarded port	5	

You can also set parameters for Dropbear Instance for SSH Access and you can paste public SSH-Keys (one per line) for SSH public-key authentication.

By default the remote SSH access over WAN is disabled, you need to send an SMS from a registered admin number to enable remote SSH access. Please refer to section Services / SMS



12.3 Software

Software page give you access to the list of package installed, you can also add package or filter packaged installed on your router.

a Configuration						
ackage lists available	pdate lists					
space: 82% (992.00 KB)						
wnload and install package:	ок					
Elter		ind nackage				
- 100 -		ino packaga				
13.1 Interface E200 has vario	es us physical interf	aces nar	nely,			
 Wired LAI Wired WA Wi-Fi Cellular 						
 Wired LAI Wired WA Wi-Fi Cellular 						
 Wired LAI Wired WA Wi-Fi Cellular 	N AN Status	Actions				
 Wired LAI Wired WA Wi-Fi Cellular 	N AN Status Unsupported protocol type. Install protocol syse.	Actions # Connect	Stop	d Ed	2	
)) Wired LAI ()) Wired WA ()) Wi-Fi ()) Cellular erfaces erface Overview etwork ()) Wi-Fi	N N N Status Unsupported protocol type. Install protocol extensions	Actions # Connect	Stop	Ed	R	
Wired LAI Wired WA Wi-Fi Cellular erfaces erface Overview etwork tax	N N Status Unsupported protocol (ype. Install protocol educations Uptime: Oh 26m 25s MAC-Address: A6:AE:SA:00:11:59	Actions Connect Connect	 Stop Stop 	Ed	8	
Wired LAI Wired WA Wi-Fi Wi-Fi Cellular orfaces face Overview twork twork two the second	N N N N Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address: A62AE:94(s) TX: 600.29 KB (3627 Arts.) TX: 600.29 KB (3606 Pkts.)	Actions @ Connect @ Connect	StopStop	Ed	e S	
s)) Wired LAI s)) Wired WA s)) Wi-Fi s)) Cellular erfaces rface Overview rfwork www.minute two the set of	Status Status Unsupported protocol (spe. Install protocol edensions Uptime: On 26m 25s MAC-Addree KS (362E Pets.) TX: 603.29 KB (0680 Pets.) IPv6: 192:168.1.1/24 IPv6: 192:4630:F7CAd:0:0:0:1/60	Actions Connect Connect	 Stop Stop 	Ed	t.	
Wired LAI Wired WA Wi-Fi Cellular Cellular Annual Statement Annual Statement Annual Statement Annual Statement Annual Statement Statement	N N N N Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address: A&AE:0A:00:11:59 PX: 404.59 KB (3627 Pkts.) TX: 603.29 KB (3627 Pkts.)	Actions # Connect # Connect	 Stop Stop Stop 	Ed	a a	
Wired LAI Wired WA Wi-Fi Cellular erfaces rface Overview twork tax	N N N N Status Unsupported protocol type. Install protocol extensions Uptime: Oh 26m 25s MAC-Address: ABAE:BA:00211159 RX: 404.99 KB (3627 Pkts.) TX: 603.29 KB (3627 Pkts.) TX: 603.29 KB (3626 Pkts.) ITX: 603.29 KB (3626 Pkts.) ITX: 603.29 KB (3626 Pkts.) ITX: 603.09 B (0 Pkts.) TX: 603.09 B (0 Pkts.) TX: 603.09 B (0 Pkts.)	Actions & Connect & Connect & Connect	 Stop Stop Stop 	Ed	a a	
Wired LAI Wired WA Wi-Fi Cellular erfaces rface Overview rtwork KAN KAN<	N N N N N Status Unsupported protocol type. Install protocol extensions Uptime: Ch 26m 25s MAC-Address: ABAE:0A-0021159 RX: 404.99 KB (3086 Pkts.) IPve: 192.948 (3086 Pkts.)	Actions Connect Connect Connect	 Stop Stop Stop 	Ed	a	
 Wired LAI Wired WA Wi-Fi Cellular 	N N N N N Status Chaupported protocol type. Install protocol extensions Uptime: Ch 26m 25s MAC-Address: ASIAE:0A-00211:59 RX: 404.99 KB (3086 Pkts.) IPve: 192.948 (3086 Pkts.) IPve	Actions Connect Connect Connect	 Stop Stop Stop 	Ed	a a a	
Wired LAI Wired WA Wi-Fi Cellular Cellular Certaces Enface Overview Entace Overview<	Status Status Unsupported protocol type. Install protocol extensions Uptime: Oh 26m 25is MAC-Address: A6AE:0A:00:11:59 RX: 404.99 KB (3686 Pkts.) IPwit: IED:34580:F7CA:0:00:00:160 RX: 000 B (0 Pkts.) TX: 000 B (0 Pkts.)	Actions Connect Connect Connect	 Stop Stop Stop 	C Ed	a a	
») Wired LAI ») Wired WA ») Wi-Fi ») Cellular verfaces erface Overview www. verfaces erface Overview erfac	Status Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address: AB/247-Pits.) TX: 600.29 KB (3627-Pits.) TX: 600.29 KB (3627-Pits.) TX: 600.29 KB (3626 Pits.) IPv4: 192.168.1.1/24 IPv6: F079-4580:F7CA:0.00:01.60 RX: 0.00 B (0 Pits.) TX: 0.00 B (0 Pits.)	Actions Connect Connect Connect	 Stop Stop Stop 	Ed	8 8	
») Wired LAI ») Wired WA ») Wi-Fi ») Cellular verfaces erface Overview www. verfaces erface Overview erfac	Status Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address:: A82AE-94302:11:59 RX:: 404.94 KB (3626 Pkts.) IPvid: 192.108.1.1/24 IPvid: 192.108.1.1/24 <	Actions Connect Connect Connect Connect	 Stop Stop Stop Stop 	2 Ed		
») Wired LAI ») Wired WA ») Wi-Fi ») Cellular erfaces erface Overview www. www. www. ••••••••••••••••••••••••••••••••••	N N N N N N Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address:: A62AE-964:00:11:59 RX:: 404:94 KB (3620 Pkts.) PH4: 192.108.1.1/24 IPH4: 192.108.1.1/24 IPH4: 192.1.1/24 IPH4: 192.108.1.1/24 IPH4: 192.1.1/24 IPH4: 192.108.1.1/24 IPH4: 192.1.1/24 IPH4: 192.108.1.1/24	Actions Connect Connect Connect Connect	 Stop Stop Stop Stop 	2 Ed	a	
 Wired LAI Wired WA Wi-Fi Cellular 	N N N N N N Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address:: A62AE-96A:00:11:59 RX:: 404:94 KB (3626 Pkts.) Prets.) TX:: 603:29 KB (3626 Pkts.) Prets.) PWI: 192:108.1.1/24 Prets.) TX:: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) TX:: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) RX:: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) RX:: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) RX:: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Actions Connect Connect Connect Connect Connect	 Stop Stop Stop Stop 	Image: Control of the second		
 Wired LAI Wired WA Wi-Fi Cellular 	N N N N Status Unsupported protocol (ype. Install protocol extensions Uptime: Oh 26m 25s MAC-Address:: A62AE-96A:00:11:59 RX:: 40-94 KB (3620 FMts.) IPve: 192.108.1.1/24 IPve: 192.108.1.1/24 IPve: 192.1.1/24 IPve: 192.108.1.1/24 IPve: 192.1.1/24 IPve: 192.108.1.1/24 IPve: 192.1.1/24 IPve: 192.108.1.1/24 IPve: 192.1.1/24 <tr< td=""><td>Actions Connect Connect Connect Connect Connect Connect Connect</td><td> Stop Stop Stop Stop Stop </td><td>Image: Control of the second second</td><td></td><td></td></tr<>	Actions Connect Connect Connect Connect Connect Connect Connect	 Stop Stop Stop Stop Stop 	Image: Control of the second		



In addition to these pre-created interfaces, you can add Virtual interfaces. You can also delete those virtual interfaces

However, you cannot delete the LAN, WAN and cellular interface.

When Wi-Fi is set-up as Client, interface WWAN will turn active.

Next to the interfaces, there is information regarding the interfaces like connection time, Packets sent, Packets received and IP address.

Connect button will connect the interface or reconnect if already connected. Stop will stop the interface. Click Edit to change the Interface Parameters.


13.2 LAN interface

13.2.1 General Setup

Click edit next to the LAN interface to access configurations

General Setup	Advanced 1	Settings I	Physical Settings		Firewall Settings	
	Status		gø br-lan		Uptime: 0h 24m 23s MAC-Address: A6:AE:9A:00:22:BD RX: 5.32 MB (27231 Pkts.) TX: 36.57 MB (38773 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDC5:3A09:62E0:0:0:0:1/60	
	Protocol	Static addre	55	÷		
IP	v4 address	192.168.1.1				
IP	v4 netmask	255.255.255	.0	÷		
IP	v4 gateway					
IPv	4 broadcast					
Use custom D	NS servers				2	
IPv6 assign	ment length	60	ssign a part of giver	0 n ler	ngth of every public IPv6-prefix to this interface	
IPv6 assig	gnment hint			٦		

DEFINITION
Be absolutely sure that you choose Static address
for LAN else you will end up losing access to Web-
Interface.
Accidently if you choose any other option other than
Static address for LAN and loose access to the Web
Page. Please perform a Hardware factory reboot.
The IPv4 address of your LAN interface
The IPv4 netmask of your LAN interface
Assign a part of given length of every public IPv6-prefix to
this interface
Assign prefix parts using this hexadecimal subprefix ID for this interface.

maestro

13.2.2 Advanced Settings

Interfaces - LAN On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: etb0.1).				
Common Cor	nfiguratio	n		
General Setup	Advanced	Settings	Physical Settings	Firewall Settings
Bring	up on boot	đ		
Use builtin IPv6-ma	anagement	2		
Override MA	VC address	a6:ae:9a:	00:22:bd	
Ovi	erride MTU	1500		
Use gate	way metric	0		

ITEM	DEFINITION
Bring up boot	This option will enable LAN interface to start on every boot. Please be aware that un-ticking this box will not bring up the LAN interface in the next boot cycle and you will no longer be able to access the Web Interface of the Router until you perform a Factory Reboot.
Use built-in IPv6 management	If ticked it enables IPv6 support in the LAN side.
Override MAC address	
Override MTU	
Use gateway metric	It is advisable to enter metric for every interface. Metric indicates the priority of the interface. The lower the value the higher the priority of the interface. If no metric is added, it will assume a default value of "0" The default metric for LAN interface is "0"



13.2.3 Physical Settings

On this page you can configure network interfaces separated by	the network y spaces. Ye	interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several in can also use <u>VLAN</u> notation INTERFACE.VLANINR (e.g.; eth0.1).
Common Configuration	n	
General Setup Advanced	d Settings	Physical Settings Firewall Settings
Bridge interfaces	2	Creates a bridge over specified interface(s)
Enable STP		Enables the Spanning Tree Protocol on this bridge
Interface	0	Ethernet Switch: "eth0"
	1	VLAN Interface: "eth0.1" (lan)
	0	#* VLAN Interface: "eth0.2" (wan)
		Ethernet Adapter: "gretap0"
	1	👳 Wireless Network: Master "Maestro E200" (an)
	63	3 Custom Interface

The configuration shown above is the default configuration. Unless you are an advanced user, we recommend not making any changes to this page.

13.2.4 Firewall Settings

Interfaces - LAN On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).				
Common Configuration				
General Setup Advanced Settings Physical Settings Firewall Settings				
Create / Assign firewall-zone 💿 Ian: Ian: 💒 🔮				
🔿 wan: 👷 3g: 🐘				
Unspecified -or- create:				
Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.				

It is extremely critical that you assign every interface to a Firewall Zone. By default LAN is assigned to a LAN firewall Zone.

You can also create a different Firewall Zone and assign your interface to the New Created Zone.

Why creating a different Firewall Zone?

You can create a different VLAN interface and assign the same to a different Firewall Zone. You can then set rules and policies in the firewall section on how you want to channelize the Traffic between two LAN zones. For details, please refer to the firewall section.



13.2.5 DHCP server

Here you can set your LAN side DHCP network.

13.2.5.1 General Setup

HCP Server	
General Setup Advanced	Settings IPv6 Settings
Ignore interface	Disable DHCP for this interface.
Start	100
	Lowest leased address as offset from the network address.
Limit	150
	Maximum number of leased addresses.
Leasetime	12h
	Expiry time of leased addresses, minimum is 2 minutes (2n).

ITEM	DEFINITION
Ignore interface	Disable DHCP for this interface. Please note that if you disable DHCP for this interface, all the LAN devices connected to the router should have a static LAN IP configured
Start	Lowest leased address as offset from the network address.
Limit	Maximum number of leased addresses.
Leasetime	Expiry time of leased addresses, minimum is 2 minutes. Please note that the IP address allocated by the router will disappear from the Wi-Fi / Overview / Associates stations list only after individual lease time for each IP expires.

13.2.5.2 Advanced Settings

HCP Server			
General Setup	Advanced	Settings	IPv6 Settings
Dyna	amic DHCP	2	Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
	Force	0	Force DHCP on this network even if another server is detected.
IPv	4-Netmask		
			Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHC	P-Options		a
		servers to	Define additional DHCP options, for example * 6,192.168.2.1,192.168.2.2 * which advertises different DNS of clients.

ITEM	DEFINITION
Dynamic DHCP	Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force	Force DHCP on this network even if another server is detected.



IDv4 Notmook	Override the netmask sent to clients. Normally it is
IF V4-INELIIIASK	calculated from the subnet that is served.
DHCP-Options	Define additional DHCP options, for example
	"6,192.168.2.1,192.168.2.2" which advertises different
-	DNS servers to clients.

13.2.5.3 IPv6 Settings

This help will help you setup a DHCP IPv6 network on your LAN side.

OHCP Server	
General Setup Advanced	Settings IPv6 Settings
Router Advertisement-Service	server mode 💠
DHCPv6-Service	server mode \$
NDP-Proxy	disabled \$
DHCPv6-Mode	stateless + stateful \$
Always announce default router	Announce as default router even if no public prefix is available.
Announced DNS servers	2
Announced DNS domains	2

ITEM		DEFINITION
	Disabled	
Router Advertisement-	server mode	
Service	relay mode	
	hybrid mode	
	Disabled	
	server mode	
DHCPV6-Service	relay mode	
	hybrid mode	
	Disabled	
NDP-Proxy	relay mode	
	hybrid mode	
	stateless	
	stateless +	
DITCF V0-WIDde	stateful	
	Stateful only	
Always announce default	ault If ticked Announce as default router even if no put	
router	prefix is available.	
Announced DNS servers		
Announced DNS		
domains		



13.3 Wired WAN interface

Click edit next to the wired WAN interface to access configurations

13.3.1 General Setup

etwork interfaces	separated by	spaces. You	u can also use <u>VLAN</u> r	notat	tion INTERFACE.VLANNR (0.g. eth0.1).
common Cor	nfiguratio	n			
General Setup	Advanced	Settings	Physical Settings		Firewall Settings
	Status		eth0.2		Uptime: 1h 23m 6s MAC-Address: A8:AE:9A:00:22:BE RX: 96.69 MB (68942 Pkts.) TX: 13.81 MB (62013 Pkts.) IPv4: 192.168.81.142/24
	Protocol	DHCP di	ent	\$	
Hostname to	send when sting DHCP	Maentro			

ITEM	DEFINITION
Static address	This option will enable the user the assign WAN side IP address to E200. Be sure that the IP that you enter in Static address mode is in the same LAN domain as the Router or ISP that it is connected to.
DHCP client	This will enable the Router to acquire WAN IP from the DHCP Router it is connected to
PPPoE	This option will enable dial-up over Ethernet network. Your ISP should support PPPoE and you need appropriate login credentials for the same
PPPoATM	This is a specialized protocol supported by a few ISPs. You need appropriate login credentials from your ISP for the same
	we there are to and other there DUCD. Chatter, DDDaE are

Do not select any other protocol other than DHCP, Static, PPPoE or PPPoATM.



13.3.2 Advanced Settings

The configuration options are mostly similar to the LAN options.

Common Configuratio	n				
General Setup Advanced Settings		Physical Settings Firewall Settings			
Bring up on boot					
Use builtin IPv6-management					
Use broadcast flag		Required for certain ISPs, e.g. Charter with DOCSIS 3			
Use default gateway	2	If unchecked, no default route is configured			
Use DNS servers advertised by peer	2	If unchecked, the advertised DNS server addresses are ignored			
Use gateway metric	4				
Client ID to send when requesting DHCP					
Vendor Class to send when requesting DHCP					
Override MAC address					
Override MTU	1500				

ITEM	DEFINITION	
Use Gateway metric	The default value is "3". Between all the available physical WANs, this interface has the highest default priority.	
The Load Palancer will use these Matrie Values to determine priority of a		

The Load Balancer will use these Metric Values to determine priority of a particular WAN.

13.3.3 Physical Settings

General Setup	Advanced	d Settings	Physical Settings Firewall Settings
Brid	ge interfaces		(a) creates a bridge over specified interface(s)
	Interface	0	Ethernet Switch: "eth0"
		0	WLAN Interface: "eth0.1" (an)
		•	VLAN Interface: "eth0.2" (wan)
		0	Ethernet Adapter: "gretap0"
		0	🙅 Wireless Network: Master "Maestro E200" (lan)
		0	E Custom Interface:



Unless you are an advanced user do not change setting of this page.

maestro))

13.3.4 Firewall Settings

Common Configuration	1	
General Setup Advanced S	iettings P	Physical Settings Firewall Settings
Create / Assign firewall-zone	🔾 lan: la	lan: 💯 👻
	wan:	wan: 25 3g: 商品
	unspeci	cified -or- create:
	Ch associated zon	hoose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the one or fill out the create field to define a new zone and attach the interface to it.

It is extremely critical that you assign every interface to a Firewall Zone. By default the WAN interfaces is assigned to a 'wan' firewall zone. In firmware version 2.0, you cannot create a WAN side firewall zone (Planned in firmware release 2.1). Hence it is advisable to keep this configuration untouched.



13.4 Cellular interface (3G or 4G)

Click edit next to the 3G interface to access configurations



General Setup	Advanced	ced Settings Firewall Settings					
	Status		∰ 3g-3g	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)			
	Protocol	UMTS/GPRS	\$				
S	ervice Type	UMTS/GPRS	\$				
	APN						
	PIN						
	Usemame	admin					
	Password	••••		ø			

ITEM		DEFINITION	
Protocol	Be absolutely sure that you select only UMTS/GPRS incase of E205 and UMTS/GPRS or EVDO in case of E206. Please do not select any other protocol.		
	UMTS/GPRS	The router will select the best service available	
Service Type	UMTS	The router will connect only to 3G/ UMTS network	
	GPRS	The router will connect only to GPRS network	
APN	Enter the APN provided by your network operator		
PIN	Enter the SIM PIN if any		
Username	Username for your SIM card if any		
Password	Password Password for your SIM card if any		
Protocol Service Type APN PIN Username Password	UMTS/GPR EVDO in case of protocol. UMTS/GPRS UMTS GPRS Enter the APN pro- Enter the SIM PIN Username for you Password for you	S incase of E205 and UMTS/GPRS or E206. Please do not select any other The router will select the best service available The router will connect only to 3G/ UMTS network The router will connect only to GPRS network ovided by your network operator N if any ur SIM card if any r SIM card if any	



13.4.2	Advanced	Settings
--------	----------	----------

Common Cor	nfiguratio	n	
General Setup	Advanced	Settings	Firewall Settings
Bring	up on boot	2	
Use builtin IPv6-m	anagement	1	
Enable IPv6 negotia	tion on the PPP link		
Modem i	init timeout	20	
			Maximum amount of seconds to wait for the modem to become ready
Use defa	uit gateway	2	If unchecked, no default route is configured
Use gate	way metric	0	
Use DNS servers	advertised by peer	2	If unchecked, the advertised DNS server addresses are ignored
LCP echo failun	e threshold	0	
		-	Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP ed	ho interval	5	
			Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactiv	ity timeout	0	
		_	Close inactive connection after the given amount of seconds, use 0 to persist connection

ITEM	DEFINITION
Bring up boot	Keep the tick on for "Bring up on Boot" if you want the 3G
	Interface to be live on every reboot.
Use gateway metric	Enter the gateway metric if you wish to use this WAN as a failover
LCP echo failure	Enter LCP details only if you have the correct information
threshold	default value
	"0" value will keep the 3G connection always on. Any
Inactivity timeout	seconds of inactivity



13.4.3 Firewall Settings

Common Configuratio	n	
General Setup Advanced	Setting	s Firewall Settings
Create / Assign firewall-zone	Θ	lan: 📰 🙊
	۲	wan: 👷 3g: 📷
	Θ	unspecified -or- create:
	associ	Occupies the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the ated zone or fill out the create field to define a new zone and attach the interface to it.

13.5 Add VPN interface

In addition to configuring the above-mentioned 3 basic interfaces, you can add virtual interfaces by clicking on the "Add VPN Interface" Button.

Name of the new interface	- -							
	-	The allowed of the	characte	rs are: A	-Z. a-z.	0-9 and _		
Protocol of the new interface	Static	address		\$				
Create a bridge over multiple interfaces	٥							
Cover the following interface	0	2 Ethernet	Switch	"eth0"				
	0	VLAN Int	terface:	"eth0.1"	(an)			
	0	WLAN Int	terface:	"eth0.2"	(wan)			
	0	Ethernet	Adapte	r: *gretap	·0*			
	0	@ Wireless	Networ	k: Maste	"Maestro	E200* (lan)		
	0	2 Custom	Interfac	80				

You can add either PPTP or L2TP interface.

For more details on adding PPTP or L2TP interface, please refer to the PPTP and L2TP configuration guides.





13.5.1 PPTP

13.5.1.1 General Setup

Point-to-Point Tunneling Protocol (PPTP) is used for creating VPN tunnels over the Internet between two networks.

When you create a new VPN interface (refer to chapter 13.5) select PPTP

Interfaces On this page you connetwork interfaces Common Corr	PPTP an configure the ne separated by space nfiguration	twork interfaces. You can bridge s es. You can also use <u>VLAN</u> notation	everal interfac	es by ticking the "bridge in . VLANNR (<u>e.g.</u> : eth0 . 1).	terfaces* field and enter the names of several
General Setup	Advanced Settin	gs Firewall Settings			
	Status	PPTP	i.	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	
	Protocol	p •			
,	VPN Server				
PAP/CHAF	username				
PAP/CHAF	P password		8		
					Save & Apply Save Reset

Enter the IP address of the VPN server in your network, followed by the username and password for this server. Click **save and apply** to add the PPTP VPN interface.

maestro)

Interfaces On this page you can network interfaces s	- PPTF an configure t separated by	he network inte spaces. You ca	rfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several in also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Con	figuratio	n	
General Setup	Advanced	Settings F	irewall Settings
Bring u	up on boot	2	
Use builtin IPv6-ma	anagement	2	
Use defau	ilt gateway	ø () If unchecked, no default route is configured
Use gatev	way metric	0	
Use DNS servers	advertised by peer	e .) If unchecked, the advertised DNS server addresses are ignored
LCP echo failure	e threshold	ି 🎯 Pr	esume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP ed	ho interval	5 👩 Se	and LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactivi	ity timeout	0	per institue connection after the given amount of seconds use 0 to persist connection
Ove	arride MTU	1500	use inscrive connection and the given amount of seconds, use ono persist connection
			Save & Apply Save Reset

ITEM	DEFINITION
Bring up boot	Keep the tick on for "Bring up on Boot" if you want the 3G Interface to be live on every reboot.
Use builtin IPv6-	
management	
Use gateway metric	Enter the gateway metric if you wish to use this WAN as a failover. If unchecked, no default route is configured.
Use DNS servers	If unchecked, the advertised DNS server addresses are
advertised by peer	ignored
LCP echo failure threshold	Enter LCP details only if you have the correct information on the same from your operator else use 0 to ignores failures
LCP echo interval	Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactivity timeout	"0" value will keep the 3G connection always on. Any other value 'X' will turn off the 3G connection after 'X' seconds of inactivity
Override MTU	

Press Save and Apply to apply your settings.



13.5.1.3 Firewall Settings

The firewall settings tabs show you the existing firewall zone.

Interfaces - On this page you can network interfaces so	- PPTF n configure to eparated by	P the networks	rork interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several . You can also use <u>VLAN</u> notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Conf	figuratio	n	
General Setup	Advanced	Setting	5 Firewall Settings
Create / Assign fire	wall-zone	Θ	lan: 📰 💇
		Θ	wan: wan: 📰 3g: 📠
		۲	unspecified -or- create:
		assoc	Ohoose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the ated zone or fill out the create field to define a new zone and attach the interface to it.
			Save & Apply Save Reset

You can choose to add the new interface to the WAN zone or create a new zone for the interface. Choose the appropriate button, and enter a name for the new zone and click on SAVE AND APPLY button.

When you assign the new VPN interface to a zone it implies that the properties associated with that zone get applied to the VPN interface. The properties of a zone can be set under **Network > Firewall**. Please refer to the document on Firewalls and Port forwarding.

Implications of the VPN Interface: Once you create a VPN interface on the router, it implies that the router is placed in the company network, even if it is located at a remote location. It can be accessed by a device in the company network for controlling it and acquiring any data associated with it.

13.5.2 OpenVPN

Open VPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-tosite connections. It uses the Open SSL library to provide encryption of both the data and control channels. Open VPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. Open VPN fully supports IPv6 as protocol of the virtual network inside a tunnel and the Open VPN applications can also establish connections via IPv6. It has the ability to work through most proxy servers (including HTTP) and is good at working through Network address translation (NAT) and getting out through firewalls.



options to the clients. These include IP addresses, routing commands, and a few connection options

E200 series supports Open VPN client, Server and Pass Through.

Quick Setup	Status	System Netv	ork Services	Logout				
N								
instances of configured Ope	erVPN insta	tces and their curren	t state					
	Enable	d Started	Start/Stop	Port	Protocol			
config		no	🦉 start	1194	udp		🛃 Edit	Delete
erver		no	🖉 start	1194	udp		🛃 Edit	E Delete
lient		no	🛢 start	1194	udp		🔀 Edit	E Delete
	Client o	onfiguration for an e	then 🔹 🎦 Add					
	Ouick Setup N instances of configured Ope config erver lient	Quick Setup Status N instances of configured Open/VPN instar config erver lient Client Client c	Quick Setup Status System Network N instances of configured OpenVPN instances and their current instances Instances config no no erver no no lient no Instances	Quick Setup Status System Network Services N instances instances instances of configured OpenVPN instances and their current state Enabled Started Start/Stop config no @ start erver no @ start lient no @ start Client configuration for an ethen Add	Quick Setup Status System Network Services Logout N instances of configured Open/VPN instances and their current state V V Port instances Enabled Started Start/Stop Port config no @ start 1194 erver no @ start 1194 lient no @ start 1194 Client configuration for an ethen Add	Quick Setup Status System Network Services Logout N instances of configured OpenVPN instances and their current state Very Started Started Start Stop Port Protocol Image: Starter Starter Start Image: Starter Starter Start Image: Starter	Quick Setup Status System Network Services Logout N instances of configured OpenVPN instances and their current state V Port Protocol instances Enabled Started Start/Stop Port Protocol config no @ start 1194 udp erver no @ start 1194 udp lient no @ start 1194 udp	Quick Setup Status System Network Services Logout N instances of configured OpenVPN instances and their current state Frabled Started Starti Stop Port Protocol config no @ start 1194 udp @ Edit erver no @ start 1194 udp @ Edit lient no @ start 1194 udp @ Edit Client configuration for an ethen ************************************



13.5.2.1 OpenVPN client

You can access the OpenVPN client under Services / OpenVPN.

OpenVPN Client will attach itself to the configured OpenVPN server over any available WAN interface. If the auto-connect function is enables, OpenVPN will not only connect over available WAN but also switch between WANs as and when one WAN fails-over to another and also auto starts in every reboot. This can be achieved by clicking on the '**enabled**' tick box.

You can either edit the sample client or create your own configuration from ground up.

Click on the Edit sample_client and you will see the following menu

Ĵ	, II	٩	્રા	<u>و، ا</u>	E2	00 Series	maestro))
Maestro o	luick Setup	Status	System	Network	Services	Logout	
Overview » I Switch to advance	nstance " d configuratio	sample _.	_client"				
	verb	3		٠			
		(Set output	verbosity			
	tun_ipv6		Make t	un device IPv	6 capable		
	nobind	2	🗿 Do not	bind to local	address and p	port	
	comp_lzo	yes		•			
			Use fast Li	ZO compressi	on		
	proto	udp		٠			
			Use proto	ol			
	client	2	Config	ure client mod	le		
clie	nt_to_client		O Allow o	lient-to-client	traffic		
	remote	my_serv	er_1 1194		20		
		(Remote ho	ost name or ip	address		
- Additional Field	I	* Add					

This is the basic configuration menu, which you need to configure

ITEM	DEFINITION
Verb	Here you can set the output verbosity level. Higher the verbosity, higher will be the internal log details
Tun_ipv6	This will make the tunnel IPv6 capable
Nobind	Does not bin local address and port
Comp_lzo	Uses Izo compression



Proto	Allows you to choose between TCP and UDP
Client	Tick for client mode and on tick for Open VPN server Mode
Client to Client	Facilitates client to client communication for clients connected to the same VPN server
Remote	VPN server IP

In addition to the above configuration, you need to add the following for basic Open VPN client creation.

comp izo	ves		
	O Use fast L	ZO compression	
- Additional Field	udp	•	
lice port sort fcontig server server_bridge secpative secret secret	Use proto Onfig Allow (col ure client mode client-to-client traffic	
a a In vert	ny_server_1 1194	ost name or ip address	
oey - Additional Field	▼ Add		

ITEM	DEFINITION
Port	Open VPN server Port
Са	Authority certificate common to both Server and Client. Browse to the location where Ca certificate is located on the computer. Select and upload
Cert	Client certificate generated at the server side. Browse to the location where client.cert certificate is located on the computer. Select and upload
Кеу	Client key generated at the server side. Browse to the location where client key is located on the computer. Select and upload

(Select each and add to enter configuration)



Once you have the entire configuration loaded and certificates loaded, your screen should look like this:

Maestro Quick Setup	Status System Network Services Logout
verb	3 Y
port	1193
	TCP/UDP port # for both local and remote
tun_jov8	Make tun device (Pv0 capable
nabind	Do not bind to local address and port
comp_izo	yes V
	Use fast LZO compression
proto	udp 🔻
	Use protocol
client	Configure client mode
client_to_client	Allow client-to-client traffic
remote	223.30.182.58
	Remote host name or ip address
CB	
	Centificate authority
cert	Uploaded File (3.90 KB)
kay	Uploaded File (918.00 B)
	Local private key
- Additional Field -	Add



Once this is configured, go to advanced option and choose configuration as per your VPN scheme.

) –	٩	0	زە 🛄	E2	00 Series	maestro)))
Maestro	Quick Setup	Status	System	Network	Services	Logout	
Overview	» Instance "	sample	_client"				
Configuration of	category: Service	Networkin	VPN	ptography			
VPN							
	client		Config	ure client mod	5e		
	pull	R	Accept	toptions push	ed from serve	r.	
	remote	223.30.1	82.58		3		
			Remote he	ost name or ip	address		

Pull – Accept options pushed from the Server – enabling this option will enable the router to accept the routes pushed from the OpenVPN server. It is recommended to keep it ticked.



Once you have the entire configuration in place, you can start the VPN service as follows

Aaestro	Quick Setup	Status	System Network	Services	Logout		UNSAVED C	MNOES
DpenVP	N							
DoenVPN i	instances							
Below is a list o	f configured Op	enVPN instan	ces and their current st	ate				
		Enabled	Started	Start/Stop	Port	Protocol		
custom_c	onfig	0	no	🥵 start	1194	uđp	Edit D	elete
sample_se	erver	0	no	💋 start	1194	udp	🖉 Edit 💌 D	elete
sample_cl	lient	×	yes (7070)	🔵 stop	1193	udp	🛃 Edit 💌 D	elete
		Client cor	nfiguration for an ethic	• 🔝 Add				

The above screen shows that Open VPN service has started and the below screen shows OpenVPN is connected and running smoothly.

) – – – – – – – – – – – – – – – – – – –		E200 S		0 Series		maestro)))				
Maestro	Quick Setup	Status	System	Network	Services	Logo	ut					AUTO REFRESH ON
Network			Status			Acti	ons					
	WWAN		1000			1	Connect	0	Stop	1.00	Edit	
wan	Install pro	Install protocol extensions										
	LAN g# (g# br-lan	#)	Uptime: 0h 40m 49s MAC-Address: A6 AE 9A 00 26 C8 RX: 1.72 MB (10397 Pkts.) TX: 3.88 MB (9247 Pkts.) IPv4: 192 168.1.1/24		2	Connect	0	Stop		Edit		
	36		Uptime: (h 9m 10s		3	Connect	0	Stop	1	Edit	
	3g-3g		TX: 456.0 IPv4: 100	RX: 436.00 B (16 Pkts.) TX: 456.00 B (17 Pkts.) IPv4: 100.89.123.80/32		1						
	OPENVPN		Uptime: (h 4m 5s								
	tun0		MAC-Add RX: 1.04 TX: 31.04 IPv4: 10.0	Iress: 00:00:0 KB (8 Pkts.) MB (22758 F 3.0.14/32	0:00:00:00							



14 Wi-Fi

14.1 Introduction

The router can work in 2 modes:

- Wi-Fi as access point: It provides Internet to other host machines in its network over Wi-Fi. It can get Internet connection from WAN or cellular. If you have a cellular SIM card inserted in the router, it has a capability to switch between WAN and cellular in case either of them fails. However, at any point of time only one of the networks will be active.
- Wi-Fi as client mode: the router will act as a client to existing wireless networks. The router will accept the Internet access through wireless access provided by another service provider and then distribute the access to the machines connected to the router on its LAN interface.

At any point of time, the router can work either in client mode or in Master mode.

The lease						
2	Generic MAC80211	802.11bgn (radio0)			🔯 Sca	n 🎦 Add
	No network configured on	this device				
ssiD	MAC-Address	IPv4 Address	Signal	Noise	RX Rate	TX Rate
Collecting data						

It shows a Generic connection, with no network configured on the router. To enable connection click the edit button to configure the default network with the SSID Maestro E200.

14.2 Wi-Fi as Access Point



evice Config	guration							
General Setup	Advanced	nd Settings						
	Status	iii SSID 0% Wirek	I: Maestro E200 Mode: Unknown less is disabled or not associated					
Wireless network	is disabled	Enable						
	Channel	11 (2.462 GHz)	٥					
Tran	smit Power	20 dBm (100 mW)	\$					
		(D al Dan						

You can choose the channel frequency from the drop down menu, or choose 'auto', to select it automatically.

You can also choose transmit power, the default being 20dBM or 100mW, which is the maximum value.



evice Config	guration			
General Setup	Advanced	Settings		
	Band	2.4GHz (802.11g+n)	•	
HT mod	le (802.11n)	20MHz	4	
Country Code		00 - World	1 3166 ainta2 no stru notas	
Distance O	ptimization	Options to	atheat actuad member in maters	
Fragmentation	n Threshold	Unstance to	intrest network memoer in meters.	
RTS/CTS	3 Threshold			

14.2.2	Device	Configuration	- Advanced	Settings
--------	--------	---------------	------------	----------

ITEM	DEFINITION
Band	Default value is 2.4GHz
HT mode	Default value is 20MHz, this can be set to 40MHz or disabled
Country Code	Choose the country code corresponding to the country where the router is operational. This ensures that the channels available in that country are enabled. By choosing '00' (World), the router will select the appropriate channel in your country.
Distance Optimization	You can optimize the operation of your Wi-Fi network, if you know the distance of the farthest machine in your network from the router. Value is meter.
Fragmentation Threshold	Choose Fragmentation threshold value (in number of bytes). Fine-tuning Fragmentation Threshold parameter can result in good throughput but a wrong value can result in low throughput. The range of values is 256 to 2346 bytes. In a noisy environment, a smaller value of Fragmentation Threshold may result in more efficient communication.
RTS/CTS Threshold	You can choose RTS/CTS threshold between 0 to 2347 bytes, typical value being 500. This setting is for advanced users. It prevents collision of wireless packets, particularly in case of hidden nodes or in a noisy environment. In case of access point setting, it is recommended not to use RTS/CTS threshold.



14.2.3	Interface Conf	iguration — (General S	etup	
Configuration					

nterface Co	nfiguratio	n
General Setup	Wireless \$	Security MAC-Filter
	Mode	Access Point \$
	ESSID	Maestro E200
	Network	🕑 lan: 💇 🙊
		🛛 wan: 📰
		wwan: (no interfaces attached)
		create: admin
		Ochoose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.
	Hide ESSID	0
	WMM Mode	ø

ITEM	DEFINITION
Mode	Should be set-up as Access Point
ESSID	ESSID shows the device name you have assigned to the router, by default, it is Maestro E200
Network	In Access Point LAN must be selected, as the router will supply Wi-Fi internet to its clients on LAN
Hide ESSID	Select Hide SSID, if you want your router SSID to be hidden when client machines scan for available Wi-Fi networks
WMM	 Wi-Fi Multimedia (WMM), is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets. 802.11n spec requires devices to support 802.11e (Quality of Service [QoS] enhancements for wireless LAN) in order to use HT (High Throughput) link rates, i.e. higher than 54 Mbps. WMM's Traffic Identifier (TID) field is key to aggregation mechanisms, including block acknowledgement (block ACK), that enable 802.11n's high throughput rates. Since WMM support is required for products to be certified for 802.11n, WMM comes enabled by default in all Wi-Fi Certified n APs and wireless routers. So even if you don't have any WMM-aware devices on your network, leave WMM enabled or you may find your clients connecting only at 54 Mbps rates.



Interface Cor	nfiguration						
General Setup	Wireless Se	curity	MAC-Filter				
	Encryption	WPA-P	SK/WPA2-PSK Mixed N \$				
	Cipher	auto	\$				
	Key			ø			

14.2.4 Interface Configuration – Wireless Security

	-
ITEM	DEFINITION
Encryption	Choose the type of encryption for your Wi-Fi network,
-)1	default is WPA-PSK/WPA2-PSK Mixed mode
	Choose the cipher type from the drop down as
Cypher	appropriate for your router. Similarly enter the key that a
	client machine must enter to join this network.
Key	Enter the key corresponding to your cypher type

14.2.5 Interface Configuration – MAC-filter

Interface Con	nfi	gur	ation			
General Setup	Jeneral Setup Wireless Se		curity	MAC-Filter		
MAC-Ad	dre	iss F	liter	disable		ŧ

You can:

- Disable
- Allow listed Mac addresses
- M Allow all EXCEPT listed MAC addresses.

When entering the last 2 options, use '+' button to the right of the MAC Address List field. You can choose the MAC addresses that are currently connected to the router. If you choose 'Custom' a new field is added to the screen, in which you may enter any other MAC address likely to join the network. Please take care that you enter the MAC address in the required format, else, the field will be shown RED.

After you are satisfied with all your selections, press SAVE AND APPLY button. Your settings will be applied to the router.



14.3 Wi-Fi as Client

In Client mode, the router will act as a client to existing wireless networks. The router will accept the Internet access through wireless access provided by another network and then distribute the access to the machines connected to the router on its LAN interface.

At any point of time, the router can work either in client mode or in Master mode. To change from Access Point mode to client mode, you have to remove all networks in Access Point mode.

Under Network > Wi-Fi click on Scan.

a	Scan	1	Add
	۵	🗋 Scan	🖸 Scan 🔛

Select the Wi-Fi network you want to join and click Join Network.

WPA passphrase	<i>a</i>
	Specify the secret encryption key here.
Name of the new network	wwan
	The allowed characters are: A-Z, e-z, 0-9 and _
reate / Assign firewall-zone	Ian: Ian:
	wan: wan: gr:
	unspecified -or- create:
	Choose the finewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

IIEM	DEFINITION
WPA passphrase	Enter the WPA pass phrase for the chosen network.
Create / Assign firewall-	Assign this network to firewall zone. Since you want your router to work in client mode, the internal network is
zone	side. Alternatively vou can create vour own firewall zone.



14.4 Creating multiple SSID

Though only one router is physically present to provide Internet access to any host machines in your network, it is possible to create virtual interface so that you can restrict and control access to different groups of users based on security and functionality. This is achieved by creating multiple SSIDs and assigning separate SSIDs to group of users. Please note that only one router is servicing multiple SSIDs.

	Gene	ric MAC80211 802. el: 2 (2.417 GHz) Bitri	Scan	12	Add						
	95%	SSID: Maestro Mo BSSID: A4:AE:9A:1 (CCMP)	ode: Master 00:26:C5 Encrypti	on: mixed W	PA/WPA2	PSK	🔵 Disable		Edit		Remove
ssociat	ed Sta	tions									
ssociat	ssiD	MAC-Address	IPv4 Address	Signal	Noise	RX Rate		1	X Rate		

Click on **Add** button (next to Generic interface) to add another network (SSID).

Follow the same procedure as given in Wi-Fi section to create ANOTHER interface in Access Point mode. Please note that the device configuration for both interfaces remain the same. However, the Interface configuration can be different.

Assign a new ESSID to the interface.

You can make different choices for Network, Security and MAC address filtering, so that you can differentiate between different groups of users.

For example, you can choose one interface with MAC Address filtering DISABLED whereas another with 'ALLOW only listed MAC Addresses'. This way, you can provide full Internet access to only second group while restricting it for former group.

After you make all the settings, click on SAVE AND APPLY button to create the new interface.

Back to the **Network / Wi-Fi** you will see the second SSID.

maestro))

	98%	SSID: Maestro Mo BSSID: A4:AE:9A:0 (CCMP)	de: Master 0:26:C5 Encryptic	on: mixed W	PA/WPA2	PSK 🧕	Disable		Edit	×	Remove
	SSID: Maestro2 Mode: Master BSSID: A4: AE:9A:00:26:C4 Encryption: None									×	Remove
ociat	ssiD	MAC-Address	IPv4 Address	Signal	Noise	RX Rate		1	TX Rate		
ociat	ssiD Maestro	MAC-Address 64:09:80:C6:B3:F8	IPv4 Address 192.168.1.216	Signal -41 dBm	Noise 0 dBm	RX Rate 6.0 Mbt/s, M	CS 0, 20MHz	1	TX Rate	a, MCS	7, 20MH

64 Maestro E200 Series

maes<mark>t</mark>ro **))**

15 Setting up Failover and Load Balancing

Maestro E200 and E220 series Router can be configured in a way that it could have 3 sources of WAN:

- Mired Ethernet WAN
- M Wi-Fi when configured in Client Mode (WWAN)

You can setup the Load Balancing functions in two different way depending what you want to achieve:

- M Failover to provide connectivity persistency
- Load Balancing to distribute traffic among different WAN



Please note that once configured for load balancing, the router can't be used for failover and will assume that all available WAN are connected. The router will balance the load among WANs as per the policies and

rules set.

If configured for failover, the router will only use 1 WAN at a time.

15.1 Failover mode configuration

By default the following is the priority assigned to each interface

- M Priority 1 Wired WAN
- Priority 2 Wi-Fi WAN (Wi-Fi setup in Client Mode)
- Priority 3 Cellular

This section will guide you through the following

M Change the priority of WAN interfaces

Setup failover policies to facilitate automatic failover between various
 WAN interfaces

Once all the three interfaces are setup as WAN, go to **Network > Load Balancing**. The page will show live view of available active and available inactive WAN Interfaces.



15.1.1 Setting up Load Balancing for Failover

15.1.1.1 Overview

Maestro	Quick Setup	Status	System	Services	Network	Logout		AUTO REFRESH ON
Overview	Configuration	Advance	Id					
Interface S	latus Detailed	Status						
MWA	N Interface I	ive Stat	15					
	wan (eth) Online (tracking).2) g active)		ww	ran (X) filine		3g (3g-3g) Online (tracking active)	

Above screenshot indicated that wired Wan is available and connected as well as 3G is available and connected while Wi-Fi WAN is offline.

Overview Configuration Advanced Interface Status Detailed Status MWAN Interface Live Status MWAN Interface Live Status Online (tracking active) Online (tracking active) MWAN Interface Systemlog Last 50 MUN systemleg entries. Nevest entries sorted at the top : Hed Teb 18 11:48:02 2015 user_notice mvan3; ifup interface wan (vian0)	RESH O
Interface Otatus Detailed Otatus MWAN Interface Live Status www.an (wfan0) Online (tracking active) 3g (3g:3g) Online (tracking active) MWAN Interface Systemlog Itast 50 MMAN systemlog entries. Nevest entries sorted at the top : Ned Feb 18 11;48:02 2015 user_notice mvan3; ifup interface wwan (vlan0)	
MWAN Interface Live Status Omine (tracking active) Omine (tracking active) Omine (tracking active) MWAN Interface Systemlog Last 50 MGAN systemlog entries. Nevest entries sorted at the top : Hed Feb 18 11;48:02 2015 user.notice mvan3; ifup interface vvan (vlan0)	
MWAN Interface Live Status wan (oth0.2) Online (tracking active) Online (tracking active) Online (tracking active) MWAN Interface Systemlog Lest 50 MMAN systemlog entries. Nevest entries sorted at the top : Wed Feb 18 11;48:02 2015 user.notice mvan3: ifup interface vvan (vlan0)	
WWAN Interface Live Status wan (wisn0) 3g (3g 3g) Online (tracking active) Online (tracking active) MWAN Interface Systemlog Last 50 MMAN systemlog entries. Newest entries sorted at the top : Ned Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (wlan0)	
wan (wilsn0) Online (tracking active) 3g (2g, 3g) Online (tracking active) MWAN Interface Systemlog Lest 50 MMAN systemlog entries. Nevest entries sorted at the top : Wed Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (vlan0)	
MWAN Interface Systemlog Last 50 MMAN systemlog entries. Nevest entries sorted at the top : Ned Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (vlam0)	
MWAN Interface Systemlog Last 50 MMAN systemlog entries. Newest entries sorted at the top : Ned Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (wland)	
Last 50 MMAN systemlog entries. Nevest entries sorted at the top : Ned Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (wland)	
Last 50 HHAN systemlog entries. Newest entries sorted at the top : Wed Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (wlam0)	
Wed Feb 18 11:48:02 2015 user.notice mwan3: ifup interface wwan (wland)	
Wed Feb 10 11:43:03 2015 user.notice mwan3: ifup interface wan (eth0.2) Wed Feb 18 11:23:36 2015 user.notice mwan3: ifup interface 3g (3g-3g)	
Ned Feb 18 11:43:03 2015 user.notice mwan3: ifup interface wan (eth0.2) Ned Feb 18 11:23:36 2015 user.notice mwan3: ifup interface 3g (3g-3g)	

Above screenshot indicates all three interfaces active

When all three interfaces are active, the one used for data transmission is as per the priority setup in **Load Balancing / Configuration** tab as shown below. Rest of the interfaces are still beings used for "tracking interface up / down" purposes.

You can re-assign or change the interface priority and failover policies by clicking on the **Configuration** tab.



15.1.1.2 Configuration

Maestro	Quick Setup	Status	System	Network	Senices	Logout		
Oveniew	Configuration	Advanced						
Interfaces	Members	Policies	Rules					
MWAN I Members Members are p Names may co	profiles attaching	a metric and v A-Z, a-z, 0-9,	veight to an	MWAN interfa	ice			
Members may Member	not share the sa	ime name as o face	configured in Metric	terfaces, polici Weight	ies or rules	Sort		
m1	w	an	1	2		• •	🛃 Edit	N Delete
<i>m</i> 2	1010	ian	2	2		• •	🛃 Edit	Delete
m3	3	9	3	2		• •	🗹 Edit	Delete
		Add						

Metric defines the priority. The screenshot shown above is the default configuration.



You assign **Rules** for **Policies** which are associated with **Members** which are linked to **Interfaces**



15.1.1.2.1 Interface

Maestr	o 0	Quick Setup	Status	System	Network	Services	Logout						
Overview	w C	Configuration	Advanced										
Interfac	es	Members	Policies	Rules									
MWA There are	N In e currer	terface ntly 3 of 250	Config supported inte	uration enfaces con	1 figured								
MWAN se MWAN re Names m Interfaces	upports o equires to sust mate ay conta a may no	up to 250 phy hat all interfac ch the interfa ain characters at share the s	/sical and/or log ces have a uniq ce name found s A-Z, a-z, 0-9, ame name as c	ical interfac ue metric co in /etc/confi _ and no sp configured m	es onfigured in /e g/network (se aces embers, polic	etc/config/net e advanced t	work ab)						
Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	MetricErrors	S	ort		
wan	Yes	8.8.8.8	1	5	3s	5s	3	2	1	•	•	Edit	Delete
wwan	Yes	8.8.8.8	1	5	3s	5s	3	2	2	٠	٠	Edit	Delete
3g	Yes	8.8.8.8	1	5	3s	15s	5	2	3	•	+	Edit	Delete
			Add 🔝										

Here you can see that there are 3 Interfaces: wan, wwan and 3g.

ITEM	DEFINITION
Tracking IP	This IP will be used to determine if the interface is active or inactive. You can enter more than one Tracking IP
Tracking Reliability	"1" determines the number of Tracking IP successes to be considered. Meaning, if there are more than one Tracking IPset, the above configuration will determine WAN active or inactive status depending on the result of any one Tracking IP.
Ping Count	Indicates the number of PING packets sent in every Ping Session to determine the interface availability / un- availability
Ping Timeout	Time to wait for PING response
Ping Interval	How frequently should the PING packets be sent
Interface down / interface	Number of iterations before declaring interface up/down and eventually switching to another interface
Metrics	These are Network Interface Metrics, the default values are 1 for WAN, 2 for WWAN and 3 for 3G. It is extremely critical these values are exactly same as the values in Load Balancing / Members. If you choose to change these values, please ensure that they are same at both places.



The above configuration will facilitate failover between WAN, WWAN and 3G in order of priority and will facilitate roll back when connection on respective interface is back as per order of priority.

Please note that Tracking IP, Ping Count and Ping Interval will consume data.

High Tracking IPs, Higher Ping count and low Ping interval will result in faster switchover but will consume high amount of data and vice-e-versa. Please be careful in adjusting these values as per your requirements.

15.1.1.2.2 Policies and Rules

You need to note that in Failover Mode, the following is the configuration for Policies and Rules. Changing these parameters will revert the router in Load Balancing.

	dance overup	Status	System	Network	Services	Logout				
Ovennew	Configuration	Advanced								
Interfaces	Members	Policies	Rules							
MWAN	Policy Co	onfigur	ation							
Policies										
Policies are p Member inter Load-balance Names may o Policies may	rofiles grouping o faces with lower n d member interfac contain characters not share the san	ne or more me netrics are use ces distribute s A-Z, a-z, 0-9 ne name as c	mbers contr ed first. Interf more traffic o , _ and no sp onfigured inte	olling how M laces with the out those with paces. Name enfaces, mem	WAN distribut same metric higher weight s must be 15 bers or rules	es traffic Ioad-balance Is characters o	e r less			
Policy	Members a	ssigned		Last reso	n .	Errors	Sort			
p1	m1 m2 m3			nreachable (n	eject)		••	1	Edit 💌 D	eloto
		Ada	1							
Maastro	Onich Datus	Charles	Sustan	Network	Parties	Land				
	GUICK GROUP	Status	aystem	THELEVER	Serrices	Logour				
Overview	Configuration	Advanced								
Overview	Configuration Members	Advanced Policies	Rules							
Overview Interfaces	Configuration Members Rule Con	Advanced Policies	Rules							
Overview Interfaces MWAN Traffic Ru	Configuration Members Rule Con	Advanced Policies	Rules							
Overview Interfaces MVVAN Rules specify Rules are mai Traffic destine down will be b Names may oc Rules may no	Configuration Members Rule Configuration les which traffic will a tiched from top to old for known (othe Nackholed contain characters to share the same	Advances Policies ifigurat bottom, Rules e than default) a A.Z, a-z, 0-9 name as con	Rules	licy based or tching rule ar handled by t baces aces, membe	IP address, j e ignored. Tra he main routir es or policies	port or protoc ffic not matc ig table. Traff	col hing any rule is rout fic matching a rule, b	ed using the but all WAN	main routing ta interfaces for th	ble at policy are
Overview Interfaces MVVAN Traffic Ru Rules specify Rules are mai Traffic destine down will be t Names may o Rules may no Rules Source	Configuration Members Rule Configuration les which traffic will a teched from top to al for known (othe blackholed contain characters at share the same address Source	Advances Policies offigurat use a particuli bottom. Rules e than default) a A-Z, a-Z, 0-9 name as com	Rules	licy based or tching rule an handled by t paces aces, membe ress Destin	IP address, j e ignored. Tra he main routir ers or policies nation port f	port or protoc disc not matc ng table. Traff Protocol Po	col hing any rule is routr fic matching a rule, b slicy assigned Erro	ed using the cut all WAN	main routing ta interfaces for th	ble at policy are
Overview Interfaces MWVAN Traffic Ru Rules specify Rules are mai Traffic destine doem will be b Names may no Rule Source r1	Configuration Members Rule Configuration les which traffic will a tached from top to de for known (othe hanckholed contain characters it share the same address Source	Advances Poisces ifigurat use a particulu bottom. Rules e than default) a A-Z, a-Z, 0-9 name as con ce port. Dest	Rules Ion In MWAN po below a main networks is and no sp figured interfit instition add	licy based or tching rule ar handled by t paces aces, membe ress Destir	IP address, j e ignored. Tra he main routin es or policies nation port f	port or protoc fic not mate ng table. Traff Protocol Po all	ol hing any rule is route fic matching a rule, b plicy assigned Erro p1	ed using the but all WAN	main routing ta interfaces for th	ble at policy are



15.2 Load balancing mode configuration

Load Balancing Mode configuration will enable the router to use all three WANs simultaneously and facilitate the user to associate policies and rules for each interface.

Exemples"

- You can bind a particular interface with a particular source or destination IP;
- You can bind a particular interface with a particular protocol like TCP, UDP, L2TP etc.

To set the Router in Load Balancer Mode, you need to first assign Metric and Weight to all the Members and create more Members if necessary

vlembers						
Members are profile Names may contair Members may not :	s attaching a metric a n characters A-Z, a-z, share the same name	and weight to an 0-9, _ and no sp as configured int	MWAN interface aces erfaces, policies or	rules		
Member	Interface	Metric	Weight	Sort		
m1	wan	1	2	• •	🔀 Edit	E Delete
<i>m</i> 2	wwan	2	2	••	🔀 Edit	Delete
	30	3	2		Z E-R	Delete

Next step would be to create Policies corresponding to each Member

	roney congula						
Policies							
Member inter Load-balance	faces with lower metrics are used d member interfaces distribute mo	first. Interfaces with the same me re traffic out those with higher we	tric load-balance ights				
Names may Policies may	contain characters A-Z, a-z, 0-9, _ not share the same name as conf	and no spaces. Names must be igured interfaces, members or rul	15 characters or es	less	112		
Names may Policies may Policy	contain characters A-Z, a-z, 0-9, _ not share the same name as conf Members assigned	and no spaces. Names must be Igured interfaces, members or rul Last resort	15 characters or es Errors	less Se	ort		
Names may Policies may Policy p1	contain characters A-Z, a-z, 0-9, _ not share the same name as conf Members assigned m1	and no spaces. Names must be igured interfaces, members or rul Last resort unreachable (reject)	15 characters or es Errors	less Se	ort	Edt	E Delete
Names may o Policies may Policy p1 p2	contain characters A-Z, a-z, 0-9, _ not share the same name as conf Members assigned m1 m2	and no spaces. Names must be igured interfaces, members or rui Last resort unreachable (reject) unreachable (reject)	15 characters or es Errors	Second Second	ort	🖉 Edit	E Delete

Next would be create rules for each Policy

Fra f	fic Rules								
Ruler Traffi down	s specify which that s are matched from c destined for know will be blackholed es may contain cha	top to bottom. n (other than d aracters A-Z, a-	Rules below a matching efault) networks is hand z, 0-9, _ and no spaces	g rule are ignored. Tr led by the main rout	rafic not m ing table. 1	atching any rule is route Traffic matching a rule, b	ed using the ut all WAN	main routing tal interfaces for the	ble at policy are
Rule:	s may not share the	e same name a	is configured interfaces,	members or policies	s				
Rule: Rule	s may not share the Source address	Source port	Destination address	Destination port	s Protocol	Policy assigned Erro	rs Sort		
Rule: Rule r1	s may not share the Source address 192.168.1.104	Source port	Destination address	Destination port	Protocol udp	Policy assigned Erro	rs Sort	• 🛛 Edt	🔳 Delete
Rule: Rule r1 r2	s may not share the Source address 192.168.1.104	Source port 	Destination address 223.30.182.58	Destination port 	s Protocol udp tcp	Policy assigned Erro p1 p2	s Sort	• Z Edt	Delete Delete

In the above screenshot, you can see that there are 3 rules created

Rule r1 is linked to policy p1 which is linked to member m1 which is linked to Interface wan

Rule r2 is linked to policy p2 which is linked to member m2 which is linked to Interface wwan

Rule r3 is linked to policy p3 which is linked to member m3 which is linked to Interface 3G

The above configuration means

- M UDP connections from LAN IP 192.168.1.104 will be sent via WAN
- All requests to WAN IP 223.30.182.58 on Port 2404 will be sent via WWAN
- M All incoming and outgoing PING will be sent via 3G



maestro)

16 Firewall Basics

E200 and E220 Series follows a Zone Based firewall concept.

Every interface of E200 Router physical or virtual needs to be assigned to a firewall zone however one firewall zone can have multiple interfaces.

By default, two zones exists namely LAN zone and WAN zone as shown in the screenshot below.

You can create a new zone either from the Firewall section nuder **Network / Firewall** or when you create an additional network interface.



For the current version of Firmware, only LAN side Firewall Zones can be created and you can associate multiple VLANs to the LAN side firewall Zones. However there will be a single WAN side firewall

zone.

one ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
an: lan: 💥 👷 = Wan	accept	accept 💌	accept			🗾 Edt	E Delete
van: 3g: 👔 wan: 📰 = 🔝	accept	accept	accept	*	•	🛃 Edit	E Delete
Add							
					Save & Apply	Save	Reset


17 Services

17.1 Dynamic DNS

The E200 and E220 series router gets the internet access through WAN or 3G. The LAN interface is used for connecting to the local network. The service provider for WAN or 3G will periodically change the IP address assigned to the router, unless you ask for a static IP address.

However, it is not possible for a remote client of the router to change the address in tune with the service provider. In such case, Dynamic DNS or DynDNS comes in handy. The concept is same as DNS, however, it retains the "Name" given to the router even if the underlying IP address is changed.

For this, you need to register with the provider of dynamic DNS and configure the router with the details. Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

The following note describes the procedure to create Dyn DNS.

Click on Services / Dynamic DNS.

Dynamic DNS Dynamic DNS allows that your re	outer can be reached with a fixed ho	stname while having a dynamically changing IP address.
		Delete
MYDDNS		
Enable	0	
Event interface	wan \$	
	Network on which the operation of the	idns-updater scripts will be started
Service	dyndns.org \$	
Hostname	mypersonaldomain.dyndns.org]
Username	myusername]
Password		<i>a</i>
Source of IP address	URL \$	
URL	http://checkip.dyndns.com/]
Check for changed IP every	10]
Check-time unit	min \$	
Force update every	72]
Force-time unit	h ‡	
	Add 1	

ITEM	DEFINITION		
Enable	Enable DynDNS service		
Event interface	Network on which the ddns-updater scripts will be started		
Service	Your DynDNS service provider		
Hostname	Hostname received from your DynDNS service provider		
Username	Username received from your DynDNS service provider		
Password	Password received from your DynDNS service provider		

Next, you have to choose the source of IP address and the network. The source of IP address can be either Network or Interface or URL. This is the mechanism through which an IP address is assigned to the router.

If you choose Network, then you have to choose the type of network namely WAN or 3G.

Similarly, if you choose Interface, then you have to choose the appropriate interface from the dropdown.

If you select the option URL, then a URL needs to be given which fetches IP address of the router from Internet. An example of such URL is http://checkip.dyndns.com/ and appears by default.



Next, choose the frequency with which you want to check, if the IP address is changed, minutes or hours.

You can also force a change in IP address, after an assigned period of time.

After making these entries, you can enable the new DDNS entry by checking the **Enable** box at the top of the page.

Choose **Save and Apply** to effect the change. You will see the new entry with your parameters in addition to any old entries.

Now, you will be able to access the router with the hostname assigned, rather than the IP address.

You can add a new DynDNS by choosing a name and clicking on ADD button.

17.2 SMS diagnostic

SMS diagnostic let you configure up to 4 admins to receive diagnostic information of the router after a command is send by SMS.

International number format is as follow: <countrycode><phonenumber>

SMS Configuration		
SMS Configuration		
SMS Administrator	Mobile Number	
	Please enter the mobile number with country code	
Admin 1	0	
Admin 2	0	
Admin 3	0	
Admin 4	0	



COMMAND	DEFINITION
AT+REBOOT=1	Reboot: reboot the modem
AT+CELLDIAG?	Cell diagnostics: will give you IMEI, CREG, COP, CSIG
AT+LANDIAG?	LAN diagnostics: Will give LAN IP address,
AT+WANDIAG?	Wired WAN diagnostics:
AT+WANPING= <ipa></ipa>	Wired WAN ping: will ping the wired WAN interface
AT+LANPING= <ipa></ipa>	LAN ping: will ping the wired LAN interface
AT+REMACC=<1/0>	Remote access: will enable; AT+REMACC=<1> or
	UISADIE AT+REIMACC= <u> TEITIOLE ACCESS</u>
AT+HWI?	Hardware information: will give you hardware information
,	such as model number
AT+S/1/12	Software information: will give you software information
	such as firmware version

ist of Commands		
List of Co	ommands	
No.	Command name	Command
1	Reboot	AT+REBOOT=1
2	Cell Diagnostics	AT+CELLDIAG?
3	LAN Diagnostics	AT+LANDIAG?
4	WAN Diagnostics	AT+WANDIAG?
5	WAN Ping	AT+WANPING= <ipa></ipa>
6	LAN Ping	AT+LANPING= <ipa></ipa>
7	Enable Remote access	AT+REMACC=<1/0>
8	Hardware information	AT+HWI?
9	Software information	AT+SWI?

17.3 DOTA

DOTA (download over the air) will allow you to remotely update your firmware, enter your server IP address the filename, username and password

DOTA			
Server]	
Filename]	
User	admin]	
Password		8	



17.4 GPS

You can get GPS	parameters as	describes	below
-----------------	---------------	-----------	-------

GPS	
Parameter	Value
Time	GPS_ERROR
Latitude	GPS_ERROR
N/S-Indicator	GPS_ERROR
Longitude	GPS_ERROR
E/W-Indicator	GPS_ERROR
Position-Fix-Indicator	GPS_ERROR
Satellites-Used	GPS_ERROR
HDOP	GPS_ERROR
MSL-Attitude	GPS_ERROR
Protocol	
Enable Data Send	

By clicking **Enable Data Send** you will open a new menu where you could select the IP address, the port and the protocol format to receive the data, etheir TCP, UDP or HTTP. You can also setup a backup server by clicking on the **Backup** checkbox

Protocol	
Enable Data Send	e d
Protocol	TCP \$
IP1	0.0.0.0
Port1	0
Backup	If selected and data sending failed on primary lp then backup ip will be used. If backup ip failed then again primary ip will be used. There will be 3 such tries
Send Interval in Minute	0



17.5 Event

The Event menu let you set-up action based on preset event.

Those events can be:

- ၏ GPIO_H
- ၏ GPIO_L
- ℬ SIM_CHANGE

Available actions are:

-)∭ SMS
-)) REBOOT

International number format is as follow: <countrycode><phonenumber>

On the text box enter a text (max.160 characters) that will be send to the corresponding mobile number when a change of event occurs.

Click add once your rules are set-up.

Click Save and Apply to save preset events.

	Enable 🖂		
nt	Action	Mobile Number	Text
vents:			
vents:	Action	Mobile Number Text	



18 Appendix

18.1 Default settings

The following tables list the default settings for the E200 Series router.

LAN (MANAGEMENT)		
Static IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	
ADMIN MANAGER ACCOUNT		
Username: admin		
Password:	admin	

18.2 Reset to factory default setting

Restoring factory defaults will reset the E200 Series router to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your E200 Series router such as:

- You have lost your username and password and are unable to login to the web configuration page
- M You are asked to perform a factory reset by Maestro support staff.

There are two methods you can use to restore factory default settings on your E200, using the web-based user interface or using the reset button on the side of the router.

18.2.1 Using the web-based user interface

To restore your router to its factory default settings, please follow these steps:

Open a browser window and navigate to the IP address of the router (default address is http://192.168.1.1). Login to the router using **admin** as the User Name and **admin** as the password.

Click the **System** item from the top menu bar, then **Backup / Flash Firmware** and then under **Flash operations** select the **Actions** tabs.

Under the **Actions** tabs, click the **Perform reset** button. The router asks you to confirm that you wish to reset all changes. Click OK to continue. The router will erase the configuration partition and reboot.

18.2.2 Using the reset button on the side of the router

Use a pin to push the Reset button on the device for 10 seconds. The router will restore the factory default settings and reboot.



When you have reset your E200 Series router to its default settings you will be able to access the device's configuration web interface using http://192.168.1.1 with username **admin** or **root** and password **admin**.

18.3 List of acronyms

Acronym	Expansion / Meaning
2G	2nd Generation
3G	3rd Generation
ADSL	Asymmetric digital subscriber line, ADSL is a type of DSL broadband communications
	technology used for connecting to the Internet
AES	Advanced Encryption Standard
AP Client	Access Point Client
CSQ	
DHCP	Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol
	used on Internet Protocol (IP) networks for dynamically distributing network
	configuration parameters, such as IP addresses for interfaces and services.
DIN	DIN connector is an electrical connector that was originally standardized by the
	Deutsches Institut für Normung (DIN)
DMZ	In computer security, a DMZ or Demilitarized Zone is a physical or logical sub network
	that contains and exposes an organization's external-facing services to a larger and
	un-trusted network, usually the Internet.
DNS	Domain Name System (DNS) is a hierarchical distributed naming system for
	computers, services, or any resource connected to the Internet or a private network
DynDNS, DDNS	Dynamic DNS (DDNS) is a method of automatically updating a name server in the
	Domain Name System (DNS), often in real time, with the active DNS configuration of
	its configured hostnames, addresses or other information.
EDGE	Enhanced Data rates for GSM Evolution (EDGE) is a digital mobile phone technology
	that allows improved data transmission rates as a backward-compatible extension of
CDDC	Concret neglect redia contine (CDDS) is a period or instal markite data and in the
GPK5	General packet radio service (GPRS) is a packet oriented mobile data service on the
GSM	Clobal system for mobile communications
	High Throughput Dhysical Made
	Internet Centrel Measure Protocol (ICMP) is one of the main protocols of the Internet
	Protocol Suite. It is used by network devices, like routers, to send error messages
IGMP	Interpet Group Management Protocol is a communications protocol used by bests and
IGIMI	adjacent routers on IP networks to establish multications protocol used by hosts and
IP Sec	Internet Protocol Security is a protocol suite for securing Internet Protocol (IP)
1 000	communications by authenticating and encrypting each IP packet of a communication
	session
ISP	Internet service provider
L2TP	Laver 2 Tunneling Protocol is a tunneling protocol used to support virtual private
	networks
LAN	Local Area Network
Acronym	Expansion / Meaning
LLTD	Link Layer Topology Discovery is a proprietary Link Layer protocol for network
	topology discovery and quality of service diagnostics
M2M	Machine to machine
MAC address	Media access control address is a unique identifier assigned to network interfaces for
	communications on the physical network segment
MTU	Maximum transmission unit of a communications protocol of a layer is the size (in
	bytes) of the largest protocol data unit that the layer can pass onwards
NAT	Network address translation is a methodology of modifying network address
	information in Internet Protocol (IP) datagram packet headers while they are in transit
	across a traffic routing device for the purpose of remapping one IP address space into
	another.
NIP	Network Time Protocol is a networking protocol for clock synchronization between
DDD=E	Computer systems over packet-switched, variable-latency data networks
	Point-to-Point Plotocol over Ethemet
	Point-to-Point Tunneing Protocol
	Cuelity of Service
QU3 DE	Podia Fraguanay
Ri Py	Percention
SIM	Subscriber identity module
SMA	SMA (Sub Miniature version A) connectors are semi-precision coavial RF connectors
SMS	Short Message Service
SPI	Serial Peripheral Interface
SSID	Service set identification
TCP	Transmission Control Protocol
TKIP	Transmission Control Protocol
Тх	Transmission
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VPN	Virtual private network
WAN	Wide Area network

WCDMA	Wideband Code Division Multiple Access
WDS	Wireless distribution system
WEP	Wired Equivalent Privacy, is a wireless network security standard
Wi-Fi	Local area wireless technology that allows an electronic device to exchange data or connect to the internet using 2.4 GHz UHF and 5 GHz SHF radio waves
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

82 Maestro E200 Series

18.4 Support

There are several resources available to you for support and troubleshooting of your Maestro product or for resolving configuration difficulties at Maestro's support website, <u>http://support.maestro-wireless.com/knowledgebase.php</u>.

Try these troubleshooting steps to eliminate your problem. After working through these steps and if your problem is not solved, please send a ticket to Maestro support team.

Fill out an Online Support Request via: <u>http://support.maestro-</u> <u>wireless.com/index.php?a=add</u>. You will need to create a user account if one is not already set up.

When submitting a support request, please include a copy of the **System Log** file from the unit's and the **configuration files**. This will greatly improve the quality of the initial response you receive. Without this file, it is often very difficult for the support team to provide accurate answers to your queries.

To create a copy of the system login on your router and go to **Status > System Log.**

					_			
Maestro	Quick Setup	Status	System	Network	Services	Logout		
System	Log							
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: ^M					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: ^M					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: OK					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: go	t it				
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: send	(AT+CGDCO	NT=1,"IP",""^N	D		
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: timeo	ut set to 30 s	econds	-		
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: experi	ot (OK)				
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: ^M					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: ^M					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chatf	12783]: OK					
Tue Mar 10 0	3:05:04 2015 loca	al2.info chatf	12783]: 00	t it				
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: send	(ATD*99***1#	^M0			
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: expe	t (CONNECT	D			
Tue Mar 10 0	3:05:04 2015 loca	al2.info chat[12783]: ^M					
Tuo Mar 10.0	2.05-04 2015 loss	Itodo oboi Cle	107931 AM					

Select the entire log, copy it and paste it on a new document file .

To generate an archive of your configuration go to System > Backup / Flash Firmware, under the Actions tabs click on Generate archive.

Flash operations							
Actions	Configuration						
Backup / Click *Gene with squash	/ Restore rate archive" to dow rfs images). Download backup: Reset to defaults:	nload a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible Generate archive Perform reset					



An archive file "backup-Maestro-201x-xx-xx.tar.gz will be downloaded on your default download folder, please attached the file while filling the support request online.