MAR-2000 Software Manual

First Edition, May 2015

www.moxa.com/product

MAR-2000 Software Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

Toll-free:	1-888-669-2872
Tel:	+1-714-528-6777
Fax:	+1-714-528-6778

Moxa Europe

Tel:	+49-89-3 70 03 99-0
Fax:	+49-89-3 70 03 99-99

Moxa India

Tel:	+91-80-4172-9088
Fax:	+91-80-4132-1045

Moxa China (Shanghai office)

Toll-free:	800-820-5036
Tel:	+86-21-5258-9955
Fax:	+86-21-5258-5505

Moxa Asia-Pacific

Tel:	+886-2-8919-1230
Fax:	+886-2-8919-1231

Table of Contents

1

Introduction

Thank you for purchasing the MAR-2000 for your mobile wireless applications.

The MAR-2000 is a compact, programmable, RISC-based wireless mobile router with strong multiple-WAN management capabilities. It features a built-in GPS module, HSPA+ cellular and 802.11a/b/g/n wireless capability, and with high thermal tolerance. In addition, the MAR-2000 is compliant with a portion of EN 50155 specifications. The built-in 32 MB NOR Flash ROM and 512 MB SDRAM give you enough memory for your application software, and the 512 MB NAND Flash can be used to provide additional data storage. It has one CompactFlash socket for future storage expansion, and the built-in GPS module supports geo-fencing functionality, making it ideal for managing wireless connections in cross-WAN environments, as are found in rolling stock or other vehicle applications.

When a train travels between different regions, it is often confronted with different wireless interfaces, including WiFi, UMTS, and HSPA+. With multiple-WAN support and backup, the MAR-2000 helps ensure the availability of your wireless connection, enhancing wireless quality, stability, and reliability.

The MAR-2000 series includes wide temperature models designed to operate reliably in environments with temperatures ranging from -25 to 70°C.

The MAR-2000 provides an easy way to configure routing between your various network interfaces. Advantages of the MAR-2000 include:

- **Intelligent policy configuration:** Easily automate system configuration for heterogeneous networks.
- **Multiple routing technology:** Network bandwidth efficiency is easily optimized and network slowdowns due to heavy data loads can be avoided.

The following topics are covered in this chapter:

Getting Started

This chapter walks you through the initial configuration of the MAR-2000. The initial configuration will be restricted to a simple, bare-bones setup to give you easy access to a working MAR-2000 platform. You may pick and choose which features to enable; all of the base configuration parameters can be accessed from the **Settings** section of the main user interface (UI).

Connecting to the MAR-2000

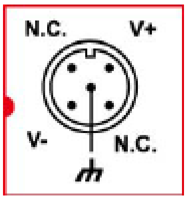
The MAR-2000 can be configured via a Web console.

It is recommended that you use the Chrome web browser to configure and manage the MAR-2000. Use the serial and SSH consoles for advanced command-line configuration. To access the MAR-2000 over the serial console, connect a COM port on your computer to the serial console on the MAR-2000 using a serial cable. To access the web console over the SSH console or web browser, you must be connected to the MAR-2000 through an Ethernet LAN or the Internet.

NOTE For detailed information about how to connect to the MAR-2000 over the serial console, see **Appendix B**.

Powering on the MAR-2000

Before you continue, make sure that the central pin of the MAR-2000's M12 power connector is properly connected to a shielded ground.



Power on the MAR-2000 by connecting it to a power source. The MAR-2000 does not have an on/off or power switch. It takes about four minutes for the system to complete the start-up process. After the start-up process is complete, the **Ready** LED lights up.

Accessing the Web Console

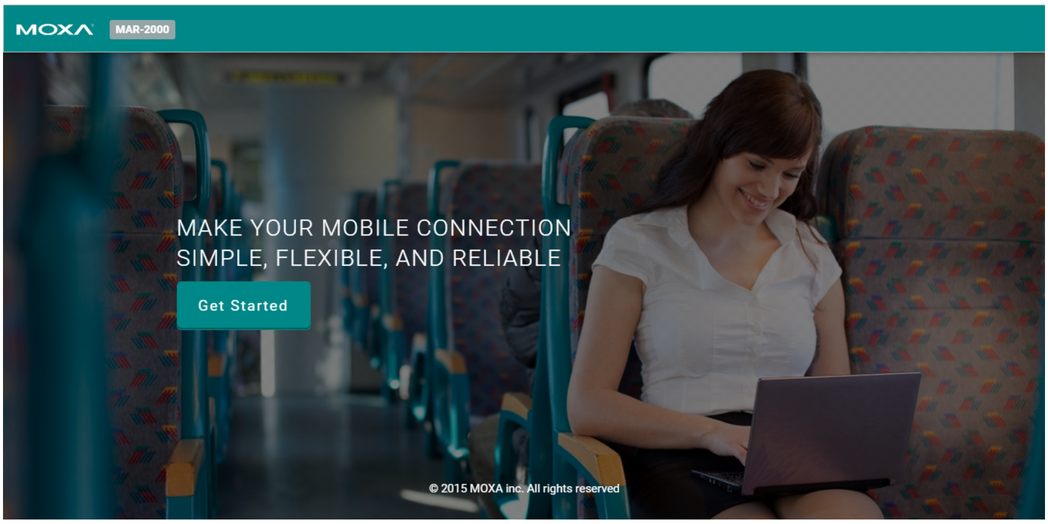
The most convenient way of accessing the MAR-2000's web console is via web browser. To connect using a web browser, either add the MAR-2000 to the LAN or connect your computer directly to the M12 Ethernet port on the MAR-2000 (you can use either straight-through or crossover cable). When connecting to the MAR-2000 from a LAN, make sure that your computer and the MAR-2000 are on the same logical subnet.

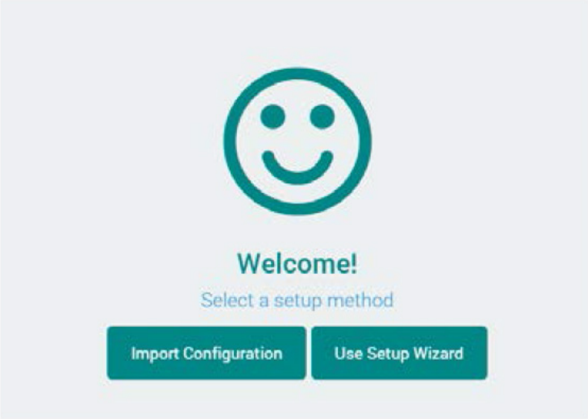
Connect the Ethernet cable to the computer and then open a web browser. The IP address for the web console varies depending on the Ethernet port your computer is connected to. The following shows the default IP addresses on the MAR-2000:

• **LAN 1:**	192.168.3.127
• **LAN 2:**	192.168.4.127

To access the web console on the MAR-2000:

1. Open a web browser. We recommend using Chrome V33, or more recent versions.
2. Enter the IP address in the address bar. The main screen appears as shown below. Click **Get Started** to open the **Welcome** page.


MOXA
MAR-2000
MAKE YOUR MOBILE CONNECTION
SIMPLE, FLEXIBLE, AND RELIABLE
Get Started
© 2015 MOXA inc. All rights reserved



Note: This page will only be shown the first time you open this page, or after a factory reset.

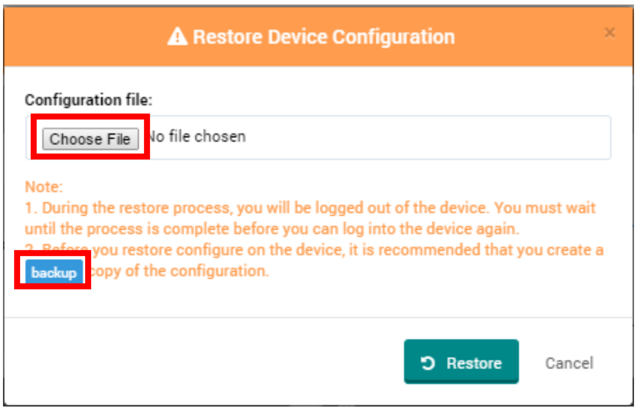
3. Select one of the following options:
   a. Import Configuration: Imports configuration from a file.
   b. Use Setup Wizard: Runs the setup wizard that guides you through the initial configuration process.

NOTE The Welcome screen does not appear again after you have configured the MAR-2000 for the first time. The system automatically logs you out of the web console after five minutes of inactivity.

Importing Configuration from a File

If you have already configured the MAR-2000, you can use this method and choose the **Configuration Using the Setup Wizard**. After you reset the device back to the factory default settings, you can use this method to reload a backup configuration to quickly restore the device to working status. After you have successfully restored a configuration, the system will be reset to its typical working configuration and this welcome page will no longer be accessible.

After selecting the **Import Configuration** option, a dialog box appears as shown in the following figure. You can choose a configuration file to load.



Restore Device Configuration

Configuration file: No file chosen

Note:
1. During the restore process, you will be logged out of the device. You must wait until the process is complete before you can log into the device again.
2. Before you restore configure on the device, it is recommended that you create a backup copy of the configuration.

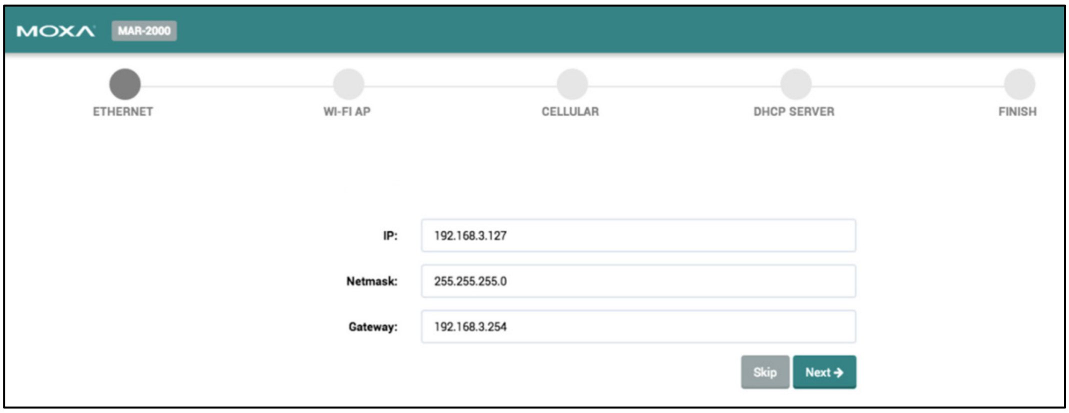
Click **Choose File** to select a configuration file (a tar file) you want to restore; then, click **Restore**. The system reloads the configuration and automatically reboots. This process might take up to four minutes.

Configuration Using the Setup Wizard

The setup wizard provides an easy way to get the MAR-2000 up and running, in five quick steps.

Step 1: Ethernet Interfaces Setup

Specify the static IP address, network mask, and default gateway for the Ethernet interfaces on the MAR-2000.



IP: 192.168.3.127

Netmask: 255.255.255.0

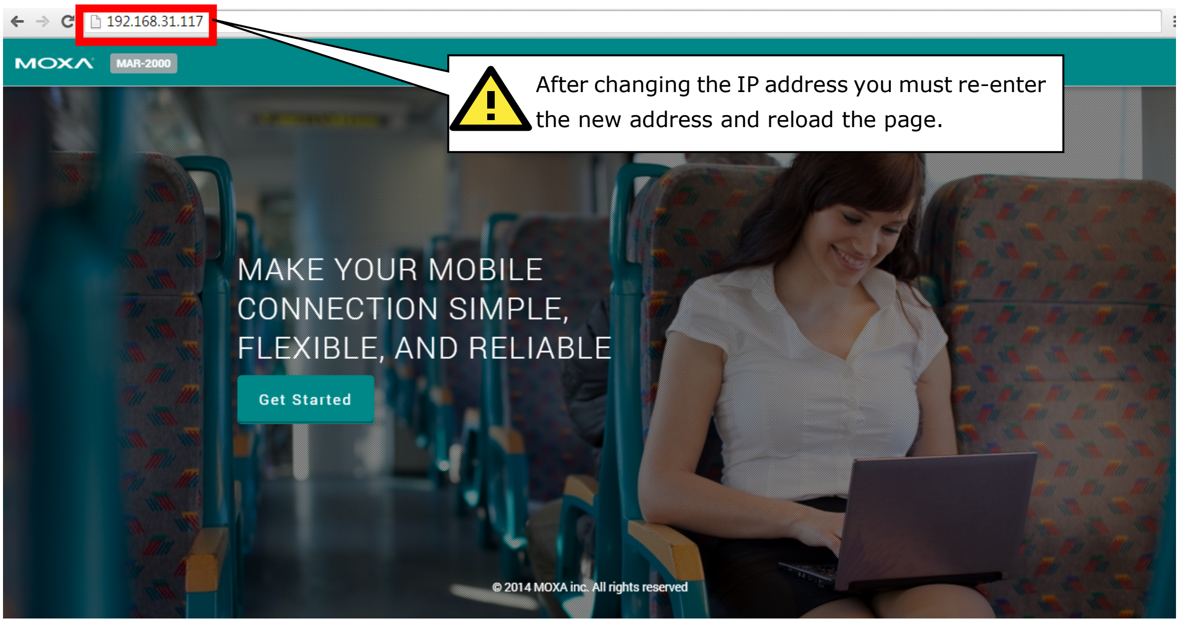
Gateway: 192.168.3.254

Field	Description
IP	Set a static IP address for the selected interface.
Netmask	Set the network mask for the selected interface.
Gateway	Set the default gateway for the selected interface.

After you set the information in the configuration fields settings, click **Next** to save the settings. The information is used to initialize the MAR-2000.

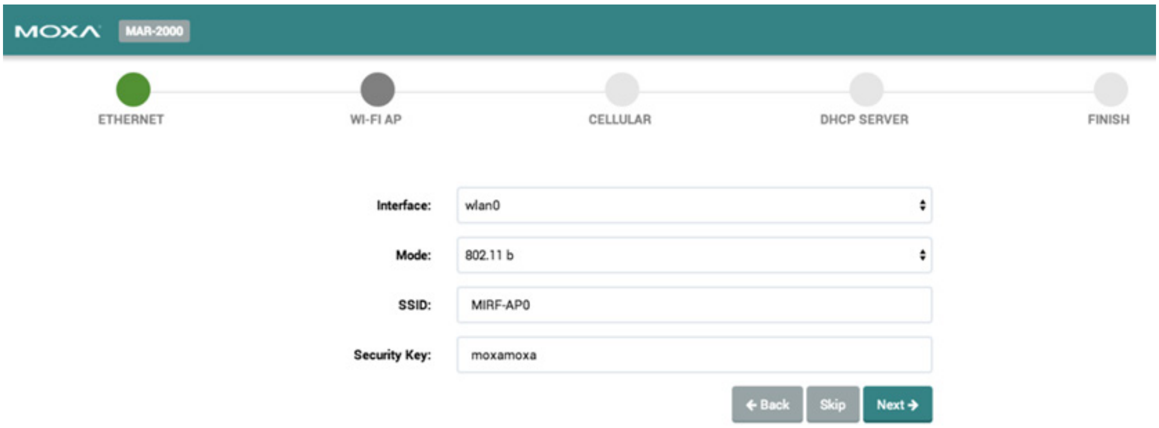
NOTE Only the Eth0 interface can be configured while using the Wizard.

NOTE If you change the IP address, your web browser will lose connection to the MAR-2000. To re-connect to the MAR-2000 and continue to use the setup wizard, enter the new IP address in the address bar on the web browser and reload the page.


192.168.31.117
MOXA MAR-2000
MAKE YOUR MOBILE CONNECTION SIMPLE, FLEXIBLE, AND RELIABLE
Get Started
© 2014 MOXA inc. All rights reserved

After changing the IP address you must re-enter the new address and reload the page.

Step 2: Wi-Fi Access Point Setup



Interface: wlan0

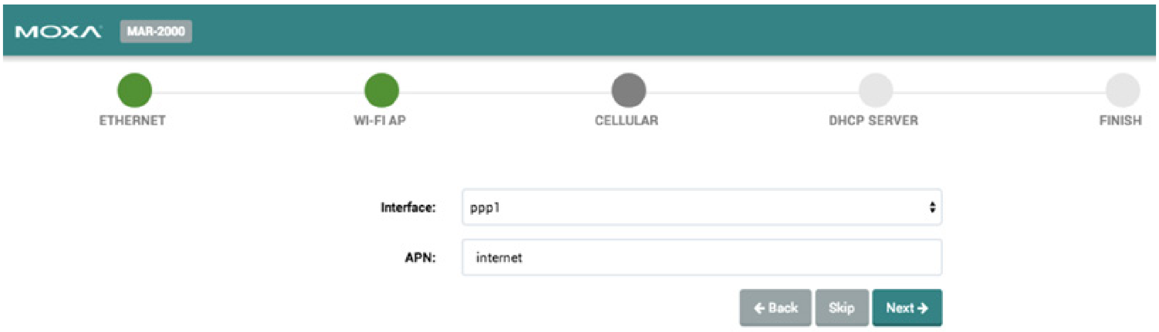
Mode: 802.11 b

SSID: MIRF-AP0

Security Key: moxamoxa

Field	Description
Interface	Select which 802.11 interface to configure.
Mode	Select the 802.11 mode (a, b, g, or n) for the interface.
SSID	Set the SSID of the wireless network.
Security Key	Enter your security key here; the default encryption is WPA+WPA2.

Step 3: Cellular Client Setup

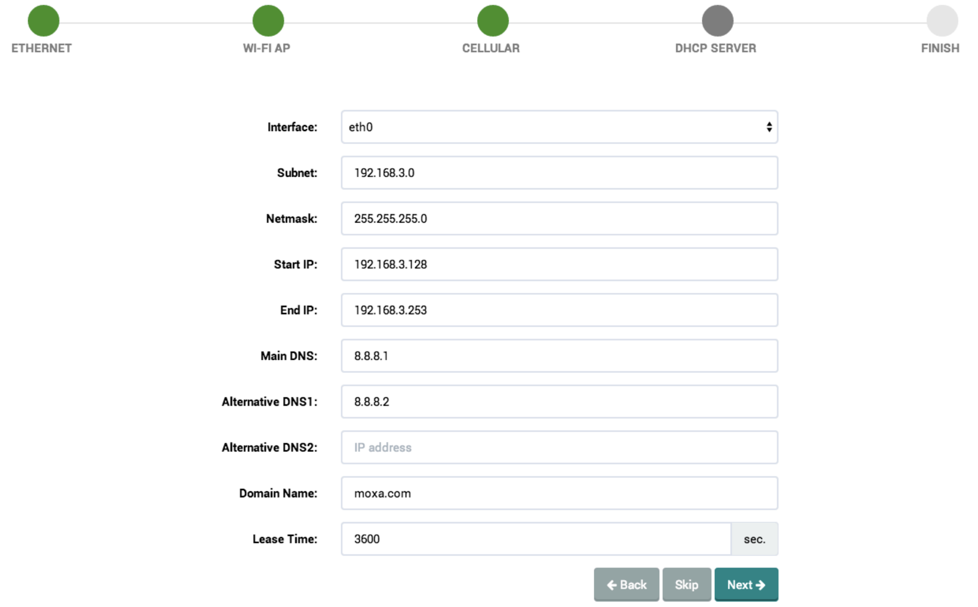


Interface: ppp1

APN: internet

Field	Description
Interface	Cellular interface list.
APN (Access Point Name)	For use with private accounts. Enter the network identifier (APN) that has been assigned to you by your cellular service provider.

Step 4: DHCP Server Setup



Interface: eth0

Subnet: 192.168.3.0

Netmask: 255.255.255.0

Start IP: 192.168.3.128

End IP: 192.168.3.253

Main DNS: 8.8.8.1

Alternative DNS1: 8.8.8.2

Alternative DNS2: IP address

Domain Name: moxa.com

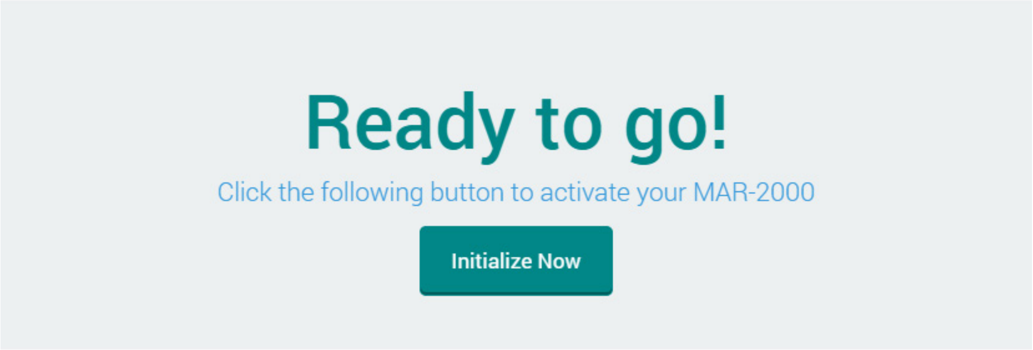
Lease Time: 3600 sec.

Field	Description
Interface	Select which interface to configure.
Subnet	An IP address that provides a template for IP addresses allowed on the subnet.
Netmask	Determines, together with the subnet address, which IP addresses will be allowed on the subnet.
Start IP	Enter the first (lowest) IP address of the IP assignment range.
End IP	Enter the last (highest) IP address of the IP assignment range.
Main DNS	Enter the main DNS server IP address.
Alternative DNS1	Enter an alternative DNS server IP address.
Alternative DNS2	Enter an alternative DNS server IP address.
Domain Name	Individual ports may be configured with distinct domain names to separate local devices into independent network segments for easier administration and identification.
Lease Time	Enter the lease time for the Domain Name server (in seconds).

Step 5: Initialize Configuration on the MAR-2000

In the last step of the setup wizard, click **Initialize Now** to initialize the configuration and activate default routing on the MAR-2000.

After the process is complete, you can start using the MAR-2000 on your network.



Ready to go!

Click the following button to activate your MAR-2000

2

Login, Dashboard, and Account Pages

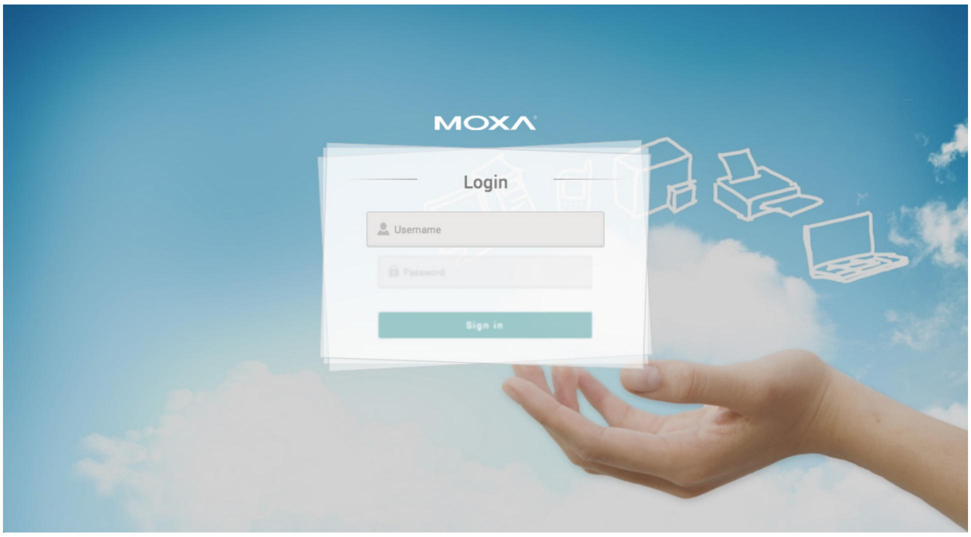
This chapter shows you how to use a web browser to manage the administrative account and review the basic monitoring features of the MAR-2000.

The following points are covered in this chapter:

Login Page

This page allows you to set up an initial administrative account on your MAR-2000. The default username and password to log in to the system is **admin**. You can change the password on the **Account Settings** page, under **Password**.

Login:	**admin**
Password:	**admin**

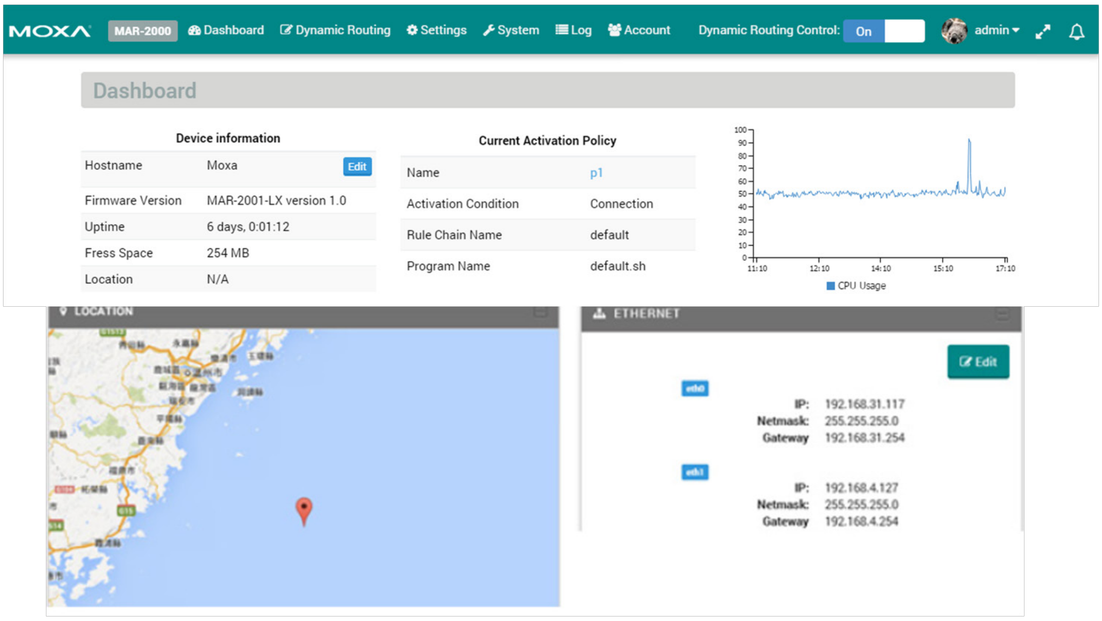


After successfully entering the login and password, the **Dashboard** screen appears.

NOTE The system automatically logs you out of the web console after five minutes of inactivity.

The Dashboard

The dashboard is the main page of the MAR-2000 web console. From here you can access all the configuration screens, and set up monitors to display device states, your current connection zone, CPU usage, and connection states for Ethernet, Wi-Fi, and cellular interfaces.



Dynamic Routing Control: On

Dashboard

Device information

Hostname	Moxa	Edit
Firmware Version	MAR-2001-LX version 1.0	
Uptime	6 days, 0:01:12	
Fress Space	254 MB	
Location	N/A	

Current Activation Policy

Name	p1
Activation Condition	Connection
Rule Chain Name	default
Program Name	default.sh

eth0

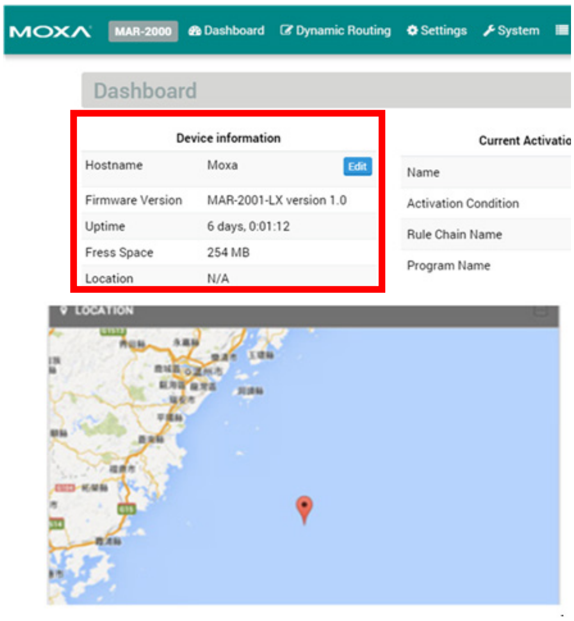
IP: 192.168.31.117
Netmask: 255.255.255.0
Gateway 192.168.31.254

eth1

IP: 192.168.4.127
Netmask: 255.255.255.0
Gateway 192.168.4.254

Device Information

The **Device Information** box lists basic information about and the status of the device.



Device information

Hostname	Moxa
Firmware Version	MAR-2001-LX version 1.0
Uptime	6 days, 0:01:12
Fress Space	254 MB
Location	N/A

Name

Activation Condition

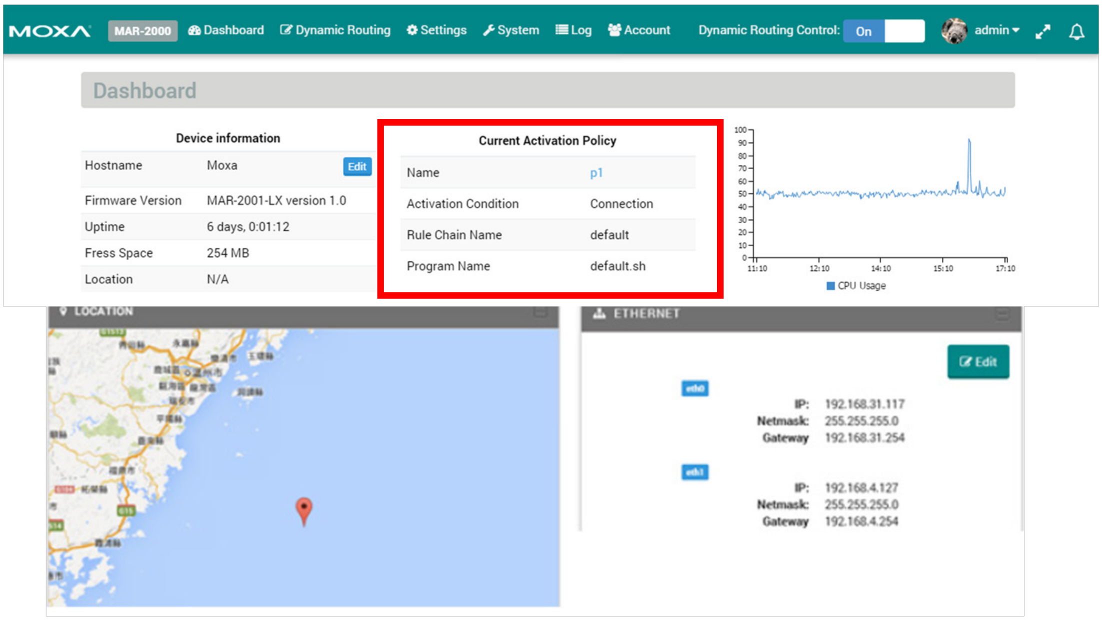
Rule Chain Name

Program Name

Field	Description
Hostname	Shows the device's host name, which is used for identification over a network.
Firmware Version	Displays which version of the firmware is currently being used.
Uptime	Shows how long the device has been operating.
Free Space	Shows the amount of available storage space on the device.
Location	Displays the latitude and longitude of the device's current location as measured by GPS. A small active map is also displayed. Note: When GPS and the Internet are not available, N/A will be displayed in the Location field and the map won't be displayed.

Current Activation Policy

The **Current Activation Policy** screen shows which connection policy is currently activated.



Device information

Hostname	Moxa
Firmware Version	MAR-2001-LX version 1.0
Uptime	6 days, 0:01:12
Fress Space	254 MB
Location	N/A

Current Activation Policy

Name	p1
Activation Condition	Connection
Rule Chain Name	default
Program Name	default.sh

eth0

IP: 192.168.31.117
Netmask: 255.255.255.0
Gateway 192.168.31.254

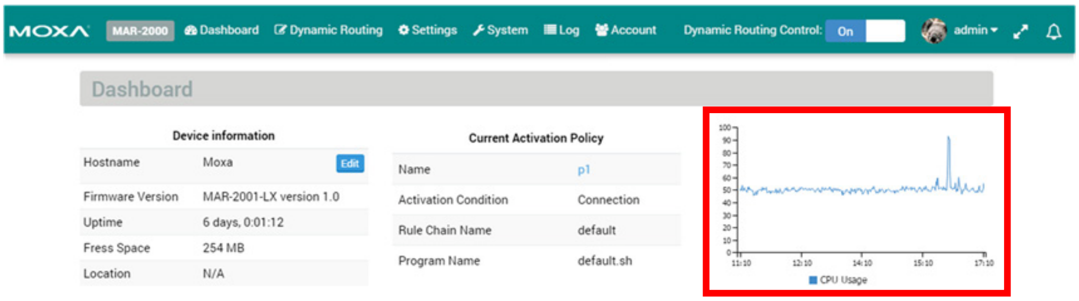
eth1

IP: 192.168.4.127
Netmask: 255.255.255.0
Gateway 192.168.4.254

Field	Description
Name	Shows which WAN zone the device is currently connected to.
Activation Condition	Shows which connection parameter the device has used to activate the current zone.
Rule Chain Name	Shows which firewall rule chain is currently being used.
Program Name	Shows the name of any scripts or programs currently activated under this zone.

CPU Usage Graph

The **CPU Usage** graph (as indicated in the following figure) shows the CPU load over the past six hours. The graph is generated based on the minute-by-minute information polling on the MAR-2000.



Dashboard

Device information

Hostname	Moxa	Edit
Firmware Version	MAR-2001-LX version 1.0	
Uptime	6 days, 0:01:12	
Fress Space	254 MB	
Location	N/A	

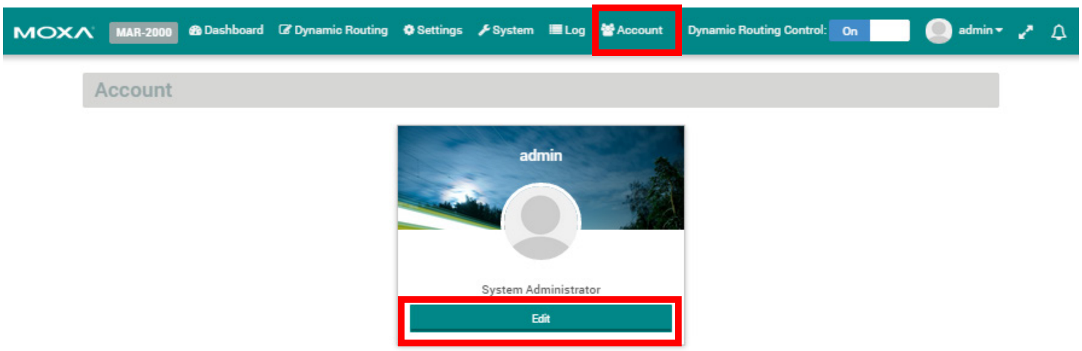
Current Activation Policy

Name	p1
Activation Condition	Connection
Rule Chain Name	default
Program Name	default.sh

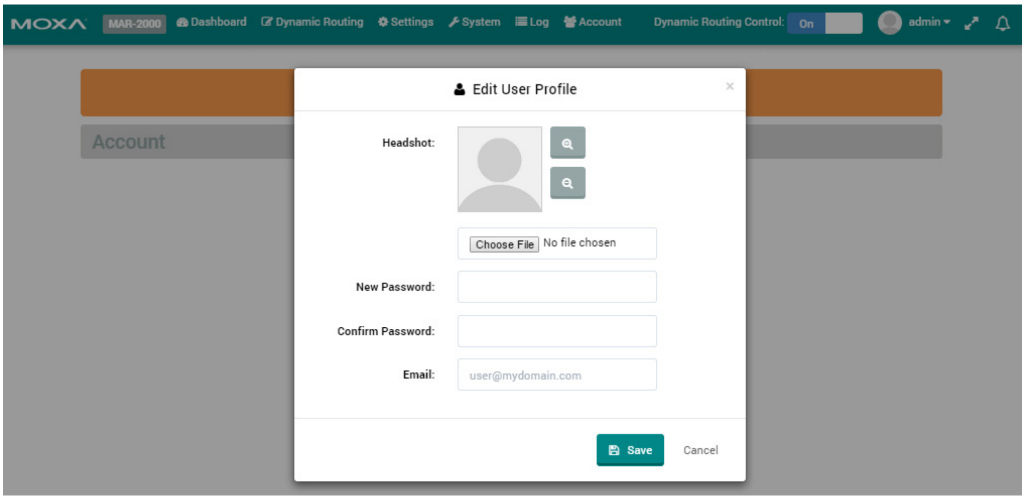
The Account Page

This page allows you to manage the administrative account. The MAR-2000 supports only one administrative account. Use the Account screen to reset the password and upload a photo.

Click **Edit** to edit your user profile.



In the Edit User Profile dialog box, configure the account settings. Then, click **Save** to save the settings and make the changes take effect.



Headshot:

Choose File No file chosen

New Password:

Confirm Password:

Email: user@mydomain.com

Field	Description
Headshot	Upload a user headshot by selecting an image file. You can edit the selected image with the zoom in and zoom out buttons, or by dragging the image.
New Password	Type the new password (must be at least five characters in length).
Confirm Password	Type the new password again to confirm.
Email	Type the administrator’s email address to which the system sends notifications.

3

Basic Settings

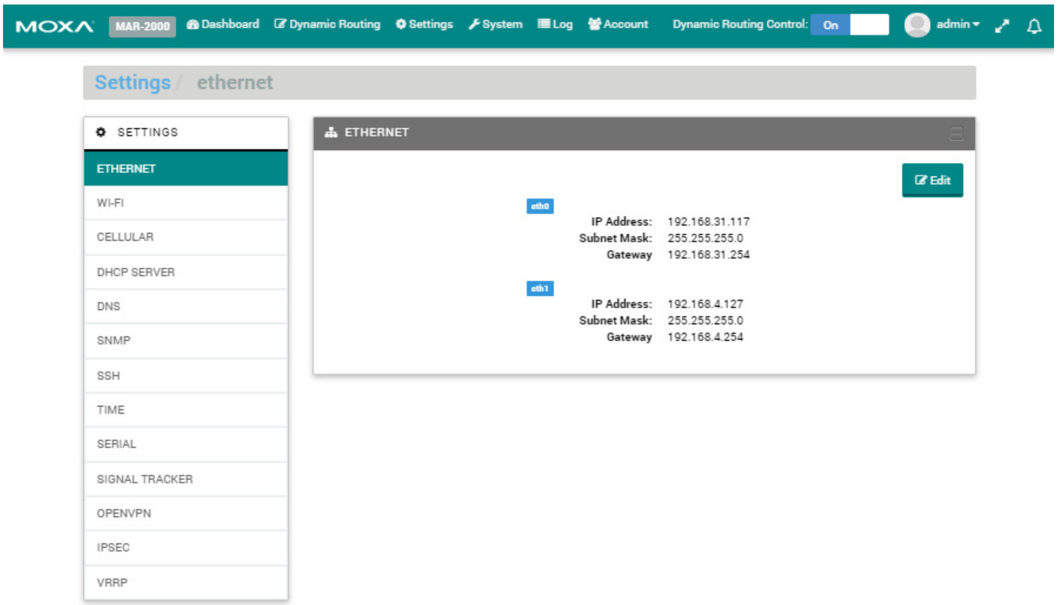
This chapter describes how to configure basic settings for the MAR-2000.

The following topics are covered in this chapter:

- **The MAR-2000 Settings Page**
- **Ethernet Interfaces**
  - Viewing Current Configuration
  - Configuring an Ethernet Interface
- **Wi-Fi Interface**
  - View Current Configuration
  - Configuring a WiFi Interface: AP
  - The Configuration Window: AP Blacklist
  - The Configuration Window: 802.11 Client
- **Cellular Interfaces**
  - View Current Configuration
- **DHCP Server**
  - DHCP Configuration Window
- **DNS Management**
  - DNS Configuration Window
- **SNMP Status Window**
  - SNMP Configuration Window
- **SSH Status and Configuration**
- **The System Time Status Window**
  - Software Clock Configuration Windows
- **Serial Port**
  - Serial Port Status Window
  - Serial Port Setup Window

The MAR-2000 Settings Page

Use the Settings page to configure your MAR-2000's network interfaces and services, and routing and security rules.



eth0
IP Address: 192.168.31.117
Subnet Mask: 255.255.255.0
Gateway 192.168.31.254

eth1
IP Address: 192.168.4.127
Subnet Mask: 255.255.255.0
Gateway 192.168.4.254

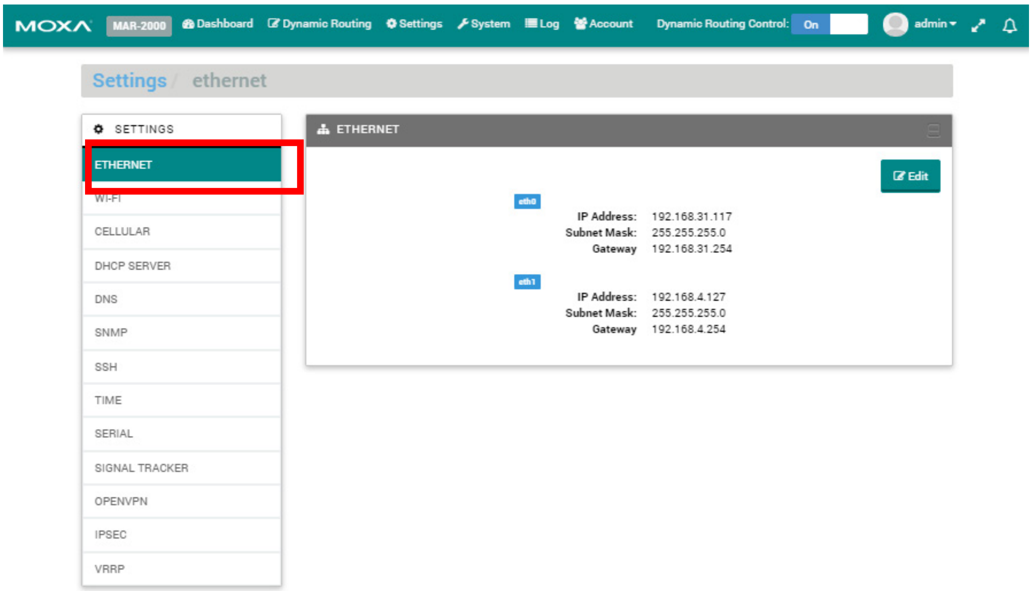
The following table lists the sub-sections of the **Settings** page.

Ethernet	**DNS**	**Serial**
Wi-Fi	**SNMP**	**Signal Tracker**
Cellular	**SSH**	**OpenVPN**
DHCP Server	**Time**	**IPSec**

For information on the Signal Tracker and OpenVPN screens, refer to the **The Signal Tracker** and **Setting up OpenVPN** chapters respectively.

Ethernet Interfaces

The MAR-2000 Ethernet interfaces can be configured either for LAN (internal) or WAN (external) service. You can also configure an interface to receive either a static or dynamic IP address. See the following sections to view and change the current settings.



eth0
IP Address: 192.168.31.117
Subnet Mask: 255.255.255.0
Gateway 192.168.31.254

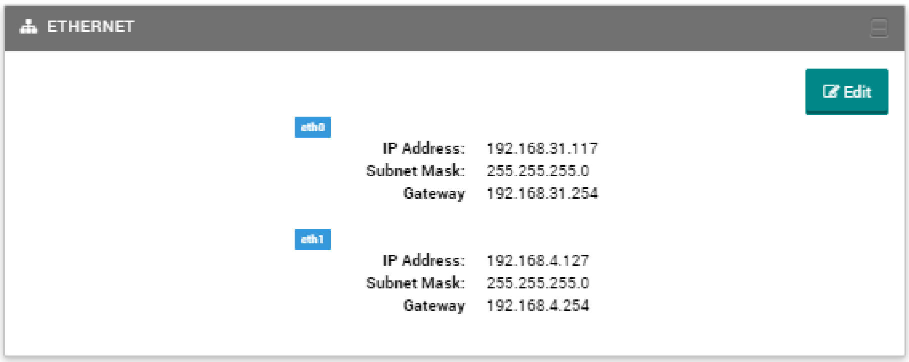
eth1
IP Address: 192.168.4.127
Subnet Mask: 255.255.255.0
Gateway 192.168.4.254

WARNING

If you change the settings on the **Ethernet** page and you have previously configured the interface as a DHCP server, the interface will stop assigning addresses. In this case, open the **DHCP Server** tab and restart the server.

Viewing Current Configuration

When you click the **ETHERNET** tab, a dialog box appears showing the current interface information. The following figure shows an example.



eth0

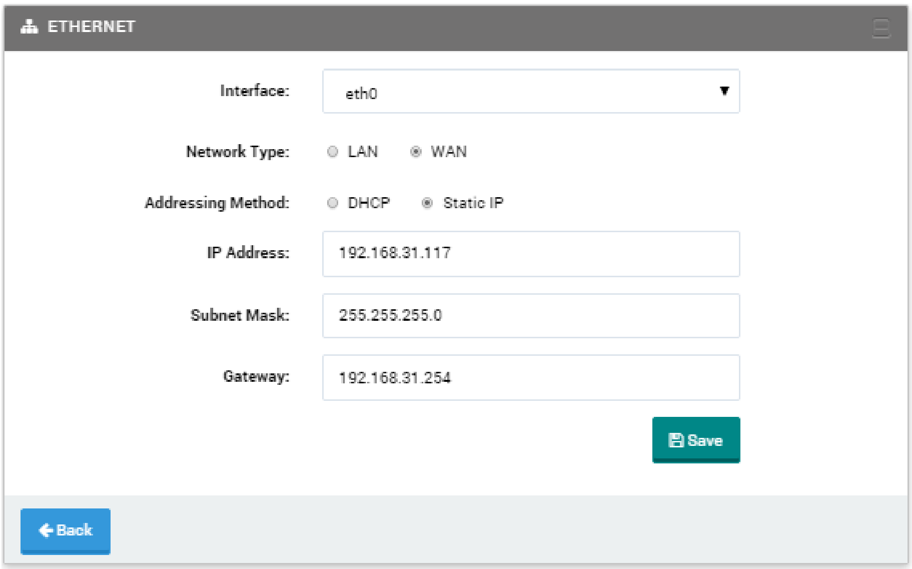
IP Address: 192.168.31.117
Subnet Mask: 255.255.255.0
Gateway 192.168.31.254

eth1

IP Address: 192.168.4.127
Subnet Mask: 255.255.255.0
Gateway 192.168.4.254

Configuring an Ethernet Interface

To configure an Ethernet interface, click **Edit** to display the configuration screen. The following figure shows an example.



Interface: eth0 ▾

Network Type: ○ LAN ● WAN

Addressing Method: ○ DHCP ● Static IP

IP Address: 192.168.31.117

Subnet Mask: 255.255.255.0

Gateway: 192.168.31.254

After you configure the settings for an interface, click **Save** to save the settings and make the changes take effect.

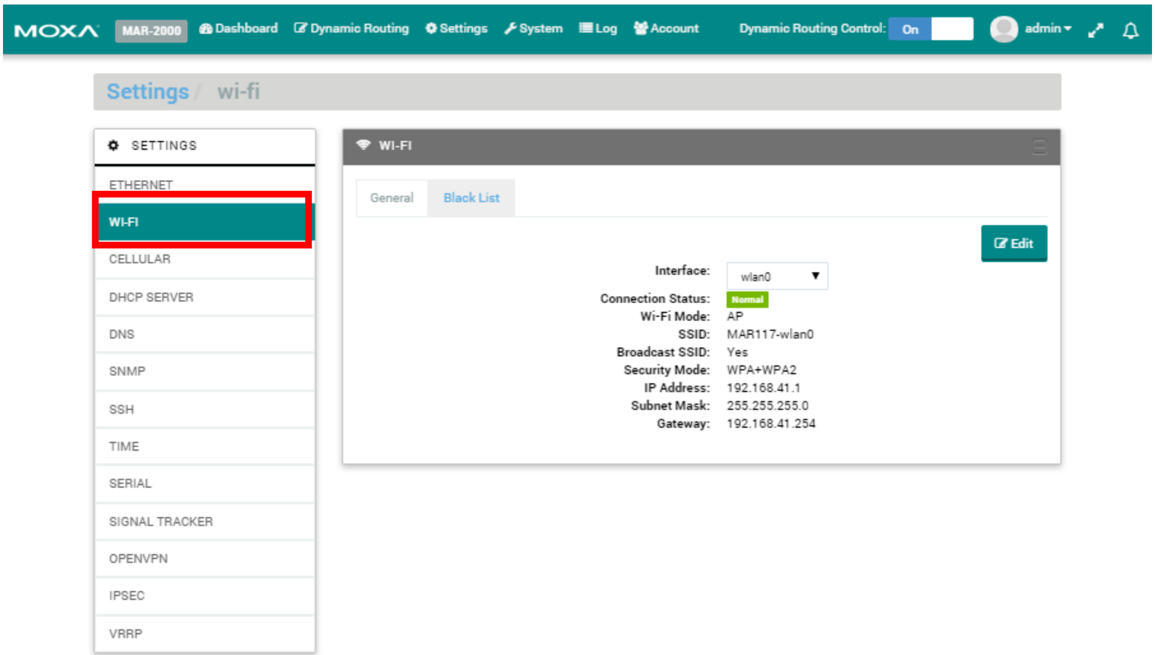
The following table describes the fields in this screen.

Field	Description
Interface	Select an interface (for example, eth0 or eth1) from the drop-down list.
Network Type	Set the interface for use as a WAN client (external) or as a LAN server (internal)
Addressing Method	Set the interface to use a static IP address (Static IP) or dynamic IP address (DHCP).
IP Address	If you select the Static IP addressing method, enter the static IP address (for example, 192.168.3.127).
Subnet Mask	If you select the Static IP addressing method, enter the subnet mask (for example, 255.255.255.0) to specify the network size.
Gateway	Enter the IP address of the default gateway for the interface.

Wi-Fi Interface

You can use the **Wi-Fi** tab to configure the 802.11 wireless interfaces. You can set each interface as an 802.11 access point (to set up a wireless network) or as an 802.11 client (to connect to a wireless network).

From the **Settings** menu, click **WI-FI** to display the status screen.



Interface: wlan0
Connection Status: Normal
Wi-Fi Mode: AP
SSID: MAR117-wlan0
Broadcast SSID: Yes
Security Mode: WPA+WPA2
IP Address: 192.168.41.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.41.254

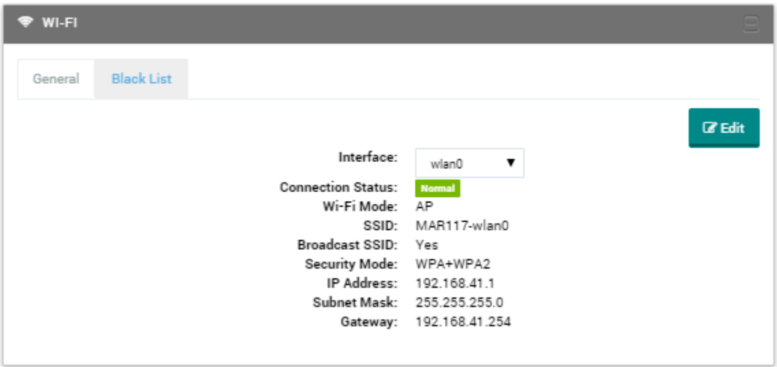
ATTENTION

The **MAR-2001-T** has **two** 802.11n interfaces and **two** 3G cellular interfaces.
The **MAR-2002-T** has **one** 802.11n interface and **three** 3G cellular interfaces.

View Current Configuration

The status window shows the wlan0 interface. The wlan0 interface is configured as an 802.11 access point (AP), and the Normal status shows that it is operating properly.

To configure a wireless interface, open **Configuring a WiFi Interface: AP** by clicking **Edit**.



Interface: wlan0
Connection Status: Normal
Wi-Fi Mode: AP
SSID: MAR117-wlan0
Broadcast SSID: Yes
Security Mode: WPA+WPA2
IP Address: 192.168.41.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.41.254

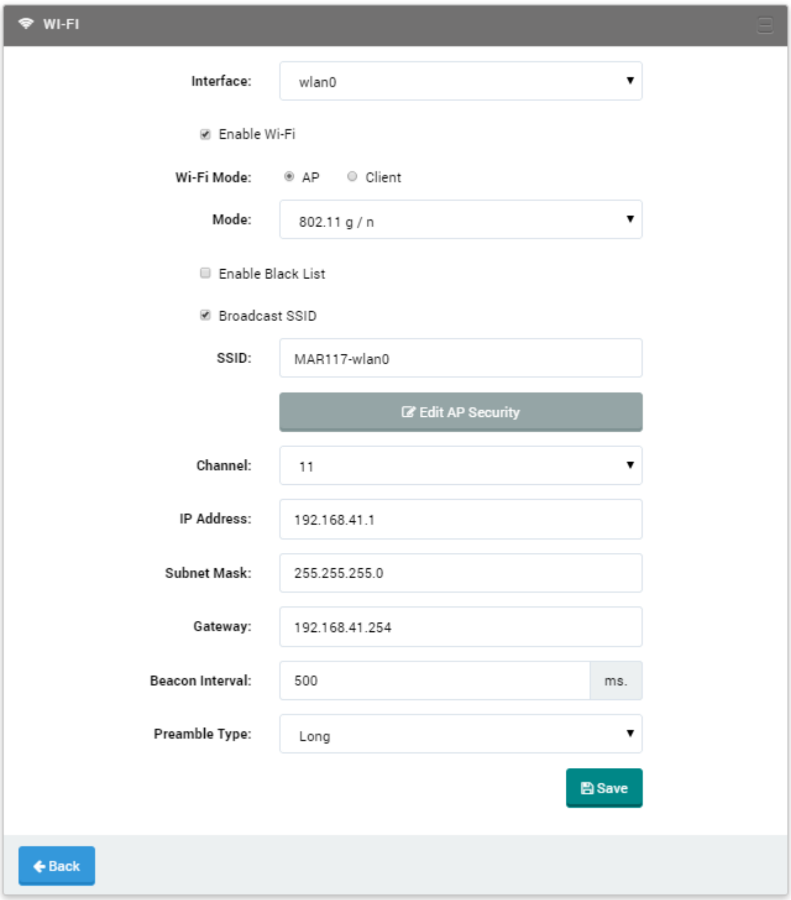
The following table describes the fields.

Field	Description
Interface	**Select the interface you want to display (for example, wlan0 or wlan1).**
Connection Status	Shows the current status of the interface: Normal or Abnormal. Go to the Log page to check if it shows Abnormal.
Wi-Fi Mode	Shows whether the interface is configured as an 802.11 Access Point (AP) or Client
SSID	The network identifier (SSID) the AP will use to identify itself to supplicant clients
Broadcast SSID	Choose to publicly broadcast the SSID or keep the SSID private.
Security Mode	Shows which security protocol (if any) is being used to encrypt communications on the interface. Choices are: None, WPA, WPA2, WPA+WPA2, or RADIUS.
IP Address	Shows the IP address of the access point.
Subnet Mask	Shows the subnet mask, for determining the size of the network.
Gateway	Shows the default gateway the interface will communicate with.

Configuring a WiFi Interface: AP

This example describes how to configure an 802.11 interface as a wireless access point.

NOTE After updating the configuration for the selected interface, click **Save** to save the settings and make the changes take effect. If you navigate away from the configuration screen without saving, the system discards the changes.



WI-FI

Interface: wlan0

☑ Enable Wi-Fi

Wi-Fi Mode: ● AP ○ Client

Mode: 802.11 g / n

□ Enable Black List

☑ Broadcast SSID

SSID: MAR117-wlan0

Channel: 11

IP Address: 192.168.41.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.41.254

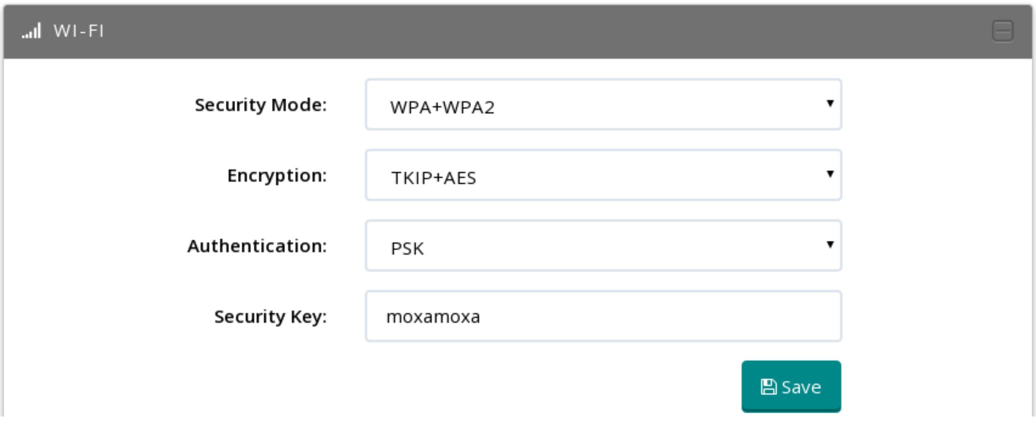
Beacon Interval: 500 ms.

Preamble Type: Long

The following table describes the fields.

Field	Description
Interface	Select an interface you want to configure from the drop-down list. If an Ethernet interface is installed but not shown in the drop-down list, there may be a problem with its base configuration (such as the kernel module)
Enable Wi-Fi	Select this checkbox to enable the selected wireless interface.
Wi-Fi Mode	Sets the interface to serve either as an Access Point (AP) or an 802.11 client.
Mode	Sets which version of 802.11 the interface will communicate with. The value used depends on client hardware, but setting this to 802.11n is probably the safest setup: along with strong improvements in speed, 802.11n has full backwards compatibility with all other 802.11 protocols. To set up full 802.11n broadcast capabilities, you will need two radio modules set as APs, with one on the 802.11a/n range, and the other on the 802.11b/n range. The MAR-2000 does not provide MIMO capabilities.
Enable Black List	Select this checkbox to enable the MAC address black list function.
Broadcast SSID	Select to enable or disable SSID broadcasting.
SSID	Sets the wireless network’s SSID (up to 32 characters).
Channel	Sets the broadcast channel for this interface; useful for resolving interference problems.
IP Address	Sets the Access Point’s IP address.
Subnet Mask	Sets the subnet mask, which determines the number of available addresses on the LAN served.
Gateway	Sets the IP address for the default routing gateway.
Beacon Interval	Sets the frequency interval for the beacon, which is a packet broadcast by the AP to synchronize the wireless network. The interval range is between 15 and 65,000, with intervals of 1.024 milliseconds (rather than exactly 1). Approximately 100 ms is suitable for most environments. 50 ms is typical in areas with poor reception, but this may result in increased bandwidth overhead and power draw.
Preamble Type	The preamble is used by the AP to notify attached clients that data is on its way. Preamble values may be long or short, and this setting may be configured to predict and automatically serve attached clients. Long preambles are undesirable, and are deprecated for most clients. Unless the access point is serving 802.11b clients, there is no need for a long preamble; but if 802.11b clients are a possibility, then select Auto.

The Access Point Security Configuration Window



Security Mode: WPA+WPA2

Encryption: TKIP+AES

Authentication: PSK

Security Key: moxamoxa

Field	Description
Security Mode	None, WEP, WPA, WPA2, WPA+WPA2, and RADIUS; each of these is explained in detail in the Protocols and Encryption Algorithms section.
Encryption	Selects the data encryption algorithm that will be used. Note that TKIP has been deprecated since 2012, and is no longer considered secure. For strong, secure encryption, AES is the only choice.
Authentication	PSK (pre-shared key) is designed for home and small office networks and doesn't require an authentication server.
Security Key	Enter a pre-shared or enterprise key.

Protocols and Encryption Algorithms

Network negotiations and encrypted transmissions are the guarantees that keep communications between an 802.11 AP and clients secure from eavesdropping by random strangers. A strongly encrypted security layer is also a factor in protecting your AP against hostile hacking. The AP security window allows you to configure encryption and authorization protocols for 802.11 interfaces. To access the security configuration window, click **Edit AP Security**.

You can select one of four encryption methods: **None**, **WEP**, **WPA** (including WPA, WPA2, and WPA+WPA2), and **RADIUS**. By default, the MAR-2000 uses pre-shared key (PSK) encryption with WPA-WPA2 / TKIP-AES algorithms. The following sections describe each method.

None

No security is used. This option is not recommended, but may be used where communications are intended to be freely available to any clients within the broadcast area.

WEP

Wired Equivalent Privacy (WEP) is a basic security protocol for wireless networks. Note that WEP provide simple data encryption that can be easily broken.

Field	Description
Default Tx Key	Default key for data encryption.
Key 1 to Key 4	WEP keys in HEX or ASCII. For ASCII, the length will be 5, 13, 16, or 29 characters. For hexadecimal keys, the format will be 10, 26, 32, or 58 characters.

WPA / WPA2 / WPA+WPA2

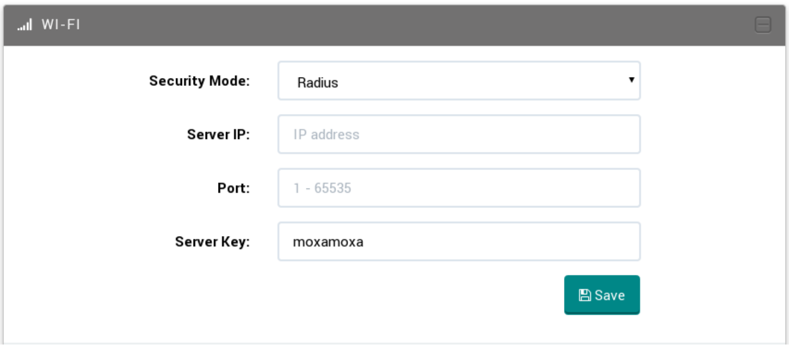
WPA was the Wi-Fi Alliance's response to the critical weaknesses in WEP; it is essentially a wrapper around the WEP protocol, with a few enhancements in encryption and authentication. While WPA was a huge improvement over WEP, it still shared significant security flaws with its predecessor, and is now also deprecated. WPA is not recommended for regular use.

The strongest protocol currently available is WPA2, or IEEE 802.11i-2004. WPA2 has been mandatory for Wi-Fi–certified devices since 2006, and is fully compatible with all 802.11 interfaces made since.

WPA+WPA2 is an operation mode that permits an access point to associate with a client using either WPA/TKIP (a weak, deprecated encryption protocol), or WPA2/AES clients. If some wireless clients can do WPA2 but others only WPA then set the router for WPA+WPA2 with **TKIP+AES**. This will allow your access point to connect with either WPA2 or WPA clients.

RADIUS

When the **Security Mode** is set to **RADIUS**, the AP may be configured to serve as the front-end for a RADIUS AAA (Authentication, Authorization, and Accounting) server. The MAR-2000 uses Protected EAP (PEAP) as its authentication protocol; PEAP uses TLS encryption.



Security Mode: Radius

Server IP: IP address

Port: 1 - 65535

Server Key: moxamoxa

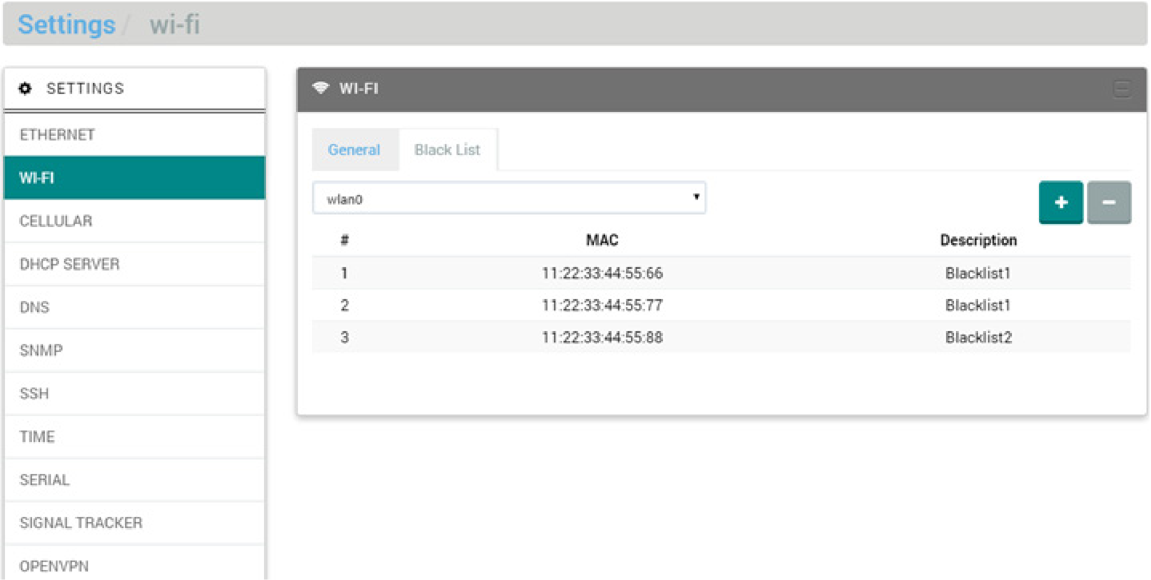
Field	Description
Server IP	The public IP address for the RADIUS gateway.
Port	The port over which RADIUS negotiations are communicated by the gateway.
Security Key	The Security Key is a key stored on both the RADIUS client and server; it is used to aid in encryption and to verify message integrity. Shared keys are case sensitive, should be randomized lists of characters (i.e., not words found in a dictionary), should include numbers and special characters, and should be greater than 22 characters in length. For maximum security, use a key that is 128 characters long. The Security Key should never be transmitted over the Internet.

WARNING

If the **802.11/Wi-Fi** configuration is changed and you have previously configured the interface as a DHCP server, the interface will stop serving addresses. You must return to the **DHCP Server** tab and re-start the server.

The Configuration Window: AP Blacklist

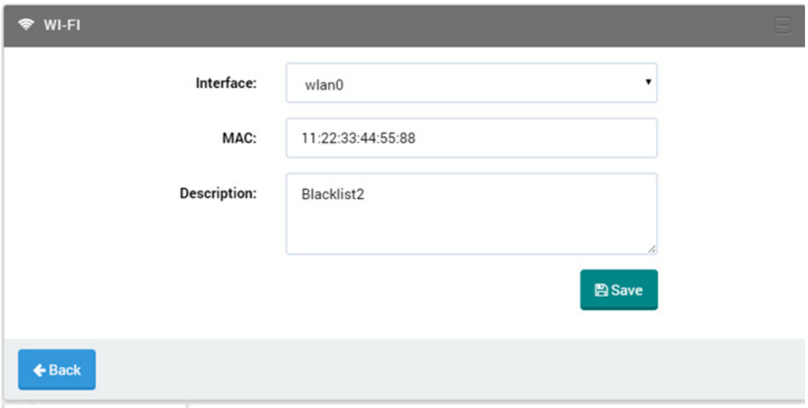
You can configure the **Black List** tab to block connection from un-wanted MAC addresses.



wlan0

#	MAC	Description
1	11:22:33:44:55:66	Blacklist1
2	11:22:33:44:55:77	Blacklist1
3	11:22:33:44:55:88	Blacklist2

Click + to display the Black List editing page.



Interface: wlan0

MAC: 11:22:33:44:55:88

Description: Blacklist2

Field	Description
Interface	Select the interface you wish to configure from the drop-down list.
MAC	Enter the MAC address that you want to block access to the interface.
Description	Enter a description for this configuration.

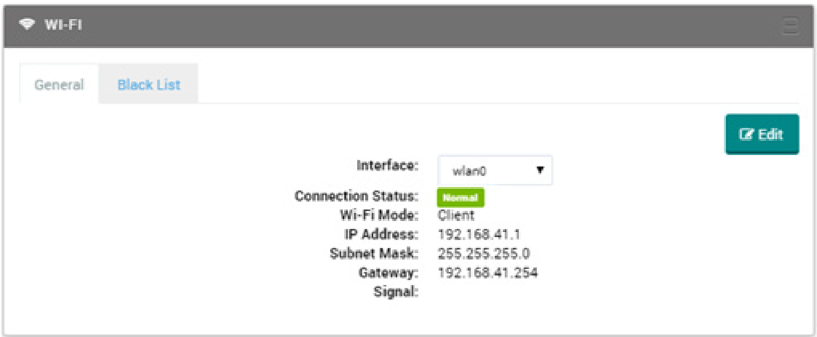
The Configuration Window: 802.11 Client

The MAR-2000 uses the **`wpa-supplicant`** utility to configure interfaces as wireless clients. Multiple WANs may be configured, and prioritized. A higher priority means the network is preferred over those that follow.

NOTE After updating the configuration for the selected interface, click **Save** before selecting another interface from the drop-down box; otherwise, your changes will not be saved.

The Status Window

The following settings show that *wlan0* is configured as a wireless client and is operating normally (**Normal**). The meaning of each field under client mode is shown below:

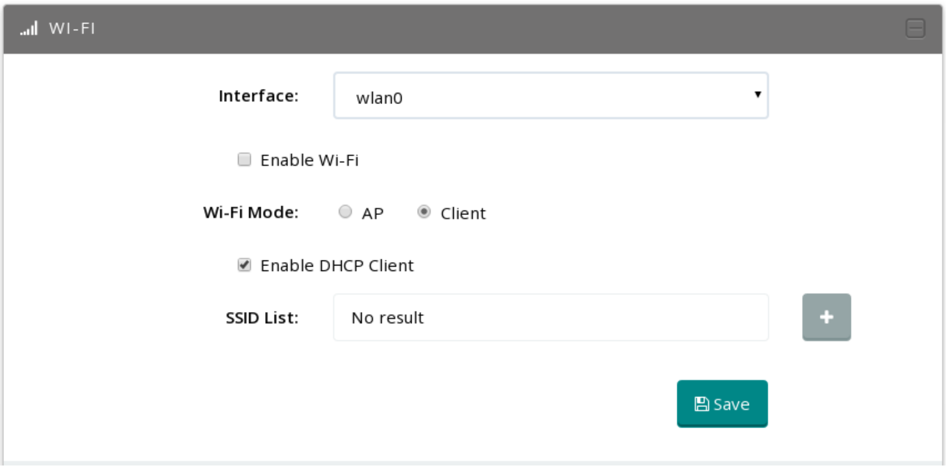


Interface: wlan0
Connection Status: Normal
Wi-Fi Mode: Client
IP Address: 192.168.41.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.41.254
Signal:

Field	Description
Interface	Select the interface you wish to configure from the drop-down list. If an interface is not listed, it is not being detected by the system, which is most often because of an issue with the kernel module.
Status	Current status of the interface: Normal or Abnormal. Go to Log page to check if it shows Abnormal.
Wi-Fi Mode	Sets the interface to serve either as an AP or client (here it is a client).
IP Address	Shows the client's IP address.
Subnet Mask	Shows the subnet mask, which determines the number of available addresses on the LAN served.
Gateway	Shows the IP address for the default routing gateway.
Signal	Shows the current signal level (in dBm).

Editing an 802.11 Client Configuration

Click **Edit** to open the configuration page for the wireless client. At least one SSID item must be entered into the **SSID List** or the client will not be able to connect to an AP.



Interface: wlan0

□ Enable Wi-Fi

Wi-Fi Mode: ○ AP ● Client

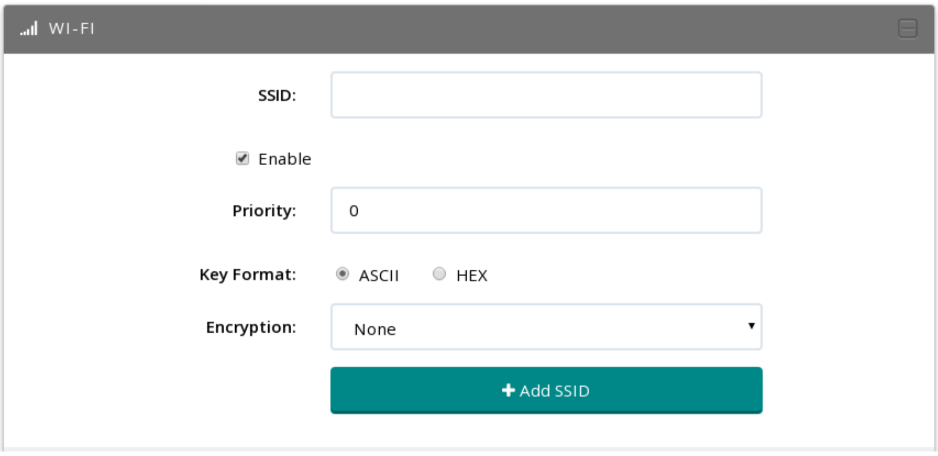
☑ Enable DHCP Client

SSID List: No result

Field	Description
Interface	Selects an interface.
Enable Wi-Fi	Enables or disables the interface.
Wi-Fi Mode	Sets the interface as either a client or an access point (here, it is set to Client).
Enable DHCP Client	This sets up the interface to receive a dynamic IP from a DHCP server. If this is left unchecked, then a static IP address must be configured.
IP Address	The IP address the client is currently using.
Subnet Mask	The subnet mask for the interface
Gateway	The default gateway for the interface
SSID List	A list of SSIDs the client may connect to, with highest priority listed first. SSIDs are identifiers that are broadcast as beacons by a wireless AP.

Adding an SSID

In order for an 802.11 client to connect to a network, it must first have the network identified in its SSID list. To add a network to the SSID list, click the **+** button to open the **ADD an SSID** window, shown below.



SSID:

☑ Enable

Priority: 0

Key Format: ● ASCII ○ HEX

Encryption: None

These are the settings for an SSID entry:

Field	**Description**
SSID	An identifier of up to 32 characters, used to distinguish available wireless networks.
Enable	Indicates to the client that it may search for and associate with this network.
Priority	The priority for the network (higher numbers indicate higher priority.
Key Format	ASCII or HEX
Encryption	Select a security method from the drop-down list. The following sections describe the configuration fields for each method.

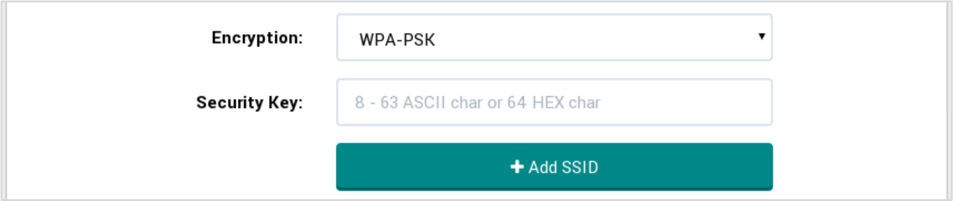
Configuring 802.11 Client Security

Clients may choose from three types of security: WEP, WPA-PSK, or WPA-EAP. It is also possible to configure the interface for no encryption by choosing None, but this is not recommended.

WEP

Moxa does not endorse the use of WEP encryption.

WPA-PSK: WPA With a Pre-Shared Key

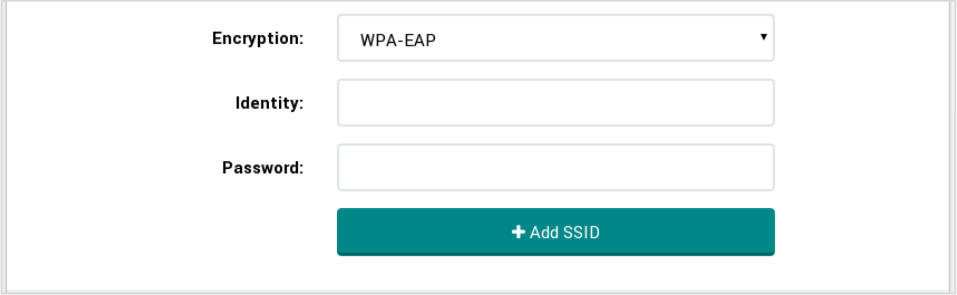


Encryption: WPA-PSK

Security Key: 8 - 63 ASCII char or 64 HEX char

In the **Security Key** field, enter the pre-shared key, 8 to 63 characters for ASCII or 64 characters for HEX.

WPA-EAP



Encryption: WPA-EAP

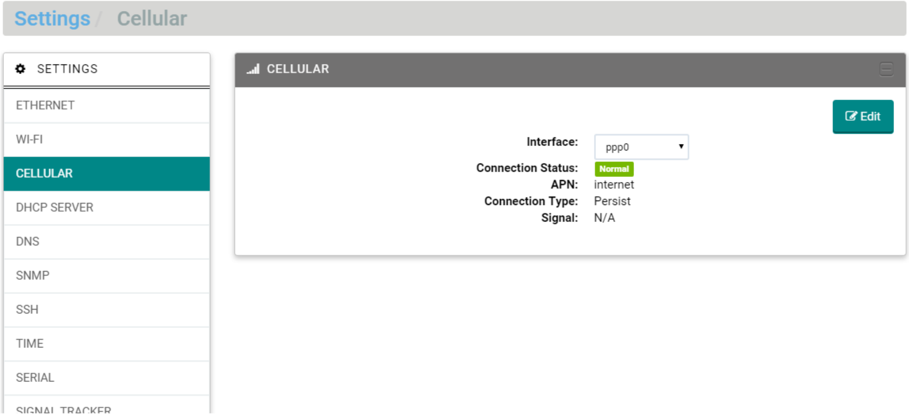
Identity:

Password:

Field	Description
Identity	The identity of the authentication server.
Password	The password of the authentication server.

Cellular Interfaces

Click the **Cellular** tab to display the cellular interfaces status window.



Interface: ppp0
Connection Status: Normal
APN: internet
Connection Type: Persist
Signal: N/A

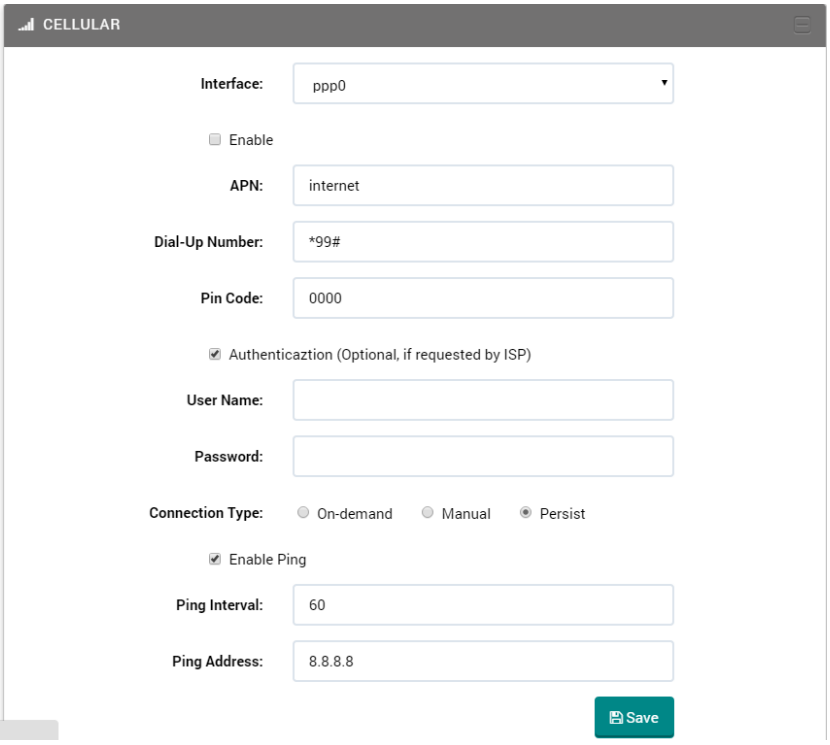
Field	Description
Module	Lists all cellular modules by their Linux device name; e.g., ppp0, ppp1, etc. If a device is not listed, it has not been detected by the system.
Status	Indicates if the interface is functioning properly (Normal) or not (Abnormal). Go to Log page to check if it shows Abnormal.
APN	Displays the currently configured Access Point Name (APN).
Connection Type	Displays current connection type: • Manual • On-demand • Persist
Signal	Current signal level, displayed in dBm (decibel-milliwatts)

Click **Edit** to open the cellular configuration window.

View Current Configuration

The configuration window allows you to set the properties for the cellular interfaces.

Click **Save** before selecting another interface from the drop-down box; otherwise, your changes will not be saved).



Interface: ppp0

□ Enable

APN: internet

Dial-Up Number: *99#

Pin Code: 0000

☑ Authenticaztion (Optional, if requested by ISP)

User Name:

Password:

Connection Type: ○ On-demand ○ Manual ● Persist

☑ Enable Ping

Ping Interval: 60

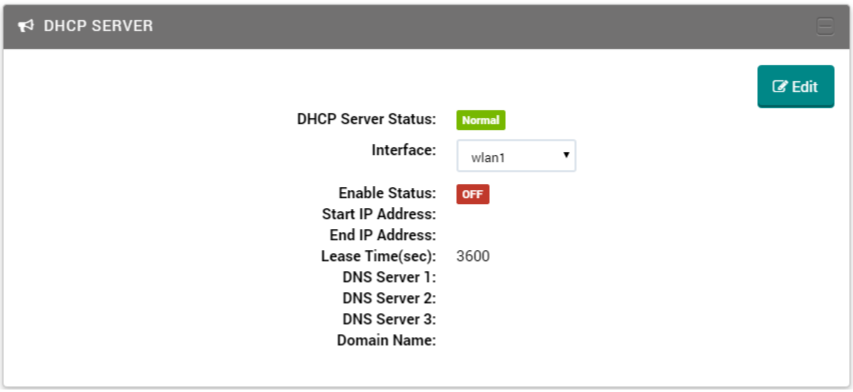
Ping Address: 8.8.8.8

Field	Description
Interface	Lists all of the available cellular interfaces using Linux device conventions: e.g., ppp0, ppp1, etc. Select a device from the drop-down list to configure it.
Enable	Check this box to enable a selected device. For Enabled devices, all changes will be applied (including the execution of the dialup command) as soon as you save the settings. Note: Each interface needs to be saved after it is updated.
APN	Enter the APN assigned to you by your ISP. The APN (Access Point Name) is a network identifier used by cellular providers to determine what sort of network your device should be assigned to, and what parameters are associated with it.
Dial-Up Number	This box allows you to change the ATD prefix the computer must dial to connect to a cellular network (i.e., to initiate a layer 2 connection). This number sometimes changes according to region and country. Check with your service provider, or try searching the Internet to find the appropriate ATD prefix for your area.
Pin Code	Enter the PIN code of the cellular module.
Enable Authentication	If necessary, contact your ISP for the authentication information.
Connection Type	Choose one of the following connection types: • On-demand–The computer will maintain a connection to the cellular network only when the network is active. If the computer is idle for longer than the configured idle time, the cellular connection will be terminated. After choosing an on-demand connection, a configuration box titled Idle Time will appear. Enter a timeout value (in seconds) for idle connections. • Manual–Connection to the cellular network can only be initiated manually, by the system administrator. • Persist–Provides a continuous live connection to the cellular module.

DHCP Server

Click the **DHCP Server** tab to display the DHCP server status window.

Click **Edit to** open the DHCP server configuration window.



DHCP Server Status: Normal
Interface: wlan1
Enable Status: OFF
Start IP Address:
End IP Address:
Lease Time(sec): 3600
DNS Server 1:
DNS Server 2:
DNS Server 3:
Domain Name:

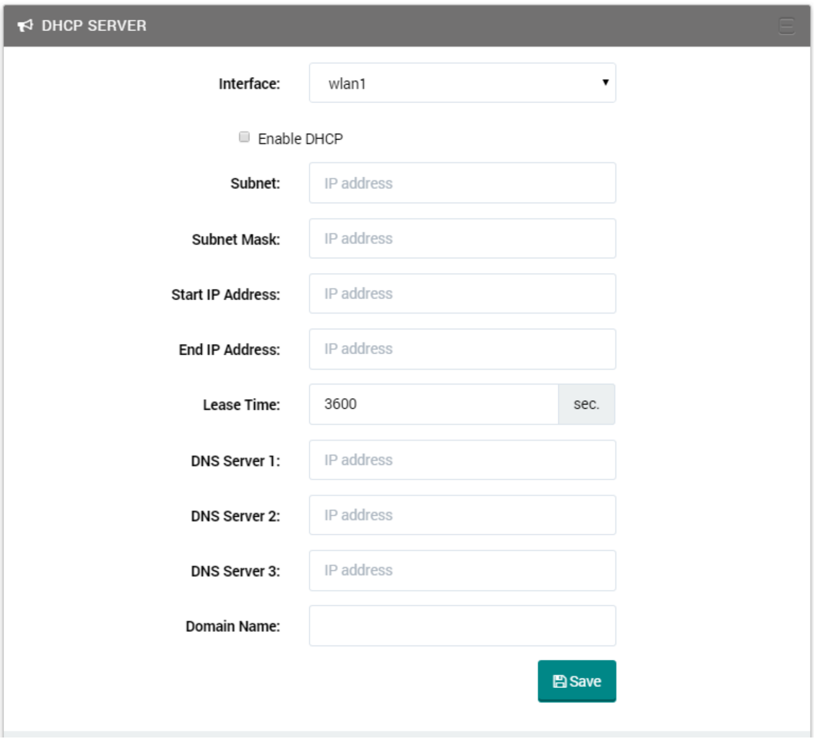
Field	**Description**
DHCP Server Status	Indicates if the DHCP server status is normal or abnormal. Go to Log page to check if it shows abnormal.
Interface	This is a list of all available network interfaces (e.g., eth0, wlan0, ppp0, etc.). Select which interface is configured with a DHCP server.
Enable Status	Indicates whether or not the selected interface is configured with a DHCP server.
Start IP	The DHCP server will assign IP addresses between the "Start IP" and the "End IP".
End IP	
DNS Server 1/2/3	Currently configured DNS servers 1/2/3.
Domain Name	Current domain name.
Lease Time(sec)	Current lease time for the DHCP server (in seconds)

ATTENTION

If the status is abnormal, click the **Edit** button and then check the configuration of the interface and DHCP server.

DHCP Configuration Window

The configuration window allows you to configure a DHCP server for any available interface. Click **Save** to save the settings and restart the DHCP Server.



DHCP SERVER

Interface: wlan1

□ Enable DHCP

Subnet: IP address

Subnet Mask: IP address

Start IP Address: IP address

End IP Address: IP address

Lease Time: 3600 sec.

DNS Server 1: IP address

DNS Server 2: IP address

DNS Server 3: IP address

Domain Name:

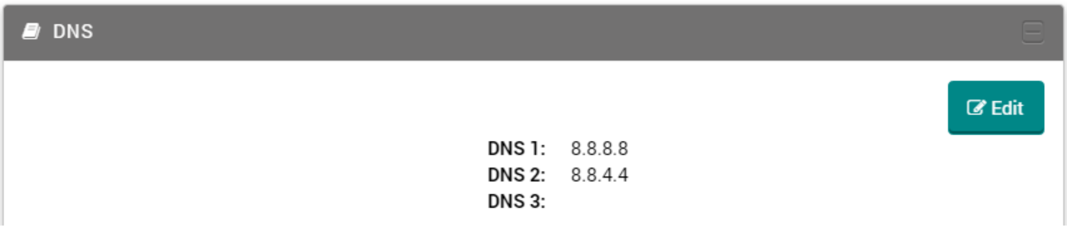
Field	Description
Interface	Lists all available network interfaces. Select which interface you would like to configure with a DHCP server.
Enable DHCP	Select to activate the DHCP server on the selected interface.
Subnet	An IP address that provides a template for IP addresses allowed on the subnet.
Subnet Mask	Determines, together with the subnet address, which IP addresses will be allowed on the subnet.
Start IP Address	The DHCP server will assign IP addresses between the “Start IP” and the “End IP”.
End IP Address	
DNS Servers 1/2/3	Enter IPs for up to 3 DNS servers; they will be prioritized in numerical order, with 1 as the default.
Domain Name	To separate local devices into network segments (for easier administration and identification), each cellular port may be configured with its own, distinct domain name.
IP Lease Time (sec)	Enter the default time, in seconds, the DHCP server will lease an IP address without renewal.

WARNING

If the **802.11/Wi-Fi** or **Ethernet** configuration is changed, the DHCP server automatically stops. After you change the DHCP server settings of an interface, you must go to the **DHCP Server** tab and re-start the server.

DNS Management

Click the **DNS** tab to enter the DNS status view. Click **Edit** to display the configuration window.



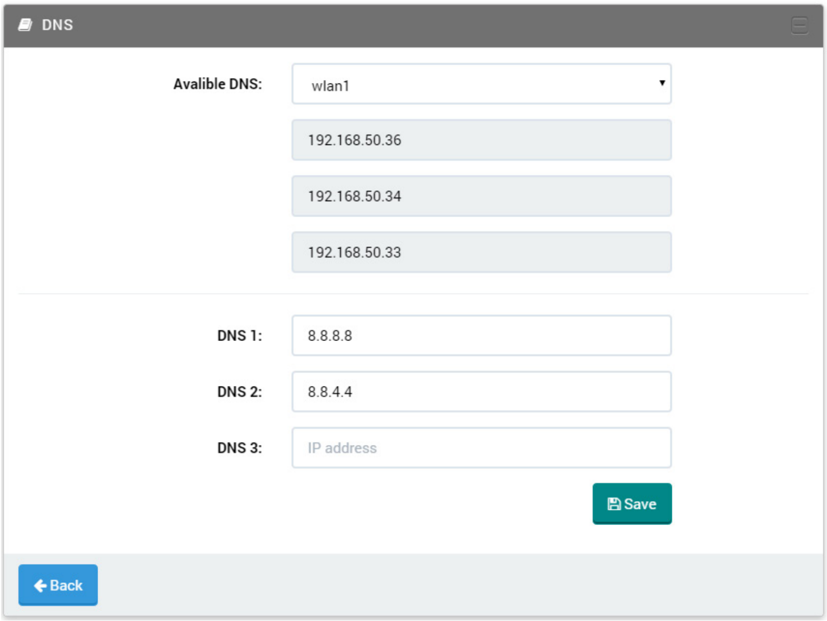
DNS 1: 8.8.8.8
DNS 2: 8.8.4.4
DNS 3:

DNS servers are prioritized from **1** (the default/main DNS) to **3** (lowest in the hierarchy).

Field	Description
DNS1	Current machine’s main DNS (Domain Name System).
DNS2	The most preferred alternative DNS server.
DNS3	The least preferred alternative DNS server.

DNS Configuration Window

Use the DNS configuration screen to configure the DNS server information for the selected interface. Click **Save** to save and make the changes take effect.



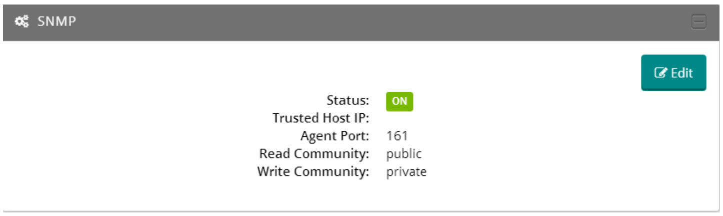
Avalible DNS: wlan1
192.168.50.36
192.168.50.34
192.168.50.33
DNS 1: 8.8.8.8
DNS 2: 8.8.4.4
DNS 3: IP address

Field	Description
DNS 1	This is the main DNS server for this interface. It may use a local (LAN) address.
DNS 2/ DNS 3	These are alternative DNS servers that are used if the default server (DNS1) is not available.

SNMP Status Window

The SNMP (SNMP v1, SNMP v2c, SNMP v3) status window displays all of the current information about the MAR-2000's local SNMP agent; this is the service that your MAR-2000 router uses to communicate with a remote network management station (NMS). **Status** indicates if the local agent is **ON** or **OFF**.

Click **Edit** to display the SNMP configuration window.



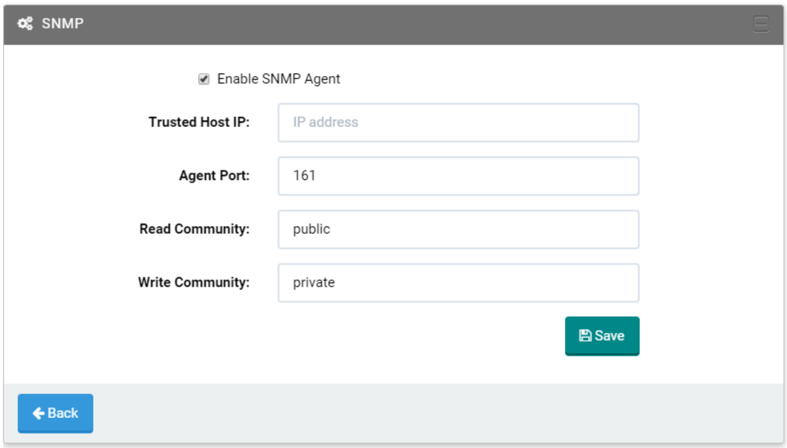
Status: ON
Trusted Host IP:
Agent Port: 161
Read Community: public
Write Community: private

ATTENTION

The SNMP agent on the MAR-2000 does not support traps (i.e., notifications sent from the local *agent* to the remote *manager)*. This means that while the MAR-2000 may be monitored by a remote NMS, it is not possible to configure the MAR-2000 to deliver messages or alarms by snmp.

SNMP Configuration Window

The following figure shows the settings page of the SNMP agent. Be sure to click the **Save** button to save the settings to the system after you have made the changes.



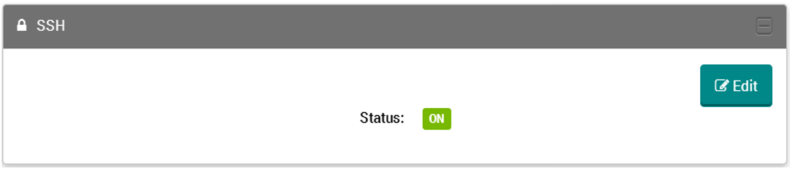
☑ Enable SNMP Agent
Trusted Host IP: IP address
Agent Port: 161
Read Community: public
Write Community: private

Field	Description
Enable SNMP Agent	Check the box to Enable the local SNMP agent. Unchecked means it is Disabled.
Trusted Host IP	This is the IP address of the computer host that your network management station (NMS) resides on, and to which your local agent will respond. Note: The MAR-2000 does not support multi-trusted IPs.
Agent Port	Resets the port number over which the local Agent will listen for requests from the remote NMS. The default port is 161 for general messages (the MAR-2000 does not support traps, i.e., active local messaging), but you will need to change this if the remote NMS has been configured to communicate over a different port.
Read Community	Input a key to associate this device with a community of other SNMP agents and management stations. This string effectively serves as a password that allows other devices within that community to read data from this device.
Write Community	Input a key that identifies this device as part of a Read-Write community, giving other devices that share the same string read-write permissions to the SNMP strings.

SSH Status and Configuration

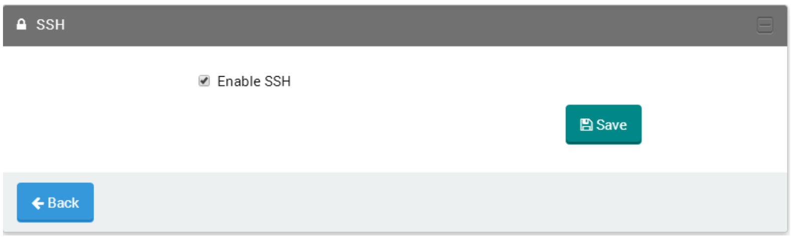
SSH is a secure replacement for TCP that allows users to log in to the computer console from a remote source using a program like **PuTTY**, or some other SSH client.

To see the status of the SSH daemon, click the **SSH** tab.



To enable or disable SSH, click **Edit**.

Select the **Enable SSH** check box to enable SSH; otherwise, clear the check box. Then, click **Save** to save the changes and make the changes take effect.



When the SSH daemon is enabled, users can remotely log in to the local console using the system user account and password.

ATTENTION

To keep your equipment secure, we strongly recommend changing the Web and Console passwords.

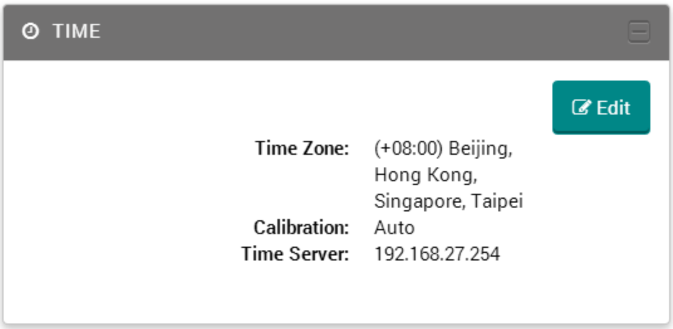
ATTENTION

If you disable SSH, you cannot log in to the system remotely using an SSH client (such as PuTTY).

The System Time Status Window

The system time status window shows the system time, whether the device is using Network Time Protocol (NTP), and what NTP server is being used (if any).

Click **Edit** to display the configuration window.



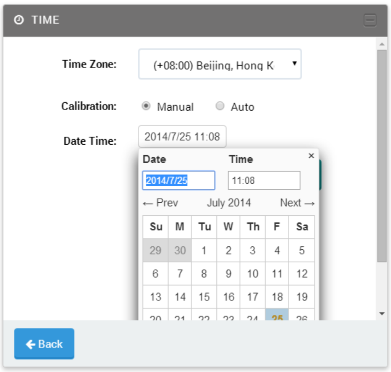
Time Zone: (+08:00) Beijing, Hong Kong, Singapore, Taipei
Calibration: Auto
Time Server: 192.168.27.254

Field	Description
Time Zone	Current time, and the current time zone for which the device is configured (this is not automatically adjusted; it must be changed through the configuration interface).
Calibration	Current means of setting the time: Automatic or Manual
Time Server	Current NTP Server address (only enabled when Calibration is set to Auto).

Software Clock Configuration Windows

The software clock configuration window lets you set the system clock for manual or automated management.

The Manual Configuration Window



TIME

Time Zone: (+08:00) Beijing, Hong K

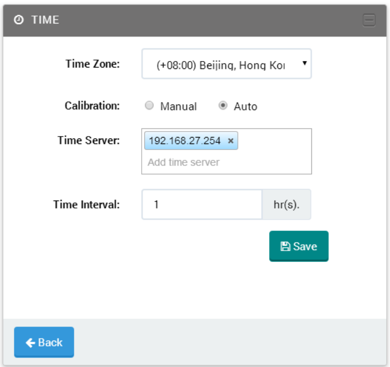
Calibration: ● Manual ○ Auto

Date Time: 2014/7/25 11:08

Date: 2014/7/25

Time: 11:08

The Auto Configuration Window



TIME

Time Zone: (+08:00) Beijing, Hong Koı

Calibration: ○ Manual ● Auto

Time Server: 192.168.27.254 ×

Add time server

Time Interval: 1 hr(s).

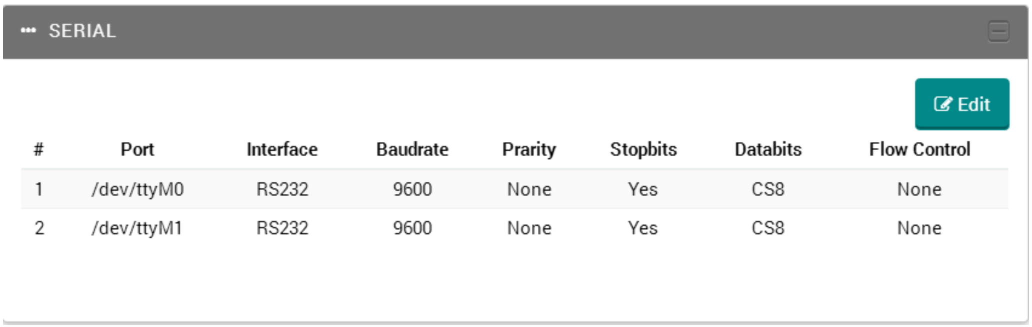
Field	Description
Time Zone	Enter the base time zone the device will use.
Calibration	Select one of the following options to set the clock: • Manual: Allows you to specify the date and time manually. • Auto: To synchronize the system time with a remote NTP server, you must configure the following fields to specify the Time Server and Time Interval.
Time Server	If you select the **Auto** calibration method, enter the IP address of an NTP server. You may add more than one time server.
Time Interval	If you select the **Auto** calibration method, set the update interval (in hours) for the NTP agent. After you manually set the software clock for the first time, you may set the NTP agent to sychronize the clock once every half-day or day.

Serial Port

The MAR-2000 has two serial ports, each of which may be configured as RS-232, RS-422, or 2- or 4-wire RS-485. The MAR-2000 supports baudrates from 75 bps to 921,600 bps, and supports both software and hardware flow control.

Serial Port Status Window

Click the **SERIAL** tab to open the serial status window. See the section below for a more detailed explanation of each of the columns.

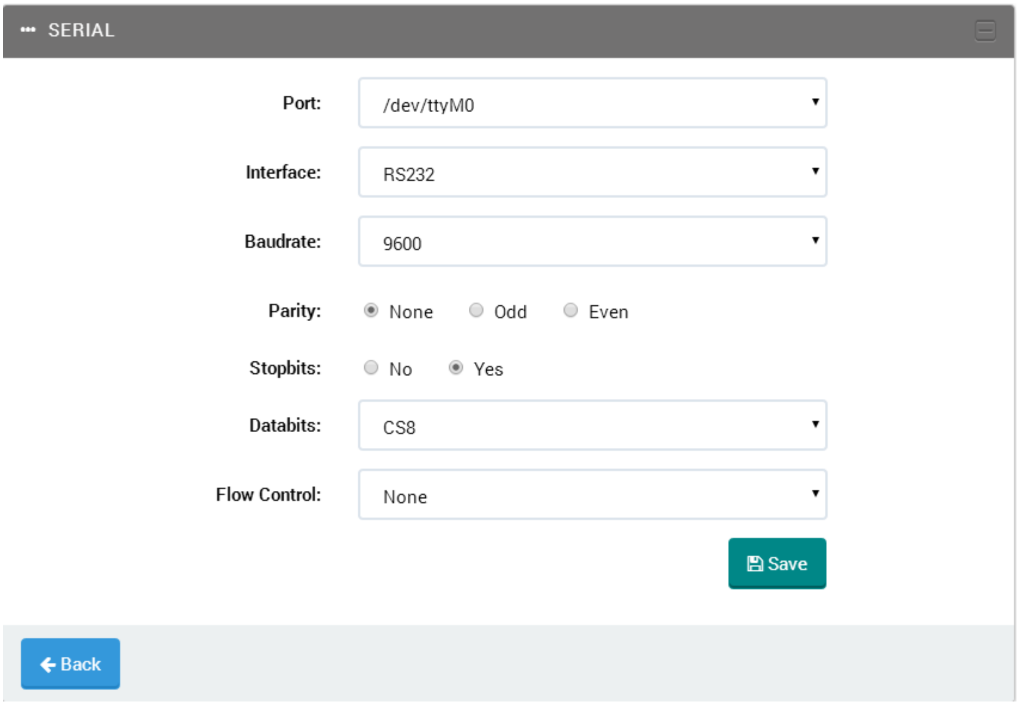


SERIAL

#	Port	Interface	Baudrate	Prarity	Stopbits	Databits	Flow Control
1	/dev/ttyM0	RS232	9600	None	Yes	CS8	None
2	/dev/ttyM1	RS232	9600	None	Yes	CS8	None

Serial Port Setup Window

Click **Edit** to configure the serial ports.



Port: /dev/ttyM0

Interface: RS232

Baudrate: 9600

Parity: ● None ○ Odd ○ Even

Stopbits: ○ No ● Yes

Databits: CS8

Flow Control: None

After setting up the serial ports, click **Save** to save the settings and make the changes take effect.

Field	Description
Port	The device node with which each serial port is associated; /dev/ttyM0 (port 1), dev/ttyM1 (port 2).
Communication Mode	Sets the serial communication mode for this interface. The choices are RS-232, RS-422, RS-485 2-wires, or RS-485 4-wires.
Baudrate	Sets the baudrate for the serial port. The range is from 75 to 921,600 (bps).
Parity	Available choices are: Odd, Even, or None.
Stopbits	Yes: use Stopbits No: do not use Stopbits
Databits	Select one of four options: CS5, CS6, CS7, or CS8
Flow Control	Select whether to use SW flow control, HW flow control, or both.

4

The Signal Tracker

Moxa's Signal Tracker provides administrators with a powerful visual aid for WAN management along the vehicle's route. The tracker samples a cellular signal over time and records its strength at configured intervals. The MAR-2000 shows this information on a map that displays how signal strength varies as the router travels along its way.

The following topics are covered in this chapter:

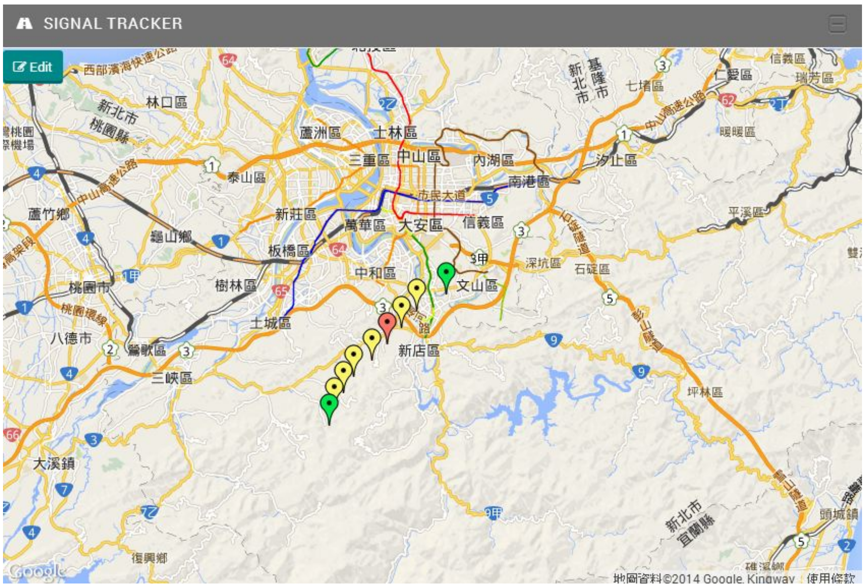
Signal Tracker

Moxa's Signal Tracker utility tracks the strength of the cellular signal received over the ***ppp0*** interface (i.e., on devices with two cellular modules, signal strength may only be measured over the first one).

The tracker monitors and records cellular signal strength at configured intervals, and then displays this information on a map using colored pinpoints that show how signal strength varies as the router travels along its way. This provides administrators with a powerful visual aid when configuring the MAR-2000 for WAN management along a complicated route.

The Signal Tracker Status Window

The signal tracker's status window displays a Google map with colored pinpoints indicating where the signal has been sampled. The map's resolution may be changed using the scroll wheel on a scrolling mouse, or by clicking on the window and using **CTRL+ and CTRL−**. To open the signal tracker's configuration window, click on the green **Edit** button located in the upper left corner of the window.



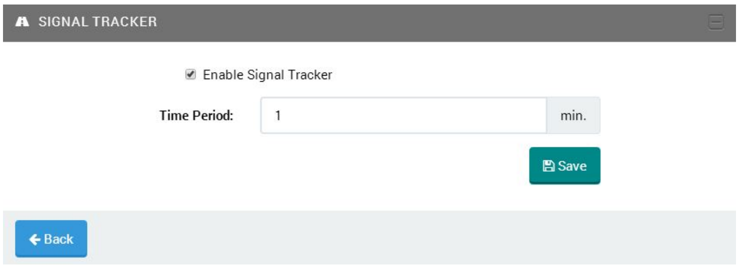
The picture above shows a sample tracking result: green markers indicate that the signal strength is greater than -69 dBm, yellow markers indicate that the signal strength is between -70 and -89 dBm, and red markers indicate that the signal strength is less than -90 dBm.

ATTENTION

An active Internet connection is required to use the Map service.

The Signal Tracker's Configuration Window

For two module devices, the signal tracker may only be used to monitor the first cellular module (i.e., ***ppp0***). To configure the signal tracker, users simply check the box next to Enable Signal Tracker and then enter the time intervals (in minutes) at which the signal will be sampled. Time intervals may only be indicated in whole numbers.



SIGNAL TRACKER

☑ Enable Signal Tracker

Time Period: 1 min.

Field	Description
Enable Signal Tracker	Click on the box to start or stop signal tracking.
Time Period (min)	Enter the sampling interval, in minutes, for signal measurement.

5

Setting Up OpenVPN

The MAR-2000 features the powerful OpenVPN 2.X software package, allowing administrators to configure the MAR-2000 with a VPN link for greater security and guaranteeing reliable LAN operations. This chapter describes the details of OpenVPN configuration.

The following topics are covered in this chapter:

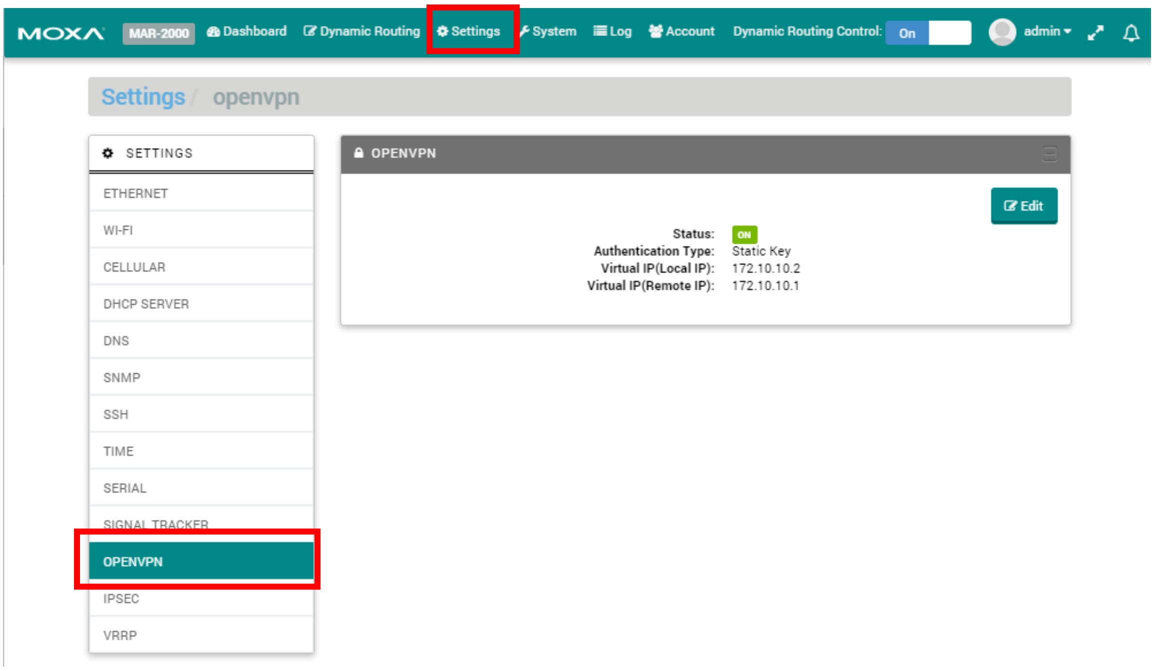
- □ **OpenVPN**
- □ **The OpenVPN Status Window**
- □ **The OpenVPN Configuration Window**
- □ **Configuring Your OpenVPN Client**
  - ➢ Upload a Configuration File
  - ➢ Manual Configuration
- □ **Static Key Authentication**
  - ➢ Key Generation
  - ➢ Uploading the Static Key: the OpenVPN File Upload UI
- □ **Asymmetric TLS: Public Key Authentication**
  - ➢ TLS Authentication & Encryption without a Password
  - ➢ Asymmetric TLS with Password
  - ➢ Renegotiation Interval
  - ➢ Use Additional TLS authentication
- □ **VPN Settings Available on All Configurations**
  - ➢ HMAC Authentication
  - ➢ Encryption Ciphers
  - ➢ Data Compression: LZO
  - ➢ Use a TCP Connection

OpenVPN

The MAR-2000 comes with VPN software, so that administrators can conveniently set up a strongly encrypted connection gateway that serves Internet connections over a virtual interface that maintains consistent routing and addressing paths. This enables passengers in the onboard environment to maintain stable Internet connectivity with external servers, even as the router shifts connections among different WAN servers.

The VPN backend used by the MAR-2000 is based on the powerful OpenVPN package. In this chapter, we show administrators detailed instructions about how to efficiently configure an OpenVPN network. Keep in mind that before the OpenVPN client can be used, you must first install and configure an OpenVPN server on the network to which you want to connect. After setting up your VPN server, be sure to note its configuration details (encryption/authentication keys, encryption protocols, communication ports, virtual and physical addresses, virtual subnet masks, etc.) before beginning the setup process described below.

Click **Settings** > **OPENVPN** to display the OpenVPN page.

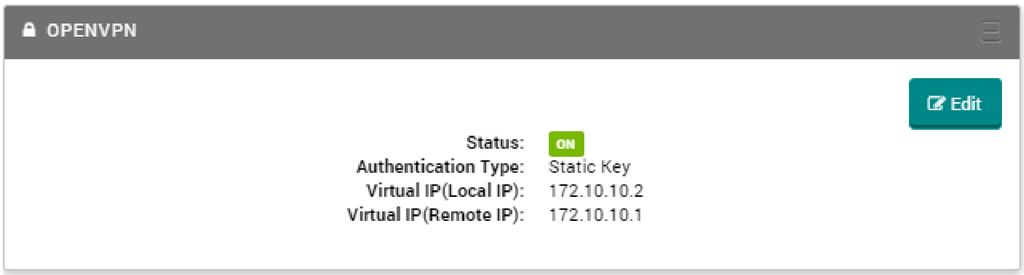


Status: ON
Authentication Type: Static Key
Virtual IP(Local IP): 172.10.10.2
Virtual IP(Remote IP): 172.10.10.1

The OpenVPN Status Window

This page shows the status of your VPN. If working correctly, the **Status** field displays **Normal**. If there are problems with the VPN, the status is **Abnormal**.

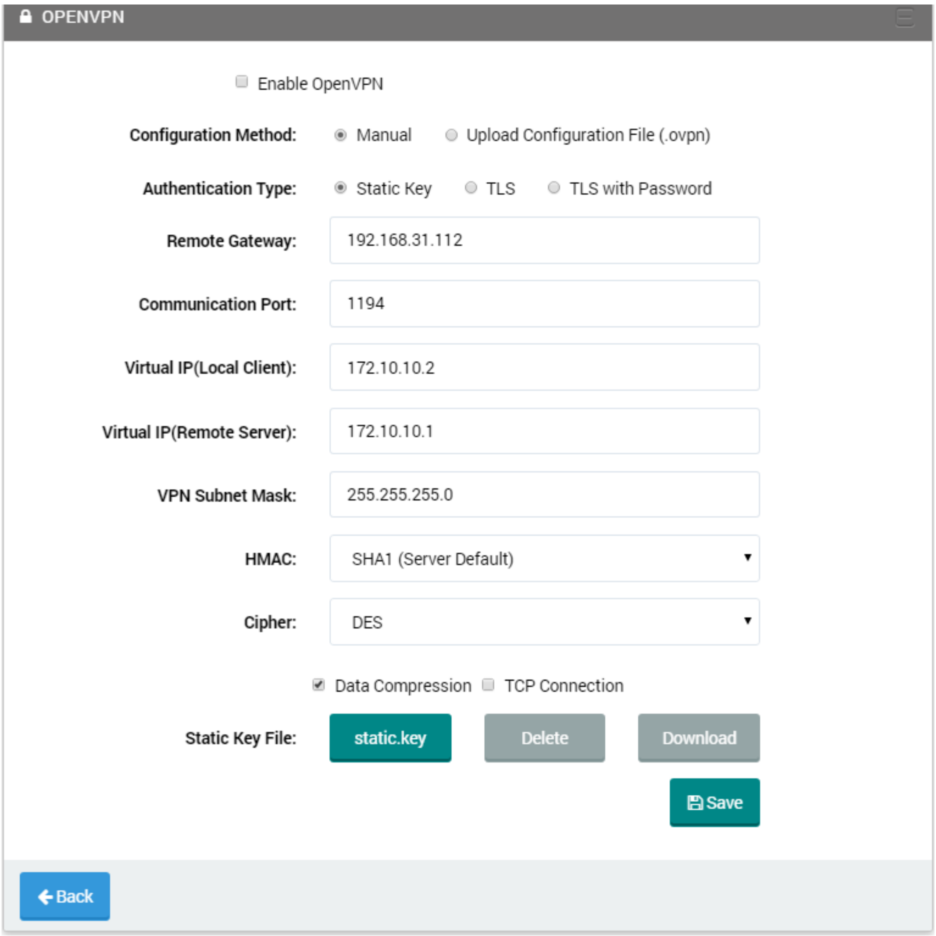
To open the VPN configuration window, click **Edit**.



Status: ON
Authentication Type: Static Key
Virtual IP(Local IP): 172.10.10.2
Virtual IP(Remote IP): 172.10.10.1

The OpenVPN Configuration Window

This window allows you to configure your MAR-2000's local VPN client.



OPENVPN

□ Enable OpenVPN

Configuration Method: ● Manual ○ Upload Configuration File (.ovpn)

Authentication Type: ● Static Key ○ TLS ○ TLS with Password

Remote Gateway: 192.168.31.112

Communication Port: 1194

Virtual IP(Local Client): 172.10.10.2

Virtual IP(Remote Server): 172.10.10.1

VPN Subnet Mask: 255.255.255.0

HMAC: SHA1 (Server Default)

Cipher: DES

☑ Data Compression □ TCP Connection

Static Key File: static.key Delete Download

Field	Description
Enable OpenVPN	Enables or disables the local client.
Configuration Method	Select a method to generate a configuration file:
Manual	Generate the configuration file manually
Import File	Upload a configuration file from another source
Authentication Type	Select how you wish your clients to authenticate themselves with the VPN:
Static Key	Uses a pre-shared key to authenticate with the remote server.
TLS	Uses Transport Layer Security (TLS) with asymmetric encryption keys to authenticate with the VPN.
TLS with Login	Uses Transport Layer Security (TLS) with asymmetric encryption keys plus an additional username and password to authenticate with the VPN.
Remote Gateway	The public IP address of the remote VPN gateway.
Communication Port	The communication port of the VPN.
Virtual IP: Local Client	Local VPN IP for communicating with the server.
Virtual IP: Remote Server	The public IP address (on the open Internet) of the remote VPN server.
VPN Subnet Mask	Subnet mask of the VPN.
HMAC: Hashed Message Authentication Code	Used to simultaneously verify both the data integrity and the authentication of a packet stream (i.e., a "message") by using an encrypted hash and a hidden key. See HMAC Authentication for a detailed explanation of the available choices. Note: For HMACs not listed in the drop-down list, you can still use the "Import File" function to include them in the configuration file.

Field	Description
Cryptographic Cipher	Sets the cipher that will be used to encrypt the packets that are carried over the TLS / IPsec layer. See **Encryption Ciphers** for a detailed explanation of the available choices. Note: For Ciphers not listed in the drop-down list, you can still use the "Import File" function to include them in the configuration file.
Data Compression	Compresses all data packets to increase speed by decreasing datastream throughput. See below for a detailed explanation of Data Compression: LZO.
TCP Connection	Use TCP transport (instead of UDP) for the tunneling protocol. Not recommended.
Static Key File	Use this to upload a static key for static/hidden key authentication.

Configuring Your OpenVPN Client

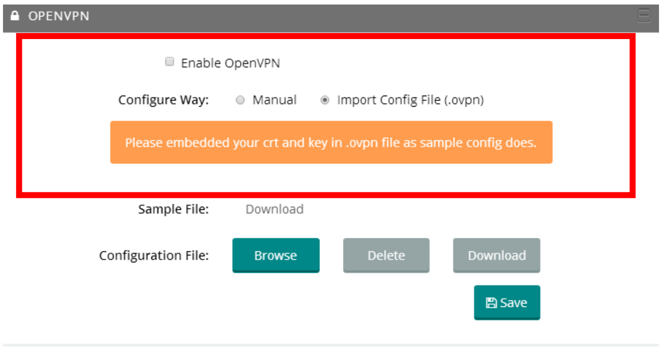
Upload a Configuration File

One of the ways to configure OpenVPN on the MAR-2000 is by filling out and uploading an OpenVPN setup template. Be sure to copy all certificates and keys into the ***.ovpn** configuration file.

Click **Download** to download the configuration template from the Moxa website.

Click **Browse** to open your file manager and select a file for upload.

After uploading the configuration file, click the **Save** to apply the configuration settings.



OPENVPN

□ Enable OpenVPN

Configure Way: ○ Manual ● Import Config File (.ovpn)

Please embedded your crt and key in .ovpn file as sample config does.

Sample File: Download

Configuration File: Browse Delete Download

Save

NOTE If you want to delete current configuration information on the MAR-200, click **Delete.** Note that if you set up your MAR-2000 using the configuration upload (*.opvn) method, then your MAR-2000 setup becomes unavailable on the next restart following the deletion of your configuration file. This does not affect the manual configuration method.

Manual Configuration

To set up OpenVPN manually, simply follow the configuration wizard. Each entry is described in detail below.

Static Key Authentication

Static Key authentication is the configuration of a hidden key that is shared (known) by both the VPN server and the remote client; it is essentially the configuration of a long, cryptographically strong password. Because the key is known by both the server and the client, this form of authentication is weaker than asymmetric (or public-key) cryptography. It is, however, typically strong enough for non-sensitive applications and is also much easier to set up and administer.

To set up static key authentication, you must first generate the key using the OpenVPN server connected to the VPN's base network. To ensure the key is fully compatible with all of OpenVPN's features, you should use the maximum key size, 2048 bits. For more information on this, read the Attention at the end of the **Asymmetric TLS: Public Key Authentication** section, farther down in this chapter.

ATTENTION

For more information about configuring static key authentication on OpenVPN, consult the **Static Key Mini-HOWTO** on the OpenVPN documentation site.

Key Generation

For detailed information on key and certificate generation, please refer to the following resources:

The official **Debian Wiki** on **configuring a static key** using the Debian OpenVPN package:
http://wiki.debian.org/OpenVPN#Static-Key_VPN

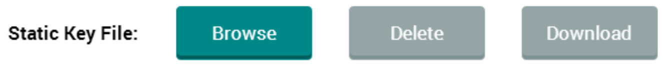
The official **Debian Wiki** on configuring an asymmetric pair (i.e., public/private) of encryption keys:
http://wiki.debian.org/OpenVPN#TLS-enabled_VPN

The official **OpenVPN How-To** page may be found here:
http://openvpn.net/index.php/open-source/documentation/miscellaneous/88-1xhowto.html

The **Easy Windows Guide** on the **OpenVPN Community Wiki**:
http://community.openvpn.net/openvpn/wiki/Easy_Windows_Guide

Uploading the Static Key: the OpenVPN File Upload UI

After a static key has been generated, you may upload it using the **Static Key File** interface. The static key upload box is found at the bottom of the **The OpenVPN Configuration Window**; click the **Browse** button, select the file you wish to upload, and then click **Save**. The key file should be in plain text format, with no other labels or information.



The **Delete** button deletes the current key, while the **Download** button retrieves the current key file from your client's repository.

ATTENTION

For more information about configuring static key authentication on OpenVPN, you may consult the **Static Key Mini-HOWTO** on the OpenVPN documentation site.

Asymmetric TLS: Public Key Authentication

Transport Layer Security (TLS) implements encryption and authentication at the transport layer, rather than at the data layer. OpenVPN achieves this using **asymmetric encryption**, which is another way of saying **public/private key encryption**. TLS encryption takes place entirely in the background, and requires no input from the user; it is, however, more difficult to set up and administer than a simple pre-shared key.
Public key encryption exploits the qualities of one-way mathematical formulas which are easy to calculate in one direction, but extremely difficult to reverse calculate. By using extremely long mathematical formulas, two ciphers are created for each machine: a hidden key that is never shared or exposed to other computers, and a public key that is shared and used by other computers to encrypt and authenticate messages with the original computer. Messages encrypted with the openly shared public key can only be decrypted using the private key, which is only known to the local computer; by this means, much stronger authentication and encryption are achieved than is possible using a static, pre-shared key.

Increasingly, in industry parlance private keys are called **keys**, while public keys are called **certificates**. Three files will therefore be needed to properly set up a client:

- The VPN authenticator's (CA's) public key (or **certificate**)
- The client's public key (or **certificate**), which it will share with the server, and
- The client's own private key (or key). On the MAR-2000, the server's public key is named **caCert.ca**, the client's public key is named **userCert.ca**, and the client's private key is called the **private.key**.

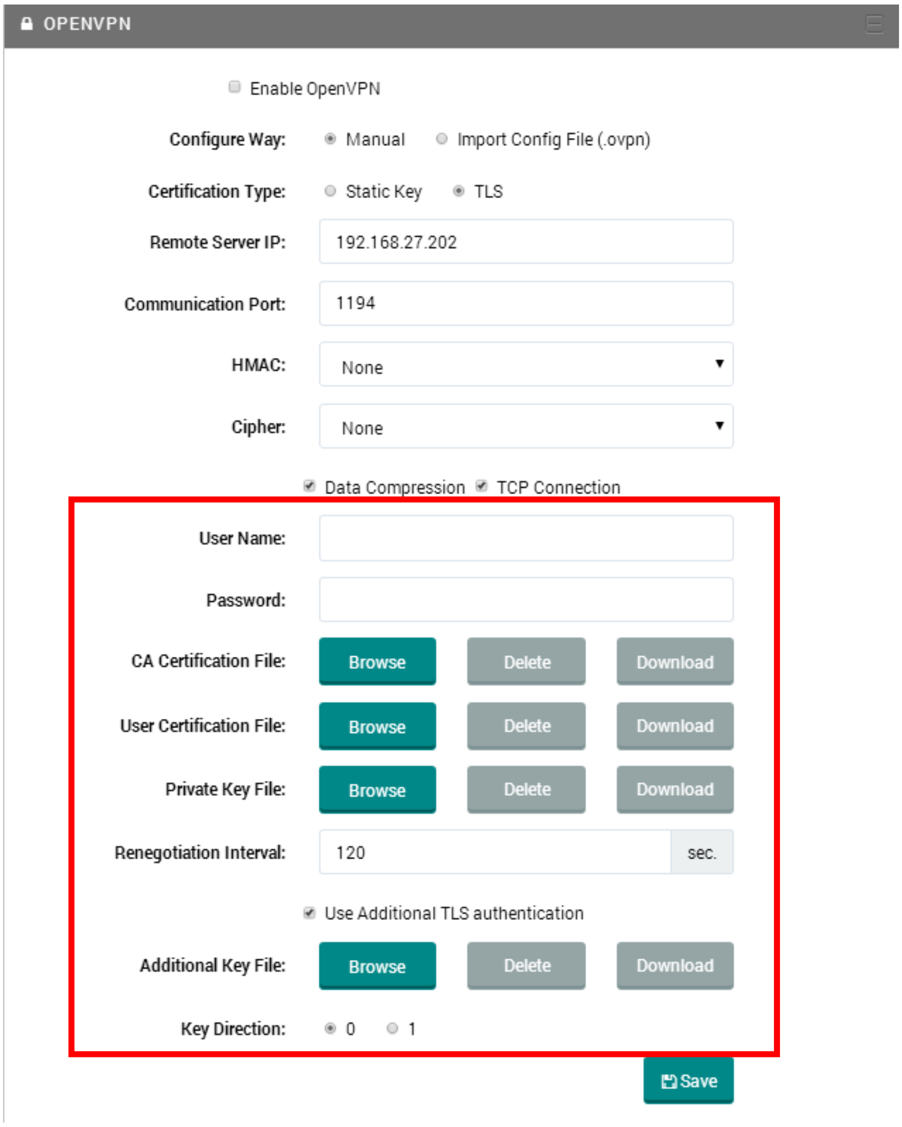
Certificates and keys may be uploaded after selecting one of the TLS authentication entries, in the dialog window shown below.

ATTENTION

Some of OpenVPN's advanced security features require 2048 bit HMAC and cipher keys. This is the maximum size OpenVPN supports, and guarantees maximum security protections. Even if the current MAR-2000 configuration does not force the use of these higher-level security features, in order to ensure that hard-to-discover bugs do not arise in possible future reconfigurations (while also maximizing system security) **Moxa recommends that all generated encryption keys (HMAC and cipher) be 2048 bits in size.**

TLS Authentication & Encryption without a Password

To set up asymmetric TLS authentication, the system administrator must first generate two pairs of keys for each computer that will be communicating over the VPN: one for the VPN server, which will likely serve as the **certificate authority** (CA), and another for the client. To achieve full use of the TLS authentication and encryption features, you must use full 2048 bit keys.



OPENVPN

□ Enable OpenVPN

Configure Way: ● Manual ○ Import Config File (.ovpn)

Certification Type: ○ Static Key ● TLS

Remote Server IP: 192.168.27.202

Communication Port: 1194

HMAC: None

Cipher: None

☑ Data Compression ☑ TCP Connection

User Name:

Password:

CA Certification File:

User Certification File:

Private Key File:

Renegotiation Interval: 120 sec.

☑ Use Additional TLS authentication

Additional Key File:

Key Direction: ● 0 ○ 1

Field	Description
User Name	This is the TLS user ID to be used for password authentication.
Password	This is the TLS password to be used for password authentication.
CA Certification File	The public key used by the remote server (default: caCert.ca).
User Certification File	The public key used by the local OpenVPN client (default: userCert.ca).
Private Key File	The private key used by the local OpenVPN client (default: private.key).
Renegotiation Interval	The interval, in seconds, at which all VPN cryptographic and authentication ciphers will be renegotiated and renewed.
Use Additional TLS Authentication	It is possible to configure OpenVPN with an additional layer of security by generating an additional HMAC layer using a hidden key. This key must be shared by all clients that will connect to the OpenVPN server.
Additional HMAC Key	This dialog manages the key for additional TLS authentication.
Key Direction	Determines the direction in which the additional HMAC key will be used. It should be set to the opposite of what the server is configured for; typically, clients are set to 1, while the server is set to 0.

Asymmetric TLS with Password

The final form of authentication is asymmetric TLS with an extra layer of security added. In addition to the public certificate and private keys that are configured for the client, one more layer of security is created by configuring a username and password for the user of the computer, so that any user of the VPN must first log in to a user account on the authentication (or VPN) server.

IMPORTANT!

When discussing cryptographic ciphers, Moxa follows the **Apache** web server standard: publicly exposed ciphers are called **certificates**, and are labeled using a ***.ca** suffix; private, undisclosed ciphers are called **keys**, and use the ***.key** suffix. Thus, the file **userCert.ca** is the ***client's*** publicly disclosed certificate (or "public key"), while the file **caCert.ca** is the issuing ***certificate authority's*** certificate (or "publicly disclosed key"). In contrast, the client's ***private key*** is found under **private.key**, and a pre-shared ***static key*** is stored as **static.key**. For clarity's sake, Moxa recommends maintaining these conventions when generating your encryption keys and certificates.

ATTENTION

When configuring OpenVPN, be sure to set a rule to allow tunneled communications through the firewall. The MAR-2000 comes with two preconfigured protocol exceptions, one for UDP and one for TCP. To open a port for the VPN:

- Select **LAN** as the source zone
- Select **WWW** as the destination zone
- Set the **Action** dropdown to **Accept**
- Depending on which protocol you have configured the VPN to use, choose either **VPN – UDP** or **VPN – TCP** from the dropdown menu

A second rule must then be configured for the VPN server; the settings will be the same, but with the source and destination fields reversed: the source will be **WWW**, while the destination will be **LAN**.

Renegotiation Interval

For security considerations, the MAR-2000 is configured with a default renegotiation interval of 3600 seconds (i.e., one full hour). This means that after the MAR-2000 VPN client has been connected to the VPN for a full hour, it will automatically disconnect from the VPN and then reconnect, going through a full renegotiation of all authentication and encryption protocols. If you would like to change this default setting, check the Renegotiation Interval toggle and then enter the number of seconds you wish the MAR-2000 to remain connected to the VPN server before renegotiation occurs. Entering zero (0) will disable the renegotiation configuration on the local device; please note, however, that the renegotiation may still be initiated by the VPN server. So even if you have disabled renegotiations on the client side they may still occur because of configured server requirements. Also note that authentication renegotiation is not available under static configurations.

Use Additional TLS authentication

This option toggles the TLS authentication flag (--tls-auth), an OpenVPN feature that adds an additional layer of HMAC security on top of the TLS control channel. A second HMAC layer is added to the packets transporting the encrypted data (where the first layer of HMAC—for validating data authenticity and integrity—has already been added). This empowers the server to automatically drop packets which are improperly hashed, providing a strong layer of protection against buffer overflow and denial of service (DoS) attacks, particularly those that seek to exploit the authentication process. Additionally, OpenVPNs that used this additional security were not susceptible to the Heartbleed exploit.

In order to enable HMAC protection on the TLS control-channel you will need, first, to generate a 2048 bit HMAC key from the OpenVPN server. Then, you will need to share this key with every client that wishes to connect with that server. You may upload the TLS-authentication HMAC key using the OpenVPN File Uploader dialog, which can be accessed by clicking on the Modify link located next to the Key File entry.

VPN Settings Available on All Configurations

The following settings are available on both a static key or a TLS configuration.

HMAC Authentication

Hash Message Authentication Code assures **message authenticity** (i.e., packets are part of the data stream they claim to be from) and **message integrity** (i.e., the data stream content has not been meddled with or altered). HMAC does not, however, provide privacy (i.e., encryption): HMAC is a hashed code that runs on top of packets, independently of the content that is being carried (whether encrypted or not). The HMAC default is SHA-1; select **None** if you do not wish to use HMAC authentication. The accompanying table shows the relative sizes of the various algorithms; larger digests will be slower. For strong security, Moxa recommends using the SHA-2 algorithm.

Hash Name	Digest Size
SHA-1	160 bit
RIPEMD160	160 bit
SHA-2:	
• SHA-224	256 bit int / 224 ext
• SHA-256	256 bit int / 256 ext
• SHA-384	512 bit int / 384 ext
• SHA-512	512 bit int / 512 ext

Encryption Ciphers

These are the ciphers used to encrypt packet data. All of the ciphers used in MAR-2000's implementation of OpenVPN are chained block ciphers (CBC). The RC2, CAST-5, and AES-128 ciphers are included for legacy configurations; for new installations, these choices should be considered deprecated. For strongest encryption, users should select AES-192 or AES-256. If datastream encryption is unnecessary and you require faster VPN response times, you may select **None** to disable encryption.

CBC Ciphers	Key Size
RC2/ARC2-64	64 bits
CAST-5	128 bits
AES-128	128 bits
AES-192	192 bits
AES-256	256 bits

Data Compression: LZO

LZO is a lossless data compression library engineered for speed rather than compression ratio. This makes the LZO library ideal for use as a real-time compressor/decompressor. The LZO compression algorithms are extremely fast and compact; they use no RAM, and only 64 kb (kilobits) of kernel memory to work. OpenVPN utilizes LZO compression to compress data into smaller bundles, thereby increasing data throughput without resorting to increases in bandwidth. Moxa recommends using LZO compression, and it comes enabled by default; however, in some installations where kernel memory has become cluttered with competing applications, disabling LZO compression may result in noticeable increases in speed. To toggle LZO compression on or off, simply click on the dialog next to **Use LZO data compression**.

Use a TCP Connection

In some situations (e.g., to maintain connectivity) it may be necessary to use TCP transport for the tunneling protocol. If so, check this box. Keep in mind, however, that this will likely result in degraded system performance; TCP-over-TCP tunnels are many times more likely to drop packets and congest networks. Moxa recommends maintaining the default UDP transport, if possible. If you use TCP transport, be sure to modify the firewall to reflect the correct protocol.

ATTENTION

For a more detailed explanation of why TCP-over-TCP tunnels are best avoided, you may refer to the online article **Why TCP Over TCP Is A Bad Idea**, by digital encryption researcher, security hacker, and programmer Olaf Titz. Currently, the article may be found at http://sites.inka.de/~W1011/devel/tcp-tcp.html.

6

IPsec

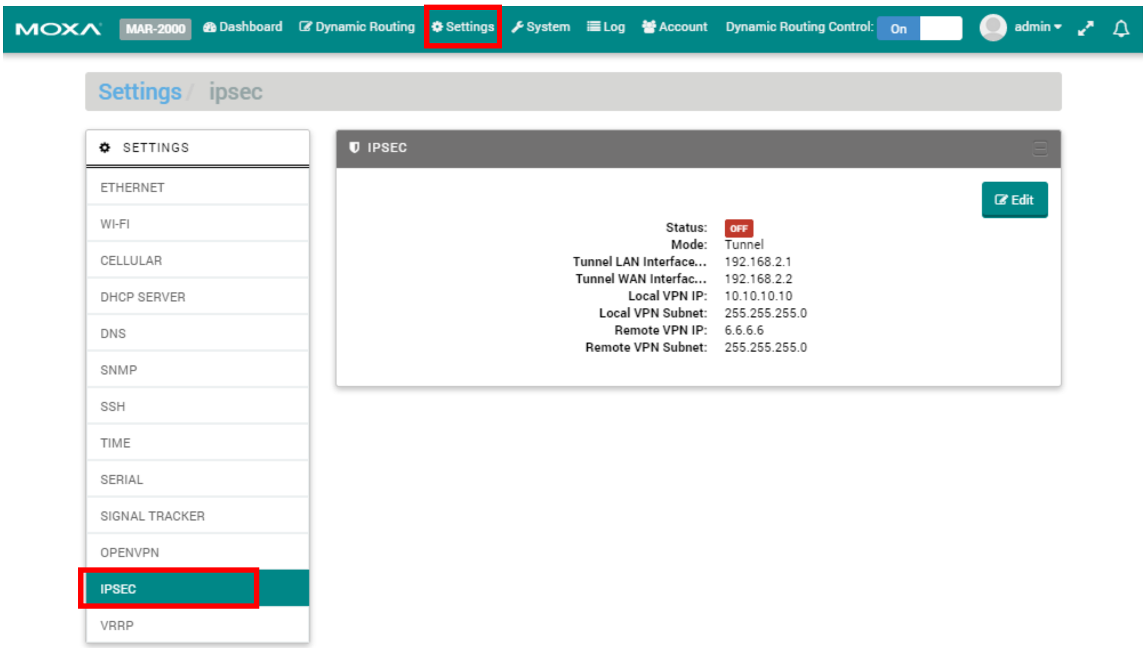
The MAR-2000 also comes with IPsec VPN capabilities, which provides an alternative approach to building VPNs. IPsec technology is valuable for established server-to-server connections, across subnets that do not change much.

The following topics are covered in this chapter:

- ❒ **IPsec**
- ❒ **The IPsec Status Window**
- ❒ **The IPsec Configuration Window**
  - ➢ Configuring Transport Mode
  - ➢ Configuring Tunnel Mode

IPsec

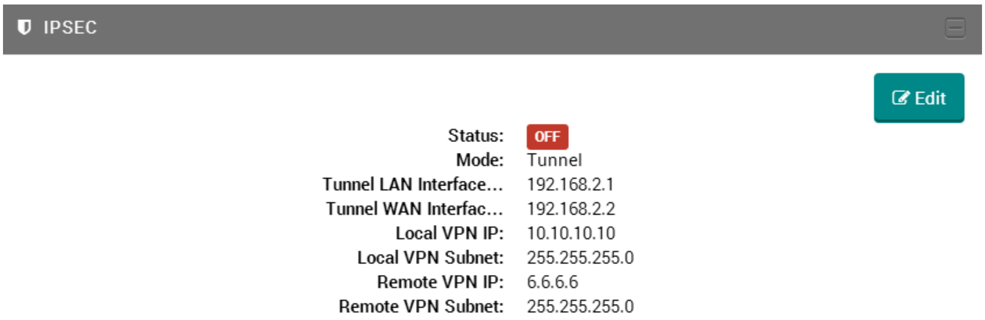
IPsec (Internet Protocol Security) is used to establish a secure tunnel over the open Internet between a pair of remote gateways serving private networks. IPsec is typically used on standalone gateways, as a means of seamlessly connecting the larger LANs behind them, merging two remote networks into a single, seamless LAN. IPsec packet translation handles authentication and encryption, and takes place within the kernel, before the packet ever arrives in user-space. For this reason, IPsec tends to take up less overhead than OpenVPN; for the same reason, IPsec packets sometimes do not play nice with firewalls and NAT. The MAR-2000 uses the IPsec Tools 0.7.3 package, which provides the Racoon key exchange daemon.



Status: OFF
Mode: Tunnel
Tunnel LAN Interface... 192.168.2.1
Tunnel WAN Interfac... 192.168.2.2
Local VPN IP: 10.10.10.10
Local VPN Subnet: 255.255.255.0
Remote VPN IP: 6.6.6.6
Remote VPN Subnet: 255.255.255.0

The IPsec Status Window

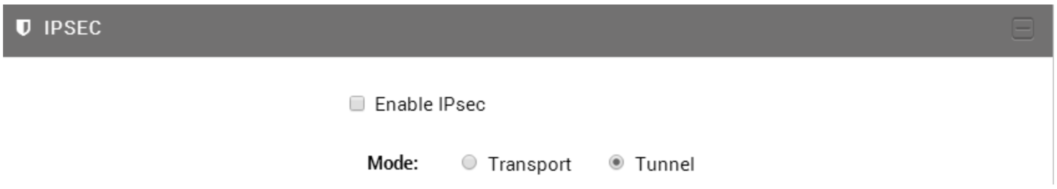
In the **Settings** menu, click the **IPSEC** entry to open the IPsec status window. This window will show you the current status and basic configuration of your IPsec VPN. The **Status** indicator shows whether your IPsec service is working properly or not. Click **Edit** to open the IPsec configuration window.



Status: OFF
Mode: Tunnel
Tunnel LAN Interface... 192.168.2.1
Tunnel WAN Interfac... 192.168.2.2
Local VPN IP: 10.10.10.10
Local VPN Subnet: 255.255.255.0
Remote VPN IP: 6.6.6.6
Remote VPN Subnet: 255.255.255.0

The IPsec Configuration Window

IPsec can be implemented in a host-to-host **transport** mode, as well as in a network **tunneling** mode. Each of these configurations has advantages and disadvantages. A quick breakdown of each is given on the pages that follow.



□ Enable IPsec

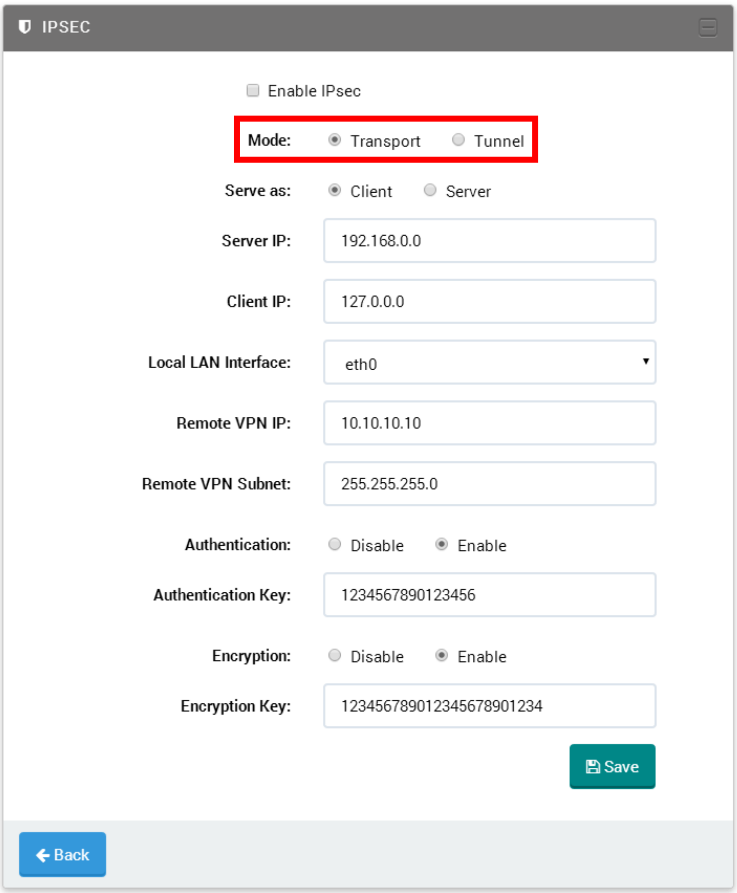
Mode: ○ Transport ● Tunnel

Field	Description
Enable IPsec	Enable or disable IPsec on the MAR-2000.
Mode	Set up IPsec in Configuring Transport mode or Configuring Tunnel Mode.

Configuring Transport Mode

IPsec transport mode is used for end-to-end communications, as with a client connecting to a remote desktop, or encrypted Telnet. In transport mode, only the payload of the IP packet is encrypted and/or authenticated; IP headers are neither modified nor encrypted. Transport mode has less overhead than tunnel mode, but it can cause problems with NAT traversal.

To configure an IPsec transport mode connection, select **Transport** and set the configuration fields.



□ Enable IPsec

Mode: ● Transport ○ Tunnel

Serve as: ● Client ○ Server

Server IP: 192.168.0.0

Client IP: 127.0.0.0

Local LAN Interface: eth0

Remote VPN IP: 10.10.10.10

Remote VPN Subnet: 255.255.255.0

Authentication: ○ Disable ● Enable

Authentication Key: 1234567890123456

Encryption: ○ Disable ● Enable

Encryption Key: 123456789012345678901234

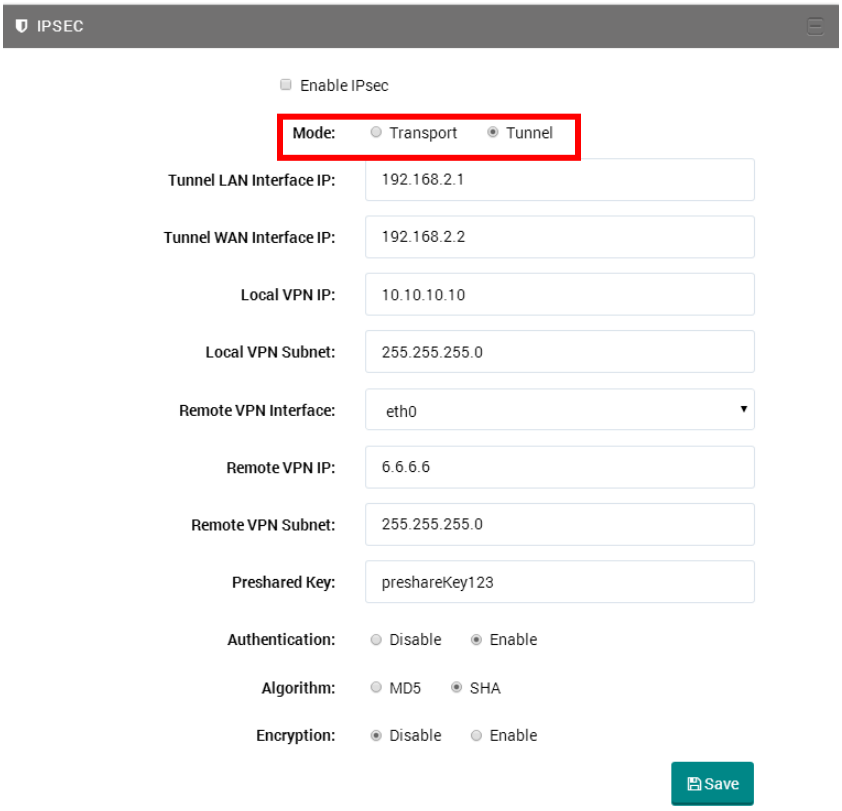
Field	Description
Serve as	Sets the MAR-2000 as either an IPsec client or server.
Server IP	The public IP address of the server that will be hosting the VPN.
Client IP	The public IP address of the client that will be connecting to the VPN host.
Local LAN Interface	The local Ethernet interface over which the VPN will be served.
Virtual IP of Server	The virtual IP address (i.e., the private address on the VPN) of the remote machine.
Remote VPN subnet	The virtual subnet (i.e., the address space of the VPN) that will be shared.
Authentication	Enable or disable message authentication.
Authentication Key	The shared key used to for message authentication.
Encryption	Enable or disable data encryption within the IP packets.
Encryption Key	The shared key used to encrypt packet data.

ATTENTION

The MAR-2000 IPsec configuration wizard only implements pre-shared key encryption and authentication. If you require asymmetric IPsec encryption and authentication, then you must configure IPsec from the backend, over the Linux console.

Configuring Tunnel Mode

Tunnel mode is most commonly used to connect two remote LAN gateways, giving computers on either LAN full access to the remote network as if it were part of the local subnet. In **Tunnel** mode the entire IP packet is authenticated or/and encrypted and then encapsulated into a new IP packet with a new IP header. IPsec tunnels take up more overhead than transport mode, but protects your private network from been spoofed by monitoring IP headers. Compare to transport mode, tunnel mode is easier to use with NAT. Tunnels, however, require smaller MTUs and deliver poor interoperability with dynamically assigned addresses.



IPSEC

□ Enable IPsec

Mode: ○ Transport ● Tunnel

Tunnel LAN Interface IP: 192.168.2.1

Tunnel WAN Interface IP: 192.168.2.2

Local VPN IP: 10.10.10.10

Local VPN Subnet: 255.255.255.0

Remote VPN Interface: eth0

Remote VPN IP: 6.6.6.6

Remote VPN Subnet: 255.255.255.0

Preshared Key: presharekey123

Authentication: ○ Disable ● Enable

Algorithm: ○ MD5 ● SHA

Encryption: ● Disable ○ Enable

Field	Description
Local LAN Interface	The LAN interface of the tunnel. This interface is used to establish the VPN tunnel with the remote machine.
Public IP Address: Local Gateway	The public IP address of the outbound interface for the local peer.
Public IP Address: Remote Gateway	The public IP address for the remote gateway interface, i.e.: the physical address of the remote peer to which we are connecting.
Virtual IP for the Local Peer	This is the virtual address that will be used on the private (i.e., encrypted) network to identify the local gateway.
Local VPN Subnet	This is the virtual subnet mask used for addressing on the local, private/encrypted network.
Virtual IP for the Remote Peer	The remote VPN IP. After the tunnel is established, the remote WAN uses this IP to communicate with us via the VPN tunnel.
Remote VPN Subnet	This is the virtual subnet mask used for private/encrypted addressing on the remote network.
Pre-shared Key	The pre-shared key of the VPN tunnel.
Authentication • **AH** • **ES**P	Select the type of authentication and encryption you wish to use The Authentication Headers protocol provides message authentication The Encapsulating Security Payload protocol provides full-packet encryption
Algorithm	Choose the algorithm to use for authentication. You may choose MD5C or SHA-2. These are described above, in the HMAC Authentication section.

7

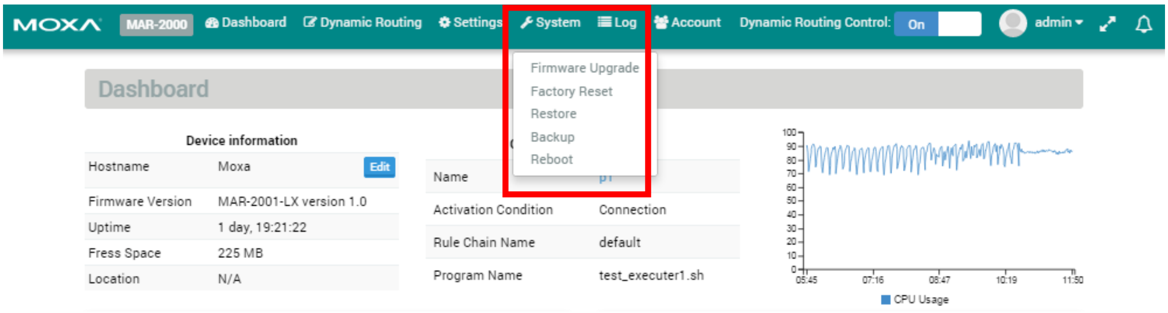
MAR-2000 System Administration

The following topics are covered in this chapter:

- ❒ **System Administration**
- ❒ **Upgrading the Firmware**

System Administration

The System tab allows you to administer the setup and basic components of the MAR-2000.



Device information

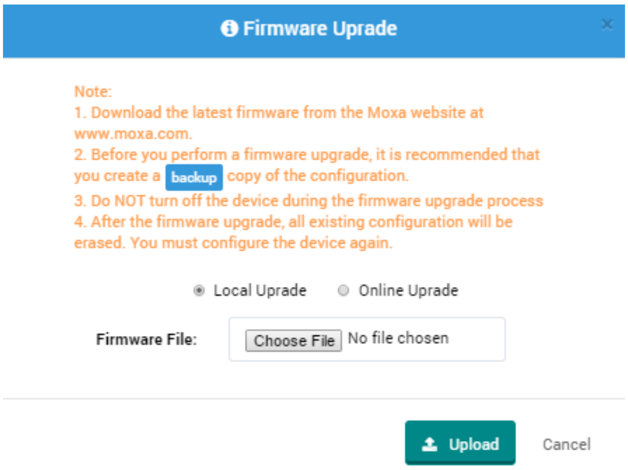
Hostname	Moxa	Edit
Firmware Version	MAR-2001-LX version 1.0	
Uptime	1 day, 19:21:22	
Fress Space	225 MB	
Location	N/A	

Name	p1
Activation Condition	Connection
Rule Chain Name	default
Program Name	test_executer1.sh

Upgrading the Firmware

The MAR-2000's kernel, and root file system are combined into one firmware file. To upgrade the firmware/kernel package, click **Firmware Upgrade** in the dropdown menu under the **System** tab, found on the menu bar at the top of the screen. You should be provided with two alternatives: **Local Upgrade** and **Online Upgrade**.

The **Local Upgrade** allows you to upload the firmware file from a PC or local storage medium. To perform a local upgrade, users must first download the firmware from Moxa's website (www.moxa.com), or click here to link directly to the download page.



Note:
1. Download the latest firmware from the Moxa website at www.moxa.com.
2. Before you perform a firmware upgrade, it is recommended that you create a backup copy of the configuration.
3. Do NOT turn off the device during the firmware upgrade process
4. After the firmware upgrade, all existing configuration will be erased. You must configure the device again.

● Local Uprade ○ Online Uprade

Firmware File: Choose File No file chosen

The filename will be in the form **FWR_MAR-20002000_V*a.b.c*_Build_*YYMMDDHH*.hfm**, with **a.b.c** indicating the firmware version and **YYMMDDHH** indicating the build date.

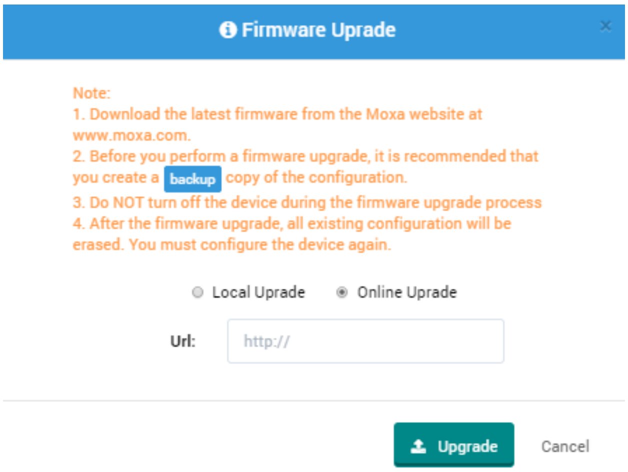
After downloading the update, first back up your current MAR-2000 configuration. This is necessary because a firmware upgrade will erase all of your current configuration and setup details. After the firmware upgrade is completed, you will be able to quickly reconfigure your MAR-2000 by using the saved configuration with the **Importing a Configuration from a File** feature described at the start of Chapter 1.

ATTENTION

Your current configuration will be erased after upgrading the firmware! It is strongly recommended that you back up the original configuration by pressing the Backup button (shown at right) before you upgrade firmware. This will download a *.htm file to your local PC. This *.htm file contains your MAR-2000's entire setup, and will allow you to quickly and conveniently restore your current configuration using the **Importing a Configuration from a File** feature described in Chapter 1.

To proceed with a local upgrade, checkmark the **Local Upgrade** selection and then click on **Choose File**. Select the firmware upgrade, and then click **Upload** to upload the firmware. Remember: ***Do not power off the MAR-2000*** while the upgrade is in process.

The other way of performing an upgrade is with **Online Upgrade**, where the firmware is automatically downloaded and upgraded. To perform an online upgrade copy the following URL into the URL input box and click **Upgrade**. You can copy the hyper link below and paste it into the Url box on the screen.



Note:
1. Download the latest firmware from the Moxa website at www.moxa.com.
2. Before you perform a firmware upgrade, it is recommended that you create a backup copy of the configuration.
3. Do NOT turn off the device during the firmware upgrade process
4. After the firmware upgrade, all existing configuration will be erased. You must configure the device again.

○ Local Uprade ● Online Uprade

Url: http://

http://www.moxa.com/support/DownloadFile.aspx?type=support&id=4674

A firmware upgrade should take about 15 minutes, depending on your network speed. Once the upgrade is completed, the system will reboot automatically. **DO NOT** power down the device during the firmware upgrade.

WARNING

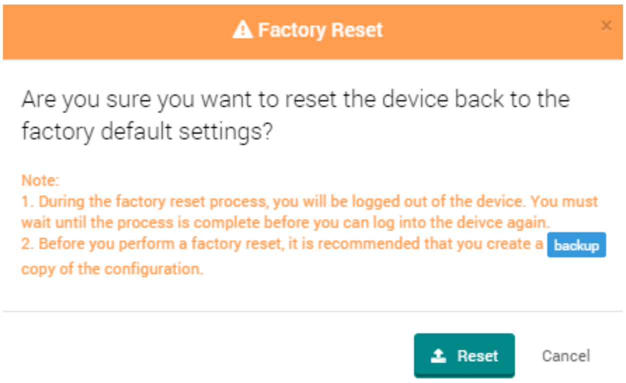
Existing configuration will be erased after the upgrade.

Reset To Factory Defaults

WARNING

The existing configuration will be erased after using **Reset To Factory Defaults**.

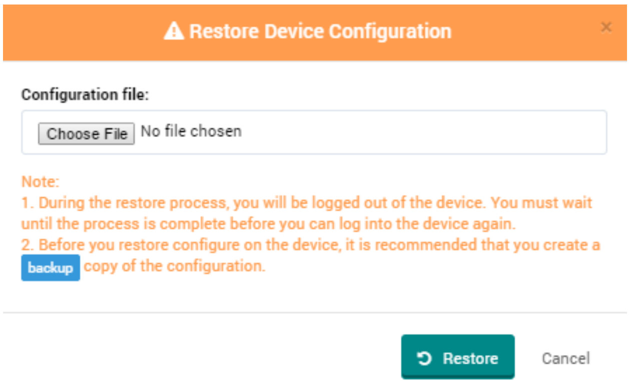
Select **Factory Reset** in the **System** menu to force the system to reload its factory default settings. A factory reset should take about 15 minutes.



Are you sure you want to reset the device back to the factory default settings?

Note:
1. During the factory reset process, you will be logged out of the device. You must wait until the process is complete before you can log into the deivce again.
2. Before you perform a factory reset, it is recommended that you create a backup copy of the configuration.

Restore Device Configuration lets you restore a configuration that was previously saved as a backup (see the next section, **Backup**, for details). To restore your system to a previous configuration, click **Restore** in the **System** menu, and then in the new window choose the configuration file you wish to import from the file system.

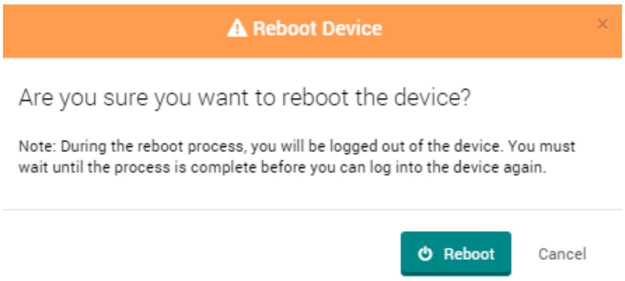


Configuration file: Choose File No file chosen

Note:
1. During the restore process, you will be logged out of the device. You must wait until the process is complete before you can log into the device again.
2. Before you restore configure on the device, it is recommended that you create a backup copy of the configuration.

All MAR-2000 settings can be exported into a configuration backup file. Just click the **Backup** item under the **System** menu and select the location to save the backup configuration (the file will be named as **export.tar**). The exported configuration can be restored as described in the previous section just above, and may also be imported by the wizard described in Chapter 1 of this manual, **Importing a Configuration from a File**.

The **Reboot** option in the System menu will immediately initiate a soft restart. A reboot should take about 4 minutes to complete.

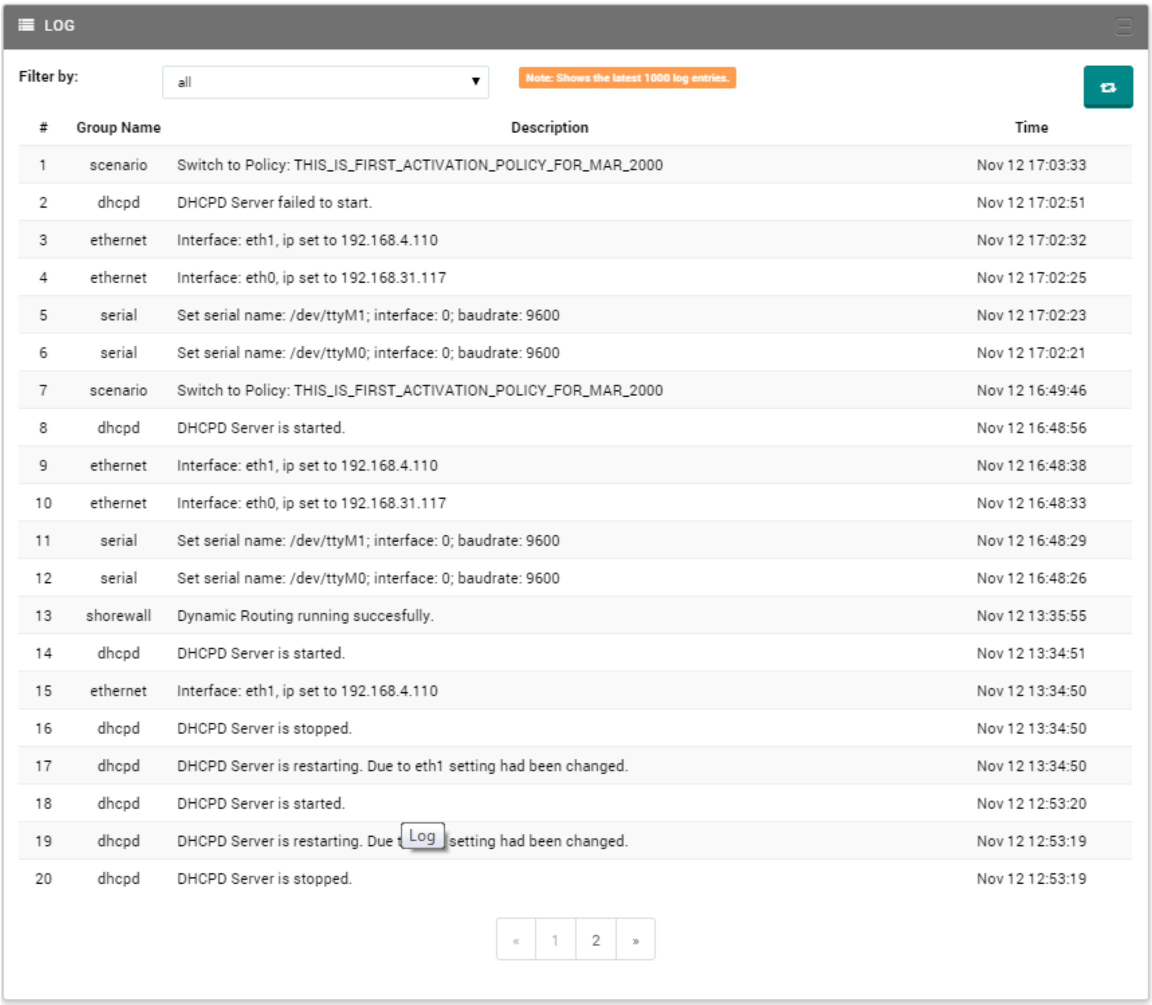


Are you sure you want to reboot the device?

Note: During the reboot process, you will be logged out of the device. You must wait until the process is complete before you can log into the device again.

The System Log

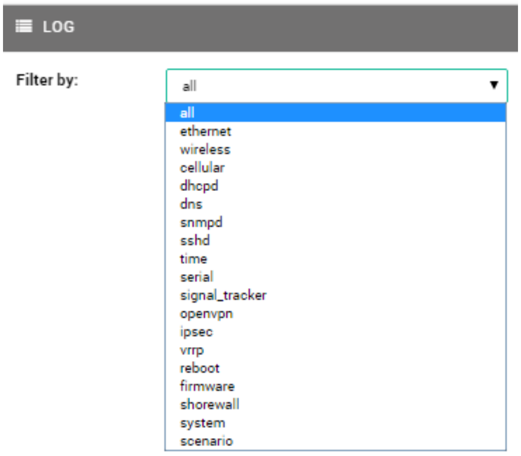
The Log selection on the top ribbon will open the Log window, which will fetch the last 100 lines of the syslog messages. Each row belongs to a different function (e.g., openvpn, time, dhcp, etc.). User could use selectbox to filter logs and also reload the current logs by clicking the refresh button.



#	Group Name	Description	Time
1	scenario	Switch to Policy: THIS_IS_FIRST_ACTIVATION_POLICY_FOR_MAR_2000	Nov 12 17:03:33
2	dhcpd	DHCPD Server failed to start.	Nov 12 17:02:51
3	ethernet	Interface: eth1, ip set to 192.168.4.110	Nov 12 17:02:32
4	ethernet	Interface: eth0, ip set to 192.168.31.117	Nov 12 17:02:25
5	serial	Set serial name: /dev/ttyM1; interface: 0; baudrate: 9600	Nov 12 17:02:23
6	serial	Set serial name: /dev/ttyM0; interface: 0; baudrate: 9600	Nov 12 17:02:21
7	scenario	Switch to Policy: THIS_IS_FIRST_ACTIVATION_POLICY_FOR_MAR_2000	Nov 12 16:49:46
8	dhcpd	DHCPD Server is started.	Nov 12 16:48:56
9	ethernet	Interface: eth1, ip set to 192.168.4.110	Nov 12 16:48:38
10	ethernet	Interface: eth0, ip set to 192.168.31.117	Nov 12 16:48:33
11	serial	Set serial name: /dev/ttyM1; interface: 0; baudrate: 9600	Nov 12 16:48:29
12	serial	Set serial name: /dev/ttyM0; interface: 0; baudrate: 9600	Nov 12 16:48:26
13	shorewall	Dynamic Routing running succesfully.	Nov 12 13:35:55
14	dhcpd	DHCPD Server is started.	Nov 12 13:34:51
15	ethernet	Interface: eth1, ip set to 192.168.4.110	Nov 12 13:34:50
16	dhcpd	DHCPD Server is stopped.	Nov 12 13:34:50
17	dhcpd	DHCPD Server is restarting. Due to eth1 setting had been changed.	Nov 12 13:34:50
18	dhcpd	DHCPD Server is started.	Nov 12 12:53:20
19	dhcpd	DHCPD Server is restarting. Due t Log setting had been changed.	Nov 12 12:53:19
20	dhcpd	DHCPD Server is stopped.	Nov 12 12:53:19

Field	Description
Description	Log messages.
Time	The message's timestamp.

The drop-down window in the upper right corner allows you to filter log messages by the program that spawned them. All user-space background processes that are currently running will be listed in the drop-down list. To filter the displayed message queue, simply select the process you wish to highlight from the menu, and the log window will automatically display the latest 1000 log messages generated by the program.



8

Dynamic Routing Setup and Management

The heart of the MAR-2000 is its dynamic routing and packet filtering capabilities. Below, we show you how to configure the router and firewall.

The following topics are covered in this chapter:

Dynamic Routing Overview

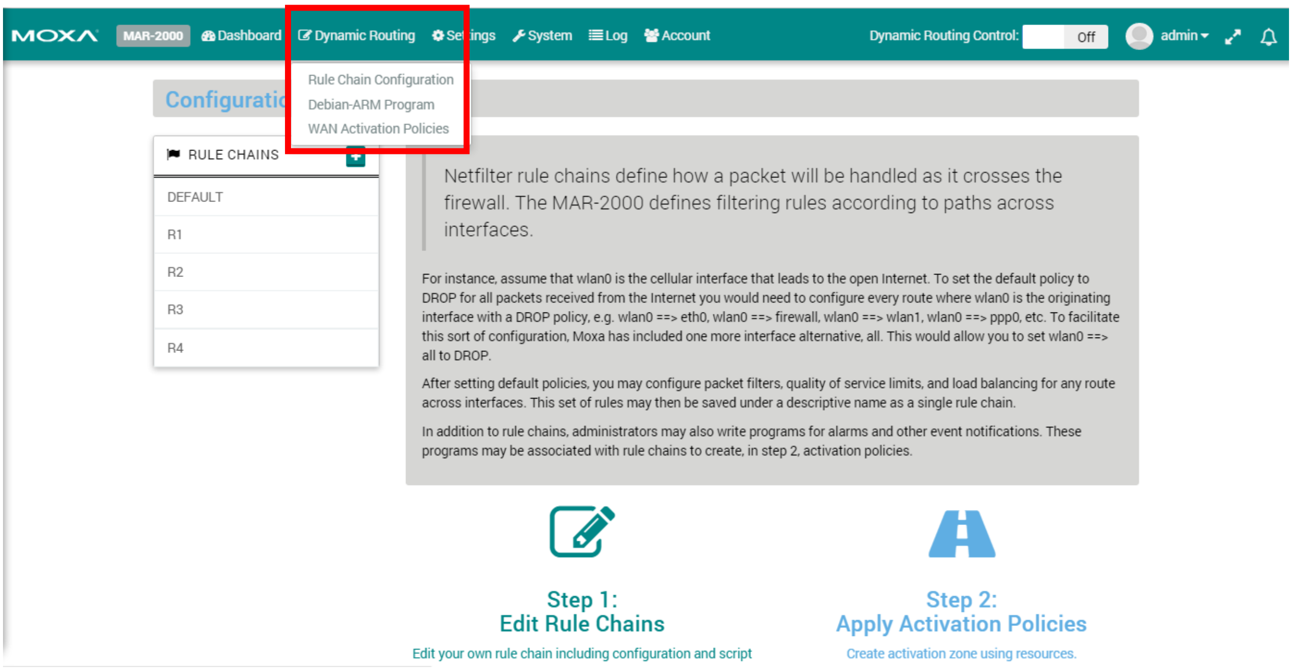
The MAR-2000 provides a powerful and easy way to set up dynamic routing rules that will automatically manage connections across a variety of available WANs. Changes from one WAN to another can be set up to be triggered by a variety of conditions: geographic location, wireless signal strength, or connectivity issues. You decide why, when, where, and which routing policies, firewall rules, and automated programs need to be launched. Only two steps are required to do this:

1. Create a rule chain for firewall, packet filtering, traffic control, or port mapping.
2. Create a policy to trigger the rule chain.

The dynamic routing configuration process may be roughly divided into three parts:

- **Rule Chain Configuration:** Packet filtering in the MAR-2000 is based on the Shoreline Firewall, which uses the IPChains packet filter as its backend. Chains of packet filtering rules allow you to set up powerful firewall and routing pathways.
- **Debian-ARM Program List:** Here, you can upload scripts and lengthier programs to more finely automate the behavior of your MAR-2000 as it travels on its way.
- **WAN Activation Policies:** In this section, you can set up which WANs you wish to route connections over according to three types of conditions: **geographic location**, **signal strength**, and **device connectivity**.

To configure active routing on your MAR-2000, simply follow the steps through, in order.



Netfilter rule chains define how a packet will be handled as it crosses the firewall. The MAR-2000 defines filtering rules according to paths across interfaces.

For instance, assume that wlan0 is the cellular interface that leads to the open Internet. To set the default policy to DROP for all packets received from the Internet you would need to configure every route where wlan0 is the originating interface with a DROP policy, e.g. wlan0 ==> eth0, wlan0 ==> firewall, wlan0 ==> wlan1, wlan0 ==> ppp0, etc. To facilitate this sort of configuration, Moxa has included one more interface alternative, all. This would allow you to set wlan0 ==> all to DROP.

After setting default policies, you may configure packet filters, quality of service limits, and load balancing for any route across interfaces. This set of rules may then be saved under a descriptive name as a single rule chain.

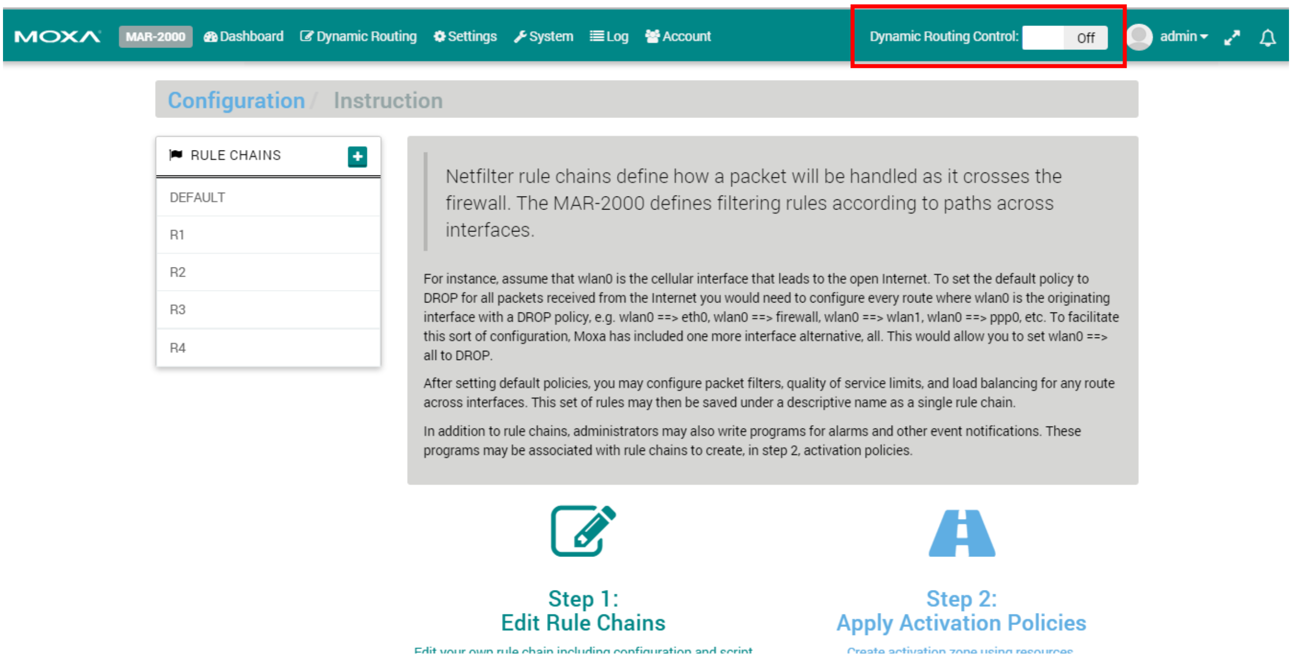
In addition to rule chains, administrators may also write programs for alarms and other event notifications. These programs may be associated with rule chains to create, in step 2, activation policies.

Step 1:
Edit Rule Chains
Edit your own rule chain including configuration and script

Step 2:
Apply Activation Policies
Create activation zone using resources.

Dynamic Routing Control

The Dynamic Routing Control lets you decide to enable or disable Dynamic Routing by toggling between Off and On. **Off** means that Dynamic Routing is currently disabled, and that the most recent WAN Activation Policy is being used. Go to the Dashboard and see which WAN Activation Policy is running.



Netfilter rule chains define how a packet will be handled as it crosses the firewall. The MAR-2000 defines filtering rules according to paths across interfaces.

For instance, assume that wlan0 is the cellular interface that leads to the open Internet. To set the default policy to DROP for all packets received from the Internet you would need to configure every route where wlan0 is the originating interface with a DROP policy, e.g. wlan0 ==> eth0, wlan0 ==> firewall, wlan0 ==> wlan1, wlan0 ==> ppp0, etc. To facilitate this sort of configuration, Moxa has included one more interface alternative, all. This would allow you to set wlan0 ==> all to DROP.

After setting default policies, you may configure packet filters, quality of service limits, and load balancing for any route across interfaces. This set of rules may then be saved under a descriptive name as a single rule chain.

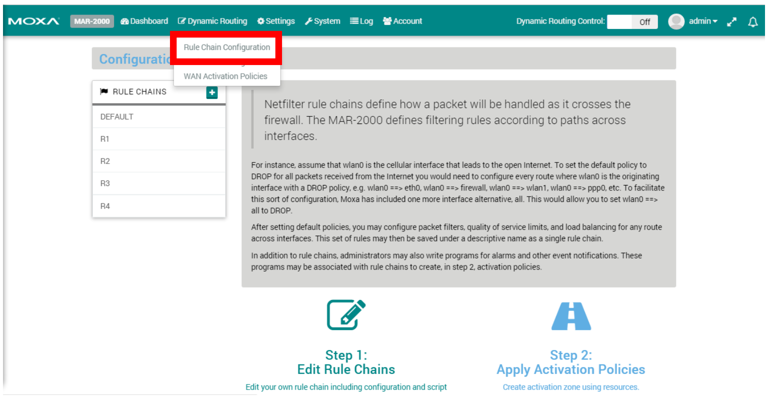
In addition to rule chains, administrators may also write programs for alarms and other event notifications. These programs may be associated with rule chains to create, in step 2, activation policies.

Edit your own rule chain including configuration and script

Create activation zone using resources

Rule Chains

This section allows you to configure Netfilter rule chains for packet filtering and firewall purposes. Rule chains are divided into four sections: basic I/O **policies** that set default behavior for an interface; packet **filtering rules**, that define how specific protocols should be handled (and over which ports); **traffic control**, which allows you to throttle bandwidth across individual interfaces; and **load balancing**, which allows you to redirect traffic from busy interfaces to less busy interfaces at the packet level.



Netfilter rule chains define how a packet will be handled as it crosses the firewall. The MAR-2000 defines filtering rules according to paths across interfaces.

For instance, assume that wlan0 is the cellular interface that leads to the open Internet. To set the default policy to DROP for all packets received from the Internet you would need to configure every route where wlan0 is the originating interface with a DROP policy, e.g. wlan0 ==> eth0, wlan0 ==> firewall, wlan0 ==> wlan1, wlan0 ==> ppp0, etc. To facilitate this sort of configuration, Moxa has included one more interface alternative, all. This would allow you to set wlan0 ==> all to DROP.

After setting default policies, you may configure packet filters, quality of service limits, and load balancing for any route across interfaces. This set of rules may then be saved under a descriptive name as a single rule chain.

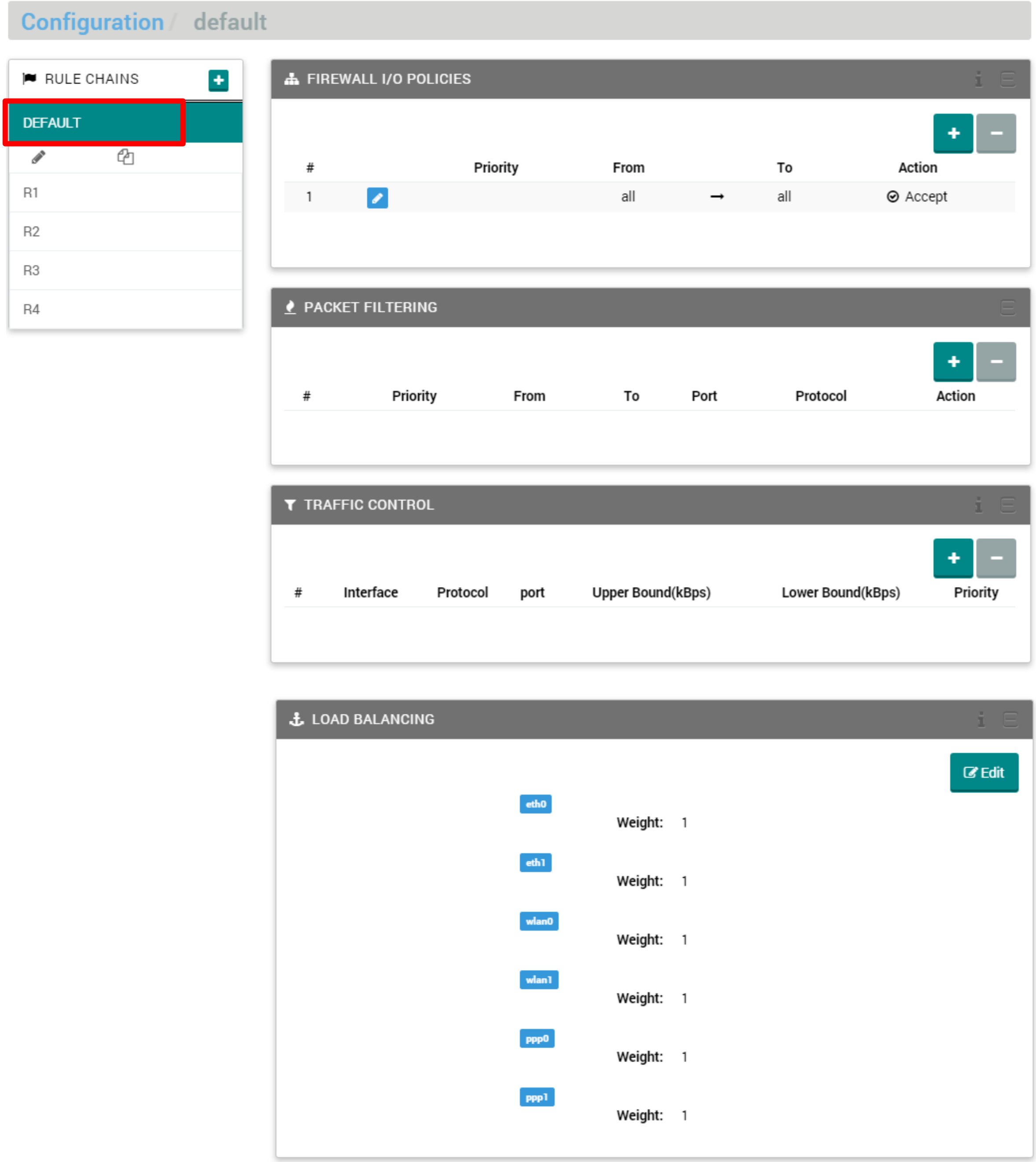
In addition to rule chains, administrators may also write programs for alarms and other event notifications. These programs may be associated with rule chains to create, in step 2, activation policies.

Edit your own rule chain including configuration and script

Create activation zone using resources.

Rule Chain Configuration Window

Click on **Rule Chain Configuration** under the **Dynamic Routing** tab in the top ribbon to enter the rule chain configuration window. Here you will see four separate boxes: **Firewall I/O Policies**, **Packet Filtering**, **Traffic Control**, and **Load Balancing**, as shown below:



Configuration / default

RULE CHAINS

DEFAULT

R1

R2

R3

R4

FIREWALL I/O POLICIES

#		Priority	From		To	Action
1			all	→	all	Accept

PACKET FILTERING

#	Priority	From	To	Port	Protocol	Action

TRAFFIC CONTROL

#	Interface	Protocol	port	Upper Bound(kBps)	Lower Bound(kBps)	Priority

LOAD BALANCING

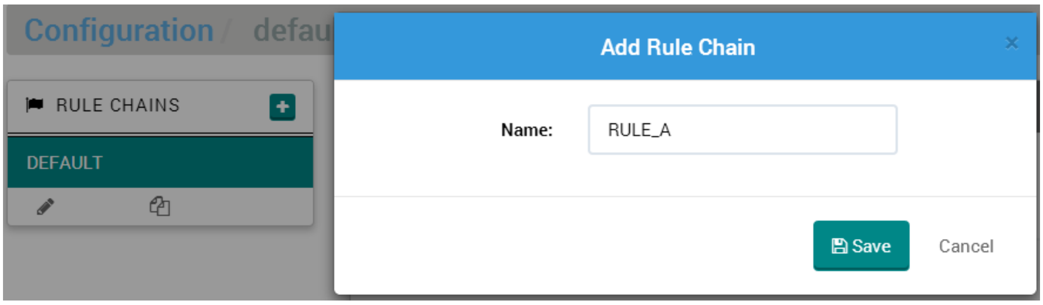
Edit

eth0	Weight: 1
eth1	Weight: 1
wlan0	Weight: 1
wlan1	Weight: 1
ppp0	Weight: 1
ppp1	Weight: 1

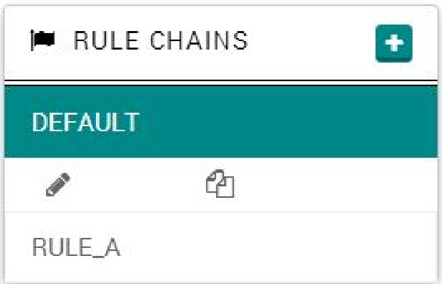
At the top left of the page (outlined in red in the picture above) you will find your rule chain manager. This box allows you to create however many rule chains you require. When you open the page, the manager will be set to the **Default** rule chain; the default rule chain is the rule chain that will be applied if you have not defined a rule chain for a connection.

Rules are applied in the order they are encountered, and inspection ends as soon as there is a match. Consequently, if a rule rejecting SSH connections is created, and later on another rule is created that allows SSH, the rule to reject will already have been applied, so the SSH connection will be killed. If a rule does not match any rules, then the final rule that is applied is the I/O policy.

Click **+** from the rule chain dropdown to add a new chain. Enter a name for the entry and click **Save** to apply.



Name: RULE_A



A new rule chain will appear beneath the **Default** chain, as shown in the image, where the name of the new rule is **RULE_A**.

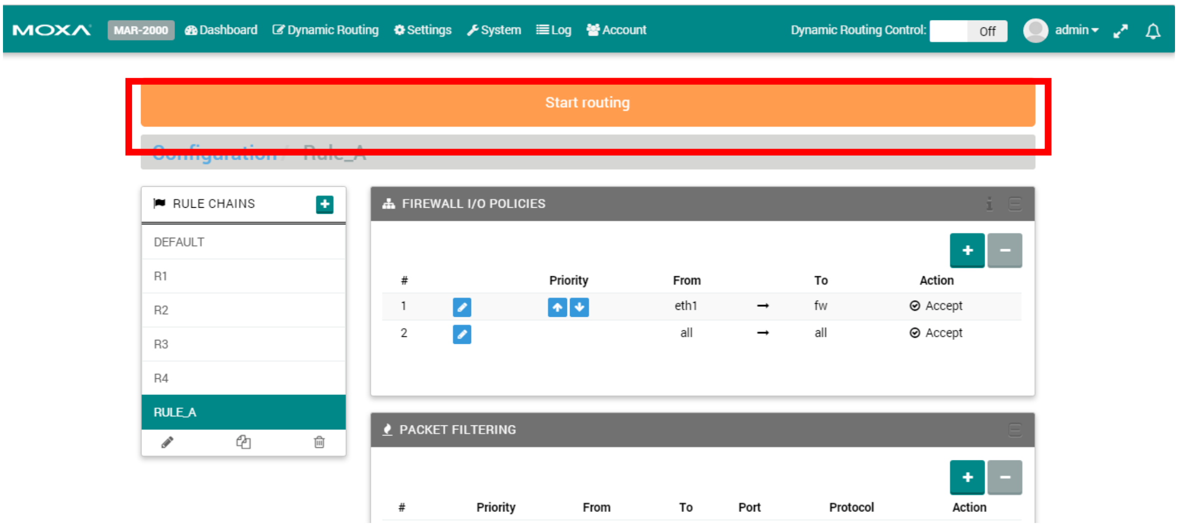
To set a rule chain for **RULE_A** simply click on the entry and the window will show the current set of rules for this rule chain. If at any time during the editing process you wish to check the behavior of what you have done, click the **Start Routing** button at the top of the page (highlighted in the screenshot below) and wait for a response. The rule chain needs to be triggered by the relevant WAN Activation Policy. If any problems occur, such as editing the wrong rule or shutting down your firewall, you can check **The System Log** for diagnosis information.

WARNING

Be careful if you want to set all to all reject/drop in each rule chain. (If set to All, you will not be able to log in to the MAR-2000 until you reset it to the factory default settings.)

Start Routing

The **Start routing** panel appears automatically whenever changes are made to the network interface settings (Ethernet, Wi-Fi, Cellular), the Rule Chain configuration, or WAN Activation Policies. Click the **Start routing** panel to apply the updated settings to the MAR-2000 immediately; the panel will disappear after it's been clicked. Otherwise, you will need to wait until the MAR-2000 is restarted for the changes to take effect.



FIREWALL I/O POLICIES

#		Priority	From		To	Action
1	✎	↑ ↓	eth1	→	fw	✓ Accept
2	✎		all	→	all	✓ Accept

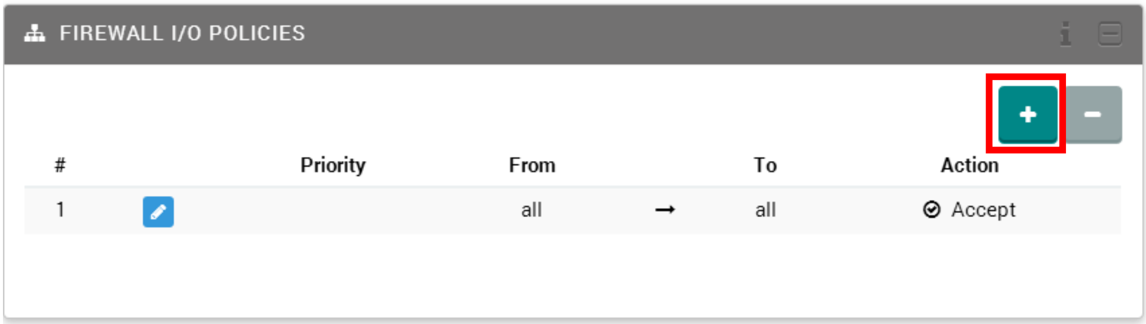
PACKET FILTERING

#	Priority	From	To	Port	Protocol	Action

Firewall I/O Policies

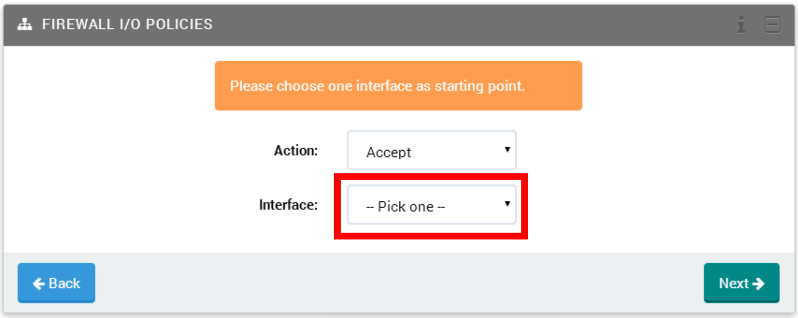
Firewall I/O Policies set the default behavior for how an interface will handle packets. A firewall policy is the action that will be applied to any packet that does not match a rule. Three choices are available: **ACCEPT**, **DROP** (which drops packets silently), and **REJECT** (which drops packets but returns an ICMP message notifying the sender that the packet has been dropped). Generally speaking, the firewall should be set to ACCEPT all traffic that originates on the internal network, and to DROP any traffic that is inbound from untrusted devices (including untrusted passenger devices, as well). A DROP policy on all inbound interfaces is the security policy recommended by all network security professionals. To configure the services and connections that will be allowed through, use the packet filtering section that follows.

Press the green **+** to add a new policy.



#		Priority	From		To	Action
1			all	→	all	Accept

Presuming that your inbound interfaces are **ppp0**, **ppp1**, and **wlan0**, then the way to set up a default DROP policy on all inbound traffic would be to select **ppp0** from the **interface** dropdown shown below. In this case, the **Action** selected should be **Drop**.



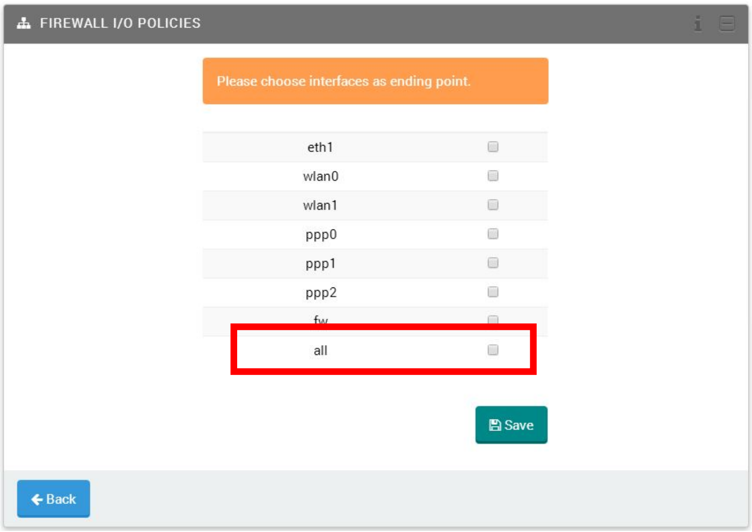
Please choose one interface as starting point.

Action: Accept

Interface: -- Pick one --

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Action</td><td>Select one of the following actions:
• Accept–Permit all packets to traverse the firewall, as if there were no firewall present.
• Reject–Prohibit a packet from passing and send an ICMP destination-unreachable back to the source host
• Drop–Prohibit a packet from passing, and send no response.</td></tr>
<tr><td>Interface</td><td>Select the path source and destination includes. The firewall indicates the MAR-2000 itself. All indicates all available interfaces, inbound and outbound.
<table>
<tr><td>Ethernet</td><td>Wi-Fi/802.11</td><td>Cellular</td><td>The Firewall</td><td>All Interfaces</td></tr>
<tr><td>eth#</td><td>wlan#</td><td>ppp#</td><td>fw</td><td>all</td></tr>
</table></td></tr>
</table>

Next, select **all** as the ending point. This means that all incoming packets coming in on your first cellular module (**ppp0**) will be dropped, no matter which interface they are destined for.

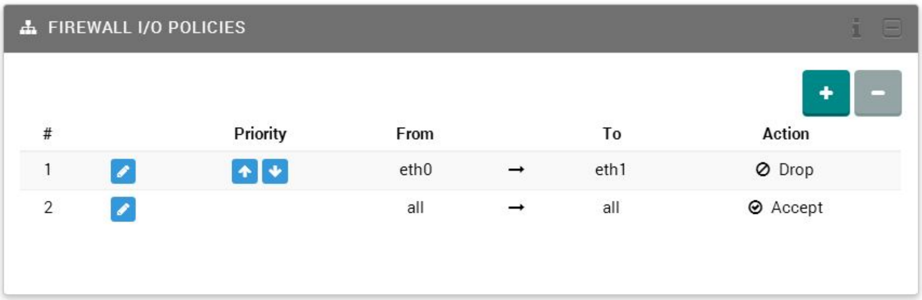


FIREWALL I/O POLICIES

Please choose interfaces as ending point.

eth1	□
wlan0	□
wlan1	□
ppp0	□
ppp1	□
ppp2	□
fw	□
all	□

After clicking **Save**, a routing policy will be generated for you and applied.

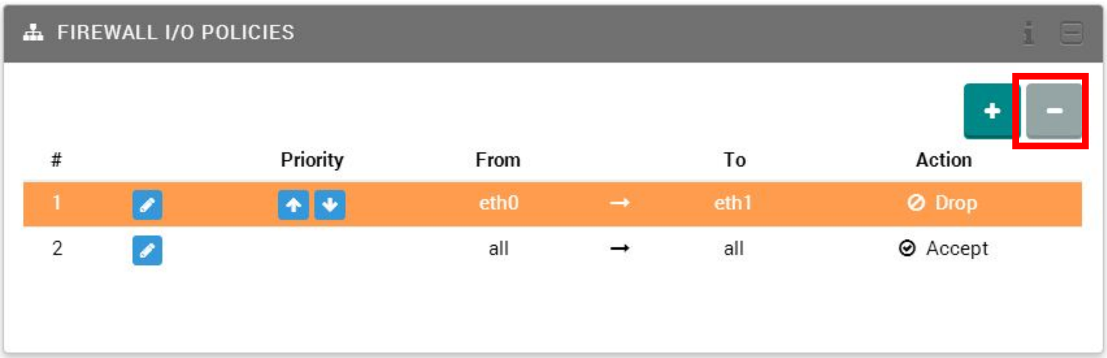


FIREWALL I/O POLICIES

#		Priority	From		To	Action
1	✎	↑ ↓	eth0	→	eth1	⊘ Drop
2	✎		all	→	all	✓ Accept

The pencil icon allows you to edit a policy you have already saved. The **Priority** column adjusts the priority in which rules will be applied. A higher place means the rule will be applied earlier in the queue; a lower place means the rule will be applied later. Please remember: as soon as a packet matches a policy, it is sent to the rule chain. The initial policy is all/all/Accept, which allows you to configure the device. However, for network security reasons, the final policy should always be all/all/Reject after you finish the firewall configuration.

You may delete policies by highlighting the policy and then clicking the minus icon in the upper right corner. The **all to all** policy cannot be deleted. The system will protect this policy from deletion.



FIREWALL I/O POLICIES

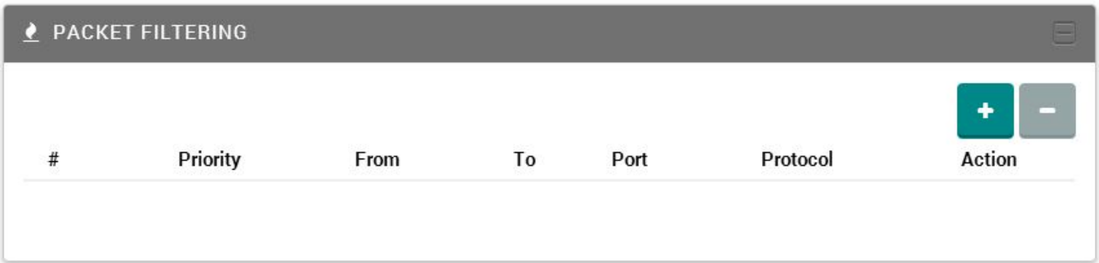
#		Priority	From		To	Action
1	✎	↑ ↓	eth0	→	eth1	⊘ Drop
2	✎		all	→	all	✓ Accept

WARNING

The MAR-2000 comes with the all-to-all policy set to Accept by default. However, to reflect good security practices, once the basic firewall policies are completed this should be changed to either Reject or Drop, and placed at the end of the policy chain.

Packet Filtering

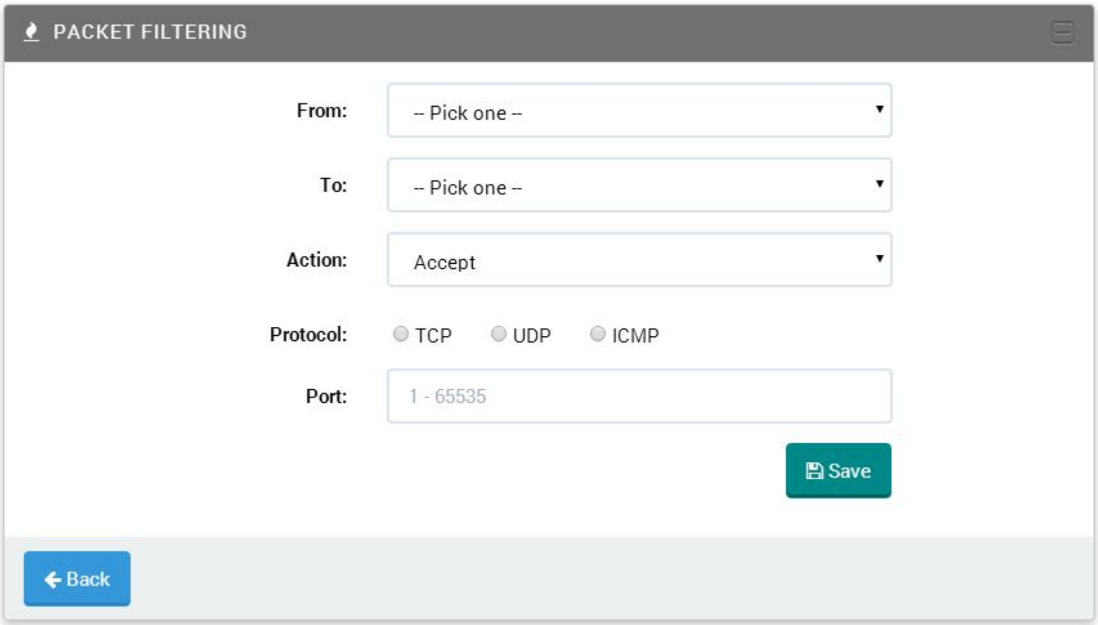
Packet filtering allows you to set up a detailed rule of what kind of packet you want to accept or reject for the path.



PACKET FILTERING

#	Priority	From	To	Port	Protocol	Action

Click + to add a new filter rule.



PACKET FILTERING

From: -- Pick one --

To: -- Pick one --

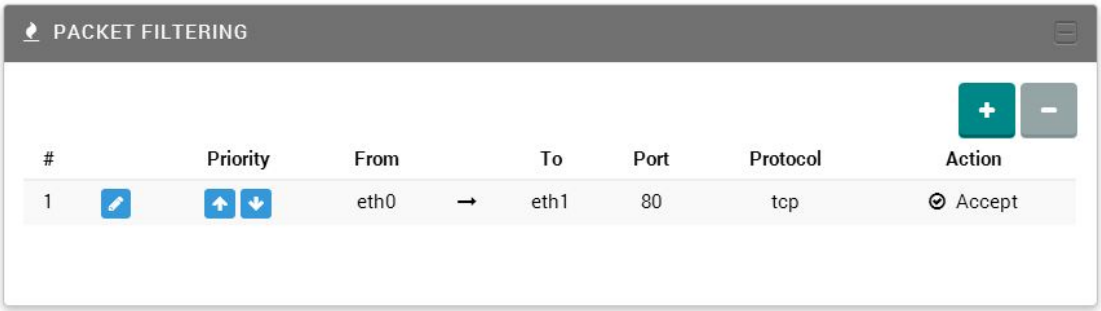
Action: Accept

Protocol: ○ TCP ○ UDP ○ ICMP

Port: 1 - 65535

Field	Description
From	Select the source Interface (Ethernet / WiFi / Cellular / Firewall / All).
To	Select the destination Interface (Ethernet / WiFi / Cellular / Firewall / All).
Action	Select an action (Accept / Reject / Drop).
Protocol	Select a protocol (TCP / UDP / ICMP).
Port	Enter the protocol port number (available when your Protocol choice is TCP or UDP).

After you click the "Save" button, you should see the new filtering rule that was generated. Note that if you choose a rule, the "minus" icon will become active, allowing you to delete the rule if you so desire.



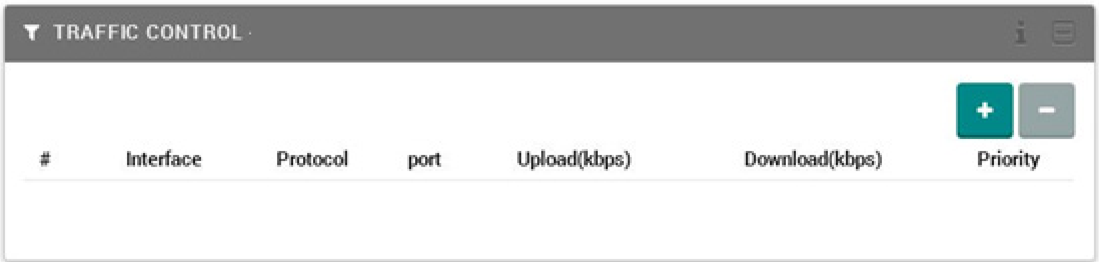
PACKET FILTERING

#		Priority	From		To	Port	Protocol	Action
1	✎	↑ ↓	eth0	→	eth1	80	tcp	✓ Accept

Traffic Control

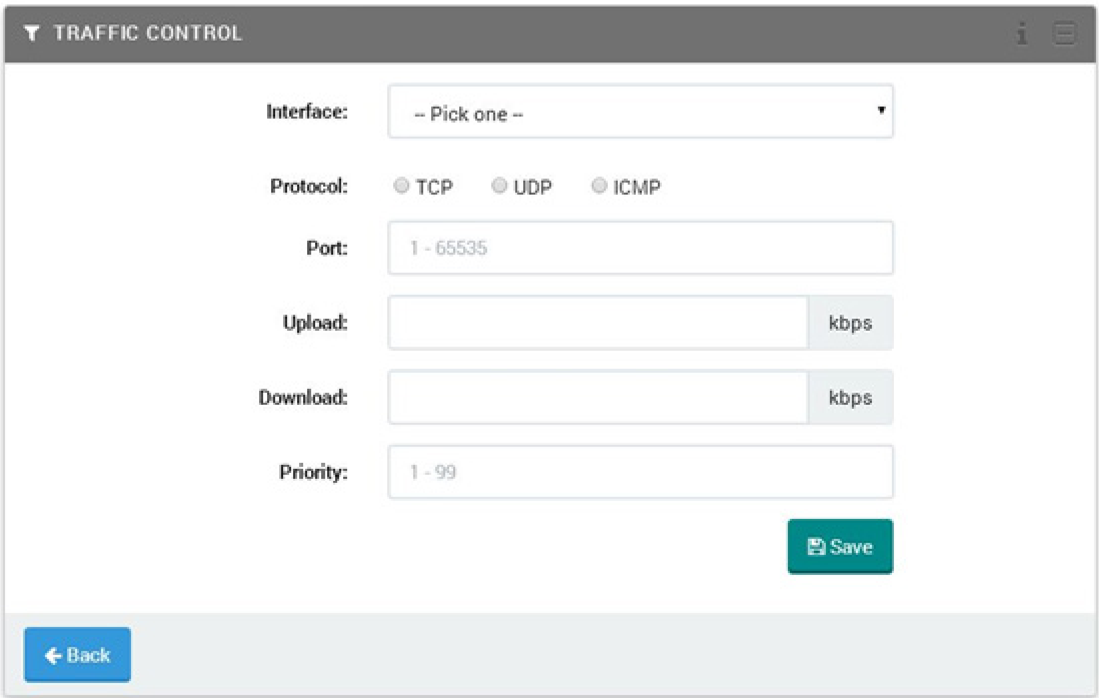
Traffic control allows you to limit the network bandwidth through the path. The input column defines the total maximum amount of traffic allowed for this interface. If the maximum rate is exceeded, excess packets will be dropped. This is valuable if you have a DSL connection, because it avoids queuing at your provider's side. If you don't want any traffic to be dropped, set this to a value faster than your interface maximum rate, or set it to 0 (zero).

To determine the optimum value of input limits, start by setting the limit significantly below your measured download bandwidth (20% or so). While downloading, measure the ping response time from the firewall to the upstream router, and gradually increase the setting. The optimal setting is at the point beyond which the ping time increases sharply as you increase the setting. For outbound traffic, specify the maximum speed the connection can handle (if you don't know this, ask your ISP for the speeds your account is rated for). Outgoing traffic above this rate will be dropped.



#	Interface	Protocol	port	Upload(kbps)	Download(kbps)	Priority

Click + to add a new traffic control rule.



Interface: -- Pick one --

Protocol: ○ TCP ○ UDP ○ ICMP

Port: 1 - 65535

Upload: kbps

Download: kbps

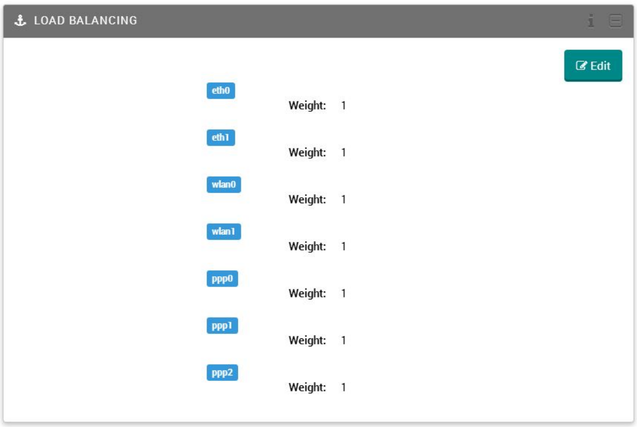
Priority: 1 - 99

Field	Description
Interface	Select the interface (Ethernet / WiFi / Cellular / Firewall / All).
Protocol	Select the protocol (TCP / UDP / ICMP).
Port	Enter the protocol port number (available when your Protocol choice is TCP or UDP).
Upload	Enter the maximum bandwidth for uploading.
Download	Enter the maximum bandwidth for downloading.
Priority	Enter the priority of these QoS rules. Smaller values have higher priority.

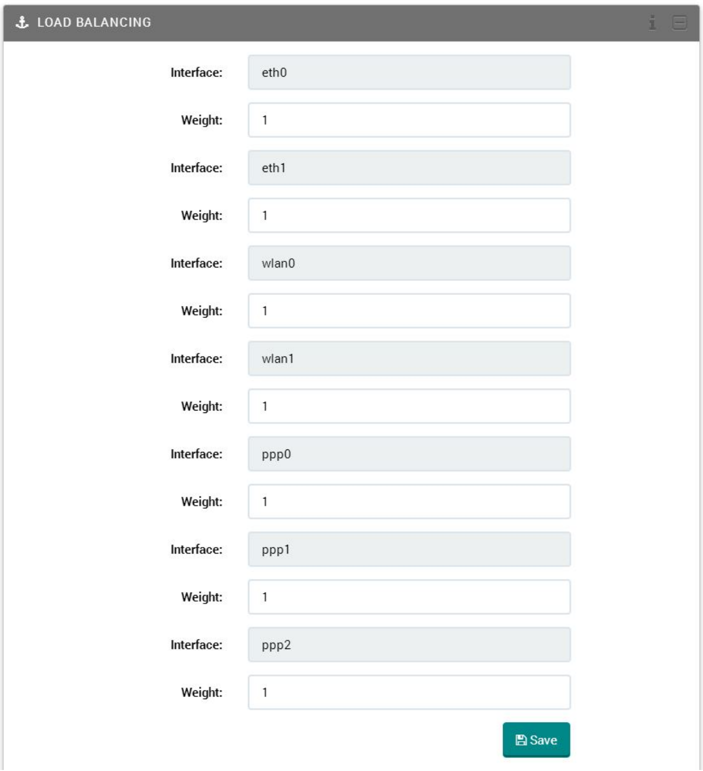
Load Balancing

The MAR-2000's load balancing feature balances outbound connections according to the destination route. Because some providers will be disproportionately accessed, and because routes are cached, certain interfaces may yet be slowed by a disproportionate load of network traffic.

When IP balancing is in effect, the kernel constructs an array of all possible routes (in this case, the interfaces) and then randomly selects the next route from among them. The system default is an un-weighted round robin, where the route to each interface is represented in the routing table once, and only once. With three interfaces, this means there will only be three entries in the table, with each route to an interface being randomly assigned a new connection one out of three times. In this load balancing interface, the numbers assigned represent the number of times each interface will be represented in a single round of route budgeting. For this reason, and to avoid taking up too much kernel space, large numbers must be avoided. Similarly, unless exceptional circumstances apply, administrators should not weight one interface too heavily relative to another; e.g., a 10 to 1 or 8 to 1 ratio is almost certain to result in undesirable network effects. Typically, no interface should be represented more than five times as often as another interface.



eth0 Weight: 1
eth1 Weight: 1
wlan0 Weight: 1
wlan1 Weight: 1
ppp0 Weight: 1
ppp1 Weight: 1
ppp2 Weight: 1



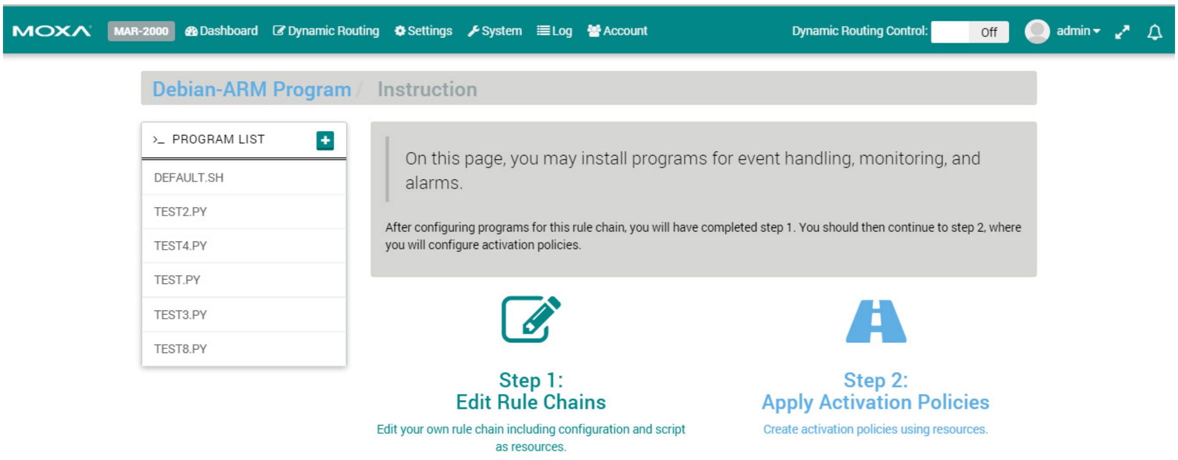
Interface: eth0
Weight: 1
Interface: eth1
Weight: 1
Interface: wlan0
Weight: 1
Interface: wlan1
Weight: 1
Interface: ppp0
Weight: 1
Interface: ppp1
Weight: 1
Interface: ppp2
Weight: 1

Field	Description
Interface	Label that indicates which interface you need to configure.
Weight	Enter a weight value from 1 to 10. Higher values have a higher weight.

Debian-ARM Program

From this page, you can import the scripts or programs that you want to execute in MAR-2000. You must use a cross compiler with Debian-ARM compliance and compile all programs in static link format.

For programs that are not compiled in static link format, make sure that you install the required executable library on MAR-2000 before you upload the programs.



On this page, you may install programs for event handling, monitoring, and alarms.

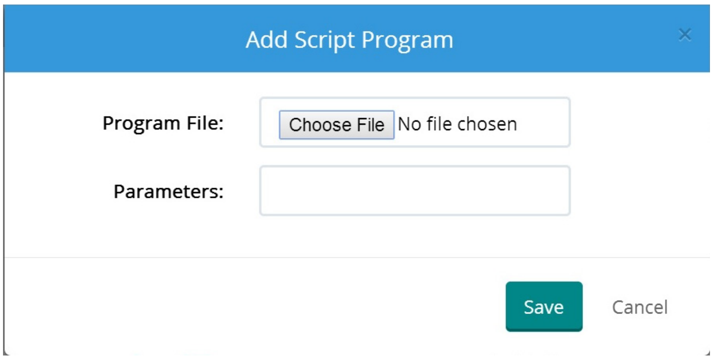
After configuring programs for this rule chain, you will have completed step 1. You should then continue to step 2, where you will configure activation policies.

Edit your own rule chain including configuration and script as resources.

Create activation policies using resources.

NOTE See Appendix A for information on how to find a tool chain for cross compiling your program.

"DEFAULT.SH" is the default program; it doesn't do anything. Click + to add your own program.

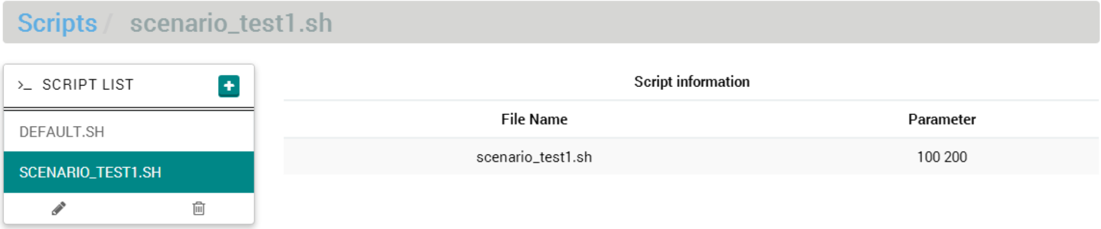


Program File: No file chosen

Parameters:

Field	Description
Program File	Import the program.
Parameters	Enter the parameters that will input into program, separated by spaces.

After you import your shell script, you will see a new script listed on the page.



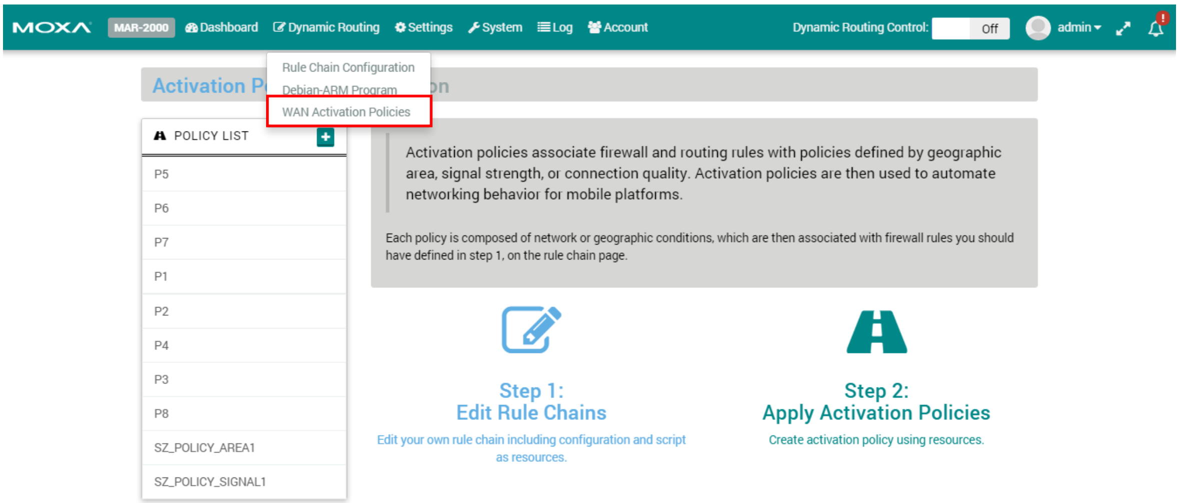
Script information

File Name	Parameter
scenario_test1.sh	100 200

The shell scripts you import will be executed automatically when some condition is met. How the mechanism works is described in the next section, "WAN Activation Policies."

WAN Activation Policies

WAN activation policies associate firewall and routing rules with zones defined by geographic area, signal strength, or connection quality. WAN activation policies are then used to automate networking behavior for mobile platforms.



P5

P6

P7

P1

P2

P4

P3

P8

SZ_POLICY_AREA1

SZ_POLICY_SIGNAL1

Activation policies associate firewall and routing rules with policies defined by geographic area, signal strength, or connection quality. Activation policies are then used to automate networking behavior for mobile platforms.

Each policy is composed of network or geographic conditions, which are then associated with firewall rules you should have defined in step 1, on the rule chain page.

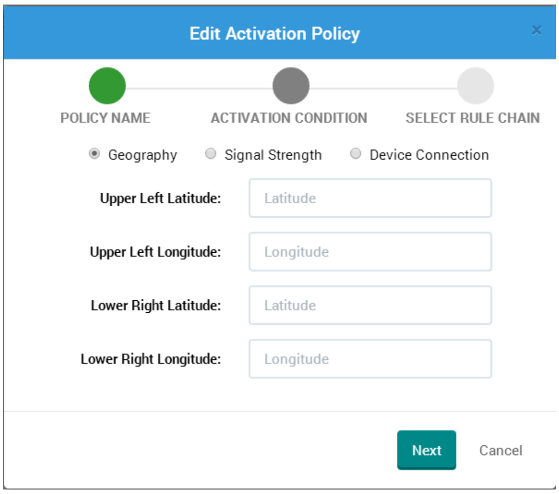
Step 1:
Edit Rule Chains
Edit your own rule chain including configuration and script as resources.

Step 2:
Apply Activation Policies
Create activation policy using resources.

Click + to add a new "Activation Policy". For example, you could add a Z3 activation policy, and then choose a type of condition (Geography, Signal Strength, or Device Connection).

Geography

If you select Geography, you will need to define a geographical region by inputting the latitude and longitude of two points. Each time the MAR-2000 enters this region, the rule chain or program you have configured/uploaded already will be triggered.



● Geography ○ Signal Strength ○ Device Connection

Upper Left Latitude: Latitude

Upper Left Longitude: Longitude

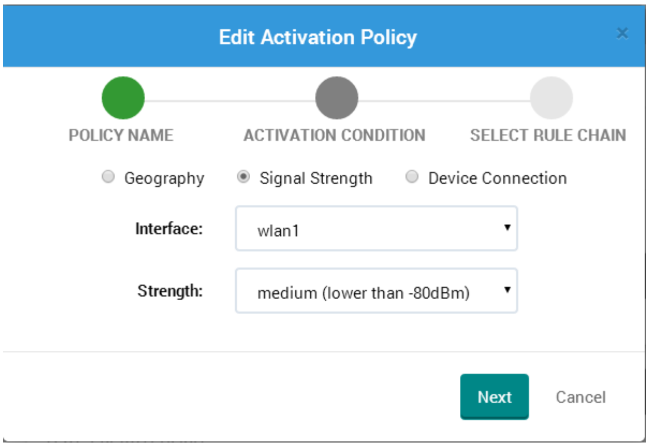
Lower Right Latitude: Latitude

Lower Right Longitude: Longitude

Field	Description
Upper Left Latitude	Enter the latitude of the upper left point.
Upper Left Longitude	Enter the longitude of the upper left point.
Lower Right Latitude	Enter the latitude of the lower right point.
Lower Right Longitude	Enter the longitude of the lower right point.

Signal Strength

If you select **Signal Strength**, choose which interface and signal strength monitor. When the condition you assigned is met, the rule chain or program you have configured/uploaded already will be triggered.



Edit Activation Policy

POLICY NAME ACTIVATION CONDITION SELECT RULE CHAIN

○ Geography ● Signal Strength ○ Device Connection

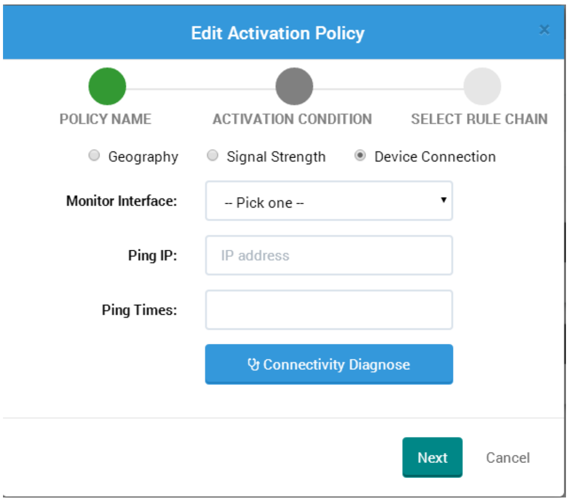
Interface: wlan1

Strength: medium (lower than -80dBm)

Field	Description
Interface	Select a WiFi or Cellular interface.
Strength	Select the signal strength.

Device Connection

If you select Device Connection, you will need to define a ping condition. When the ping is successful, the rule chain or program you have configured/uploaded already will NOT be triggered. If the ping is not successful, the rule chain or program you have configured/uploaded already will be triggered.



Edit Activation Policy

POLICY NAME ACTIVATION CONDITION SELECT RULE CHAIN

○ Geography ○ Signal Strength ● Device Connection

Monitor Interface: -- Pick one --

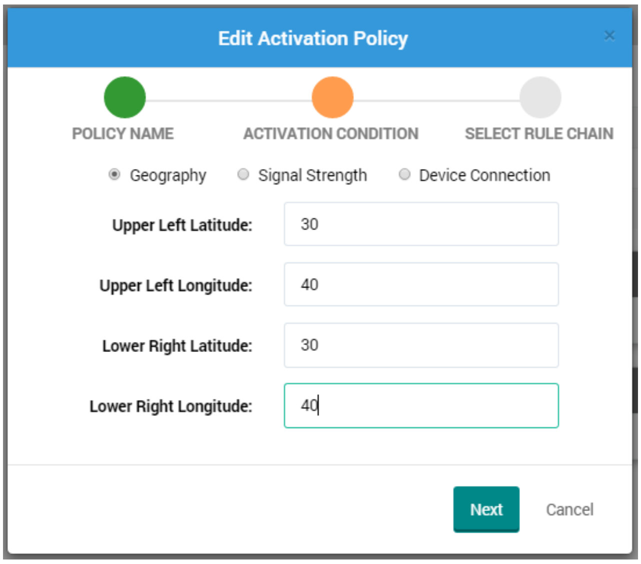
Ping IP: IP address

Ping Times:

Field	Description
Monitor Interface	Select the network interface.
Ping IP	Enter the IP address you want to ping.
Ping Times	Enter how many the ping must fail to trigger a device connection failure.
Connectivity Diagnose	Click to send a test ping to the Ping IP.

WAN Activation Policy Example

For this example, we use Geography to illustrate how to configure a WAN activation policy. First, input 30, 40, 30, and 40 into the four latitude and longitude text boxes, in that order, and then click Next.



● Geography ○ Signal Strength ○ Device Connection

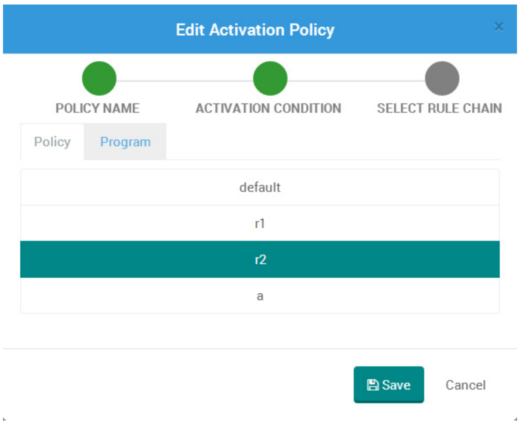
Upper Left Latitude: 30

Upper Left Longitude: 40

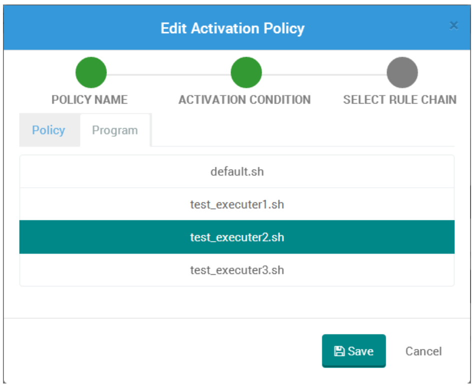
Lower Right Latitude: 30

Lower Right Longitude: 40

When the **Edit Activation Policy** window opens, click **SELECT RULE CHAIN** and then click **Policy** or **Program** to configure how the policy will be triggered. In either case, click the name of the policy you would like to use, and then click the **Save** button. If you don’t choose a Rule Chain Configuration or Program, the default Rule Chain Configuration or Default Program will be executed when the condition is met.

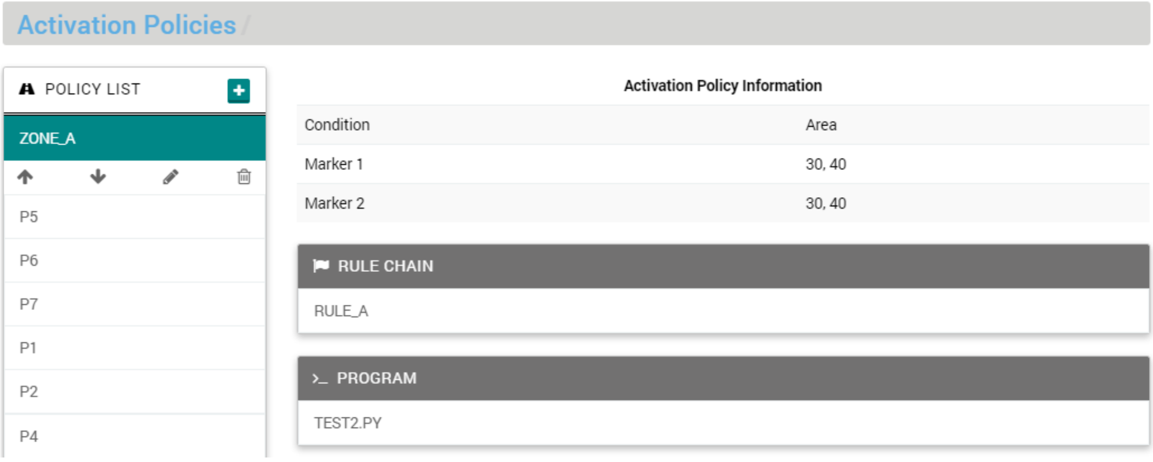


default
r1
r2
a



default.sh
test_executer1.sh
test_executer2.sh
test_executer3.sh

The following figure illustrates that the condition is Area, the Rule Chain Configuration is RULE_A, and the Program is SCENARIO_TEST1.SH. This means that both RULE_A and TEST2.PY will be triggered when the MAR-2000 enters the region defined above.



Activation Policy Information

Condition	Area
Marker 1	30, 40
Marker 2	30, 40

RULE CHAIN

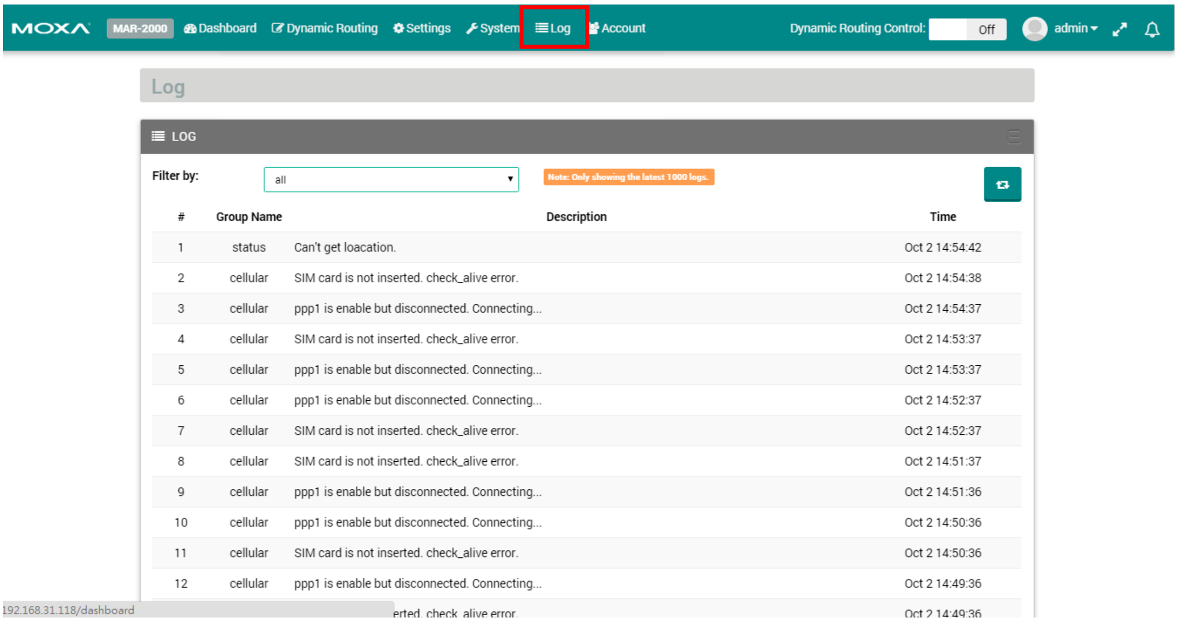
RULE_A

PROGRAM

TEST2.PY

Log

The log section provides a summary of system activity as recorded by syslog.

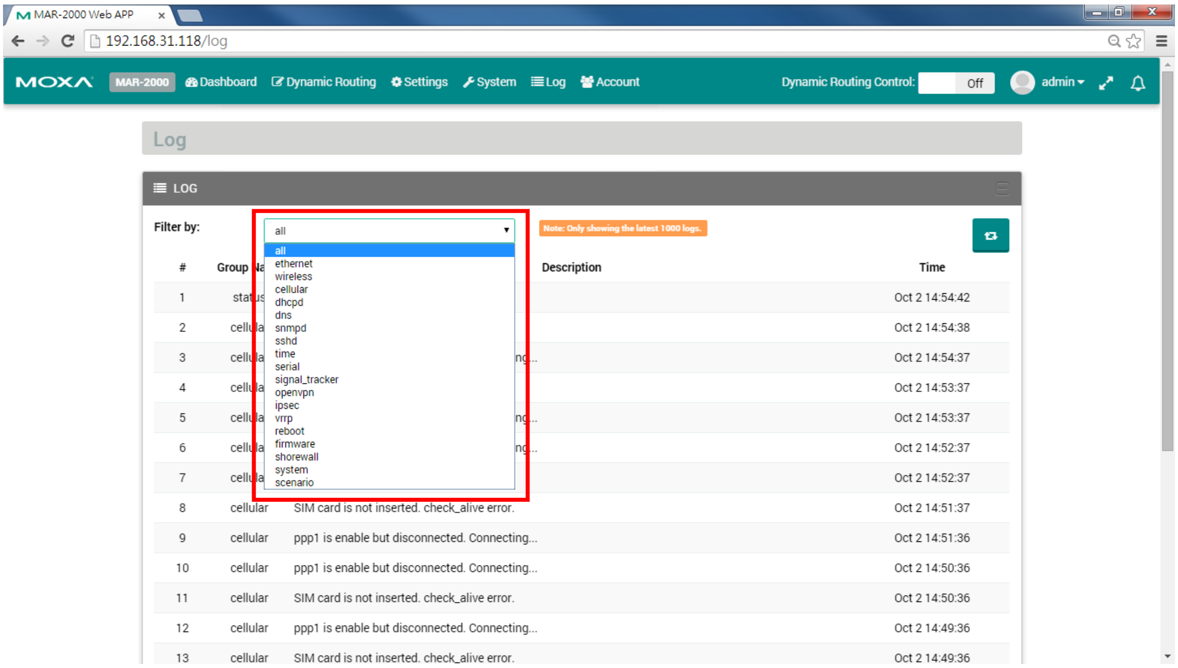


Filter by: all

Note: Only showing the latest 1000 logs.

#	Group Name	Description	Time
1	status	Can't get loacation.	Oct 2 14:54:42
2	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:54:38
3	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:54:37
4	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:53:37
5	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:53:37
6	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:52:37
7	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:52:37
8	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:51:37
9	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:51:36
10	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:50:36
11	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:50:36
12	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:49:36
		erted. check_alive error.	Oct 2 14:49:36

Select the type of log from the drop-down list, which shows specific events of the selected service.



Filter by: all

Note: Only showing the latest 1000 logs.

#	Group Na	Description	Time
1	statu		Oct 2 14:54:42
2	cellu		Oct 2 14:54:38
3	cellu	ng...	Oct 2 14:54:37
4	cellu		Oct 2 14:53:37
5	cellu	ng...	Oct 2 14:53:37
6	cellu	ng...	Oct 2 14:52:37
7	cellu		Oct 2 14:52:37
8	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:51:37
9	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:51:36
10	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:50:36
11	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:50:36
12	cellular	ppp1 is enable but disconnected. Connecting...	Oct 2 14:49:36
13	cellular	SIM card is not inserted. check_alive error.	Oct 2 14:49:36

The log section provides a summary of system activity as recorded by syslog, OpenVPN, and the Shoreline Firewall. To set up the logger, navigate to the configuration screen by clicking the **Setup** tab.

Under the **Logger** tab, select the subsystems that you want the system to monitor.

Field	Description
System status	Returns default syslog entries (severity level 7).
OpenVPN	Returns default log entries (level 4) returned by OpenVPN.
Firewall	Returns logs generated by the Shoreline Firewall.

After you have chosen the logs you want to display, click **Apply** to complete the setup.

To view the log files, click the **View** tab (just below the Setup tab). Click **Refresh** to update the window to display the most recent log entries.

A

Linux Tool Chain Introduction

The following topics are covered in this appendix:

❒ **Overview**

❒ **Cross Compiling Applications and Libraries**

Overview

To ensure that an application will be able to run correctly when installed on the MAR-2000, you must ensure that it is compiled and linked to the same libraries that will be present on the MAR-2000. This is particularly true when the RISC XScale processor architecture of the MAR-2000 differs from the CISC x86 processor architecture of the host system, but it is also true if the processor architecture is the same.

The host tool chain that comes with the MAR-2000 contains a suite of cross compilers and other tools, as well as the libraries and headers that are necessary to compile applications for the MAR-2000. The host environment must be running Linux to install the MAR-2000 GNU Tool Chain. We have confirmed that the following Linux distributions can be used to install the tool chain:

Fefora 19, Debian 6/7, Ubuntu 12/13 32-bit platform.

To use toolchain in a 64-bit environment, 32-bit libraries should be installed.

In Debian:

```
$ dpkg --add-architecture i386
$ apt-get update
$ sudo apt-get install ia32-libs
```

In Ubuntu:

```
$ apt-get update
$ sudo apt-get install libc6:i386
$ sudo apt-get install zlib1g:i386
```

In Fedora:

```
yum install glibc.i686
yum install zlib.i686
```

The Tool Chain will need about 250 MB of hard disk space on your PC. The MAR-2000 Tool Chain is located on the MAR-2000 CD. To install the Tool Chain, insert the CD into your PC and then issue the following commands:

With v1.x firmware

```
# mount /dev/cdrom /mnt/cdrom
# sh /mnt/cdrom/tool-chain/linux/arm-linux-4.7.2-v5_Build_YYMMDDHH.sh
```

Note that the toolchain is built with a 32-bit environment. If your computer is 64-bit, install **ia32-libs** before using the Tool Chain.

Wait for a few minutes while the Tool Chain is installed automatically on your Linux PC. Once the host environment has been installed, add the directory /usr/local/arm-linux-4.7.2-v5/bin/ to your path. You can do this temporarily for the current login session by issuing the following command:

```
#export PATH="/usr/local/arm-linux-4.7.2-v5/bin:$PATH"
```

Alternatively, you can add the same commands to **$HOME/.bash_profile** to force it to take effect for all login sessions initiated by this user.

Cross Compiling Applications and Libraries

To compile a simple C application, use the cross compiler instead of the regular compiler:

```
#arm-none-linux-gnueabi-gcc   –o example –Wall –g –O2 example.c
#arm-none-linux-gnueabi-strip   –s example
#arm-none-linux-gnueabi-gcc   -ggdb –o example-debug example.c
```

B

Connecting the MAR-2000 Console to a PC

There are 2 ways to connect a PC to the MAR-2000 console: directly, through the serial console port, or by SSH, over a network. Once you turn on the power, you will be able to access the MAR-2000 kernel.

The following topics are covered in this appendix:

- ❒ **Serial Console**
- ❒ **SSH Console**
  - ➢ Windows Users
  - ➢ Linux Users

Serial Console

The serial console port gives users a convenient way of connecting to the MAR-2000's console utility. This method is particularly useful when using the computer for the first time, or if you forget the MAR-2000's IP address on the network for logging in to the MAR-2000 web page. The signal is transmitted over a direct serial connection, so you do not need to know any of its IP addresses to connect.

Use the serial console port settings shown below.

Baudrate	115200 bps
Parity	None
Data bits	8
Stop bits	1
Flow Control	None
Terminal	VT100

Once the connection is established, you can begin using the system once the root prompt appears:

root@Moxa:~#

SSH Console

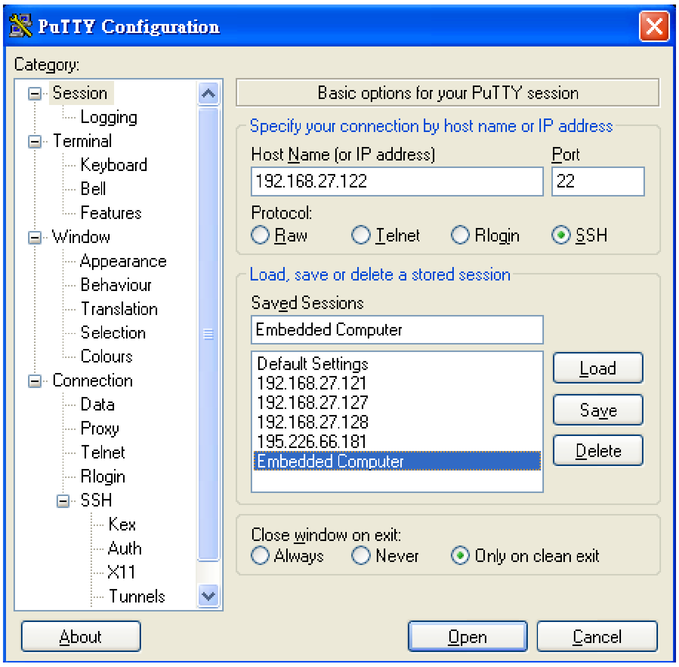
The MAR-2000 supports an SSH console to provide users with more secure login options.

Windows Users

In a Windows environment, you can use the free software PuTTY as your SSH interface. To set up an SSH console for the MAR-2000, click on the following link to download the PuTTY freeware:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The following figure shows a simple example of the required configuration:



Host Name (or IP address): 192.168.27.122

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: Embedded Computer

Default Settings
192.168.27.121
192.168.27.127
192.168.27.128
195.226.66.181
Embedded Computer

Close window on exit: ○ Always ○ Never ● Only on clean exit

Linux Users

From a Linux machine, ssh is simply called from the console prompt.

#ssh 192.168.4.127

Select yes to complete the connection.

```
[root@bee_notebook root]# ssh 192.168.4.127
The authenticity of host ‘192.168.4.127 (192.168.4.127)’ can’t be established.
RSA key fingerprint is 8b:ee:ff:84:41:25:fc:cd:2a:f2:92:8f:cb:1f:6b:2f.
Are you sure you want to continue connection (yes/no)? yes
```

To display a help screen, type “ssh –h”; for more detailed assistance, type “man ssh”.