



JetBox 5630

Web User Manual

www.korenix.com

Copyright Notice

Copyright© 2013 Korenix Technology Co., Ltd.

All rights reserved.

Reproduction without permission is prohibited.

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

The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Korenix assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.

Korenix reserves the right to make changes in the product design without notice to its users.

Acknowledgments

Korenix is a registered trademark of Korenix Technology Co., Ltd.

All other trademarks or registered marks in the manual belong to their respective manufacturers.

Table of Content

	Copyright Notice	2
	Acknowledgments.....	2
	Table of Content	3
Chapter 1	Getting Start.....	5
1-1	Web Server.....	5
1-2	Preparation for Web Interface.....	6
1-3	System Login	6
Chapter 2	System.....	7
2-1	Overview	7
2-2	Password	7
2-3	Scheduled Task.....	8
2-4	Startup	9
2-5	General Settings	9
2-6	Backup Configuration.....	10
2-7	Firmware Upgrade	11
2-8	Reboot.....	12
Chapter 3	Network	12
3-1	Status	12
3-2	Settings.....	13
3-3	WiFi Settings	13
3-4	3G Settings	17
3-5	Network Redundancy	19
3-6	MSR	21
3-7	Diagnostics	23
Chapter 4	Switch.....	24
4-1	Port Status.....	24
4-2	Port Control.....	24
4-3	VLAN.....	25
4-4	PVID.....	25
4-5	QoS.....	26
4-6	Rate Limit	29
Chapter 5	Routing.....	30
5-1	Status	30
5-2	Static Routes	31
5-3	OSPF	32
5-4	RIP	34
Chapter 6	Firewall.....	36

6-1	Forwarding	36
6-2	NAT	37
6-3	Filter	40
Chapter 7	VPN.....	41
7-1	OpenVPN.....	41
7-2	IPSec	44
7-3	Certificates	47
7-4	PPTP	49
7-5	L2TP	51
7-6	L2TPv3	55
7-7	CHAP-Secrets	57
Chapter 8	Serial.....	58
8-1	Port Settings.....	58
8-2	Serial to Network	59
8-3	ModBus Gateway.....	60

Chapter 1 Getting Start

1-1 Web Server

In JetBox5630, we will start web server automatically. You can see it with 'ps' command.

```
1175 root    /lib/udev/udevd
1440 root    {hostenv.sh} /bin/sh ./hostenv.sh host /usr/lib/lua /usr/lib/lua
1448 root    lua /web/lucid.lua
```

The default path is /web/.

```
/web $ df
Filesystem      Size      Used Available Use% Mounted on
ubi0:rootfs    95.3M    34.6M    60.7M   36% /
ubi1:etc        6.5M     580.0K    5.9M    9% /etc
ubi2:web        6.5M     3.2M     3.3M   49% /web
ubi3:opt       104.4M     1.0M   103.3M    1% /opt
tmpfs           30.0M     92.0K    29.9M    0% /tmp
tmpfs           100.0M      0      100.0M    0% /home
tmpfs           5.0M      4.0K     5.0M    0% /root
tmpfs           1.0M      0      1.0M    0% /usr/etc
tmpfs           1.0M      0      1.0M    0% /media
```

```
~ $ cd /web/
/web $
/web $ ls
build      host      hostenv.sh  lucid.lua  setup.lua
/web $
/web $
```

The default port number of web server is **80**.



NOTE

- **If unnecessary, don't modify or delete any content in /web.**
- We will keep the latest version and provide firmware to upgrade web server.

1-2 Preparation for Web Interface

Korenix web management page is developed by LUA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, Chrome, or Mozilla, to configure the JetBox from anywhere on the network.

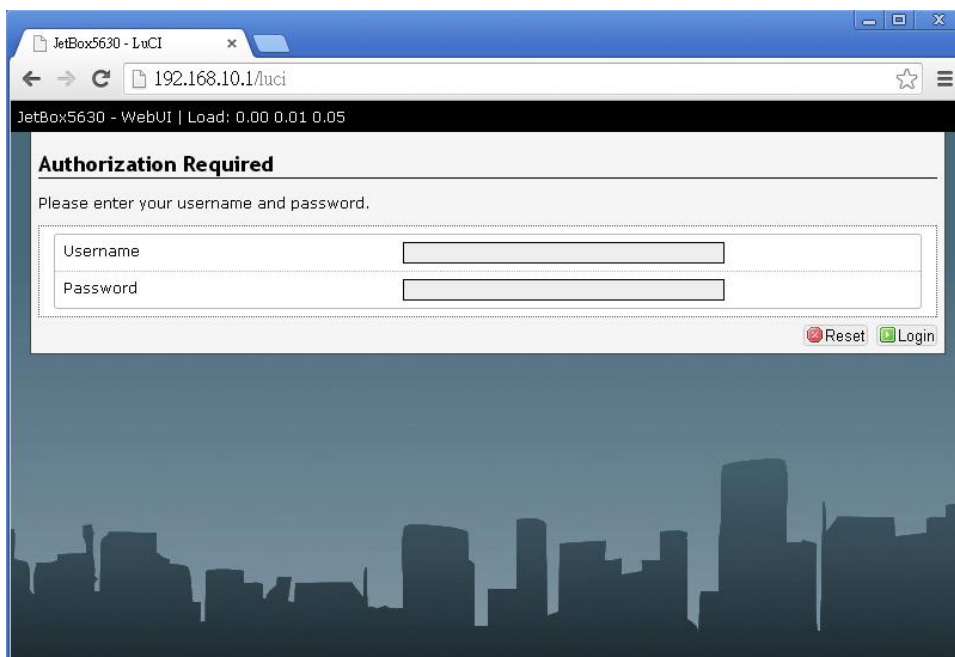
Before you attempt to use the embedded web interface to manage JetBox configuration, verify that your JetBox 5630 Series is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the JetBox and connect it to your computer via LAN port.
3. Make sure that the LAN's default IP address is 192.168.10.1.
4. Change your computer IP address to 192.168.10.2 or other IP address which is located in the 192.168.10.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode in your computer and ping 192.168.10.1 to verify a normal response time.

1-3 System Login

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Chrome) on the PC.
2. Type `http://192.168.10.1` (or the IP address of the switch). And then press Enter.
3. The login screen will appear next.



We have two user accounts to login. One is **root** without password and another is **admin/admin**.

Chapter 2 System

2-1 Overview

You can see system information on this section. Such as Hostname、Firmware version、WebUI version etc... and also display memory information.

The screenshot shows the 'System' tab selected in the navigation menu. The 'Overview' sub-tab is active. The 'Status' section is expanded, showing system and memory information.

System	
System Name	JetBox5630
Firmware Version	1.0.2 2014-09-10 15:27:06
Kernel Version	3.2.0
WebUI Version	1.1
Local Time	Fri Sep 12 13:43:06 2014
Uptime	3h 31m 46s
Load Average	0.08, 0.03, 0.05

Memory	
Total Available	492628 kB / 511928 kB (96%)
Free	481864 kB / 511928 kB (94%)
Cached	10764 kB / 511928 kB (2%)
Buffered	0 kB / 511928 kB (0%)

2-2 Password

Change login password .

The screenshot shows the 'System' tab selected in the navigation menu. The 'Password' sub-tab is active. The page title is 'Password' and the description is 'Changes the administrator password for accessing the device. (Password length 0~28)'. There are two input fields: 'Password' and 'Confirmation', each with a strength indicator icon. At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

Password length : **0~28**



NOTE

- When you change web login password, it will also change **system login password** simultaneously

2-3 Scheduled Task

It is the same with Cron daemon.

Syntax :

A crontab file has five fields for specifying day, date and time followed by the command to be run at that interval.

```
* * * * * command to be executed
- - - - -
| | | | |
| | | | +----- day of week (0 - 6) (Sunday=0)
| | | +----- month (1 - 12)
| | +----- day of month (1 - 31)
| +----- hour (0 - 23)
+----- min (0 - 59)
```

Example :

Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.

```
* * * * * date > /tmp/test
```

Reset Save & Apply

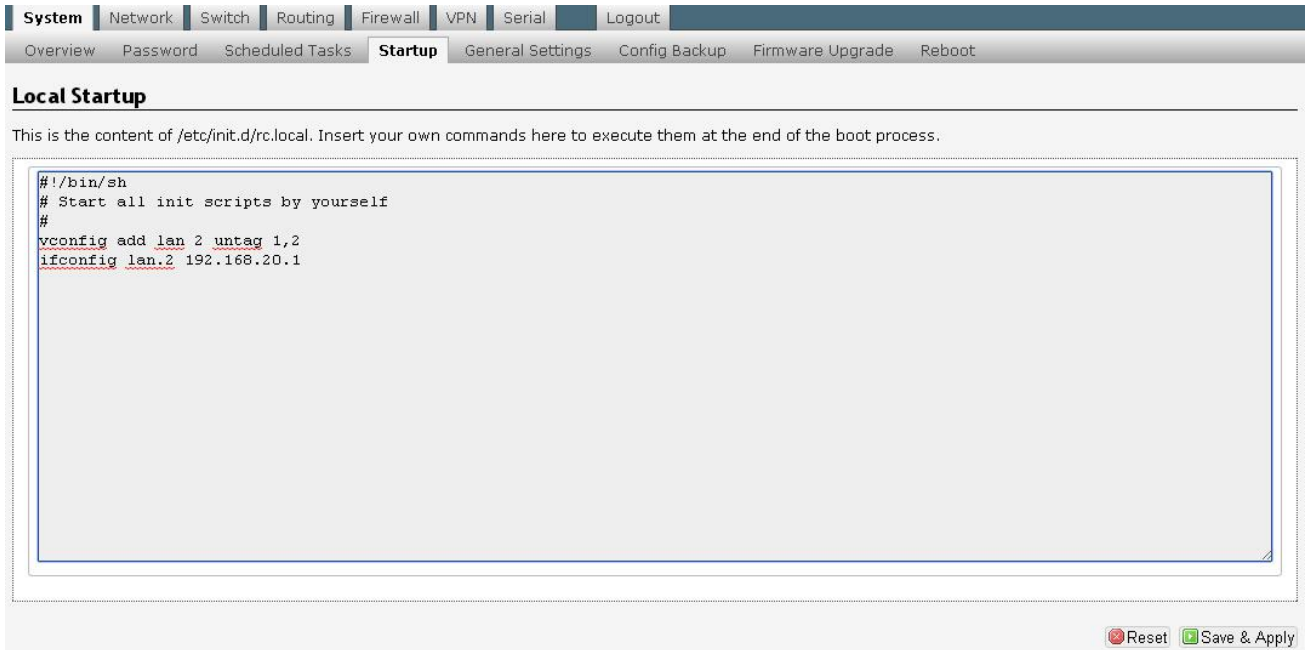
Press **Save & Apply** to save configuration and start Cron daemon.

2-4 Startup

We provide a Startup script (`rc.local`) for user can run their program when system boot up.

For example :

If we want to add a vlan 2 and set ip address 192.168.20.1 when system boot up, we can write these commands here. It will run automatically at the end of boot process.



The screenshot shows the 'Startup' configuration page. At the top, there is a navigation menu with tabs for System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below this is a sub-menu with tabs for Overview, Password, Scheduled Tasks, Startup (selected), General Settings, Config Backup, Firmware Upgrade, and Reboot. The main heading is 'Local Startup'. Below the heading is a text box containing the following content:

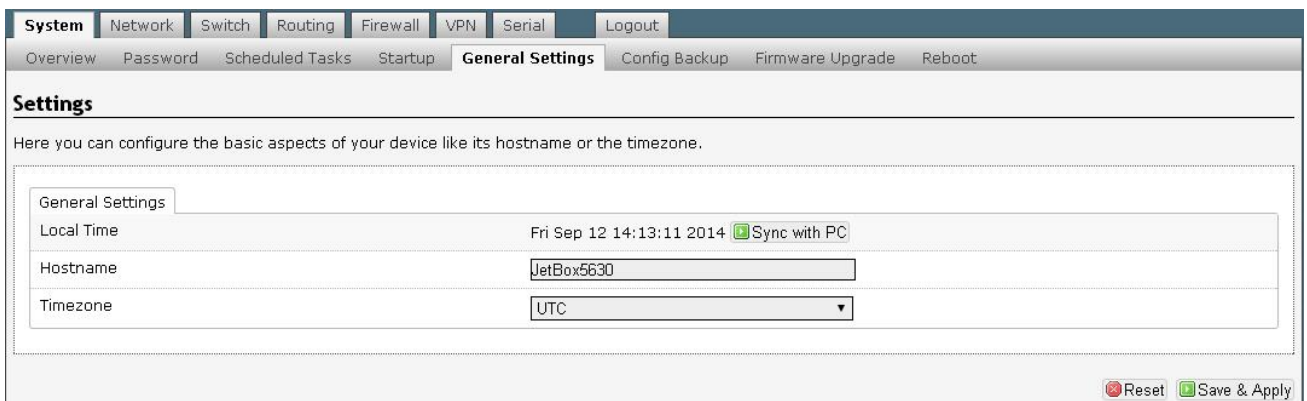
```
#!/bin/sh
# Start all init scripts by yourself
#
vconfig add lan 2 untag 1,2
ifconfig lan.2 192.168.20.1
```

At the bottom right of the page, there are two buttons: 'Reset' (with a red circle icon) and 'Save & Apply' (with a green checkmark icon).

Press **Save & Apply** to save configuration.

2-5 General Settings

Here you can configure the basic aspects of your device like its Hostname or the Timezone.



The screenshot shows the 'General Settings' configuration page. At the top, there is a navigation menu with tabs for System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below this is a sub-menu with tabs for Overview, Password, Scheduled Tasks, Startup, General Settings (selected), Config Backup, Firmware Upgrade, and Reboot. The main heading is 'Settings'. Below the heading is a text box containing the following content:

Here you can configure the basic aspects of your device like its hostname or the timezone.

General Settings	
Local Time	Fri Sep 12 14:13:11 2014 <input type="checkbox"/> Sync with PC
Hostname	<input type="text" value="JetBox5630"/>
Timezone	<input type="text" value="UTC"/>

At the bottom right of the page, there are two buttons: 'Reset' (with a red circle icon) and 'Save & Apply' (with a green checkmark icon).

Sync with PC :

It will get the UTC time from your PC. And local time have to be added with Timezone.

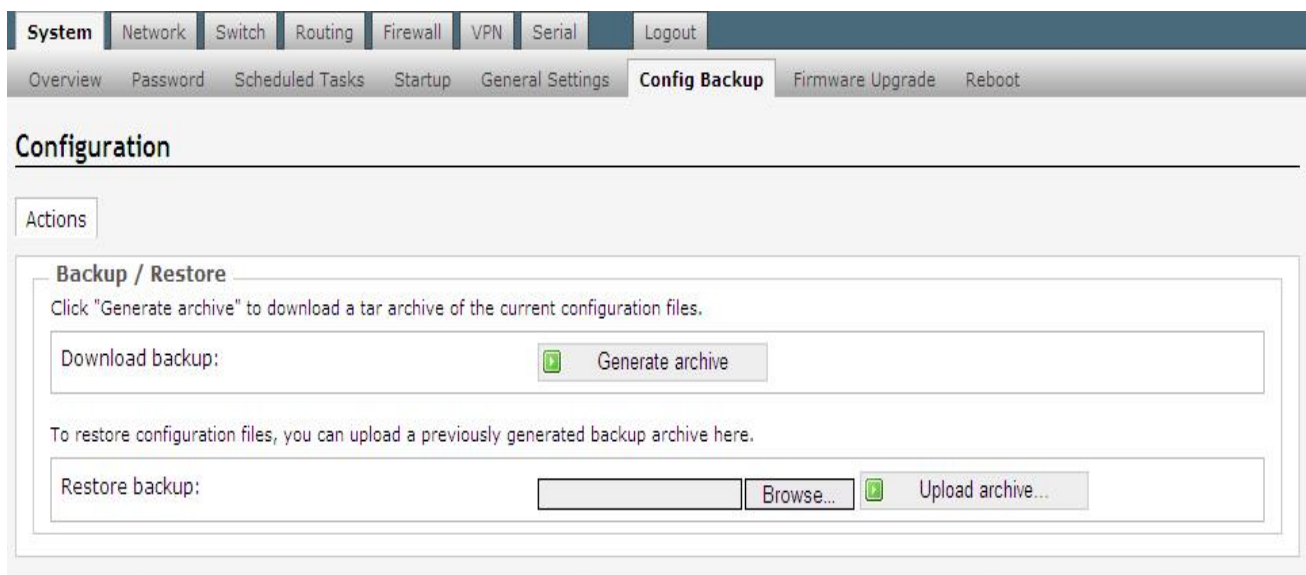
For example :

The UTC time of PC is **12:00:00 2013** and Timezone is Asia/Taipei.

So the local time will be **18:00:00 2013**.

2-6 Backup Configuration

In **Config Backup** page, user can use it to backup system configuration. It will backup all files in /etc. And user can apply these configurations to other JetBox.




The screenshot shows a web interface with a navigation menu at the top. The menu includes 'System', 'Network', 'Switch', 'Routing', 'Firewall', 'VPN', 'Serial', and 'Logout'. Below the menu is a sub-menu with 'Overview', 'Password', 'Scheduled Tasks', 'Startup', 'General Settings', 'Config Backup', 'Firmware Upgrade', and 'Reboot'. The 'Config Backup' page is active, showing a 'Configuration' section. Underneath, there is an 'Actions' tab. The main content area is titled 'Backup / Restore' and contains two sections. The first section, 'Download backup:', has a 'Generate archive' button. The second section, 'Restore backup:', has a text input field, a 'Browse...' button, and an 'Upload archive...' button.

Download Backup :

Click "Generate archive" to download a tar archive of the current configuration files

Restore Backup :

Upload a previously generated backup archive to restore configuration files.



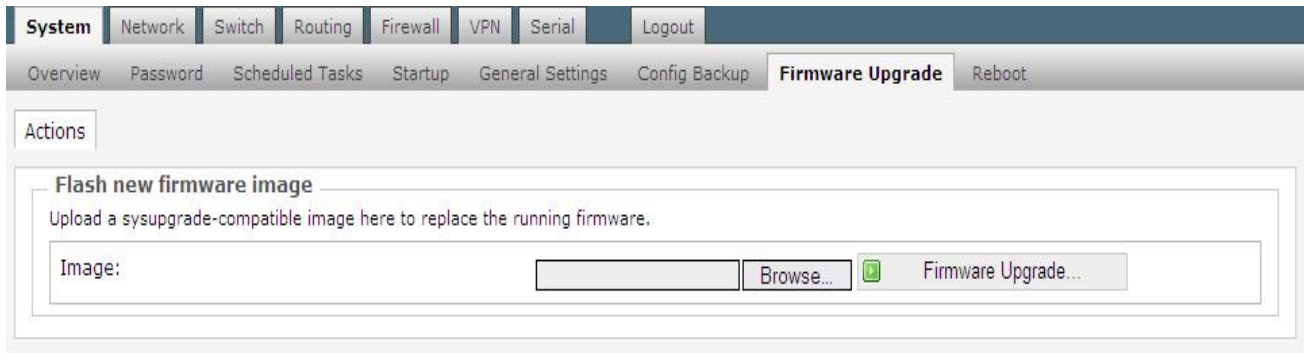
NOTE

- Restore configuration only extract all configuration files to /etc. It will not delete any files in /etc.

2-7 Firmware Upgrade

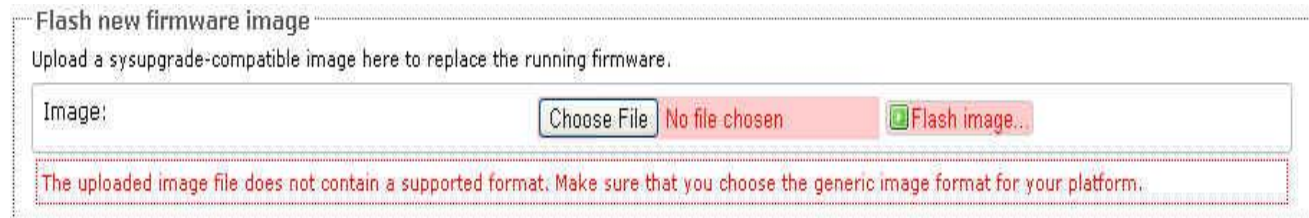
It is the same as firmware_up command in JetBox. User can upgrade firmware via Web or JetBox console.

Flash image :



The screenshot shows the 'Firmware Upgrade' section of a web interface. At the top, there is a navigation bar with tabs for 'System', 'Network', 'Switch', 'Routing', 'Firewall', 'VPN', 'Serial', and 'Logout'. Below this is a secondary navigation bar with tabs for 'Overview', 'Password', 'Scheduled Tasks', 'Startup', 'General Settings', 'Config Backup', 'Firmware Upgrade', and 'Reboot'. The main content area is titled 'Actions' and contains a section 'Flash new firmware image'. Below this title is the instruction: 'Upload a sysupgrade-compatible image here to replace the running firmware.' There is an 'Image:' label followed by a text input field, a 'Browse...' button, and a 'Firmware Upgrade...' button with a green checkmark icon.

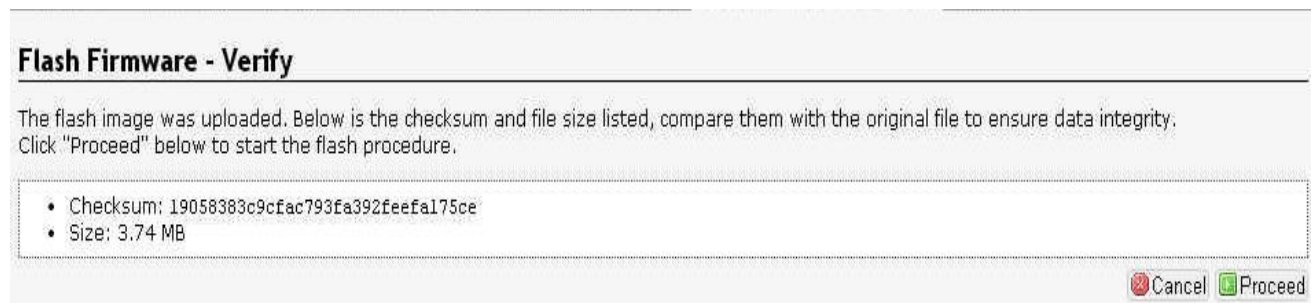
After select the image file, click it to start firmware upgrade. It will verify the image is valid or not.



This screenshot shows the 'Flash new firmware image' section with an error. The 'Image:' input field is empty, and the 'Choose File' button is highlighted. To its right, a red box contains the text 'No file chosen'. Further right is a 'Flash image..' button with a green checkmark icon. Below the input field, a red-bordered box contains the error message: 'The uploaded image file does not contain a supported format. Make sure that you choose the generic image format for your platform.'

Invalid Image

If image is valid, you will see the checksum and file size. Click "Proceed" to start flash image.

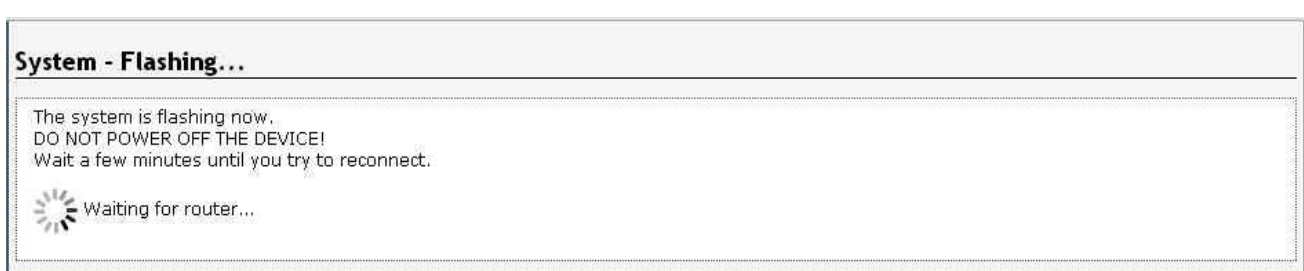


The screenshot shows the 'Flash Firmware - Verify' section. It contains the text: 'The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.' Below this text is a list of two items: 'Checksum: 19058383c9cfac793fa392feefal75ce' and 'Size: 3.74 MB'. At the bottom right of the section are two buttons: 'Cancel' with a red 'X' icon and 'Proceed' with a green checkmark icon.



NOTE

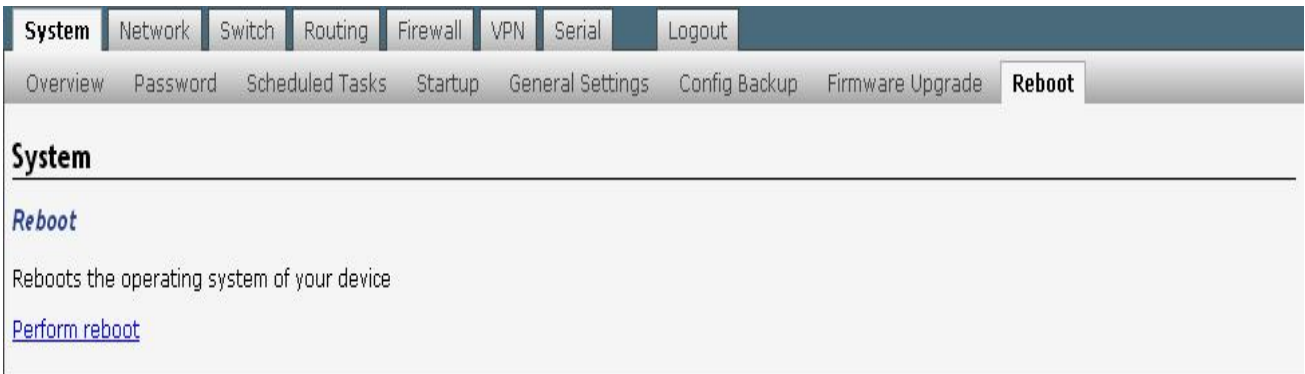
- When upgrade complete, the JetBox will reboot automatically. It will connect to web after few minutes.



The screenshot shows the 'System - Flashing...' section. It contains the text: 'The system is flashing now. DO NOT POWER OFF THE DEVICE! Wait a few minutes until you try to reconnect.' Below this text is a loading spinner icon followed by the text 'Waiting for router...'

2-8 Reboot

This page provide user can reboot the JetBox.



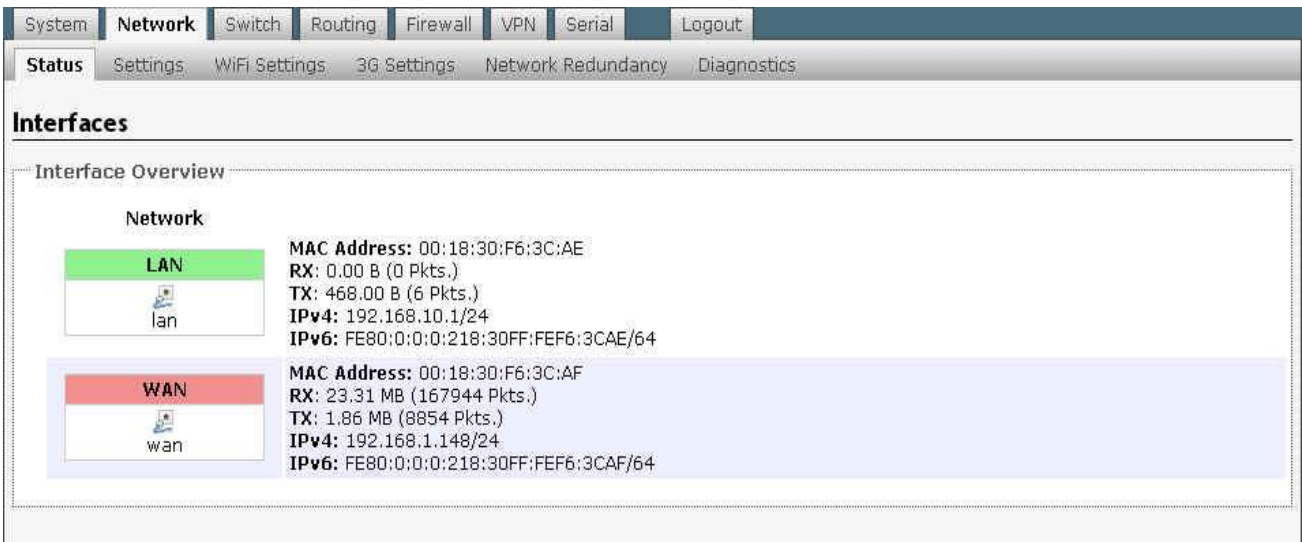
The screenshot shows the 'Reboot' page in the JetBox web interface. The navigation menu at the top includes System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. The 'Reboot' tab is selected. The page title is 'System' and the sub-section is 'Reboot'. The text states: 'Reboots the operating system of your device'. A link labeled 'Perform reboot' is provided.

Chapter 3 Network

This chapter includes information about network configuration. The information let user can easily set up the network. We also provide the wireless settings and network redundant function. These features are very useful and important for user.

3-1 Status

User can see the detail network information about LAN and WAN.



The screenshot shows the 'Network Status' page in the JetBox web interface. The navigation menu at the top includes System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. The 'Status' tab is selected. The page title is 'Interfaces' and the sub-section is 'Interface Overview'. The page displays details for two network interfaces: LAN and WAN.

Interface	MAC Address	RX	TX	IPv4	IPv6
LAN	00:18:30:F6:3C:AE	0.00 B (0 Pkts.)	468.00 B (6 Pkts.)	192.168.10.1/24	FE80:0:0:0:218:30FF:FEF6:3CAE/64
WAN	00:18:30:F6:3C:AF	23.31 MB (167944 Pkts.)	1.86 MB (8854 Pkts.)	192.168.1.148/24	FE80:0:0:0:218:30FF:FEF6:3CAF/64

3-2 Settings

User can change LAN and WAN IP address. It can specify Static IP or Dynamic IP.

System | Network | Switch | Routing | Firewall | VPN | Serial | Logout

Status | Settings | WiFi Settings | 3G Settings | Network Redundancy | MSR | Diagnostics

Network

LAN Settings

Apply immediately

Protocol: Static IP

IP-Address: 192.168.10.1

Netmask: 255.255.255.0

WAN Settings

Apply immediately

Protocol: Dynamic IP

Optional

Default Gateway (optional): 192.168.1.1

DNS-Server (optional): 168.95.1.1

Reset Save & Apply

And it also provides two optional fields, Default Gateway and DNS-Server.

- **Apply immediately**

It means that change IP address immediately. If you do not check it, the IP address will change after system reboot.

3-3 WiFi Settings

In JetBox5630, we have built-in AWUS036NEH wireless driver. You can easily install and use it to connect Ethernet. When you plug in the wireless dongle, click the WiFi settings and it will show the default wireless interface **ra0**.

System | Network | Switch | Routing | Firewall | VPN | Serial | Logout

Status | Settings | WiFi Settings | 3G Settings | Network Redundancy | MSR | Diagnostics

Wireless Overview

RaLink 802.11 Wireless Controller (ra0)

0% Wireless is disabled or not associated

Enable Edit Remove

Click **Edit** to edit the wireless configuration.

Press **“Scan”** to check how many access point in your environment.

"KorenixAP2" (ra0)

Device Configuration

General Setup

Status

10% **Mode:** Client | **SSID:** 11n-AP
BSSID: Not-Associated | **Encryption:** NONE-OPEN
Channel: 1 (2.412 GHz) | **Signal:** 0 dBm | **Noise:** 0 dBm
Bit Rate: 0.0 MBit/s

Searching wifi network

WLAN-Scan

Wifi networks in your local environment

Link	ESSID	BSSID	Mode	Channel	Encr.	Signal	Noise	Bit Rates
100/100		C8:D3:A3:40:E6:10	Managed	2.412 GHz (Channel 1)	on	-47 dBm	-92 dBm	54 Mb/s
78/100	Bearyen	8E:BE:BE:5F:A1:4C	Managed	2.412 GHz (Channel 1)	on	-59 dBm	-92 dBm	54 Mb/s
100/100	KorenixAP	60:02:B4:06:B1:8A	Managed	2.422 GHz (Channel 3)	on	-49 dBm	-92 dBm	54 Mb/s
100/100	Radius Test	62:02:B4:06:B1:8A	Managed	2.422 GHz (Channel 3)	on	-45 dBm	-92 dBm	54 Mb/s
100/100	CoovaChilli	60:02:B4:06:B4:EE	Managed	2.437 GHz (Channel 6)	off	-43 dBm	-92 dBm	54 Mb/s
94/100	JetWave2300_1	00:03:7F:48:99:85	Managed	2.437 GHz (Channel 6)	off	-53 dBm	-92 dBm	54 Mb/s
100/100	KorenixAP2	A8:54:B2:90:CC:D2	Managed	2.437 GHz (Channel 6)	on	-27 dBm	-92 dBm	54 Mb/s
37/100		FC:75:16:C0:2C:A0	Managed	2.437 GHz (Channel 6)	on	-75 dBm	-70 dBm	54 Mb/s
100/100	richard-2	00:1F:1F:C0:AA:3C	Managed	2.452 GHz (Channel 9)	on	-35 dBm	-92 dBm	54 Mb/s
37/100	CHT Wi-Fi(HiNet)	9C:D6:43:64:E9:A1	Managed	2.457 GHz (Channel 10)	off	-75 dBm	-78 dBm	144 Mb/s
42/100	APTG Wi-Fi	9C:D6:43:64:E9:A2	Managed	2.457 GHz (Channel 10)	off	-73 dBm	-82 dBm	144 Mb/s
99/100	KorenixGuest	00:16:01:29:D9:DC	Managed	2.462 GHz (Channel 11)	on	-51 dBm	-92 dBm	270 Mb/s
42/100		FC:75:16:C0:27:40	Managed	2.462 GHz (Channel 11)	on	-73 dBm	-74 dBm	54 Mb/s
37/100	dlink	00:1E:58:4A:EA:C9	Managed	2.412 GHz (Channel 1)	on	-75 dBm	-84 dBm	54 Mb/s
37/100	CHT Wi-Fi Auto	9C:D6:43:64:E9:A0	Managed	2.457 GHz (Channel 10)	on	-75 dBm	-78 dBm	144 Mb/s
37/100	water	FE:9B:9C:8A:30:9A	Managed	2.462 GHz (Channel 11)	on	-75 dBm	-78 dBm	72 Mb/s
83/100	JetWave_Demo	60:02:B4:78:63:C0	Managed	2.437 GHz (Channel 6)	on	-57 dBm	-92 dBm	54 Mb/s
37/100	brucelai	C8:6C:87:25:9F:C3	Managed	2.412 GHz (Channel 1)	on	-75 dBm	-70 dBm	54 Mb/s
83/100	jetboxdemo	60:02:B4:78:69:0E	Managed	2.437 GHz (Channel 6)	on	-57 dBm	-92 dBm	54 Mb/s
37/100	12109	14:D6:4D:4A:3B:6C	Managed	2.437 GHz (Channel 6)	on	-75 dBm	-82 dBm	54 Mb/s
89/100	JetWave_Demo	60:02:B4:78:69:31	Managed	2.437 GHz (Channel 6)	on	-55 dBm	-92 dBm	54 Mb/s
100/100	TP-LINK_Stone	E8:94:F6:C9:18:68	Managed	2.437 GHz (Channel 6)	on	-49 dBm	-92 dBm	54 Mb/s
26/100	CHT Wi-Fi(HiNet)	9C:D6:43:65:6E:01	Managed	2.447 GHz (Channel 8)	off	-79 dBm	-74 dBm	144 Mb/s

Interface Configuration

Interface Configuration

General Setup

AutoStart Automatically Start after reboot.

ESSID

Mode

Encryption

IP Configuration

AutoStart : If you check this option, all settings will be apply and the wifi device will start automatically after system reboot.

ESSID : Choose your AP name

Mode : We provide Client and Ad-Hoc Mode

Encryption : Select which encryption mode that you want to connect.

IP Configuration : Select Dynamic IP or Static IP.

Example: WPA-PSK Mode

Interface Configuration

General Setup

AutoStart Automatically Start after reboot.

ESSID

Mode

Encryption

Cipher

Key

IP Configuration

Example: WPA2-PSK with AES Mode

Interface Configuration

General Setup

AutoStart Automatically Start after reboot.

ESSID

Mode

Encryption

Cipher

Key

IP Configuration

IP-Address

Netmask

Example: WEP Open System Mode

Interface Configuration

General Setup

AutoStart Automatically Start after reboot.

ESSID

Mode

Encryption

Used Key Slot

Key #1

Key #2

Key #3

Key #4

IP Configuration

Example: Ad-Hoc Mode

Interface Configuration

General Setup

AutoStart Automatically Start after reboot.

ESSID

Mode

IP-Address

Netmask

Encryption

Used Key Slot

Key #1

Key #2

Key #3

Key #4

When you select Ad-Hoc mode, you must specify the IP address to connect another AP.

Press **Save & Apply** to save configuration. And go back to WiFi settings page to enable wireless device.

Wireless Overview

 **Ralink 802.11 Wireless Controller (ra0)**
Channel: 11 (2.462 GHz) | Bitrate: 54.0 MBit/s

SSID: KorenixAP2 | **Mode:** Client
BSSID: A8:54:B2:90:CC:D2 | **Encryption:** TKIP-WPA2PSK

IPv4: 192.168.1.126
Mask: 255.255.255.0
Tx: 172071 (168.0 KiB)
Rx: 2380631 (2.2 MiB)

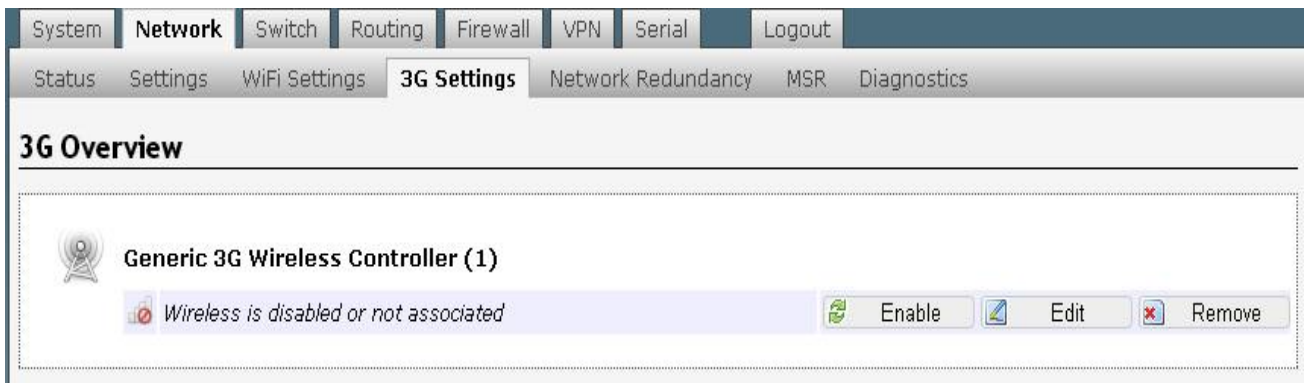
100%

Connect Successfully

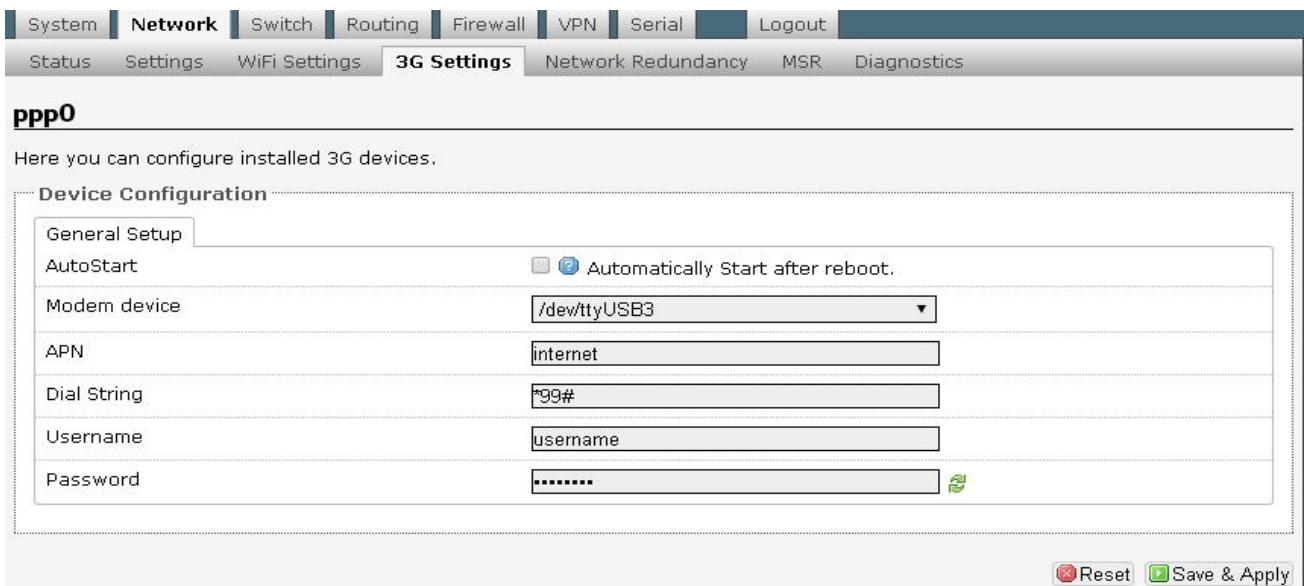
Press **Disable** button to disable wireless device if you want to disconnect it

3-4 3G Settings

Plug in the 3G dongle, click the 3G settings and it will show the wireless device.



Click **Edit** to edit the 3G configuration.



AutoStart : Check this option, all settings will be apply and the 3G/4G device will start automatically after system reboot.

Modem device : The location of the device that **wvdial** should use as your modem.
i.e.: for Sierra MC8092, it uses /dev/ttyUSB3


APN : Specify your APN name. For example, in Taiwan, we use **internet** as APN.

Dial String : Customize to your country or provider for internet connection.
i.e.: in Taiwan, we use ***99#**

Username, Password : Change with your username and password if needed.

Press **Save & Apply** to save configuration. And go back to 3G settings page to enable 3G device.

Wireless Overview

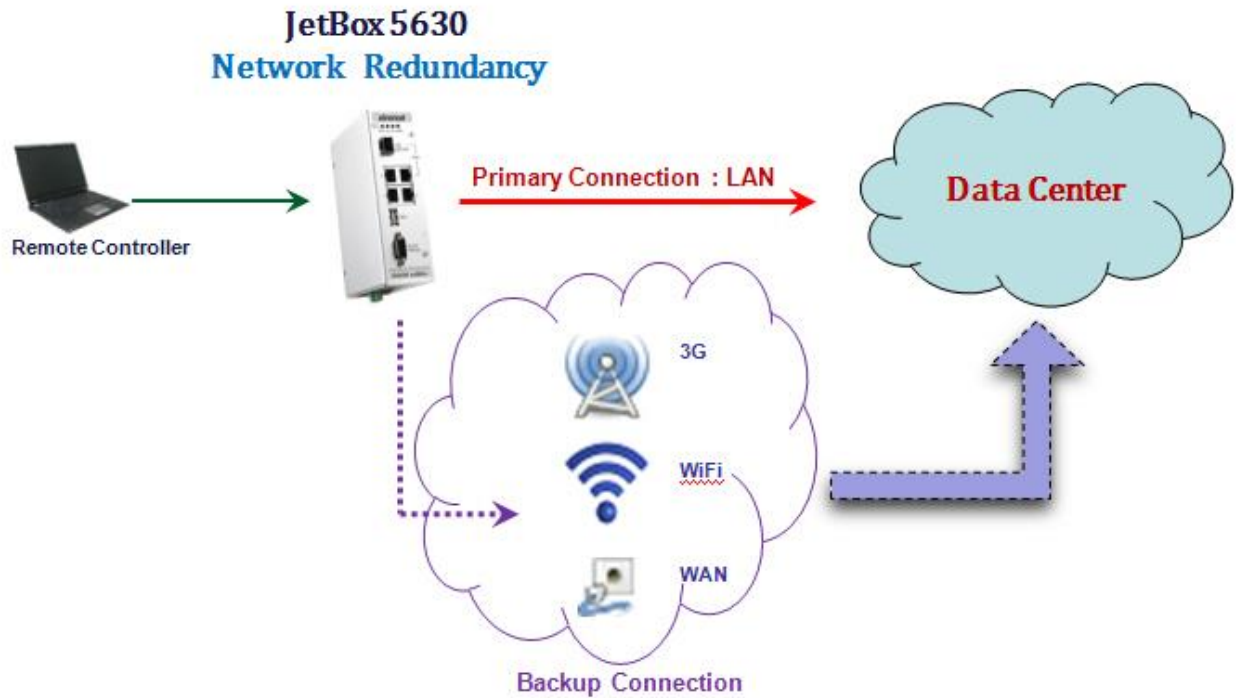
 **Generic 3G Wireless Controller (1)**
IPv4: 42.72.89.61
Mask: 255.255.255.255
Tx: 129 (129.0 B)
Rx: 78 (78.0 B)

Connect Successfully

Press **Disable** button to disable wireless device if you want to disconnect it

3-5 Network Redundancy

Redundant function checks the link status and the connection integrity. When the primary interface fails, it will switch to the backup WAN (WiFi or 3G) automatically to keep the connection alive.



Choose one of the two following conditions to activate the backup path: 1. Link Check: link down 2. Ping Check: Sends ping commands to a specific IP address

Redundant Configuration

Redundant Configuration	
AutoStart	<input checked="" type="checkbox"/> Automatically Start after reboot.
Enable Network Redundancy	<input type="checkbox"/>
IP Address	<input type="text" value="192.168.1.1"/> <input checked="" type="checkbox"/> Ping
Timeout (second)	<input type="text" value="1"/>

AutoStart :

Check it to start network redundancy after system reboot.

Enable Network Redundancy :

Check it to start network redundancy when you press Save & Apply

IP Address :

Because we will use IP address field to check link status. So user must to specify it.

And you can check link status by pressing ping.

Timeout (second) :

This value means timeout for ping. If it is less, it means switch to backup connection will take less time. Default is 5 seconds.

Primary Connection

Primary Connection	
Primary Network Interface	lan
IP-Address	192.168.10.1
Netmask	255.255.255.0
Default Gateway (optional)	192.168.10.250

Here user can specify the primary connection and set up its IP address. We support LAN 、 WAN 、 WiFi 、 3G and Other network interface. Usually, LAN or WAN will be specified with primary connection.

Backup Connection

Backup Connection	
Backup Network Interface	wan
IP-Address	192.168.10.100
Netmask	255.255.255.0
Default Gateway (optional)	192.168.10.250

Set up backup connection to make sure the links status can keep alive automatically when primary connection is disconnect. Backup connection can be specified with WiFi or 3G interface.

Backup Connection : 3G interface

Backup Connection	
Backup Network Interface	3G
Modem device	/dev/ttyUSB3
APN	internet
Dial String	*99#
Username	username
Password	*****

When you choose 3G interface for backup connection, you have to specify some settings, like APN, Modem device, Dial String...etc. These settings are the same as network 3G setting.

Backup Connection : WiFi interface

Backup Connection	
Backup Network Interface	wifi
interface name	ra0
ESSID	KorenixAP2
Encryption	WEP_Open System
Used Key Slot	Key #1
Key #1
Key #2	
Key #3	
Key #4	

When you choose WiFi interface for backup connection, you have to specify some settings. These settings are the same as network WiFi setting besides interface name. User has to specify WiFi interface name to make sure that we can use right interface to connect.

After all setting, click “Save&Apply” to start Network Redundancy function.

3-6 MSR

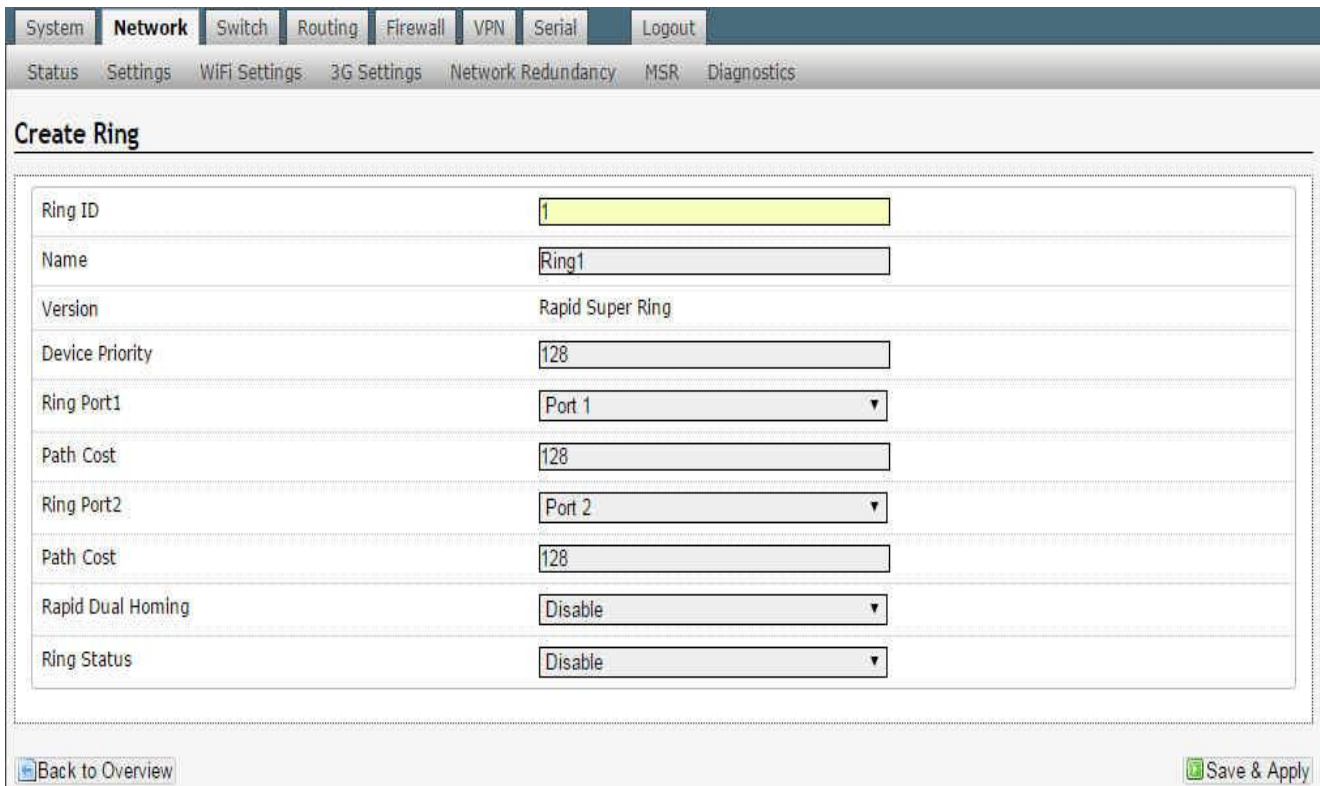
Korenix is proud to announce that it has launched its patented Rapid Super Ring (RSR) network redundancy technology in its JetBox 5630 / 5633 series industrial embedded Routing Computers for ensuring reliability, scalability and high performance of industrial network infrastructures.

The RSR provides less than 5millisecond recovery time and ZERO ms restoration time, allowing users to perform reliable data transmission and computing without link loss, topology change or data failure.

With the new RSR feature, IPC providers can easily setup the industrial network with automatic Ring Master selection, efficiently control the ring status with minimum bandwidth consumption as well as detect and fast react to the failures through received notifications and alarms. The RSR is backward compatible with Super ring technology and therefore can be used in a large network along with other redundant rings providing a complete reliable networking solution.

Create (Add) a ring:

Go to MSR page and click  button to create a ring.



The screenshot shows the 'Create Ring' configuration page. The page has a navigation bar at the top with tabs for System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below the navigation bar, there are sub-tabs for Status, Settings, WiFi Settings, 3G Settings, Network Redundancy, MSR, and Diagnostics. The main content area is titled 'Create Ring' and contains a form with the following fields:

Ring ID	1
Name	Ring1
Version	Rapid Super Ring
Device Priority	128
Ring Port1	Port 1
Path Cost	128
Ring Port2	Port 2
Path Cost	128
Rapid Dual Homing	Disable
Ring Status	Disable

At the bottom of the form, there are two buttons: 'Back to Overview' and 'Save & Apply'.

Ring ID : <0-31>

Name : Change ring name, the default ring name is “Ring RINGID”

Device Priority : Change ring priority, default is 128.

Ring Port1 : Change the id of ring port 1, default is 1.

Path Cost : Change the cost of ring port 1, default is 128.

Ring Port2 : Change the id of ring port 2, default is 2.

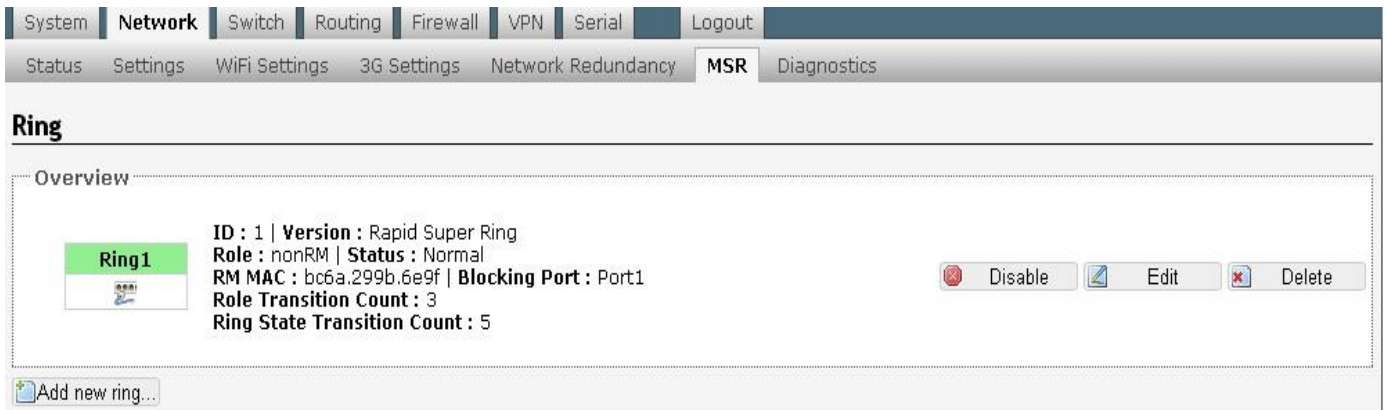
Path Cost : Change the cost of ring port 2, default is 128.

Rapid Dual Homing : Enable/Disable Rapid Dual-Homing feature, default is disable.

Ring Status : Enable or Disable ring when you click “**Save & Apply**” button.

Show Ring Status

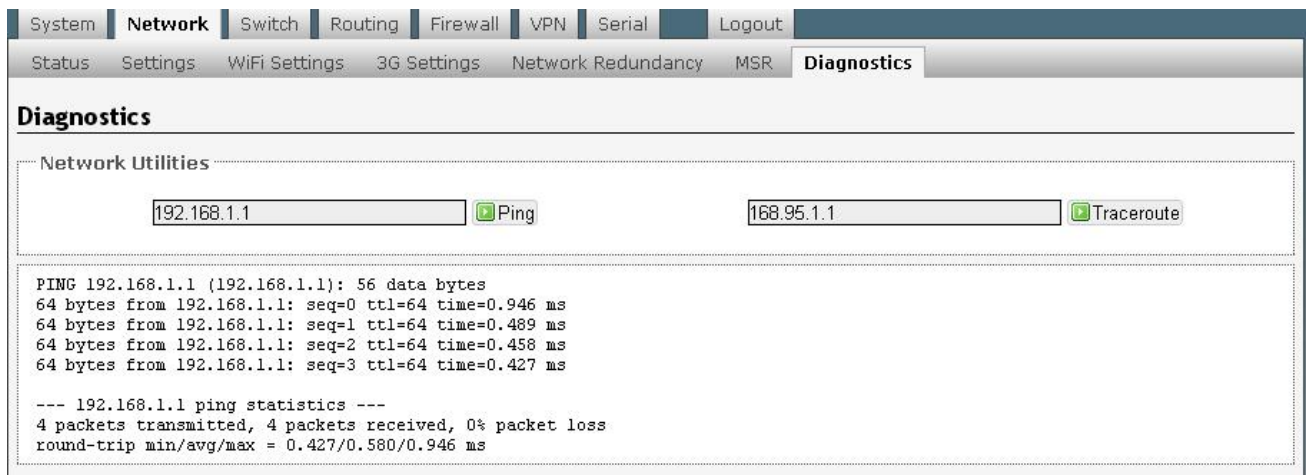
When you start ring and you can see the ring status in MSR page.



The screenshot shows the MSR Network configuration page. The top navigation bar includes System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below this, a secondary bar contains Status, Settings, WiFi Settings, 3G Settings, Network Redundancy, MSR, and Diagnostics. The main heading is "Ring". Under "Overview", there is a card for "Ring1" with the following details: ID: 1, Version: Rapid Super Ring, Role: nonRM, Status: Normal, RM MAC: bc6a.299b.6e9f, Blocking Port: Port1, Role Transition Count: 3, and Ring State Transition Count: 5. To the right of the card are buttons for Disable, Edit, and Delete. At the bottom left of the overview section is a button labeled "Add new ring..."

3-7 Diagnostics

We provide a network diagnostic tool to verify network connection. User can use ping or traceroute function to check it



The screenshot shows the MSR Diagnostics page. The top navigation bar includes System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below this, a secondary bar contains Status, Settings, WiFi Settings, 3G Settings, Network Redundancy, MSR, and Diagnostics. The main heading is "Diagnostics". Under "Network Utilities", there are two input fields: one containing "192.168.1.1" with a "Ping" button, and another containing "168.95.1.1" with a "Traceroute" button. Below the input fields is a text area displaying the results of a ping command:

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.946 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.489 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.458 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.427 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.427/0.580/0.946 ms
```


Chapter 4 Switch

In this chapter, we will show you how to configure switch function via web interface.

4-1 Port Status

Port	Medium	Link	State	Speed/Duplex	Flow Control	Type	Vendor Name	Wavelength	Distance
1	Copper	Down	Enable	100Mb/s Full	Disable	100BASE	-	-	-
2	Copper	Up	Enable	100Mb/s Full	Disable	100BASE-TX	-	-	-
3	Copper	Down	Enable	100Mb/s Full	Disable	100BASE	-	-	-
wan	Copper	Up	Enable	100Mb/s Full	-	100BASE-TX	-	-	-

Here, you can see the all ports status of JetBox 5630 series.

4-2 Port Control

LAN Port Configuration

Port	State	Speed/Duplex	Flow Control
1	Enable	Auto-Negotiation	Disable
2	Enable	Auto-Negotiation	Disable
3	Enable	Auto-Negotiation	Disable

WAN Port Configuration

Port	State	Speed/Duplex	Flow Control
4	Enable	Auto-Negotiation	-

Reset Save & Apply

You can set up the each port configuration. Just like ethtool command in JetBox console.



NOTE

1. To change SFP speed you need to reboot the system to make it effective.
2. Please make sure the spec of SFP matching with the SFP speed setting, or exception conditions would happen.

4-3 VLAN

You can add or delete vlan interface via web. Just like vconfig command in JetBox console.

The screenshot shows the 'VLAN Configuration' page for 'LAN_2'. The navigation bar includes 'System', 'Network', 'Switch', 'Routing', 'Firewall', 'VPN', 'Serial', and 'Logout'. Below the navigation bar are tabs for 'Port Status', 'Port Control', 'VLAN', 'PVID', 'QoS', and 'Rate Limit'. The 'VLAN Configuration' section has a 'General Setup' tab. The configuration fields are as follows:

VLAN ID	2
Port 1	Un-Tag
Port 2	Not Member
Port 3	Not Member
IP-Address	192.168.30.1
Netmask	255.255.255.0

At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

Here, you also can directly specify IP address of vlan interface.

Back to VLAN setting page, you can press Enable button to link up the vlan interface. And the IP address will be set automatically according to settings.

The screenshot shows the 'Switch' interface overview page. The navigation bar is the same as in the previous screenshot. Below the navigation bar are tabs for 'Port Status', 'Port Control', 'VLAN', 'PVID', 'QoS', and 'Rate Limit'. The 'Switch' section has an 'Interface Overview' tab. The interface overview shows a network diagram with a green box labeled 'lan.2'. Below the diagram, it says 'Interface not present or not connected yet.' To the right of the diagram are 'Enable', 'Edit', and 'Delete' buttons. At the bottom left, there is an 'Add new interface...' button. At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

4-4 PVID

The screenshot shows the 'PVID' configuration page. The navigation bar is the same as in the previous screenshots. Below the navigation bar are tabs for 'Port Status', 'Port Control', 'VLAN', 'PVID', 'QoS', and 'Rate Limit'. The 'PVID' section has a 'PVID Settings' tab. The configuration fields are as follows:

Port 1	1
Port 2	1
Port 3	1

At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

User can change port's pvid via web. It is the same as "ethtool -P" command.

4-5 QoS

In the past, the concept of quality in networks meant that all network traffic was treated equally. The QoS (Quality of Service) concept means that some traffic needs preferential treatment because the requirements of some applications and users are more critical than others. In addition, QoS for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications.

When QoS is enabled, packets are queued based on the port trust mode, which is derived from the incoming port configurations, CoS queue mapping, or DSCP queue mapping.

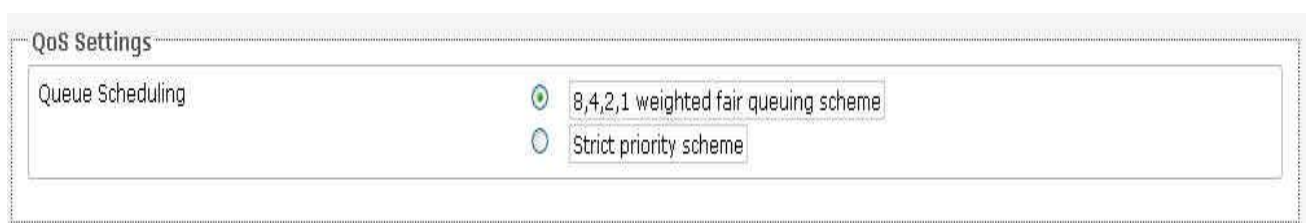
Through this section, you can set up the priority level for port based CoS value, incoming CoS (CoS-Queue Mapping), or incoming DSCP (DSCP-Queue Mapping) and define the way to process all ingress packets by either the strict priority scheme or the weighted fair queue according to the priority levels of port based, CoS only, DSCP only, CoS first, or DSCP first. JetBox 5630 supports 4 physical queues from 0 to 3.

Queue scheduling

Use an 8,4,2,1 weighted fair queuing scheme: This is also known as WRR (Weight Round Robin). JetBox 5630 follows the rate of 8:4:2:1 to process the packets with the high, the medium, the low, and the normal priority in a queue. For example, the system processes 8 packets with the high priority in the queue, 4 with medium priority, and 2 with low priority and 1 with the normal priority at the same time.

Use a strict priority scheme: Packets with higher priority in the queue will always be processed first, unless there is no packet with higher priority in a queue.

The default is using an 8,4,2,1 weighted fair queuing scheme.



Port setting

Priority:

You can choose the QoS priority levels for each Ethernet port of JetBox 5630 from 0 to 7.

Trust Mode

Trust Mode	Description
Port Based	Use the priority level of the port configuration
CoS Only	Use the priority level of CoS Queue Mapping only
DSCP Only	Use the priority level of DSCP Queue Mapping only
DSCP First	Use the priority level of both CoS and DSCP Queue Mapping, but DSCP Queue Mapping first
CoS First	Use the priority level of both CoS and DSCP Queue Mapping, but CoS Queue Mapping first

Port	Priority	Trust Mode
1	0	CoS First
2	0	Port Based
3	0	CoS Only
WAN	0	DSCP Only
		CoS First
		DSCP First

JetBox 5630 will give all ingress packets the priority tag based on the priority level (CoS Value) of the ingress port. The CoS value maps to physical queue in the page of CoS Queue Mapping.

CoS (Class of Service): Layer 2 prioritization of packets is based on a CoS value.

CoS Value	Traffic Type
0	Best effort
1	Background
2	Standard
3	Excellent load
4	Controlled load
5	Voice and Video
6	Layer 3 network control reserved traffic
7	Layer 2 network control reserved traffic

QoS priority level follows 802.1p

CoS-Queue Mapping

The default setting follows IEEE802.1p standard to map the CoS values to the physical queues. You can modify the physical queue of each item here.

CoS Value	Physical	Queue
0	Normal	1
1	Low	0
2	Low	0
3	Normal	1
4	Medium	2
5	Medium	2
6	High	3
7	High	3

The CoS values map to the physical queues

CoS Setting

CoS	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

DSCP (Differentiated Services Code Point): Layer 3 prioritization of packets is based on a DSCP value. A network could have from 0 to 64 different traffic classes using different markings in the DSCP.

DSCP-Queue Mapping

The default setting follows IEEE802.1p standard to map the DSCP values to the physical queues. You can modify the physical queue of each item here.

DSCP Value	Physical	Queue
0~15	Low	0
16~31	Normal	1
32~47	Medium	2
48~63	High	3

The DSCP values map to the physical queues

DSCP Setting

DSCP	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Queue	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

DSCP	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Queue	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

DSCP	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Queue	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

DSCP	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Queue	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

It is the same as `ethtool -q` and `ethtool -Q` command in JetBox console. As below

```

~ $ ethtool -q lan:1
Queue Scheduling:
    8,4,2,1 weighted fair queuing

Port Setting:
    Port 1   : CoS First, Priority : 0
    Port 2   : CoS First, Priority : 0
    Port 3   : CoS First, Priority : 0
    Port WAN : CoS First, Priority : 0

IEEE Tag CoS Mapping:
    Queue 0:1,2,
    Queue 1:0,3,
    Queue 2:4,5,
    Queue 3:6,7,

IP DSCP Mapping:
    Queue 0:
    00,01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,
    Queue 1:
    16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,
    Queue 2:
    32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,
    Queue 3:
    48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,
  
```

4-6 Rate Limit

Rate limiting is used to control the rate of traffic that is sent or received on a network interface. For ingress rate limiting, traffic that is less than or equal to the specified rate is received, whereas traffic that exceeds the rate is dropped. For egress rate limiting, traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped.

Rate Limit Configuration

Ingress Rate : Range is from 1 Mbps to 1000 Mbps and Zero means no limit. Increments of 1Mbps.
 Egress Rate : 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit. Egress packet type is All.

Port	Ingress Packet Type	Ingress Rate (Mbps)	Egress Rate (Mbps)
1	Broadcast Only	10	0
2	Broadcast Only	10	0
3	Broadcast Only	10	0
WAN	Broadcast Only	10	0

Ingress Packet type : Select the packet type that you want to filter. The packet types have all types of packets, Broadcast Only, Broadcast/Unknown Multicast, and Broadcast/Unknown Multicast /Unknown Unicast packets.

Rate Limit Configuration

Ingress Rate : Range is from 1 Mbps to 1000 Mbps and Zero means no limit. Increments of 1Mbps.
 Egress Rate : 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit. Egress packet type is All.

Configuration

Port	Ingress Packet Type	Ingress Rate (Mbps)	Egress Rate (Mbps)
1	Broadcast Only	10	0
2	All	10	0
3	Broadcast Only	10	0
	Broadcast/Unknown Multicast	10	0
WAN	Broadcast/Unknown Multicast/Unknown Unicast	10	0

Reset Save & Apply

Ingress Rate (Mbps) : Ingress rate in Mbps, the rate range is from 1 Mbps to 1000 Mbps, increments of 1Mbps. Zero means no limit. The default ingress rate is "10 Mbps".

Egress Rate (Mbps) : Egress rate in Mbps, the rate range is from 1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps. Zero means no limit. The default egress rate is "no-limit". Egress rate limiting has an effect on all types of packets, including unicast, multicast and broadcast packets.

Chapter 5 Routing

In this chapter, we provide users how to configure JetBox routing configuration via web interface. We support Static routes 、 OSPF and RIP routing protocol.

5-1 Status

Check routing status and you also can see ARP table.

Status Static Routes OSPF RIP

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.116	00:07:40:ca:5e:9c	wan
192.168.1.72	00:0f:fe:60:ee:c0	wan
192.168.1.1	00:05:5d:8d:72:13	wan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	192.168.1.1	0
wan	192.168.1.0/24	0.0.0.0	0
lan	192.168.10.0/24	0.0.0.0	0

5-2 Static Routes

You can add static route with this page.

For example, we want to add a rule

`route add -net 192.168.30.0 netmask 255.255.255.0 dev lan`

```
~ $ route add -net 192.168.30.0 netmask 255.255.255.0 dev lan
~ $
~ $ route
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use  Iface
192.168.1.0      *              255.255.255.0 U        0      0      0   lan
192.168.20.0     *              255.255.255.0 U        0      0      0   wan
192.168.30.0     *              255.255.255.0 U        0      0      0   lan
~ $
```

In web, you can set up as below

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
lan	192.168.30.0	255.255.255.0		

Add

In JetBox console, add default gateway

`route add default gw 192.168.1.1`

```
~ $ route add default gw 192.168.1.1
~ $
~ $ route
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use  Iface
default          192.168.1.1    0.0.0.0        UG        0      0      0
192.168.1.0      *              255.255.255.0 U        0      0      0   lan
192.168.20.0     *              255.255.255.0 U        0      0      0   wan
192.168.30.0     *              255.255.255.0 U        0      0      0   lan
~ $
```

In web, you can set up as below

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
	0.0.0.0	255.255.255.0	192.168.1.1	

Add

5-3 OSPF

The OSPF is short of the Open Shortest Path First.

OSPF is a link-state protocol. The Link is an interface on the router, it equips the IP, mask, the type of network, the routers connected to that network. The State is its relationship to its neighboring routers. The Metric is the distance between the 2 links, it is usually the bandwidth of the link in link-state protocol. The Link State Database is the collection of all these link states. The destination network address, the shortest metric to the network and the IP address of the next hop are specified in the link state database.

OSPF Configuration

OSPF Configuration

OSPF Protocol	Enabled
Router ID	192.168.20.150

OSPF Protocol : You can Enabled or Disabled OSPF protocol after press "Save&Apply" button.


Router ID : The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier

Routing For Networks

Type the network address and the Area ID in the field. Click "Add" to apply the setting. You can see the network table in below.

Routing for Networks

Network Address	Netmask	Area
192.168.20.0	24	1
192.168.1.0	24	1





NOTE

All the Area ID of the router/switch within the same area should use the same ID. All the network address should be added.

Interface Configuration

This page allows user to specify parameters of each interface.

Interface	Cost	Priority	Transmit Delay	Hello	Dead	Retransmit	
lan	10	1	1	10	40	5	
wan	20	1	1	10	40	5	

Add

Interface: The Interface name.

Cost: The distance of this link/Interface, the default is identified depends on what the bandwidth is by the system. The value can be changed to decide the best router.

Priority: The priority of this link/Interface. Set priority to help find the OSPF designated router for a network. The default is 1. The range is 0 to 255.

Transmit Delay: The transmit delay timer of this link/Interface. Transmit Delay is the estimated number of seconds to wait before sending a link state update packet. The default value is 1 second.

Hello: The Hello timer of this link/Interface. The value must be the same for all routers/switches on a network. The default value is 10 seconds. The min. value is 1.

Dead: The Dead Interval Timer of this link/Interface. The Dead timer is the time to identify whether the interface is down or not before the neighbors declare the OSPF router to be down. The default value is 4 times (40 seconds) than the Hello interval (default is 10).

Retransmit: The count of Retransmit of this link/Interface. The Retransmit time specifies the number of seconds between link state advertisement transmissions. The default value is 5 seconds.

OSPF Neighbor Status

This section allows user to see the OSPF Neighbor information.

Below is the example of a simple OSPF environment. The Hello packets are exchanged between the switch to next switches. While the State is changed to "Full", that means the exchange progress is done. The Neighbor ID is the Router ID of the Neighbor routers/switches. The Priority is the priority of the link. The Dead Time is the activated time of the link. There are one interface attached the switch you check. The IP address shows the learnt IP interface of the next hops. And the Interface shows the connected local interface.

Neighbor ID	Priority	State	Dead Time	IP Address	Interface
192.168.20.200	1	Full/DR	32.760s	192.168.20.200	wan:192.168.20.150

Once you finish configuring the settings, click “Save&Apply” to apply your configuration.

System | Network | Switch | **Routing** | Firewall | VPN | Serial | Logout

Status | Static Routes | **OSPF** | RIP

OSPF

OSPF Configuration

OSPF Protocol: Enabled

Router ID: 192.168.20.150

Routing for Networks

Network Address	Netmask	Area
192.168.20.0	24	0
192.168.1.0	24	0

+ Add

Interface Configuration

Interface	Cost	Priority	Transmit Delay	Hello	Dead	Retransmit
lan	10	1	1	10	40	5
wan	101	1	1	10	40	5

+ Add

OSPF Neighbor Status

Neighbor ID	Priority	State	Dead Time	IP Address	Interface
192.168.20.200	1	Full/DR	32.760s	192.168.20.200	wan:192.168.20.150

Reset Save & Apply

5-4 RIP

The RIP is short of the Routing Information Protocol. RIP was in widespread use years before it was standardized in as RFC 1058 in 1988. Version 2 of RIP was completed in 1994.

RIP is the most known Distance Vector type dynamic routing protocol, or known as Hop Based routing protocol. It uses hop count as a distance metric, each router advertises its routing table every 30 seconds. The maximum routers RIP can support is 15, the 16th router represents Infinity.

RIP Configuration

This page shows how to configure RIP protocol.

RIP Protocol: Enabled or Disabled OSPF protocol after press “Save&Apply” button.

RIP Configuration

RIP Protocol: Disabled

Routing for Networks: All the networks no matter directly connected or learnt from other router/switch should be added to the switch. The format is IP Network/bit mask.

Routing for Networks

Network Address	Netmask
192.168.20.0	24
192.168.1.0	24

+ Add

RIP Interface Configuration

In RIP Interface Configuration, you can configure Send Version and Receiver Version. Select the RIP Version of the interface. Once you finish configuring the settings, click on “Save&Apply” to apply your configuration.

Interface Configuration

Interface	Send Version	Receive Version
wan	1	1

+ Add

RIP Status

Gateway	BadPackets	BadRoutes	Distance	Last Update

RIP Status

This section allows user to see the RIP Neighbor information.

RIP Status

Gateway	BadPackets	BadRoutes	Distance	Last Update
192.168.20.200	0	0	120	00:00:28

Once you finish configuring the settings, click “Save&Apply” to apply your configuration.

Chapter 6 Firewall

It is the same as iptables command in JetBox console. In web interface, we provide three basic functions for user to set up firewall in Linux.

6-1 Forwarding

The FORWARD policy allows an administrator to control where packets can be routed within a LAN. For example, to allow forwarding for the entire network, the following rules can be set:

In JetBox command :

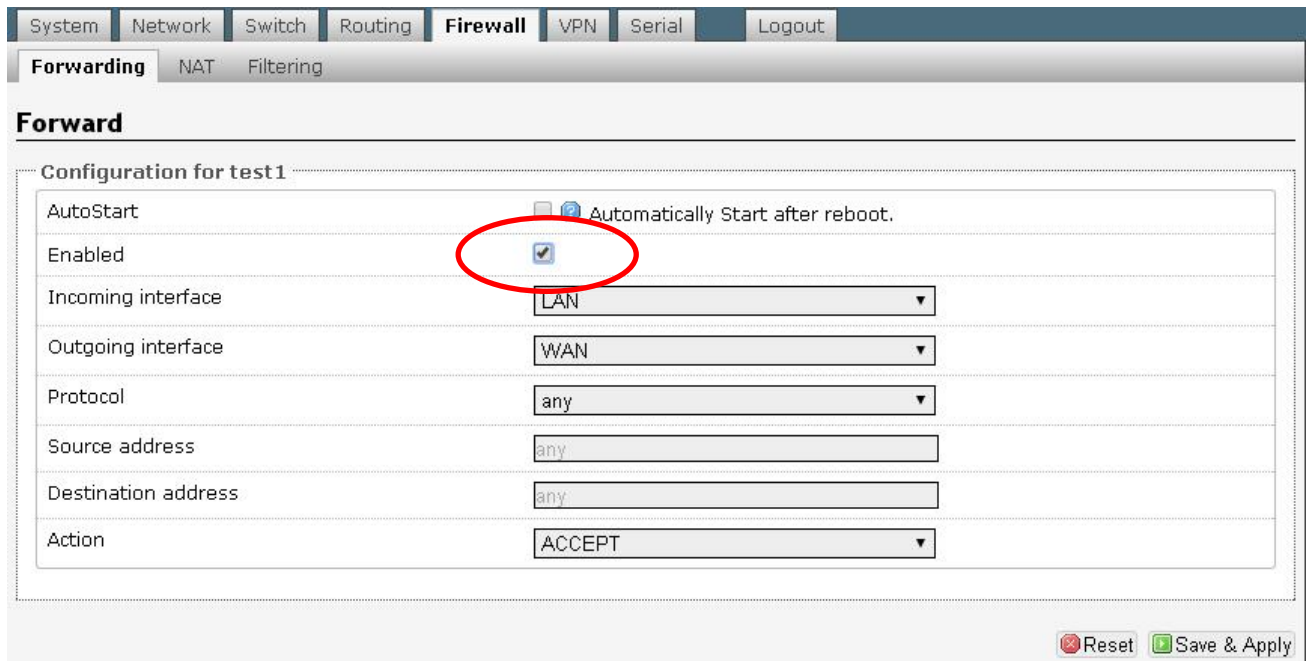
```
iptables -A FORWARD -i lan -o wan -j ACCEPT
```

```
~ $ iptables -A FORWARD -i lan -o wan -j ACCEPT
~ $ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
~ $
```

In web interface, you can specify as below



AutoStart : Check it to apply forwarding rule after system reboot.

Click on “Enabled” and it will apply this rule immediately after press “Save&Apply”

Back to Forwarding page, you can see a rule that you had added.

Rules	AutoStart	Enabled	Protocol	Source	Destination	Action	Sort
test1	No	No	Any	lan:0.0.0.0/0;*	wan:0.0.0.0/0;*	ACCEPT	↑ ↓ ↻ ✖

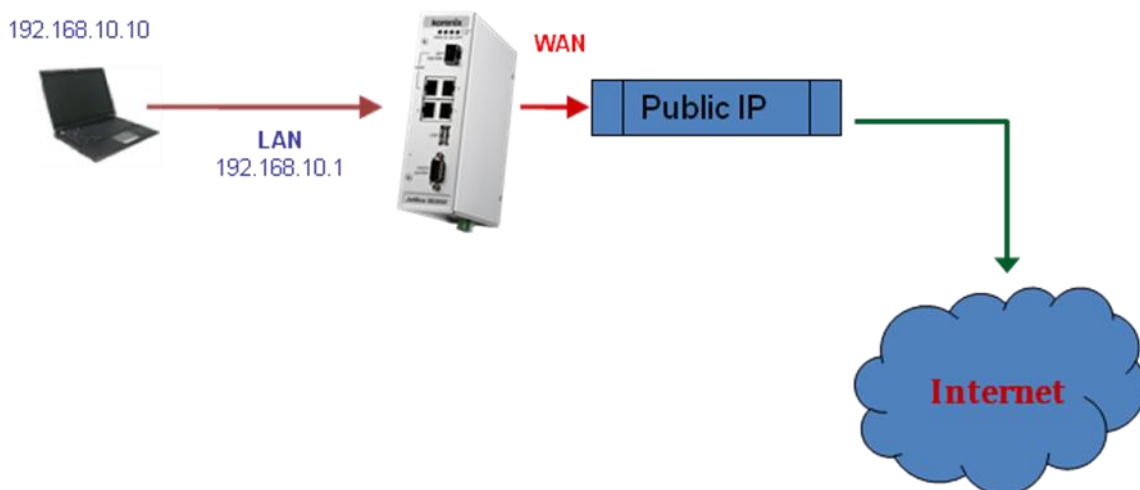
If you want to delete the rule, just click  delete button and press “Save&Apply”.

6-2 NAT

Network address translation (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Postrouting and IP Masquerade

Masquerade allow LAN nodes with private IP addresses to communicate with external public networks.



iptables command :

iptables -t nat -A POSTROUTING -o WAN -j MASQUERADE

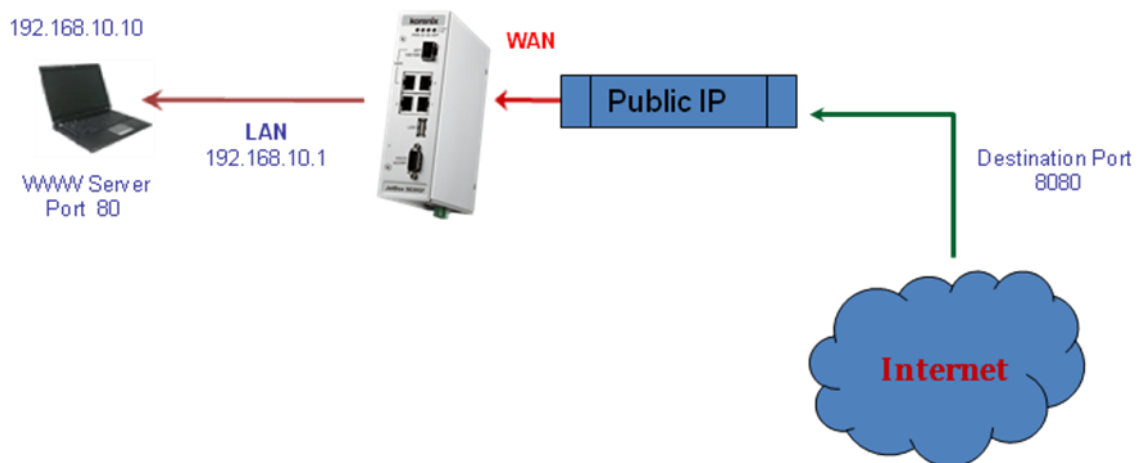
In Web interface

System	Network	Switch	Routing	Firewall	VPN	Serial	Logout
Forwarding	NAT	Filtering					
NAT							
Configuration for test3							
AutoStart	<input type="checkbox"/> Automatically Start after reboot.						
Enabled	<input type="checkbox"/>						
Apply Chain to..	POSTROUTING						
Outgoing interface	WAN						
Protocol	any						
Source address	any						
Destination address	any						
Action	MASQUERADE						
							Reset Save & Apply

AutoStart : Check it to apply NAT rule after system reboot.

DNAT and Prerouting

Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an en route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet.



iptables command :

```
iptables -t nat -A PREROUTING -p tcp -i wan --dport 8080 -j DNAT --to-destination 192.168.20.1:80
```

In Web interface

System | Network | Switch | Routing | **Firewall** | VPN | Serial | Logout

Forwarding | **NAT** | Filtering

NAT

Configuration for test2

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
Enabled	<input type="checkbox"/>
Apply Chain to..	PREROUTING
Incoming interface	WAN
Protocol	TCP
Source address	any
Source port	1-65535
Destination address	any
Destination port	8080
Action	DNAT
--to-destination	192.168.20.1:80

Reset Save & Apply

Back to NAT page, you can see a rule that you had added.

System | Network | Switch | Routing | **Firewall** | VPN | Serial | Logout

Forwarding | **NAT** | Filtering

Network Address Translation

Rules

	AutoStart	Enabled	Chain	Protocol	Source	Destination	Action	Sort	
test2	No	No	PREROUTING	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:8080	DNAT	↑ ↓	
test3	No	No	POSTROUTING	Any	*:0.0.0.0/0:*	wan:0.0.0.0/0:*	MASQUERADE	↑ ↓	

Add

Reset Save & Apply

If you want to delete the rule, just click delete button and press "Save&Apply".

6-3 Filter

In this page, we provide INPUT and OUTPUT chain for user to specify their rules.

For example : If we do not want to access any telnet connection, we can use this command
`iptables -A INPUT -i wan -p tcp --dport 23 -j DROP`

In Web interface

Configuration for test4

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
Enabled	<input checked="" type="checkbox"/>
Apply Chain to..	INPUT
Incoming interface	WAN
Protocol	TCP
Source address	any
Source port	1-65535
Destination address	any
Destination port	23
State	any
Action	DROP

Reset Save & Apply

AutoStart : Check it to apply Filter rule after system reboot.

Back to Filtering page, you can see a rule that you had added.

Filtering

Rules	AutoStart	Enabled	Chain	Protocol	Source	Destination	Action	Sort
test4	No	Yes	INPUT	TCP	wan:0.0.0.0/0:*	Device:0.0.0.0/0:23	DROP	+

Add

Reset Save & Apply

If you want to delete the rule, just click  delete button and press "Save&Apply".

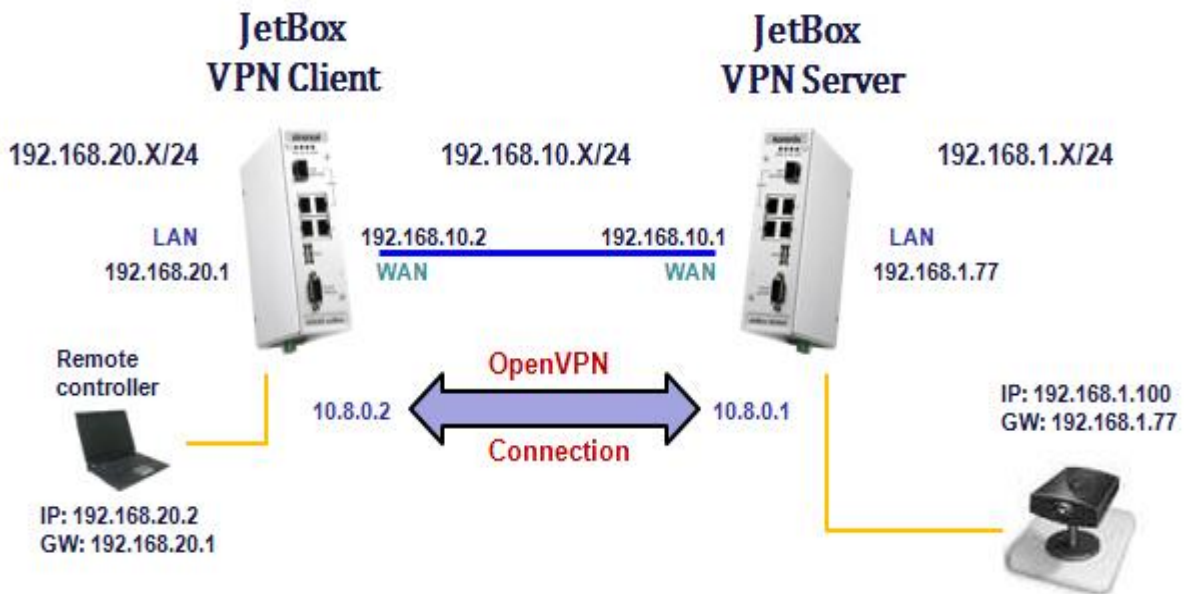
Chapter 7 VPN

In this chapter, we only provide the basic and simple configuration for user set up the various VPN connections. You can set up the VPN easily via web interface. If your environment is more complicated. We will recommend you to go into JetBox console and use command line and configuration file to set up.

7-1 OpenVPN

Simple Example

A VPN tunnel will be created with a server **vpn endpoint** of 10.8.0.1 and a client **vpn endpoint** of 10.8.0.2. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN port.



We already provide two sample configuration files for Server and Client.

System | Network | Switch | Routing | Firewall | **VPN** | Serial | Logout

OpenVPN | IPSec | Certificates | PPTP | L2TP | L2TPv3 | CHAP-Secrets

OpenVPN Connection Status

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

	AutoStart	Start	Status	Port	Remote IP Address	Protocol	
<i>openserver</i>	No	Start	no	1194	---	udp	
<i>openclient</i>	No	Start	no	1194	192.168.10.1	udp	

Add

Reset Save & Apply

Create OpenVPN Server Configuration

OpenVPN

Basic Connection Configuration for openserver

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
Encryption	secret <input type="checkbox"/> Data Channel Encryption Options
Generate Secret Key	<input type="button" value="Generate..."/>
client	<input type="checkbox"/> Configure client mode
secret	/etc/openvpn/static.key <input type="checkbox"/> Enable Static Key encryption mode (non-TLS)
ifconfig	10.8.0.1 10.8.0.2 <input type="checkbox"/> Set tun/tap adapter parameters
proto	udp <input type="checkbox"/> Tunnel protocol
Encryption Cipher for packets	Blowfish CBC
Hash Algorithm	SHA1
ping-timer-rem	<input checked="" type="checkbox"/> Only process ping timeouts if routes exist
persist-tun	<input checked="" type="checkbox"/> Keep tun/tap device open on restart
persist-key	<input checked="" type="checkbox"/> Don't re-read key on restart
port	1194 <input type="checkbox"/> TCP/UDP port # for both local and remote
keepalive	10 60 <input type="checkbox"/> Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations
route	192.168.20.0 255.255.255.0 <input type="checkbox"/> Example : 192.168.10.0 255.255.255.0
-- Additional Field -- <input type="button" value="Add"/>	

AutoStart : Check it to start OpenVPN Server after system reboot.

We use a pre-shared secret key (**Static Key mode**) mode.

You have to generate a static key first. You can press button directly with the web interface. Or type the following command In JetBox console:

```
# openvpn --genkey --secret /etc/openvpn/static.key
```

Generate Secret Key

Generate Secret Key Successfully!!!

And you can select your key file. As below.

secret

/etc/openvpn/static.key

Enable Static Key encryption mode (non-TLS)

Location: (root) / etc / openvpn

- easy-rsa/
- ca.crt
- dh1024.pem
- ipp.txt
- openclient.conf
- openserver.conf
- server.crt
- server.key
- static.key

Create OpenVPN Client Configuration

OpenVPN

Basic Connection Configuration for openclient

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
Encryption	secret <input checked="" type="checkbox"/> Data Channel Encryption Options
Generate Secret Key	<input type="button" value="Generate..."/>
client	<input checked="" type="checkbox"/> Configure client mode
remote	192.168.10.1 <input checked="" type="checkbox"/> Remote host name or ip address
secret	/etc/openvpn/static.key <input checked="" type="checkbox"/> Enable Static Key encryption mode (non-TLS)
ifconfig	10.8.0.2 10.8.0.1 <input checked="" type="checkbox"/> Set tun/tap adapter parameters
proto	udp <input checked="" type="checkbox"/> Tunnel protocol
Encryption Cipher for packets	Blowfish CBC
Hash Algorithm	SHA1
ping-timer-rem	<input checked="" type="checkbox"/> Only process ping timeouts if routes exist
persist-tun	<input checked="" type="checkbox"/> Keep tun/tap device open on restart
persist-key	<input checked="" type="checkbox"/> Don't re-read key on restart
keepalive	10 60 <input checked="" type="checkbox"/> Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations
route	192.168.1.0 255.255.255.0 <input checked="" type="checkbox"/> Example : 192.168.10.0 255.255.255.0
-- Additional Field -- <input type="button" value="Add"/>	



NOTE

- Static key of Client must **the same** as server. So you have to copy the static key from server. Can't generate another key on client site.

Start to create OpenVPN Connection

Press button.

Example:

Run VPN Server in server site

OpenVPN Connection Status							
OpenVPN instances							
Below is a list of configured OpenVPN instances and their current state							
	AutoStart	Start	Status	Port	Remote IP Address	Protocol	
openserver	No	<input checked="" type="button" value="Stop"/>	yes (26186)	1194	---	udp	<input type="button" value="Start"/> <input type="button" value="Stop"/>
openclient	No	<input checked="" type="button" value="Start"/>	no	1194	192.168.10.1	udp	<input type="button" value="Start"/> <input type="button" value="Stop"/>
<input type="button" value="Add"/>							

Test your VPN connection

For VPN client, test your VPN server is connected

```
# ping 10.8.0.1
```

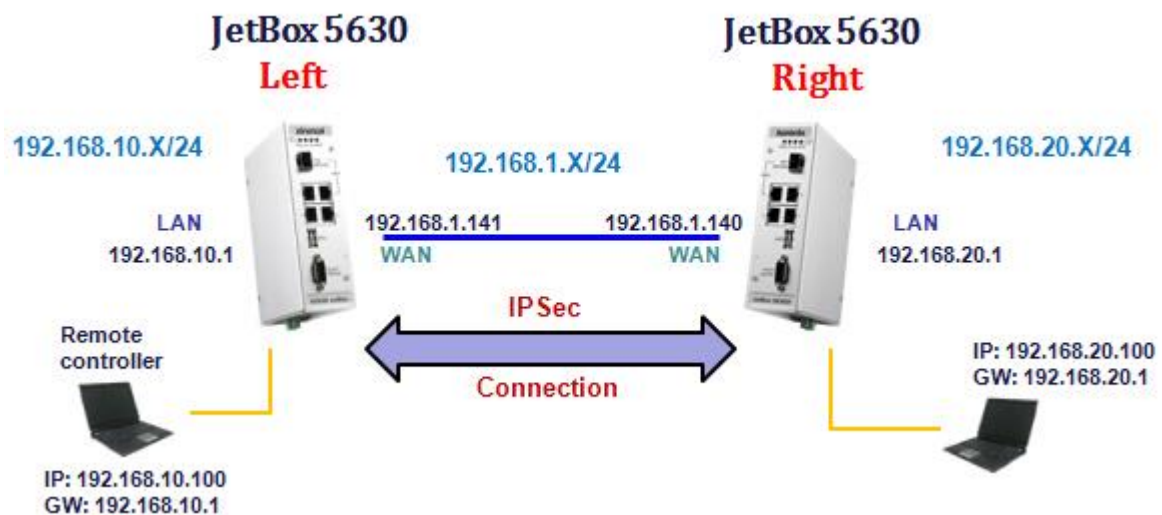
Sit at one of your local subnet nodes $*(192.168.20.1)*$, and ping a subnet node on the other $*(192.168.1.77)*$.

```
# ping 192.168.1.77
```

7-2 IPsec

Simple Example

The VPN tunnel has two participants on its ends, called **left** and **right**, and which participant is considered left or right is arbitrary. You can configure various parameters for these two ends via web interface.



It defines a tunnel between two nodes on the same LAN, with the left one as 192.168.1.141 and the right one as 192.168.1.140, as follows:

Basic Connection Configuration for ipsec_net

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
interfaces - Interfaces for IPsec to use	ipsec0=wan
Authentication method	RSA key
ESP Algorithm	AES
left - IP address of network interface	192.168.1.141
leftsourceip - Connection source IP	192.168.10.1
leftsubnet - Private subnets behind the participant	192.168.10.0/24 Example : 192.168.10.0/24
leftsasigkey - Public key for authentication	0sAQN/DB5FpQNQexylwubEyS5bp/zAReVKu
right - IP address of network interface	192.168.1.140
rightsourceip - Connection source IP	192.168.20.1
rightsubnet - Private subnets behind the participant	192.168.20.0/24 Example : 192.168.10.0/24
rightsasigkey - Public key for authentication	0sAQOoo/1DFmfglnLB2VWVsDgT3Ph5J5nMs
-- Additional Field --	<input type="button" value="Add"/>

AutoStart : Check it to enable IPsec connection after system reboot.

All settings are the same as /etc/ipsec.conf in JetBox 5630 console.

Generate a new IPsec RSA key on Left and Right

In web interface, we provide that user can generate RSA key automatically. Just press

button. Ad below

Public Key Management

Generate Public Key

 Generating

Show Public Key


Generate Hostkey Successfully

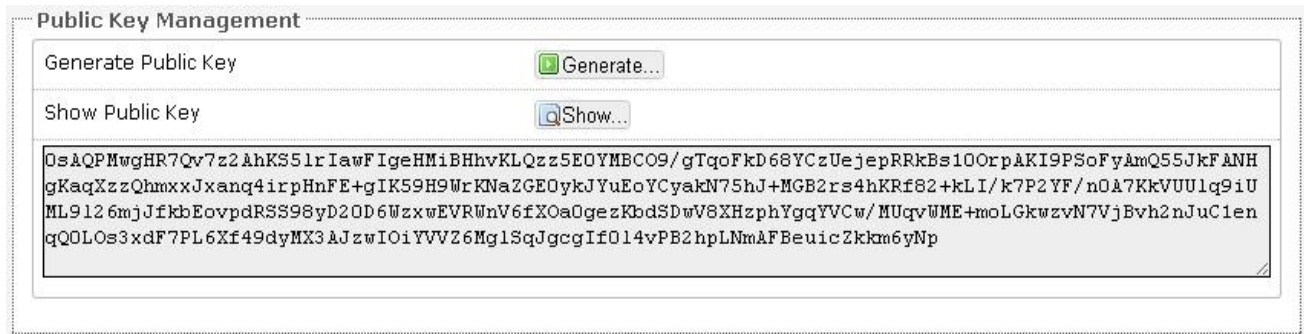
Public Key Management

Generate Public Key

Generate Hostkey Successfully!!!

Show Public Key

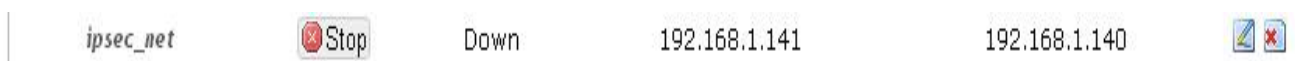
User has to fill out the left/rsa/privkey/right/rsa/pubkey. Here you just press  after generate hostkey successfully. Copy it and paste to these fields.



If you are left site, you need to copy the right rsasigkey from right site. Vice versa in right site.

Start to create IPsec Tunnel

Press  button.



Test your VPN connection

Sit at one of your local subnet nodes `*(192.168.10.100)*`, and ping a subnet node on the other `*(192.168.20.1)*`.

```
# ping 192.168.20.1
```

While still pinging, go to the right site and snoop your outgoing interface, for example:

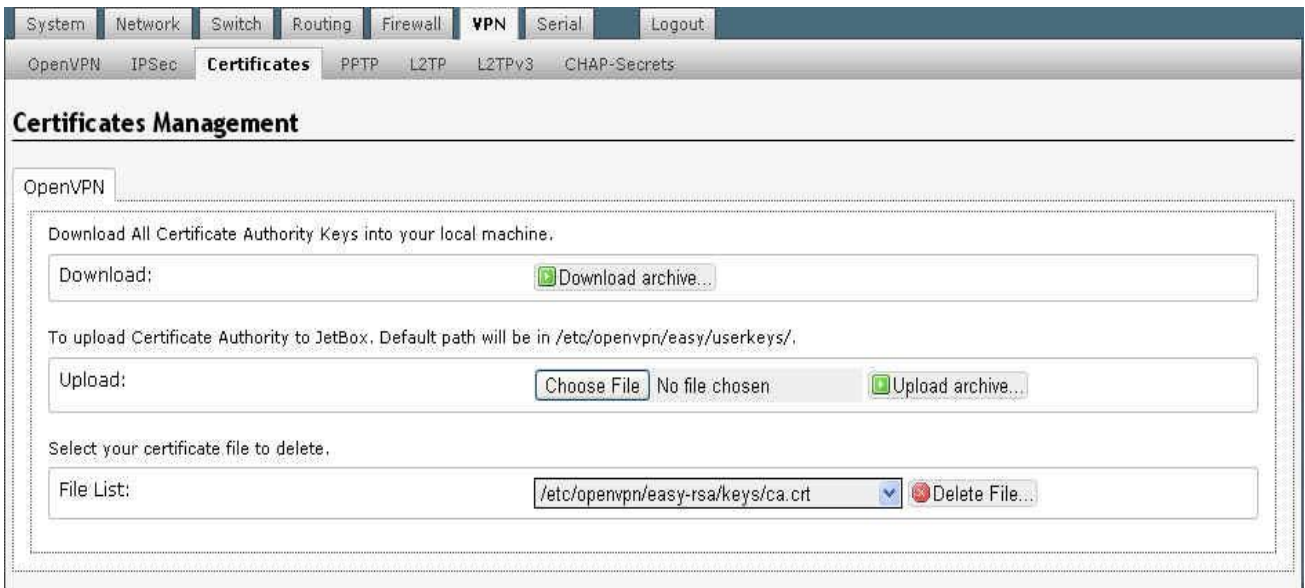
```
# tcpdump -i wan
```

You will see ESP (Encapsulating Security Payload) packets moving back and forth between the two gateways at the same frequency as your pings:

```
06:21:59.282435 IP 192.168.1.141 > 192.168.1.140: ESP(spi=0x5524c925,seq=0x17), length 100
06:22:00.282408 IP 192.168.1.141 > 192.168.1.140: ESP(spi=0x5524c925,seq=0x18), length 100
```

If you see this, congratulations are in order! You have a tunnel which will protect any IP data from one subnet to the other, as it passes between the two gates.

7-3 Certificates

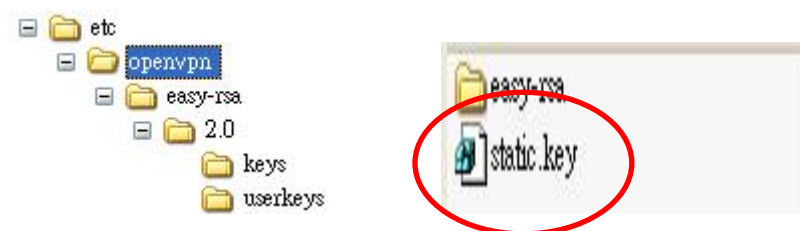


Sometimes we need to set up your own Certificate Authority (CA) and generate certificates and keys for an OpenVPN server and multiple clients. So we need to management these keys, for example, delete, backup or copy it to other clients. In this page, you can manage certificate keys of OpenVPN.

Usually, these keys are in the `/etc/openvpn/easy-rsa/2.0/keys/`. As below

```
/etc/openvpn/easy-rsa/2.0/keys $ ls
01.pem      client1.csr      client3.key      serial.old
02.pem      client1.key      dh1024.pem      server.crt
03.pem      client2.crt      index.txt       server.csr
04.pem      client2.csr      index.txt.attr  server.key
ca.crt      client2.key      index.txt.attr.old
ca.key      client3.crt      index.txt.old
client1.crt client3.csr      serial
```

If you want to backup these keys, click and it will compress all files in `/etc/openvpn`, `/etc/openvpn/easy-rsa/2.0/keys/` and `/etc/openvpn/easy-rsa/2.0/userkeys/`. For example, the compress file will be named `openvpnkey-JetBox5630-2014-09-15.tar.gz`. Uncompress it to your computer and you will see the `static.key` in `/etc/openvpn`.



And all certificate keys



When you download these keys, you can copy them to other clients. As below

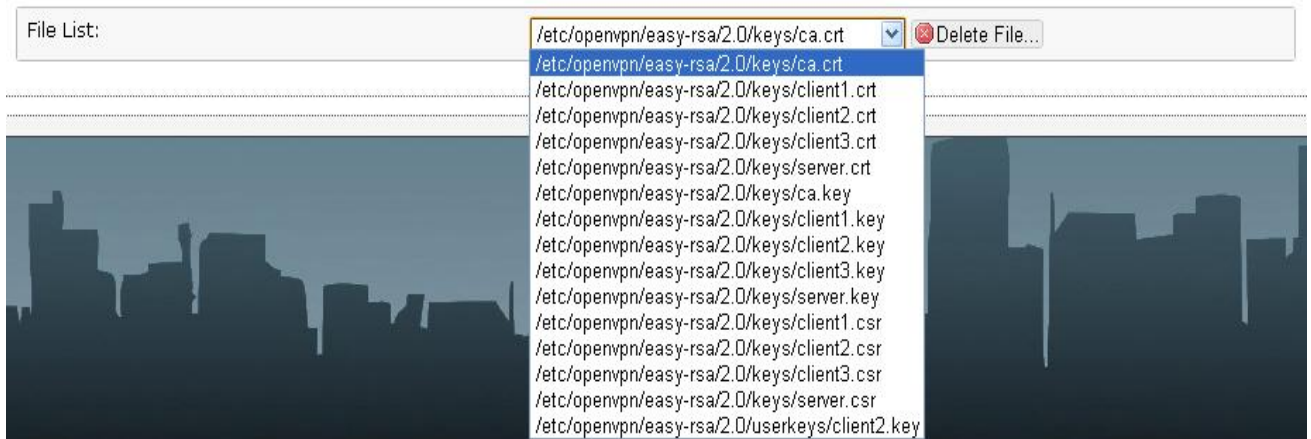
To upload Certificate Authority to JetBox. Default path will be in `/etc/openvpn/easy-rsa/2.0/userkeys/`.



Upload path is in the `/etc/openvpn/easy-rsa/2.0/userkeys/`

You can also delete the certificate keys via web interface.

Select your certificate file to delete.



7-4 PPTP

In this page, we provide PPTP server and PPTP client for user can create a VPN tunnel based on PPTP protocol. We have two sample configurations, pptp_server, pptp_client. As below

The screenshot shows the 'PPTP Connection Status' page. At the top, there are navigation tabs: System, Network, Switch, Routing, Firewall, VPN (selected), Serial, and Logout. Below these are sub-tabs: OpenVPN, IPsec, Certificates, PPTP (selected), L2TP, L2TPv3, and CHAP-Secrets. The main content area is titled 'PPTP instances' and contains a table of configured instances. Below the table is an 'Add' button. At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

	AutoStart	Type	Start	Status	Username	Remote Server	
<i>pptp_server</i>	No	server	Start	Down			
<i>pptp_client</i>	No	client	Start	Down	korenix	192.168.10.2	

PPTP Server Configuration

A PPTP Server (Point-To-Point Tunneling Protocol) allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office, etc. This way you can use the services provided in your office at the comfort of your home.

The screenshot shows the 'PPTP Connection Configuration' page for 'pptp_server'. It is divided into two sections: 'Connection Configuration for pptp_server' and 'Option File Configurations for pptp_server'. At the bottom right, there are 'Reset' and 'Save & Apply' buttons.

Connection Configuration for pptp_server

- AutoStart: Automatically Start after reboot.
- Type: Server (dropdown menu)
- timeout: 10
- speed: 115200
- localip: any
- remoteip: any
- debug: Turns on debugging mode

Option File Configurations for pptp_server

- auth: Yes (dropdown menu)
 Require the peer to authenticate itself before allowing network packets to be sent or received.
- MPPE Encryption: Enable MPPE (40/128 bit) (dropdown menu)
- MS-DNS: (empty text field)

AutoStart : Check it to enable PPTP connection after system reboot.

stimeout

Number of seconds to wait for a PPTP packet before forking the **pptpctrl** program to handle the client. The default is 10 seconds.

speed

Specifies a speed (in bits per second) to pass to the PPP daemon as the interface speed for the tty/pty pair. The default is 115200 bytes per second, which some implementations interpret as meaning "no limit".

localip

One or many IP addresses to be used at the local end of the tunnelled PPP links between the server and the client. If one address only is given, this address is used for all clients. Otherwise, one address per client must be given, and if there are no free addresses then any new clients will be refused.

remoteip

A list of remote IP addresses to be used on the tunnelled PPP links between the server and the client.

debug

Turns on debugging mode.

Option File Configuration For PPTP Server

Option File Configurations for pptp_server

auth	Yes <input checked="" type="checkbox"/> Require the peer to authenticate itself before allowing network packets to be sent or received.
MPPE Encryption	Enable MPPE (40/128 bit) Enable MPPE (40 bit) Enable MPPE (128 bit) Do not use MPPE
MS-DNS	

auth

Require the peer to authenticate itself before allowing network packets to be sent or received.

MPPE Encryption

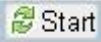
Here we provide three MPPE encryption types, MPPE with 40/128-bit, MPPE with 40-bit, MPPE with 128-bit. If you want to use CHAP or EAP encryption, select "Do not use MPPE" and you will see these options.

Option File Configurations for pptp_server

auth	Yes	<small>Require the peer to authenticate itself before allowing network packets to be sent or received.</small>
MPPE Encryption	Do not use MPPE	
CHAP	Require CHAP	
EAP	Require EAP	
MS-DNS		

MS-DNS

If pppd is acting as a server for Microsoft Windows clients, this option allows pppd to supply one or two DNS (Domain Name Server) addresses to the clients.

Click **“Save&Apply”** and back to PPTP pages. Press  **Start** button to start PPTP server and Client.






System | Network | Switch | Routing | Firewall | **VPN** | Serial | Logout


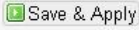
OpenVPN | IPsec | Certificates | **PPTP** | L2TP | L2TPv3 | CHAP-Secrets

PPTP Connection Status

PPTP instances

Below is a list of configured PPTP instances and their current state

	AutoStart	Type	Start	Status	Username	Remote Server	
<i>pptp_server</i>	No	server		Link			 
<i>pptp_client</i>	No	client		Down	korenix	192.168.10.2	 
<input type="text"/>							

7-5 L2TP

Here we provide the basic L2TP settings. User can create L2TP tunnel easily via web interface.

There are two sample configurations, l2tp_server, l2tp_client.








System | Network | Switch | Routing | Firewall | **VPN** | Serial | Logout


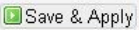
OpenVPN | IPsec | Certificates | PPTP | **L2TP** | L2TPv3 | CHAP-Secrets

L2TP Connection Status

L2TP instances

Below is a list of configured L2TP instances and their current state

	AutoStart	Type	Start	Status	Username	Remote Server	
<i>l2tp_server</i>	No	server		Down			 
<i>l2tp_client</i>	No	client		Down	korenix	192.168.10.2	 
<input type="text"/>							

L2TP Server Configuration

L2TP Connection Configuration

[Switch to Global Configuration =>](#)

Basic Connection Configuration for l2tp_server

AutoStart	<input type="checkbox"/> <input checked="" type="checkbox"/> Automatically Start after reboot.
Type	Server <small>Select Server or Client Mode</small>
ip range	192.168.10.2 - 192.168.10.100 <small>example: 192.168.10.1 - 192.168.10.100</small>
local ip	192.168.10.1 <small>example: 192.168.10.1</small>
CHAP	Require CHAP
ppp debug	no
length bit	yes

AutoStart : Check it to enable L2TP connection after system reboot.

ip range

Specify the range of ip addresses the LNS will assign to the connecting LAC PPP tunnels. Multiple ranges can be defined. Ranges are defined using the format IP - IP (example: 192.168.10.2 – 192.168.10.100).

local ip

Use the following IP as xl2tpd's own ip address.

CAHP (refuse | require chap)

require or refuse the remote peer to get authenticated via CHAP for the ppp authentication.

ppp debug

This will enable the debug for pppd

length bit

If set to yes, the length bit present in the l2tp packet payload will be used.

L2TP Client Configuration

L2TP Connection Configuration

[Switch to Global Configuration =>](#)

Basic Connection Configuration for l2tp_client

AutoStart	<input type="checkbox"/> Automatically Start after reboot.
Type	Client <input checked="" type="radio"/> Select Server or Client Mode
ppp debug	yes
Remote Server Address	192.168.10.2
Username	korenix
Password	*****
redial	No

AutoStart : Check it to enable L2TP connection after system reboot.

Remote Server Address

Set the DNS name or IP address of the LNS to connect to.

Username

Set the name of the local system for authentication purposes to *name*.

Password

Specifies the password to use for authenticating to the peer.

redial

If set to yes, xl2tpd will attempts to redial if the call get disconnected.

Remember to Press “**Save & Apply**” to apply these setting and generate configuration file.

Back to L2TP pages. Press button to start L2TP server and Client.

System | Network | Switch | Routing | Firewall | **VPN** | Serial | Logout

OpenVPN | IPsec | Certificates | PPTP | **L2TP** | L2TPv3 | CHAP-Secrets

L2TP Connection Status

L2TP instances
Below is a list of configured L2TP instances and their current state

	AutoStart	Type	Start	Status	Username	Remote Server	
<i>l2tp_server</i>	No	server	Stop	Link			
<i>l2tp_client</i>	No	client	Start	Down	korenix	192.168.10.2	
<input type="text"/>							

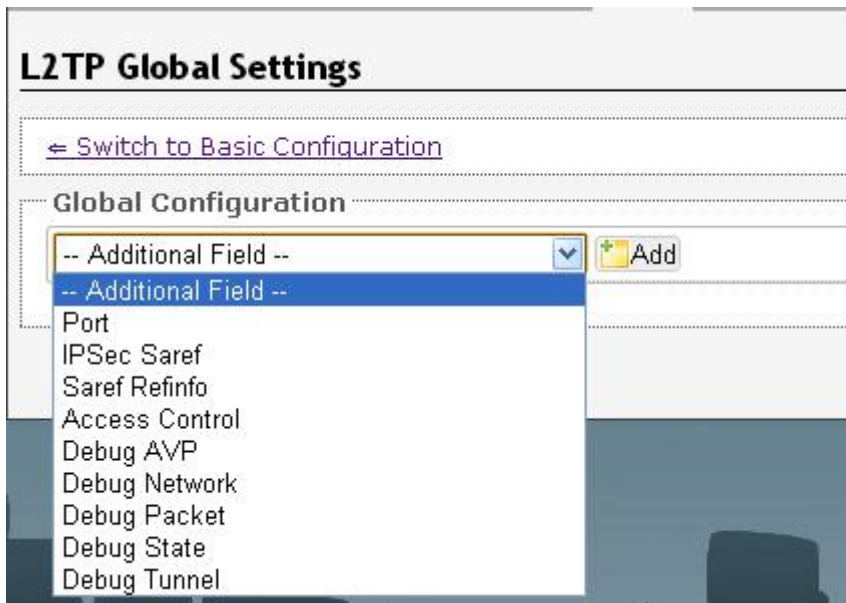


NOTE

- When you press start button with `l2tp_client`, it will also start `l2tp_server`. It is normally. So remember to stop `l2tp_server` if you do not want to enable `l2tp` daemon anymore.

Switch to Global Configuration

We also provide the Global section for L2TP. As below



port

Specify which UDP port `xl2tpd` should use. The default is 1701.

ipsec saref

Use IPsec Security Association tracking. When this is enabled, packets received by `xl2tpd` should have to extra fields (`refme` and `refhim`) which allows tracking of multiple clients using the same internal NATed IP address, and allows tracking of multiple clients behind the same NAT router. Values can be yes or no. The default is no.

saref refinfo

When using IPsec Security Association tracking, a new `setsockopt` is used. If not set, the default is to use 30.

access control

If set to yes, the `xl2tpd` process will only accept connections from peers addresses specified in the following sections. The default is no.

debug avp

Set this to yes to enable syslog output of L2TP AVP debugging information.

debug network

Set this to yes to enable syslog output of network debugging information.

debug packet

Set this to yes to enable printing of L2TP packet debugging information. Note: Output goes to STDOUT, so use this only in conjunction with the -D command line option.

debug state

Set this to yes to enable syslog output of FSM debugging information.

debug tunnel

Set this to yes to enable syslog output of tunnel debugging information.

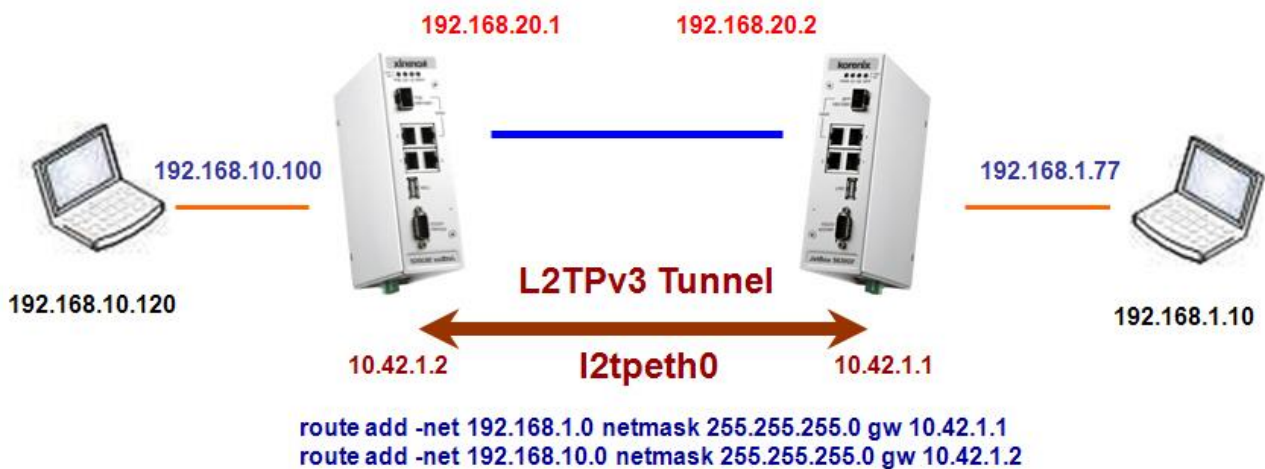
Basically, you can create L2TP tunnel easily by using basic configuration.

7-6 L2TPv3

In web interface, we provide L2TPv3 section for user can create L2TPv3 tunnel easily.

There is a sample configuration as below.

	AutoStart	Start	Link	Tunnel ID	Session ID	Local IP Address	Remote IP Address
<i>l2tpeth0</i>	No	Start	no	3000	1000	192.168.20.1	192.168.20.2



L2TPv3 Configuration

L2TPv3

L2TPv3 Tunnel Configuration for l2tpeth0	
AutoStart	<input type="checkbox"/> <input checked="" type="checkbox"/> Automatically Start after reboot.
Local IP Address	<input type="text" value="192.168.20.1"/>
Remote IP Address	<input type="text" value="192.168.20.2"/>
Encapsulation	<input type="text" value="UDP"/>
Tunnel ID	<input type="text" value="3000"/>
Peer Tunnel ID	<input type="text" value="4000"/>
UDP Source Port	<input type="text" value="5000"/>
UDP Destination Port	<input type="text" value="6000"/>
Session ID	<input type="text" value="1000"/>
Peer Session ID	<input type="text" value="2000"/>

L2TPv3 Interface Address	
Site A IP Address	<input type="text" value="10.42.1.1"/>
Site B IP Address	<input type="text" value="10.42.1.2"/>

AutoStart : Check it to create L2TPv3 tunnel after system reboot.

All the settings are the same as command in JetBox 5630 console.

For example

Site A : 10.42.1.1

```
~$ /sbin/ip l2tp add tunnel tunnel_id 3000 peer_tunnel_id 4000 encap udp local 192.168.20.1 remote 192.168.20.2 udp_sport 5000 udp_dport 6000
```

```
~$ /sbin/ip l2tp add session tunnel_id 3000 session_id 1000 peer_session_id 2000
```

```
~$ /sbin/ip link set l2tpeth0 up
```

```
~$ /sbin/ip addr add 10.42.1.1 peer 10.42.1.2 dev l2tpeth0
```

Some important parameters, like **tunnel_id**, **peer_tunnel_id**, **udp_sport**, **udp_dport** ...etc. You have to specify as same as ip command in JetBox 5630 console.

Press "**Save&Apply**" and back to L2TPv3 page. Press  to create L2TPv3 tunnel.

L2TPv3 Connection Status

L2TPv3 instances

Below is a list of configured L2TPv3 instances and their current state

	Stop	Link	Tunnel ID	Session ID	Local IP Address	Remote IP Address	
<i>l2tpeth0</i>		yes	3000	1000	192.168.20.1	192.168.20.2	
<input type="text"/>							

Reset Save & Apply

7-7 CHAP-Secrets

If you are using chap authentication, then you also need to create the secrets file. It is `/etc/ppp/pap-secrets`

The CHAP secrets file

The current pppd version requires that you have mutual authentication methods - that is you must allow for both your machine to authenticate the remote server **AND** the remote server to authenticate your machine.

The screenshot shows the 'CHAP-Secrets' configuration page. At the top, there are navigation tabs: System, Network, Switch, Routing, Firewall, VPN (selected), Serial, and Logout. Below these are sub-tabs: OpenVPN, IPSec, Certificates, PPTP, L2TP, L2TPv3, and CHAP-Secrets (selected). The main content area is titled 'CHAP Secrets' and contains the following text: 'This requires that you have mutual authentication methods - that is you must allow for both your machine to authenticate the remote server AND the remote server to authenticate your machine.' Below this text is a table for adding CHAP secrets. The table has four columns: 'User Name', 'Hostname', 'Password', and 'Acceptable local IP addresses'. The first row contains the values 'korenix', '*', 'korenix', and '*'. There is an 'Add' button below the table and 'Reset' and 'Save & Apply' buttons at the bottom right.

User Name	Hostname	Password	Acceptable local IP addresses
korenix	*	korenix	*
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

The field can be a symbol `"*"`. It means any username or hostname.

Chapter 8 Serial

In this chapter, we will explain how to set up the mode of serial port via web interface.

8-1 Port Settings

In this page, user can set up the mode of serial port. As below

The screenshot shows a web interface for configuring a serial port. At the top, there is a navigation bar with tabs for System, Network, Switch, Routing, Firewall, VPN, Serial (selected), and Logout. Below this is a sub-navigation bar with tabs for Port Settings (selected), Serial to Network, and ModBus Gateway. The main content area is titled 'Settings' and contains a 'Serial Port Configuration' section. This section includes a table of settings: AutoStart (checkbox), Port (1), Mode (RS232), Baud Rate (9600), Data Bits (8), Stop Bits (1), Parity (None), and Flow Control (None). At the bottom right of the configuration area are 'Reset' and 'Save & Apply' buttons.

Serial Port Configuration	
AutoStart	<input type="checkbox"/> Automatically apply after reboot.
Port	1
Mode	RS232
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

AutoStart : Check it to auto apply serial configuration after system reboot.

Mode

A dropdown menu showing the available serial port modes: RS232, RS422, and RS485 4 Wire. The RS232 option is currently selected and highlighted in blue.

We provide RS232 、 RS422 、 RS485 4 Wire for user select. It is the same as **serialctl** command. The other parameters are the same as general settings of serial port.

8-2 Serial to Network

In this page, user can set up the ser2net function. As below

The screenshot shows a web interface for configuring Ser2Net. At the top, there is a navigation bar with tabs for System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. Below this, there is a sub-navigation bar with tabs for Port Settings, Serial to Network, and ModBus Gateway. The main content area is titled "Ser2Net" and contains a "Port Configuration" section. This section has a table-like structure with the following fields and values:

AutoStart	<input checked="" type="checkbox"/> Automatically Start after reboot.
Apply immediately	<input type="checkbox"/>
Port	1
TCP Port (1 ~ 65535)	62001
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

At the bottom right of the configuration area, there are two buttons: "Reset" (with a red 'x' icon) and "Save & Apply" (with a green checkmark icon).

AutoStart : Check it to start ser2net after system reboot.

Apply immediately

It means that start **ser2net** immediately. If you do not check it, it will kill all ser2net process after pressing **Save&Apply** button.

8-3 ModBus Gateway

In this page, we provide the modbus gateway for user can set up. If you don't have modbus gateway program, it will not run.

The screenshot shows a web interface for configuring a ModBus Gateway. The navigation bar includes System, Network, Switch, Routing, Firewall, VPN, Serial, and Logout. The current page is titled 'ModBus Gateway' and is part of the 'Serial to Network' settings. The 'ModBus' configuration section includes the following fields:

Field	Value
Apply immediately	<input type="checkbox"/>
Port	1
Protocol	RTU
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
TCP Port (1 ~ 65535)	502
Timeout(second)	5
Scan Rate(ms)	200
TCP Aging(second)	420

At the bottom right of the configuration area, there are two buttons: 'Reset' and 'Save & Apply'.

Apply immediately

It means that start **modbus** immediately. If you do not check it, it will kill all modbus process after pressing **Save&Apply** button.

Protocol

Set Modbus protocol. **Default : RTU**

Baud Rate

Set data transfer rate. **Default: 115200**

Data Bits

Set the length of each data. **Default: 8 bits**

Stop Bits

Set the length of stop bit. **Default: 1**

Parity

Set parity check parameters to avoid errors during data transferring. **Default: None**

TCP Port

Set the port numbers of Modbus TCP server from 1~65535. **Default: 502**

Timeout

Set the wait-for-respond-time of data transferring from Modbus TCP to Modbus RTU/ASCII through Modbus Gateway. Range from 0~600 seconds. **Default: 5 seconds**

Scan Rate

Set the scan rate from 0~10000ms. **Default: 200ms**

TCP Aging

The system will automatically interrupt the connection to avoid occupying channel if the TCP connection is failed or idling abnormally. Range from 1~7200 seconds. **Default: 420s**

Korenix Technology Co., Ltd.

Business service: sales@korenixembedded.com, sales@korenix.com

Customer service: koreCARE@korenix.com

Web Site: <http://www.korenixembedded.com>, <http://www.korenix.com>