

comBOX VLL Web Manager GUI (ver 8.0.4b)

User Manual for comBOX VLL network appliance



© 2026 Protonyx Data Services

Reprinting or copying even in extracts only with written permission of Protonyx Data Services

Imprint

Producer:

Protonyx Data Services
550 Vouliagmenis Ave.
17456, Alimos
Athens, Greece

Phone: (+30) 210 990 2272

Fax: (+30) 210 990 2273

E-mail: support@protonyx.com

Web: www.combox-networks.com

© 2009 - 2025 Protonyx Data Services

Reprinting or copying even in extracts only with written permission of Protonyx Data Services.

Table of Contents

1. Introduction and scope	4
2. Glossary	5
3. Service Installation	6
3.1. Network Topology	6
3.2. ISP Modem/Router configuration	6
3.3. Connecting the cables	7
3.4. Accessing the comBOX VLL Web Manager GUI	8
4. Status	10
4.1. WAN Connection Legs status tables	10
4.1.1. Primary WAN Connection Legs Status	11
4.1.2. Backup WAN Connection Legs Status	11
4.2. LAN Interface Connected Devices	12
4.3. DHCP Clients Leases List	13
4.4. Bandwidth Usage	13
4.5. Real Time Performance Charts	14
4.6. Speed-Test Tool	15
5. LAN	16
5.1. Bridged Mode	17
5.2. NAT Mode	18
5.2.1. LAN Interface	18
5.2.2. DHCP Server	18
6. WAN	20
6.1. Leg Options	21
7. Advanced	24
7.1. Port Forwarding	24
7.2. Static Routing	26
7.3. Quality of Service (QoS)	27
7.3.1. Traffic Classes Definition	27
7.3.2. Traffic Classification Rules	28
Available Configuration Fields:	29
7.4. Policy Based Routing	30
7.4.1. WAN Priority List Definitions	31
7.5. VPN	32
7.5.1. VPN Server device configuration	33
7.5.2. Configuring VPN Client Devices	36
8. Administration	38
8.1. Device ID And Setup	38
8.1.1. WWAN Connection Legs	38
8.2. Reboot/Shutdown	40
8.3. Backup/Restore	40
8.4. Change Password	40
8.5. Factory Defaults	40
8.6. Product Activation	40

1. Introduction and scope

The comBOX VLL service provides WAN link aggregation and network optimization across multiple WAN connections.

All comBOX VLL service products, with a suite of advanced enterprise-class features, provide ideal single-box solutions for medium to large-sized business environments, and allow service providers to enable highly available, high performing professional WAN services.

This manual covers the Installation and configuration of the comBOX Virtual Leased Line (VLL) service.

2. Glossary

The following terms, acronyms and abbreviations are frequently used in this manual.

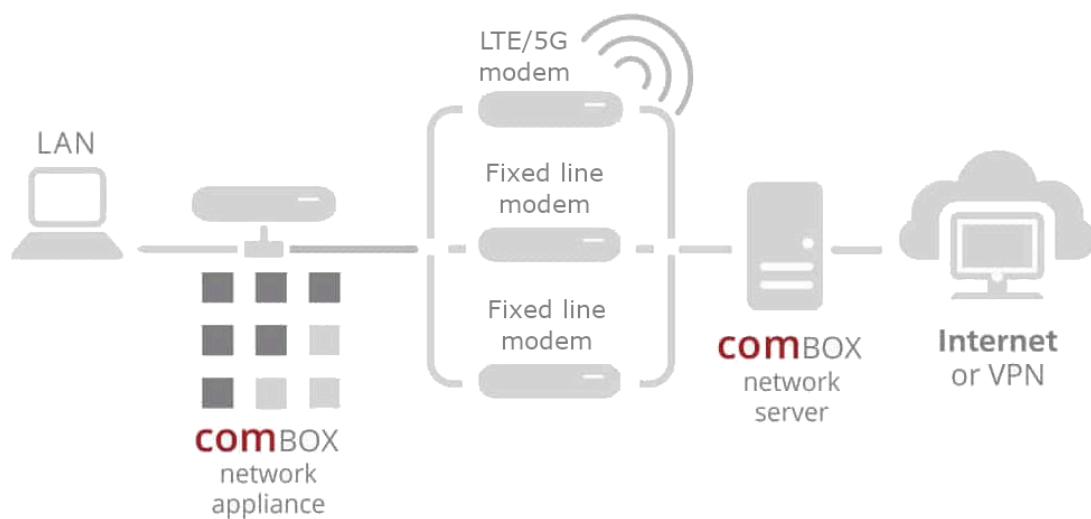
Term	Definition
4G/LTE	4th Generation of mobile network technology
5G	5th generation of mobile network technology
VDSL	Very-high-bit-rate Digital Subscriber Line
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DNS	Domain Name System
GRE	Generic Routing Encapsulation
ESP	Encapsulating Security Payload
GUI	Graphical User Interface
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
QoS	Quality of Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VLL	Virtual Leased Line
WAN	Wide Area Network
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SNR	Signal-to-Noise Ratio
RSSI	Received Signal Strength Indicator

3. Service Installation

This section outlines the initial setup procedures required to install the comBOX network appliance within the local network. These steps are essential for activating your comBOX network appliance and enabling the Virtual Leased Line (VLL) service.

3.1. Network Topology

To enable the comBOX VLL service, the comBOX network appliance must be installed between the Local Area Network (LAN) and the Internet Service Provider (ISP) modem(s), as illustrated in the figure below.



The default comBOX network appliance includes two physical network interfaces: one LAN port and one WAN port. However, it supports multiple WAN links through the use of virtual network interfaces in conjunction with an external network switch. For environments requiring multiple physical WAN connections without additional hardware, multiport comBOX appliances are available. These models come equipped with multiple physical WAN interfaces, eliminating the need for an external switch.

3.2. ISP Modem/Router configuration

Before connecting the cables, it is essential to prepare the environment to allow the comBOX network appliance to access the Internet. This preparation involves configuring the LAN IP addresses of the ISP modems so that each IP address belongs to a different subnet.

The comBOX network appliance supports multiple virtual WAN interfaces, which are pre-configured with the following default IP addresses:

- WAN IP of comBOX Virtual WAN Interface No. 1: 192.168.101.254
- WAN IP of comBOX Virtual WAN Interface No. 2: 192.168.102.254
- ...
- WAN IP of comBOX Virtual WAN Interface No. n: 192.168.10n.254

To expedite the installation process, it is recommended to configure the LAN IP addresses of the available ISP modems/routers as follows:

- LAN IP of the modem/router assigned to comBOX Virtual WAN Interface No. 1: 192.168.101.1
- LAN IP of the modem/router assigned to comBOX Virtual WAN Interface No. 2: 192.168.102.1
- ...
- LAN IP of the modem/router assigned to comBOX Virtual WAN Interface No. n: 192.168.10n.1

The default subnet mask for the LAN interface of all ISP modems should be set to 255.255.255.0.

If you are unable to modify the LAN IP settings for specific ISP modems or choose not to follow the recommended configuration, access the comBOX Web Manager GUI as outlined in the following sections and refer to the instructions in Section 6 of this manual.

3.3. Connecting the cables

Once the ISP modem IP addresses have been properly configured, you can proceed with connecting the devices.

For standard dual port comBOX network appliances, connect the LAN interfaces of the ISP modems to the comBOX WAN interface using an external network switch. This switch allows multiple ISP connections to interface with the single physical WAN port on the appliance.

If you are using a multiport comBOX appliance, the external switch is not required. In this case, each ISP modem can be connected directly to one of the available physical WAN ports on the appliance.



Important Notice: *It is recommended that you use ethernet cables with different colours to connect each of the ISP modems with the network switch so it would be easier to distinguish the available connection legs.*

3.4. Accessing the comBOX VLL Web Manager GUI

To access the **comBOX VLL Web Manager GUI**, follow the steps below:

1. **Physical Connection**

Connect an Ethernet cable from your **workstation** to the **LAN interface port** of the comBOX network appliance.

2. **IP Address Assignment**

Once connected, your workstation will automatically receive a **local IP address** via the comBOX's built-in **DHCP server**.

3. **Open a Supported Browser**

Launch a web browser that supports HTML5 such as:

- Internet Explorer 9 or later
- Firefox
- Chrome

Access the GUI

In the browser's address bar, type the following URL:

<https://192.168.1.1:8443>

Note: You may receive a **self-signed certificate warning**. Choose to proceed anyway.

Login

You will be directed to the comBOX VLL Web Manager login screen.

Enter the **username and password** provided to you to access the system.

Activate the Product

Upon first login, if your device has not been activated, you will see a **“Product not activated”** warning in the top-right corner of the interface.

To enable all features of the comBOX VLL service, you must **activate your product**.

Please follow the instructions detailed in **Section 8.6** to complete the activation.



Important Notice: *In order to activate your product you need to have connected the comBOX network appliance to the Internet, as described in the previous sections.*

The following sections contain a detailed explanation of every tab and subtab of the configuration interface in the order that they appear on comBOX VLL Web Manager GUI.

The configuration changes are applied by pressing the save button which is available on every tab and subtab of the configuration Interface and does not require a system restart.

4. Status

The **Status** tab provides a comprehensive overview of the system, including the current status of available Internet connections (Connection Legs), their usage and quality metrics, real-time performance charts, and a built-in speed test tool.

Status

LAN

WAN

Advanced

Administration

Primary WAN Connection Legs Status

Refreshes automatically every 5 seconds.
Last Refreshed on: Thu Jun 27 12:54:50 GMT+03:00 2024

Leg Id	Description	Leg Options	Traffic	State
1	RED	Full Bonding, 10Mbps U/L Cap, 50Mbps D/L Cap	17.733MB	Active
2	BLUE	Full Bonding	10.805MB	Disabled
3	YELLOW	Full Bonding	10.817MB	Down

Backup WAN Connection Legs Status

Last Refreshed on: Thu Jun 27 12:54:01 GMT+03:00 2024

Leg Id	Description	Leg Options	Traffic	State
4	GREEN	Backup	10.806MB	Disabled
5	RED2	Backup	10.806MB	Down

Refresh Now!

LAN Cable Connected. Link Speed: 100Mbps

Connected Devices

DHCP Clients Leases List

Click the following button to list all current DHCP leases

List DHCP Leases

Bandwidth Usage

Click [here](#) to view a report on your bandwidth usage

Real Time Performance Charts

Click [here](#) to watch the real time rates charts.

Speed Test

Select the connection you wish to test and click the button to perform a speedtest and estimate the current average/maximum bandwidth.

Warning: Speed Tests consume considerable bandwidth so keep this in mind in case you are using connections with restricted data allowances or volume based charges.

Select connection leg to test: Bonded VLL

☐ Measure latency and packet loss

Run Speedtest!

4.1. WAN Connection Legs status tables

This section displays status tables that provide detailed information about the available Internet connection legs. Each table contains three columns:

- **Leg ID:** A unique identifier for each Internet connection.
- **Description:** A user-defined or system-generated name that describes the connection.
- **Status:** Indicates the current state of the connection and can have one of the following values:

- **Active** – The connection is operational and in use.
- **Disabled** – The connection is manually turned off.
- **Disconnected** – The connection is unavailable or offline.



Important Notice: The number of connection legs shown in the comBOX VLL Web Manager GUI depends on the level of the comBOX VLL service license that has been purchased.

4.1.1. Primary WAN Connection Legs Status

This table displays the status of the bonded Internet connections. All connections assigned to the **Primary WAN Connection Legs** pool operate in **aggregate mode (bonding)**, meaning they are actively utilized by the comBOX VLL packet distribution algorithm for optimized traffic handling.

The status of the Primary WAN Connection Legs is automatically refreshed every **5 seconds**, ensuring real-time visibility into connection performance and availability.

Primary WAN Connection Legs Status				
Refreshes automatically every 5 seconds.				
Last Refreshed on: Tue Jul 02 10:31:46 GMT+03:00 2024				
Leg Id	Description	Leg Options	Traffic	State
1	RED	Full Bonding, 10Mbps U/L Cap, 50Mbps D/L Cap	55.81MB	Active
2	BLUE	Full Bonding	0B	Disabled
3	YELLOW	Full Bonding	13.118MB	Down

4.1.2. Backup WAN Connection Legs Status

This table displays the status of the **Backup (Failover) Internet Connections** pool. All Internet connections assigned to the **Backup WAN Connection Legs** pool operate in **failover mode** and are automatically activated **only** if all Primary WAN Connection Legs become unavailable.

If multiple WAN legs are assigned to the backup pool, the system will activate the **first available backup connection** with the **highest priority** to take over and route all network traffic.

If **two or more backup connections share the same priority**, they will be **bonded together** to form a **Backup Bonded Connection**, providing aggregated bandwidth and redundancy during failover.



Important Notice: The status of backup WAN connection legs does not refresh automatically when they are inactive. To update their status, you must manually click the Refresh button located at the bottom of the table. This design helps avoid unintended traffic charges from ISPs for inactive or metered connections.

Backup WAN Connection Legs Status				
Last Refreshed on: Tue Jul 02 10:33:01 GMT+03:00 2024				
Leg Id	Description	Leg Options	Traffic	State
4	GREEN	Backup	174.216KB	Disabled
5	RED2	Backup	174.636KB	Down
Refresh Now!				

4.2. LAN Interface Connected Devices

To view the devices connected on the LAN side, click the **“Connected Devices”** button. This will open a popup window displaying a list of all currently connected devices.

Each entry in the list provides the following information:

- **MAC Address** of the internal (LAN-side) device
- **Assigned IP Address** provided by the network

This feature offers a quick overview of active LAN clients for monitoring and troubleshooting purposes.

LAN Interface Connected Devices	
Refreshes automatically	
172.22.1.3	lladdr 00:90:fb:6d:df:28 REACHABLE
172.22.1.12	lladdr 00:0c:29:b5:85:0a REACHABLE
172.22.1.16	lladdr 00:0c:29:15:a8:76 REACHABLE
172.22.1.17	lladdr 00:0c:29:f5:e9:71 REACHABLE
172.22.1.18	lladdr 00:0c:29:e1:0b:74 REACHABLE
172.22.1.19	lladdr 00:0c:29:75:07:48 REACHABLE
172.22.1.23	lladdr 00:0c:29:92:60:fb REACHABLE
172.22.1.24	lladdr 00:0c:29:d8:80:98 REACHABLE
172.22.1.25	lladdr 54:04:a6:10:1c:98 REACHABLE
172.22.1.26	lladdr c8:cb:b8:ca:ee:bd REACHABLE
172.22.1.27	lladdr 00:0c:29:35:49:ec REACHABLE
172.22.1.32	lladdr 00:0c:29:18:98:8d REACHABLE
172.22.1.36	lladdr 00:90:fb:3a:2c:fa REACHABLE
172.22.1.37	lladdr 00:0c:29:48:5c:79 REACHABLE
172.22.1.38	lladdr 00:0c:29:e9:0c:9e REACHABLE
172.22.1.51	lladdr 00:0c:29:ec:02:15 REACHABLE
172.22.1.75	lladdr 00:0c:29:e6:7e:ec REACHABLE
172.22.1.76	lladdr 00:0c:29:98:9f:c2 REACHABLE
172.22.1.80	lladdr d0:67:e5:e7:eb:36 REACHABLE
172.22.1.81	lladdr 40:f2:e9:af:35:70 REACHABLE
172.22.1.125	lladdr 7c:03:4c:30:34:6f REACHABLE
172.22.1.145	lladdr e0:dc:ff:20:0a:e5 REACHABLE
172.22.1.147	lladdr d0:39:57:ac:20:45 REACHABLE
172.22.1.151	lladdr 38:9d:92:ee:26:a2 REACHABLE
172.22.1.160	lladdr d0:21:f9:b1:de:f0 REACHABLE
172.22.1.161	lladdr a0:43:b0:5e:7e:aa REACHABLE
172.22.1.176	lladdr 60:ab:67:8b:3b:56 REACHABLE
Scan Subnet Dismiss	

4.3. DHCP Clients Leases List

Click the “**List DHCP Leases**” button to open a popup window displaying all active DHCP leases on the network.

Each entry in the list includes the following details:

- **MAC Address** of the internal (LAN-side) device
- **Assigned IP Address**
- **Lease Time**, indicating the duration for which the IP address is assigned

This list helps you monitor IP address allocation and manage connected clients effectively.

DHCP Client Leases Listing Active Leases Only

IP Address	HW Address	Hostname	Start Date	End Date	State
192.168.130.94	1c:6f:65:fb:ef:24	pc	2016/12/07 08:10:46	2016/12/07 20:10:46	active
192.168.130.95	50:e5:49:e6:3e:1e	Xbox360	2016/12/07 09:14:37	2016/12/07 21:14:37	active
192.168.130.98	ac:9e:17:e0:ea:95	mygo-PC	2016/12/07 12:10:57	2016/12/08 00:10:57	active
192.168.130.99	b0:83:fe:a8:5f:b7	ps4-PC	2016/12/07 11:35:13	2016/12/07 23:35:13	active

List all active and expired leases

4.4. Bandwidth Usage

Clicking the hyperlink under this section’s title opens a new browser tab displaying **Bandwidth Utilization statistics**. The data is presented with **hourly**, **daily**, and **monthly** breakdowns to provide detailed insight into usage patterns over time.

This information can help you:

- Monitor network traffic trends
- Estimate potential **bandwidth utilization charges**
- Select or adjust your service plan based on actual usage needs



4.5. Real Time Performance Charts

By clicking the hyperlink under this section's title, a new page opens in a separate browser tab, displaying **real-time graphs** that show the **current utilization of each individual connection leg**, as well as the **overall utilization of the bonded connection (VLL)**



The available charts display **actual network traffic** in **kbps/Mbps**, using **green** to represent **downlink (download) traffic** and **red** for **uplink (upload) traffic**.

- The **VLL chart** that appears on top illustrates the utilization of the **aggregated bandwidth** provided by the Virtual Leased Line.
- The **Connection Legs charts** show the **individual bandwidth utilization** of each available Internet connection.



***Important Notice:** At times, you may observe higher bandwidth rates on the VLL chart than the total combined bandwidth of the individual connection legs. This is expected behavior and occurs when compressible data is being transferred. The increase is a result of the real-time data compression feature built into the comBOX VLL, which enhances effective throughput without requiring additional bandwidth.*

4.6. Speed-Test Tool

The **comBOX VLL Web Manager GUI** includes a built-in **Speed-Test tool** designed to measure the **aggregated bandwidth** between the comBOX network appliance and the comBOX network server.

By clicking the “**Run Speed-Test**” button, the system initiates a controlled traffic stream through the VLL service to calculate both the **total downlink** and **uplink speeds** of the Virtual Leased Line. After a few seconds, the test results are displayed in a **popup window** on the Status page.



***WARNING:** Use this tool with caution as Speed Tests consume considerable bandwidth. Keep this in mind in case you are using connections with restricted data allowances or volume based charges.*

5. LAN

The **LAN** tab provides access to configuration settings for the **LAN network interface** of the comBOX network appliance. It allows the system administrator to customize local network parameters to suit the specific requirements of the deployment environment.

Status

LAN

WAN

Advanced

Administration

Select Operating Mode:
☐ Bridge Mode
☒ NAT Mode

NAT Mode Selected

LAN Interface

IP Address:

Subnet Mask:

DHCP Server:
☒ Enabled
☐ Disabled

DHCP Pool Range Start Address:

DHCP Pool Range End Address:

DHCP DNS Server:
☒ This Device
☐ Custom:

Static IP address leases:

Enabled	MAC Address	IP Address	
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

The first option in this section allows you to **select the operating mode** of the comBOX network appliance. You can choose between **NAT mode** and **Bridged mode**, depending on the requirements of your internal network topology:

- **NAT Mode:** The comBOX acts as a gateway, translating internal IP addresses to a single external IP.
- **Bridged Mode:** The comBOX functions as a transparent bridge, passing traffic between the LAN and WAN without modifying IP addresses.

5.1. Bridged Mode

Bridged Mode enables the **transparent operation** of the comBOX network appliance. In this mode, the **static IP address(es)** assigned to the comBOX VLL service are **forwarded directly to the internal network**, allowing devices behind the appliance to use public IPs without NAT translation.

This mode is typically preferred by **system administrators** who require:

- **Advanced network configurations** not available through the comBOX VLL Web Manager GUI
- Support for **complex or custom network topologies**
- Full control over routing, firewall rules, or external-facing services within the internal network



***Important Notice:** When Bridged Mode is selected, the Port Forwarding options available in the “Advanced” section of the comBOX VLL Web Manager GUI are not applicable. In this mode, port forwarding must be configured directly on the internal network devices.*

If **Bridged Mode** is selected, a configuration table appears on the page displaying the required settings for the **WAN interface** of the **third-party device(s)** connected to the **LAN port** of the comBOX network appliance.

Bridge Mode Selected

Please set the following IP details on your firewall/server(s)

Available IP Addresses	5.9.236.156
Subnet Mask	255.255.255.224
Default Gateway Address	5.9.236.129
Nameserver (DNS) Address	5.9.236.129

Save

5.2. NAT Mode

When **NAT Mode** is selected, the comBOX network appliance functions as the **edge firewall** for the internal network. In this mode, it performs **Network Address Translation (NAT)** for all inbound and outbound traffic.

The default traffic policy is as follows:

- **Outbound traffic:** Allowed by default
- **Inbound traffic:** Blocked by default, unless **port forwarding rules** have been explicitly configured

This mode is suitable for standard network deployments where the comBOX appliance manages IP address translation and enforces basic security at the network perimeter.

5.2.1. LAN Interface

The available configuration fields allow you to assign a **unique private IP address** to the **comBOX LAN network interface**, as well as define the **LAN subnet mask**.

Both the **LAN IP address** and the **subnet mask** must be entered in standard **IPv4 format**:

XXX.XXX.XXX.XXX.



***Important Notice:** When you change the LAN IP address of the comBOX network appliance, ensure that the network configuration of the workstation used to access the comBOX VLL Web Manager GUI is updated accordingly.*

If the workstation is using DHCP, you may need to restart its network interface to obtain the new network settings and maintain connectivity with the appliance.

The **LAN network interface IP address** configured on the comBOX appliance should be set as the **default gateway** for all devices on the internal network.

When the **DHCP server** is enabled on the comBOX appliance, this default gateway IP address is **automatically assigned** to internal devices along with their IP configuration.

5.2.2. DHCP Server

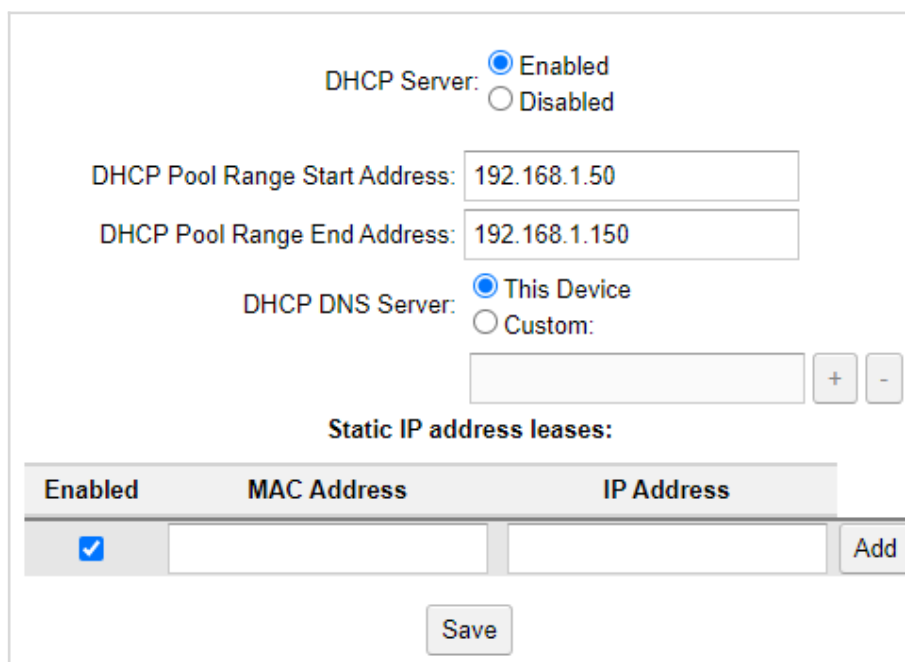
The **DHCP server** functionality on the comBOX appliance enables the **automatic assignment of IP addresses** to devices on the internal network. This feature is **enabled by default**, allowing users to easily obtain an IP address for the **initial configuration** of the comBOX network appliance.

When the DHCP server is active, you can:

- Define the **IP address range** for DHCP leases
- Manually assign a **specific IP address** to a device based on its **MAC address** (Static IP address leases)

This provides flexibility in managing both dynamic and static IP assignments within the internal network.

If you are operating an **internal DNS server** and want all LAN devices that receive an IP address via the **DHCP server** to use it instead of the default DNS server provided by the comBOX appliance, you can enable the **Custom DHCP DNS Server** option. Then, enter the **local IP address** of your internal DNS server in the designated field, as illustrated in the image below.



The screenshot shows the DHCP configuration page. At the top, the 'DHCP Server' is set to 'Enabled' with a radio button. Below this, the 'DHCP Pool Range Start Address' is '192.168.1.50' and the 'DHCP Pool Range End Address' is '192.168.1.150'. The 'DHCP DNS Server' is set to 'This Device' with a radio button, and there is an empty field for a 'Custom' DNS server with '+' and '-' buttons. Below these is a section titled 'Static IP address leases:' which contains a table with three columns: 'Enabled', 'MAC Address', and 'IP Address'. The first row has a checked checkbox in the 'Enabled' column, empty fields for 'MAC Address' and 'IP Address', and an 'Add' button. At the bottom center is a 'Save' button.

DHCP Server: ☒ Enabled ☐ Disabled

DHCP Pool Range Start Address: 192.168.1.50

DHCP Pool Range End Address: 192.168.1.150

DHCP DNS Server: ☒ This Device ☐ Custom: + -

Static IP address leases:

Enabled	MAC Address	IP Address
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Add

Save

6. WAN

The **WAN** tab allows you to configure the **available connection legs** of the comBOX network appliance. All Internet modems/routers must be connected to the **WAN port** of the appliance via **Ethernet**, using an **external network switch**. Each modem/router should be configured with an IP address that belongs to a **different subnet** to avoid conflicts and ensure proper routing.

The **comBOX VLL Web Manager GUI** displays a number of connection legs based on the level of your **purchased VLL service license**. Each connection leg can be individually configured as either **Primary** or **Backup**, depending on your desired **usage scenario** and failover strategy.

Wan Interfaces Configuration
Use the following tables to insert the ISPs' modem details.

Internet Connection Legs							
Leg Id	Enabled	ISP/Leg Description	DHCP Client	Modem/Router IP Address	Modem/Router Subnet Mask	comBOX Interface IP Address	Leg Options
1	<input checked="" type="checkbox"/>	COSMOTE-RED	Disabled	192.168.101.1	255.255.255.0	192.168.101.254	Full Bonding, 10Mbps U/L Cap, 50Mbps D/L Cap
2	<input checked="" type="checkbox"/>	FORTHNET-BLUE	Disabled	192.168.2.1	255.255.255.0	192.168.2.250	Backup
3	<input checked="" type="checkbox"/>	COSMOTE-YELLOW	Disabled	192.168.3.1	255.255.255.0	192.168.3.250	Full Bonding
4	<input checked="" type="checkbox"/>	VODAFONE-GREEN	Disabled	192.168.7.1	255.255.255.0	192.168.7.250	Full Bonding
5	<input checked="" type="checkbox"/>	VODAFONE-RED	Disabled	192.168.5.1	255.255.255.0	192.168.5.250	Backup

Bonding Options
 Select the data compression algorithm for the client-server tunnel ?
 Data Compression Algorithm: Snappy
 Should the client-server tunnel be encrypted? ?
☐ Enable Data Encryption

All **connection legs** include a set of configurable attributes, accessible through their respective fields in the **WAN tab** of the comBOX VLL Web Manager GUI:

- **Leg ID:** A unique, system-assigned identifier for each connection leg. This value is used internally and **cannot be modified** by the user.
- **Enabled:** Controls the operational status of each connection leg. Use the checkbox to **enable** or **disable** individual connections as needed.
- **ISP/Leg Description:** This field allows you to assign a **descriptive name** to each connection leg (e.g., "Office VDSL", "4G Backup", "Starlink"). The name you provide will be displayed consistently across all related sections in the Web Manager GUI.
- **DHCP Client:** Use the dropdown menu to **enable or disable the DHCP client** for the selected WAN interface. Enable this option if the WAN IP address should be **automatically assigned** by the connected ISP modem/router.
- **Modem/Router IP Address:** Enter the **IP address** of the ISP modem/router assigned to this connection leg. Each IP address must be **unique** and should belong to a **different subnet** from other connection legs.
- **Modem/Router Subnet Mask:** Specify the **subnet mask** associated with the modem/router's IP address.

- **comBOX Interface IP Address:** Enter the **IP address** assigned to the corresponding **Virtual WAN interface** of the comBOX appliance. This address must be in the **same subnet** as defined by the Modem/Router IP Address and Subnet Mask.



WARNING: *If your comBOX network appliance supports only one physical WAN interface, you can enable the DHCP client for only one virtual WAN interface. All remaining virtual WAN interfaces must be configured manually with static IP settings. You may enable the DHCP client for multiple WAN interfaces only if your appliance supports multiple physical WAN ports.*

6.1. Leg Options

The **Leg Options** column allows you to configure the **bonding mode** for each connection leg. This determines how the connection is used by the comBOX VLL traffic distribution algorithm. The available bonding modes are:

- **Full Bonding**
The connection leg is actively used by the **comBOX VLL traffic distribution algorithm** for **all WAN traffic**. This mode is ideal for maximizing throughput by aggregating all available bandwidth.
- **Selective Bonding**
The connection leg is used **only for specific QoS (Quality of Service) classes**. This is useful for Internet connections with **bandwidth caps or limited data plans**, allowing them to be reserved for **critical or real-time traffic** (e.g., voice, video conferencing).

Tip: Hover over the **Selective Bonding** label to view a **tooltip** listing the **QoS classes** that utilize this leg.
- **Bonding Disabled**
The connection leg is **not used** by the VLL bonding algorithm. However, it can still be utilized in **policy-based routing** configurations for specific network rules or advanced scenarios.
- **Backup Bonding**
The connection leg remains **inactive** during normal operation and is used **only as a failover**, when **all Full and Selective Bonding legs** are disconnected. This mode provides **redundancy** without consuming bandwidth under normal conditions.

You can configure the **bonding mode** for each connection leg by clicking the **gearbox (settings) button** located on the right side of each leg entry in the table.

When the button is pressed, a **pop-in window** appears with the following configuration options:

Leg Options
For Leg Id #1: LEG-1

Enter the APN for this SIM

Enter the username if authentication is required

Enter the password if authentication is required

Use this leg for bonding?

☒ Enable Bonding

Is this a primary or a backup leg?

☒ Primary
☐ Backup
Backup priority:

Apply a cap to this leg's maximum rates?

☒ No Upload Cap
☐ Cap Upload to: Mbps

☒ No Download Cap
☐ Cap Download to: Mbps

How much traffic is this leg allowed to consume in a month?

☒ No limit
☐ Limit usage to: B

Billing Cycle starts every month on day:

▼ Advanced

Is this leg exclusive to certain traffic Classes?

☒ Use it for ALL Traffic Classes (Default)
☐ ONLY use it for the following Traffic Classes:

☒ Class A
☒ Class B
☒ Class C
☒ Class D
☒ Class E
☒ Class F
☒ Class G
☒ Default Class

OK

Cancel

Important Notice: The below options are available on all Legs connected via the available WAN port(s) of the device:

Enable Bonding: This checkbox is **enabled by default**, allowing the connection leg to participate in the **comBOX VLL traffic distribution algorithm**. If disabled, the leg will be **excluded from the**

© 2026 Protonyx Data Services

Reprinting or copying even in extracts only with written permission of Protonyx Data Services

22

bonding process and can only be used through **Policy-Based Routing**.

Is this a Primary or Backup Leg? Select whether the connection leg will function as a **Primary** or **Backup** connection:

- **Primary legs** are used as long as they are **operational**.
- **Backup legs** are activated **only** when **no primary legs are functional**.

Backup Priority: For **Backup legs**, this setting defines the **priority level**.

- Legs with **lower priority numbers** are preferred and will be used first.
- Backup legs with the **same priority number** will be **bonded together** and used **simultaneously** during failover.

Bandwidth Limiter: Allows you to set a **cap** on both **download** and **upload bandwidth** for the selected leg.



Important Notice: This bandwidth limiter limit that is configured is subject to the overall bandwidth cap set by the service license.

Traffic Limiter: Enables you to set a **monthly data usage cap** for the connection leg.

- You can define the limit in units from **Bytes to Terabytes**.
- You can also specify the **start day of the billing cycle** to align with your ISP plan.

Advanced: Clicking the **Advanced** label reveals **Selective Bonding options**:

- **Use it for ALL Traffic Classes** (default): All traffic classes can use this leg—equivalent to **full bonding mode**.
- **ONLY use it for the following Traffic Classes:** Restricts usage of the leg to **specific QoS classes**.



WARNING: While this can be useful for managing capped or specialized connections, it may result in underutilization. Ensure you fully understand the impact before enabling this setting.



Important Notice: The following options are only available if one or more WWAN Legs have been configured. (For instructions on configuring WWAN Legs, refer to Section 8.1: Device ID and Setup.)

Set SIM APN: Allows you to enter the **Access Point Name (APN)** required by the **SIM card** on the selected leg. This is necessary for the SIM to establish a data connection.

Set SIM Username (if authentication is required): Enables you to specify the **username** used by the SIM card for network **authentication** on the selected leg.

Set SIM Password (if authentication is required): Enables you to specify the corresponding **password** used for SIM card **authentication** on the selected leg.

7. Advanced

The **Advanced** tab provides access to **application-specific configurations** for more granular control over network behavior and traffic management.

This tab includes the following **subtabs**, each dedicated to a specific feature:

- **Port Forwarding**
- **QoS (Quality of Service)**
- **Policy-Based Routing (PBR)**
- **Static Routes**
- **VPN**

These tools are intended for advanced users who require custom network setups, performance optimization, or routing control beyond the default configuration options.

7.1. Port Forwarding

The **Port Forwarding** table allows you to define rules that enable **remote access to internal network services** (e.g., web servers, VPNs, or IP cameras).

Use this feature to expose specific internal devices or applications to the Internet by forwarding traffic from designated external ports to corresponding internal IP addresses and ports.

NAT Forwarding Rules

Use the following table to configure your port forwarding rules. These rules are only going to be effective as long as **NAT Mode** is selected in the **LAN** interface configuration.

Rule Id	Enabled	Protocol	Original Destination IP Address	Original Destination Port	Original Destination End Port	New Destination IP Address	New Destination Port	New Destination End Port	Comment	
0	<input type="checkbox"/>	udp	5.9.236.156	23456	23459	192.168.1.41	23456	23459	DVR	Delete Rule
1	<input type="checkbox"/>	tcp/udp	192.168.5.250	5901	5901	192.168.1.5	5901	5901	VNC	Delete Rule
2	<input type="checkbox"/>	gre	5.9.236.156			192.168.1.198			GRE tunnel	Delete Rule
3	<input type="checkbox"/>	esp	5.9.236.156			192.168.1.195			IPSec VPN	Delete Rule
4	<input checked="" type="checkbox"/>	tcp	5.9.236.156							Add Rule

You can configure **port forwarding rules** to enable **remote access** to specific services running within your local network. Each rule can be customized using the following fields:

- **Rule ID:** A system-assigned, **unique identifier** for each port forwarding rule. This value is used internally and **cannot be edited**.
- **Enabled:** A checkbox indicating whether the rule is **active**. Toggle this to **enable or disable** the rule as needed.
- **Protocol:** Select the network **protocol** used by the service. Available options include: **TCP**, **UDP**, **TCP&UDP**, **GRE**, **ESP**, or **ANY**. Choose the protocol that matches the application/service you're configuring.
- **Original Destination IP Address:** Select the **public IP address** through which the service will be accessed remotely. You may choose between:
 - A public IP assigned by the **VLL service**
 - A public IP provided by an **individual ISP connection leg**

Note: If the selected leg's modem/router performs NAT, ensure it also forwards traffic to the comBOX IP address.

- **Original Destination Port:** Enter the **external port number** to be used for accessing the internal service.
- **Original Destination End Port (Optional):** If the service requires a **range of ports**, specify the **end port** of the external range here.
- **New Destination IP Address:** Enter the **internal (LAN) IP address** of the device hosting the service.
- **New Destination Port:** Enter the **port number** used by the internal service on the local device.
Note: This may be different from the external (original) destination port.

- **New Destination End Port (Optional):** If the internal service requires a **port range**, specify the **end port** of the internal range here.
- **Comment:** Provide a **name or description** for the rule. Use a label that identifies the associated service for easier management.

By pressing the buttons “Delete Rule” and “Add Rule” you can either delete the selected Rule or add a new port forwarding rule.



Important Notice: When bridged mode is selected, the inserted Port Forwarding rules will be disabled but would not be deleted, so you may use them again in case you decide to restore your previous configuration.

7.2. Static Routing

Use the Static Routing table to configure static routing rules for the internal network. These rules are only going to be effective as long as **NAT Mode** is selected in the **LAN** interface configuration.

Static Routing

Use the following table to configure static routing rules. These rules are only going to be effective as long as **NAT Mode** is selected in the **LAN** interface configuration.

Rule Index	Enabled	Destination IP/Subnet	Gateway IP	InternetAccess	Comment	
0	<input checked="" type="checkbox"/>	192.168.196.0/24	172.22.1.22	<input checked="" type="checkbox"/>	test 1	Delete Rule
1	<input checked="" type="checkbox"/>	192.168.194.0/24	172.22.1.22	<input type="checkbox"/>	test 2	Delete Rule
2	<input checked="" type="checkbox"/>			<input type="checkbox"/>		Add Rule

You can define **static routing rules** to manually control how traffic is directed within your network. Each static route can be configured using the following fields:

- **Rule Index:** A system-assigned, **unique identifier** for each static route. This value is used internally and **cannot be modified**.
- **Enabled:** A checkbox that determines whether the static route is **active**. Toggle it to enable or disable the rule.
- **Destination IP/Subnet:** Enter the **destination IP address** or **subnet** for which the static route should apply. This defines the **target network** for the routing rule.
- **Gateway IP:** Specify the **IP address of the gateway device** that will forward packets to the destination IP/subnet. The gateway must be reachable from the comBOX network appliance.

- **Internet Access:** Check this box to allow **Internet access** for devices matching the specified **destination IP/subnet**.
Enabling this option also allows:
 - Creation of **port forwarding rules** for remote access to services hosted at the destination
 - Configuration of **Policy-Based Routing** and **QoS rules** for the destination devices
- **Comment:** Provide a **name or description** for the static route to help identify its purpose or the associated network.

7.3. Quality of Service (QoS)

The **QoS** subtab allows you to configure **Quality of Service classes** and define **traffic classification rules** based on specific applications or host devices. These rules enable you to **prioritize network traffic** according to your operational needs, ensuring that **critical or latency-sensitive services** (such as VoIP, video conferencing, or business apps) receive appropriate bandwidth and performance levels.

By applying QoS policies, you can optimize the overall efficiency of your network and prevent lower-priority traffic from impacting essential services.


7.3.1. Traffic Classes Definition

You may define **up to 8 traffic classes**, each representing a specific priority or type of network traffic. Every class is assigned a **bandwidth ratio**, which determines its **relative share** of the available bandwidth.

Bandwidth allocation is handled **dynamically based on demand**. This means:

- If higher-priority traffic (with higher ratios) is **not fully utilizing** its allocated share,
- Then lower-priority traffic (with lower ratios) is allowed to **temporarily use the available bandwidth**.

This ensures efficient utilization of your total bandwidth while still **prioritizing critical services** when needed.

 **Traffic Classes Definition**

Traffic Class	Bandwidth Ratio	Percentage	Redundant Mode
Class A	<input type="text" value="2"/>	20.00%	<input checked="" type="checkbox"/>
Class B	<input type="text" value="5"/>	50.00%	<input type="checkbox"/>
Default Class	<input type="text" value="3"/>	30.00%	<input type="checkbox"/>

By enabling the checkbox under the **Redundant Mode** column for a given **Priority Class**, data packets associated with that **QoS class** will be **duplicated and transmitted simultaneously** over the **two best-performing WAN links**, as determined by the comBOX VLL's **real-time link monitoring** feature.

The system then delivers the **first successfully received packet**, discarding the duplicate. This feature significantly improves **reliability**, minimizes **packet loss**, and reduces **latency jitter**, especially in fluctuating network conditions.

Recommended Use Cases: Enable **Redundant Mode** for **latency-sensitive or mission-critical traffic**, such as:

- **VoIP and video conferencing**
- **Online gaming**
- **Remote desktop sessions**
- **Real-time financial or control systems**

This ensures consistent performance, even if one WAN connection temporarily degrades.



***Important Notice:** When using the Redundant mode feature for a specific QoS class, please note that this could lead to more bandwidth usage since the transmitted data is using twice the bandwidth needed.*

7.3.2. Traffic Classification Rules

The **Traffic Classification Rules** table allows you to assign specific types of traffic to the appropriate **QoS classes** based on your network priorities.

- Traffic that is **not explicitly assigned** to any class will automatically be directed to the **Default Class**.

- Similarly, traffic that is assigned to a **non-existent or undefined class** will also fall back to the **Default Class**.

Use this table to ensure that important applications and services are properly prioritized and receive the appropriate share of available bandwidth.

Traffic Classification Rules												
Rule Id	Enabled	DSCP	Protocol	Local IP/ Subnet	Local Port	Local End Port	Remote IP/ Subnet	Remote Port	Remote End Port	Class	Comment	Move Rule
0	<input type="checkbox"/>	ANY	esp	192.168.1.137			ANY			Class B	IPsec	↓ Delete Rule
1	<input type="checkbox"/>	ANY	gre	5.9.236.156			ANY			Class B	GRE tunnel	↕ Delete Rule
2	<input checked="" type="checkbox"/>	ANY	udp	172.22.1.0/24	5060	5060	ANY	5060	5060	Class A	VoIP calls	↑ Delete Rule
3	<input checked="" type="checkbox"/>		any							Class A		↑ Add Rule

Save

You can define **Traffic Classification Rules** to assign specific types of traffic to designated **QoS classes**. These rules help manage bandwidth usage and prioritize critical services.

Tip: Use the keyword **"ANY"**, the asterisk symbol (*), or leave a field **blank** to make a rule **match all values** for that attribute.

Available Configuration Fields:

- **Rule ID:** A system-assigned **unique identifier** for each traffic classification rule. This value is used internally and **cannot be edited**.
- **Enabled:** A checkbox indicating whether the rule is **active**. Click to enable or disable the rule.
- **DSCP (Optional):** Enter a **DSCP (Differentiated Services Code Point)** value to integrate with **QoS settings on third-party devices**. This is especially useful in **Bridged Mode**, where traffic classification may be performed **externally**—for example, by a **firewall, router**, or even a specific **application**. The comBOX appliance will respect the classification already applied to the packet and map it to the corresponding internal QoS class.
- **Protocol:** Select the **network protocol** used by the application or service. Options include: **TCP, UDP, TCP&UDP, or ESP**.
- **Local IP/Subnet:**
 - In **NAT Mode**: Enter the **private IP address** of the local device.
 - In **Bridged Mode**: A dropdown is displayed listing **available public IPs** assigned by the comBOX VLL service.

- **Local Port:** Enter the **local port** used by the application or service.
- **Local End Port (Optional):** If the local service uses a **range of ports**, enter the **ending port** here.
- **Remote IP/Subnet:** Enter the **remote IP address or subnet** of the service you're classifying traffic for.
- **Remote Port:** Enter the **port number** used by the remote service or host.
- **Remote End Port (Optional):** If the remote service requires a **port range**, enter the **ending port** here.
- **Class:** Select the **QoS class** to apply for this rule from the list of **enabled priority classes**.
- **Comment:** Provide a **name or description** for the rule. Use a label that reflects the **application or service** to make the rule easily identifiable.

7.4. Policy Based Routing

Use this table to configure **WAN routing policies** for specific types of traffic. By default, **all traffic is routed via the VLL connection**, leveraging the bonded bandwidth and optimized routing provided by the comBOX Virtual Leased Line service.

However, certain types of traffic may require custom routing based on performance, cost, or operational requirements. The **Policy-Based Routing** table allows you to override the default behavior and route traffic using one of the following methods:

- **Load-Balancer:** Distributes the selected traffic type across all available WAN legs based on current load and availability.
- **Specific WAN Leg:** Forces the traffic to be routed through a **single, specified WAN connection leg**.
- **WAN Priority List:** Defines an ordered list of preferred WAN legs. The system attempts to use the **highest-priority available leg**, failing over to the next one in the list if needed.

Policy Based Routing										
Rule Index	Enabled	Protocol	Local IP/ Subnet	Remote IP/ Subnet	Remote Port	Remote End Port	Routing Method	Route Option	Comment	Move Rule
0	<input checked="" type="checkbox"/>	tcp/udp	192.168.1.0/24	77.72.80.15	ANY	ANY	Load Balancer		access to WebTV	↓
1	<input checked="" type="checkbox"/>	tcp	192.168.1.0/24	ANY	25	25	WAN Leg	CONN-	mail server access	↑↓
2	<input checked="" type="checkbox"/>	tcp	192.168.1.111	ANY	ANY	ANY	WAN Priority List	myList	test priority list	↑
3	<input checked="" type="checkbox"/>	tcp					Load Balancer			

You can configure the **routing method** for each type of traffic by selecting one of the following options:

- **Load Balancer:** When **Load Balancer** is selected, each new session of the specified traffic type will be routed through one of the **available primary connection legs**.
 - Successive sessions will be distributed in a **round-robin manner** across the pool of primary connection legs, ensuring an even distribution of traffic.
- **WAN Leg:** When **WAN Leg** is selected, all new sessions of the specified traffic type will be routed exclusively through the **connection leg specified in the Routing Option field**.
 - If the specified connection leg becomes **unavailable**, new sessions will be routed based on the **Load Balancer** method until the leg becomes available again.
- **WAN Priority List:** When **WAN Priority List** is selected, all new sessions of the specified traffic type will be routed through the first active connection leg defined in the **priority list**.
 - Priority lists are configured in the **WAN Priority List Definitions** section. This routing method allows the most **granular control**, as it accounts for failures in specific connection legs and reroutes traffic based on availability.



Important Notice: The order of the rules is important. Traffic is routed according to the first rule that matches. Use the keyword "ANY", the asterisk symbol (*), or leave a field blank to make traffic match any value for that attribute.

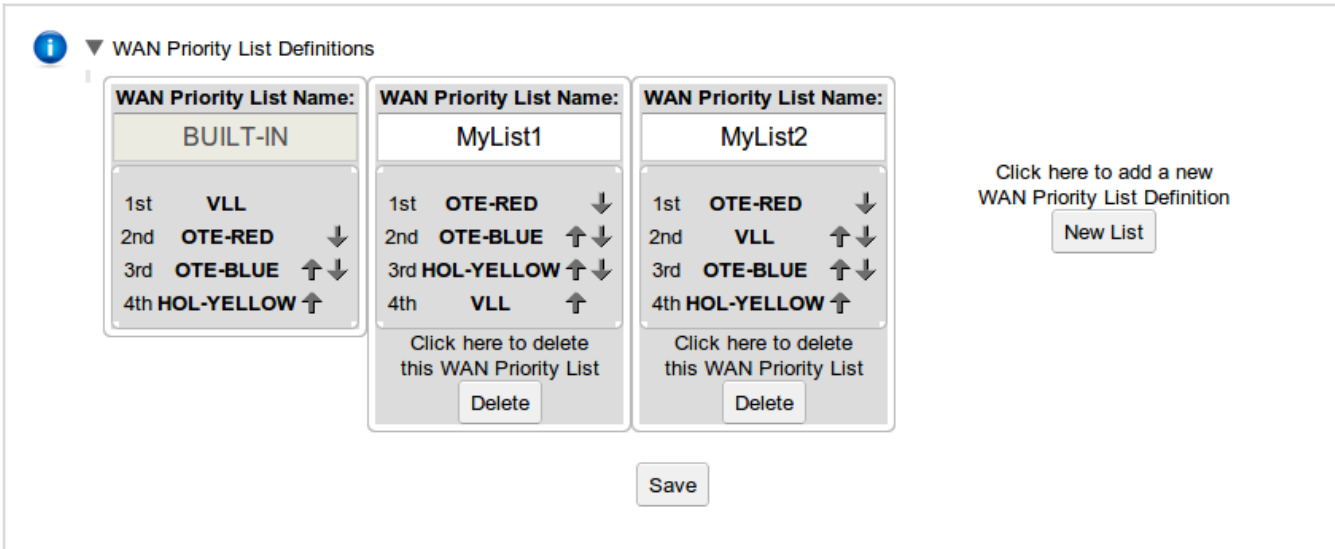
7.4.1. WAN Priority List Definitions

You can define custom **WAN Priority Lists** by expanding the **WAN Priority List Definitions** section and clicking the **"New List"** button.

To create your custom priority list:

1. **Select the WAN Legs:** Choose from the available **WAN legs** you want to include in the list.
2. **Adjust Priorities:** Use the arrows to **adjust the priority** of each WAN leg in the list. The WAN leg at the **top** of the list will have the **highest priority**.
3. **Save Changes:** After arranging the priority order, press the **Save** button to apply the changes.

This custom priority list will be used when configuring the **WAN Priority List** routing method, ensuring that traffic is routed according to your specific priorities.



WAN Priority List Definitions

WAN Priority List Name:	WAN Priority List Name:	WAN Priority List Name:
BUILT-IN	MyList1	MyList2
1st VLL	1st OTE-RED	1st OTE-RED
2nd OTE-RED	2nd OTE-BLUE	2nd VLL
3rd OTE-BLUE	3rd HOL-YELLOW	3rd OTE-BLUE
4th HOL-YELLOW	4th VLL	4th HOL-YELLOW
	Click here to delete this WAN Priority List	Click here to delete this WAN Priority List
	Delete	Delete

Click here to add a new WAN Priority List Definition

New List

Save

When **WAN Priority List** is selected as the routing option, traffic will be routed through the **first active WAN leg** in the priority list. The system will automatically attempt to use the **highest-priority available WAN leg**, ensuring optimal routing based on availability.

To remove a custom **WAN Priority List**, simply click the **Delete** button. After making any changes, press the **Save** button to apply the updated settings.

7.5. VPN

Use this section to configure the VPN tunnel between remote comBOX devices.

One device is defined as the **Server** (typically the headquarters), and the others as **Clients** (typically the branches).

This setup enables secure communication between remote sites over the internet.



Important Notice: To utilize this feature, a minimum of two comBOX devices must be activated. One device will function as the VPN server, while the remaining devices will operate as VPN clients.

7.5.1. VPN Server device configuration

To configure the VPN server:

1. Navigate to the **Advanced** tab of the comBOX GUI and select the **VPN** section.
2. On the device intended to act as the **VPN Server**, enable the option **VPN Tunnel Definition**.
3. Set the **VPN Node Type** to **SERVER/HEADQUARTERS**.
4. Assign a unique name in the **VPN Server Name** field.
5. Click the **Initialize** button to create and activate the VPN server.

Status	LAN	WAN	Advanced	Administration
Advanced Settings				
Port Forwarding	Static Routing	QoS	Policy Based Routing	VPN
VPN Tunnel Definition: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
VPN Node Type: <input type="radio"/> Client/Branch <input checked="" type="radio"/> Server/Headquarters				
VPN Server mode selected.				
VPN Server NOT Initialized To initialize the VPN Server configuration, enter a unique name for your VPN Server and click 'Initialize'. This name will help you identify the server while configuring the VPN Client nodes.				
VPN Server Name: <input type="text" value="TestComboxVPN"/>				
<input type="button" value="Initialize"/>				

Note: The initialization process may take some time.

Once completed, the server details will be displayed under the **VPN Server Details** section. This includes:

- **Server Name**
- **Creation Date**

- **Server IP Address**
- **Local Subnets** to be routed through the VPN. The LAN subnet and any other statically routed subnets (as defined in the static routing tab) will be listed here. Please select all subnets that you wish the VPN clients to have access to.

These details will be used to configure the VPN clients in the next steps.

VPN Tunnel Definition: ☒ Enabled
☐ Disabled

VPN Node Type: ☐ Client/Branch
☒ Server/Headquarters

VPN Server mode selected.

VPN Server Details:
Server Name: TestComboxVPN
Created on: 2024-11-27_15:17:46
Server IP Address: 178.21.171.102

Local Subnets: ☐ 172.22.1.0/24

Remote VPN Clients Management

Index	Status	ClientName	RemoteSubnets	Comment	
1					<div>Add Client</div>

Save

Click on the 'Start Over' button to wipe all VPN Server key information and start over.
WARNING: If you Start Over, all VPN connectivity will be lost and you will need to reconfigure all VPN Clients with new key information.

Start Over

Adding VPN Clients

To enable one or more VPN clients under the Remote VPN Clients Management section:

1. Enter the following details for each VPN client you wish to enable:
 - **Client Name:** A unique name identifying the remote comBOX device.
 - **Remote Subnets:** The local network subnets at the client site that the VPN server will have access to.

- **Comment** (*optional*): Add notes or identifiers for easier management.
2. Click **Add Client** to create the new client entry and generate the required VPN Key.

Remote VPN Clients Management					
Index	Status	ClientName	RemoteSubnets	Comment	
1	Enabled	Test	192.168.1.1/24	Test	<div>Revoke Client</div> <div>View Key Info</div>
2					<div>Add Client</div>

Save

After saving the entry:

- A new button labeled **View Key Info** will appear.
- Click **View Key Info** to display the VPN Key.
- Use **Copy to Clipboard** to easily retrieve and transfer the key for client-side configuration.

Key Information for client#1: Test

Please copy the following text and paste it in the VPN Client's Key Information Field.

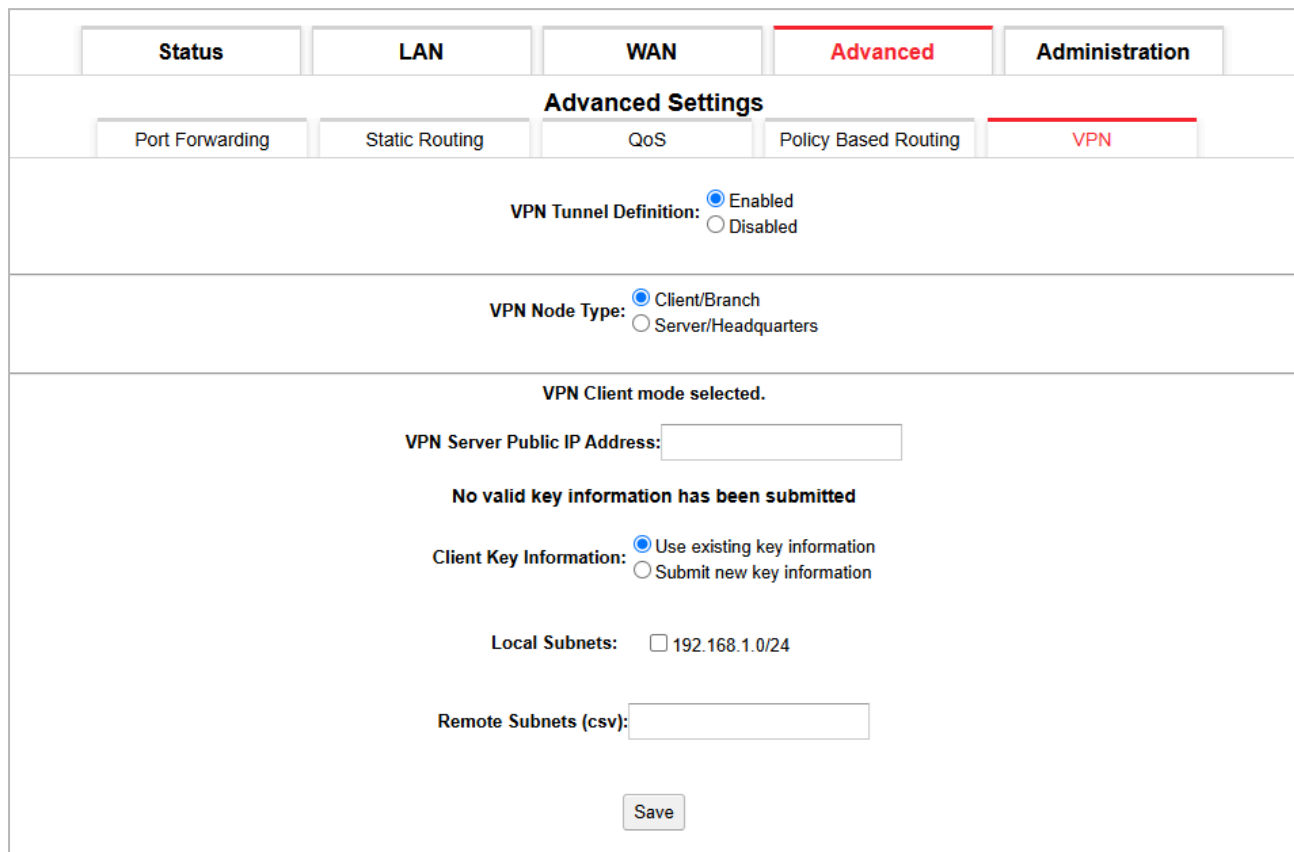
3,1196,-----BEGIN CERTIFICATE-----
MIIDRjCCAi6gAwIBAgIJAJiQ2Ru9noYQMA0GCSqGSIb3DQEBCwUAMBsxGTA

Copy To Clipboard

Dismiss

7.5.2. Configuring VPN Client Devices

To configure the comBOX units that will operate as VPN clients (e.g., branch offices):



The screenshot displays the 'Advanced Settings' section of the comBOX VLL Web Manager GUI, specifically the 'VPN' configuration page. The 'Advanced' tab is selected, and the 'VPN' sub-tab is active. The 'VPN Tunnel Definition' is set to 'Enabled'. The 'VPN Node Type' is set to 'Client/Branch'. The 'VPN Server Public IP Address' field is empty. A message states 'No valid key information has been submitted'. The 'Client Key Information' section has 'Use existing key information' selected. The 'Local Subnets' field shows '192.168.1.0/24'. The 'Remote Subnets (csv)' field is empty. A 'Save' button is at the bottom.

1. Navigate to the **Advanced** tab in the GUI, then select the **VPN** section.
2. Set the **VPN Node Type** to **CLIENT/BRANCH**.
3. In the **VPN Server Public IP Address** field, enter the **Public IP address** of the VPN Server device (typically the Headquarters comBOX).
4. In the **Client Key Information** section:
 - Select **Submit New Key Information** if a new key was recently generated on the VPN Server.
 - Paste the VPN Key obtained from the server (copied via **View Key Info**).
5. Save the configuration.

Once the correct key and server IP have been entered and saved, the VPN client will initiate the connection to the server and the tunnel will be established.

VPN Tunnel Definition: ☒ Enabled
☐ Disabled

VPN Node Type: ☒ Client/Branch
☐ Server/Headquarters

VPN Client mode selected.

VPN Server Public IP Address:

Currently loaded key information:
Client Name: TestComboxVPN
Client created on: 2024-11-27_15:17:46
For Server with Name: TestComboxVPN
Server Created on: 2024-11-27_15:17:46

☐ Use existing key information
☒ Submit new key information

Client Key Information:

FL8FF12XWQUoAhKH
7KKh+c8=
END PRIVATE KEY

Local Subnets: ☒ 172.22.1.0/24
☐ 192.168.1.1/24

Remote Subnets (csv):

Local Subnets to be routed through the VPN. The LAN subnet and any other statically routed subnets (as defined in the static routing tab) will be listed here. Please select all subnets that you wish the VPN server to have access to.

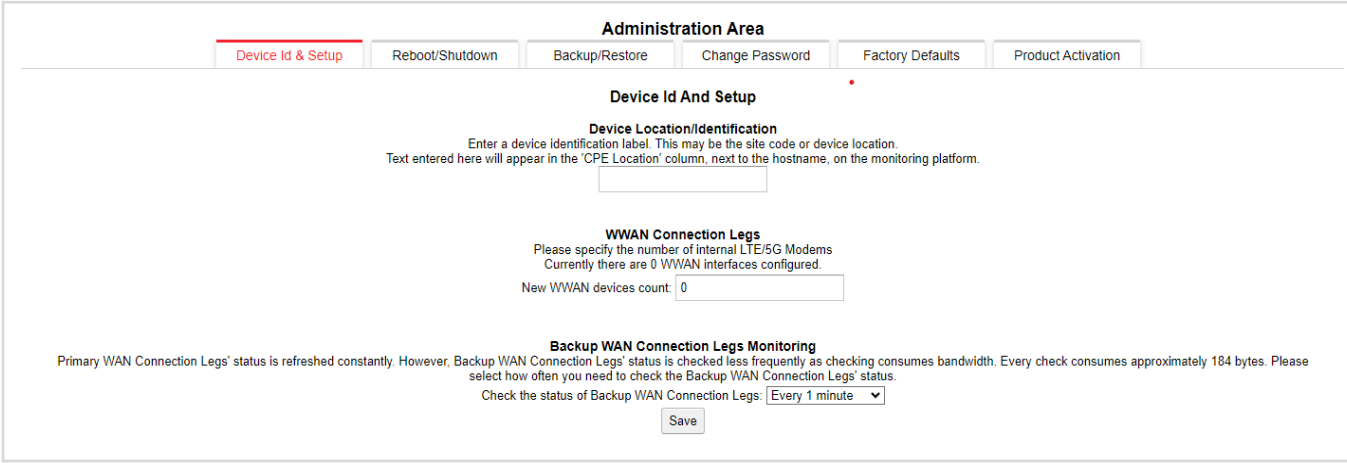
Remote Subnets (csv): Enter a comma-separated list of subnets that exist on the VPN server side which the VPN client will have access to over the VPN tunnel.

8. Administration

This section allows the configuration of various device administration settings.

8.1. Device ID And Setup

This section allows you to configure the Device Location/Label, the amount of WWAN connection Legs and the time it takes the Backup Legs connection monitor to refresh.



The screenshot shows the 'Administration Area' with several tabs: 'Device Id & Setup' (active), 'Reboot/Shutdown', 'Backup/Restore', 'Change Password', 'Factory Defaults', and 'Product Activation'. The 'Device Id And Setup' section contains three main configuration areas:

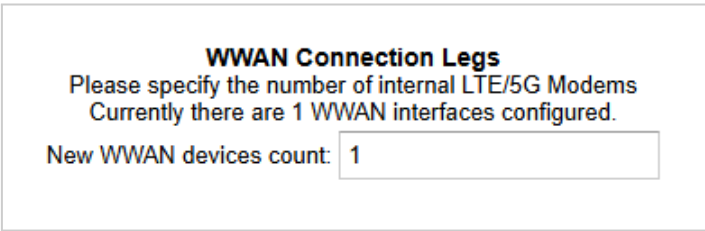
- Device Location/Identification:** A text input field for a device identification label. A note states: "Enter a device identification label. This may be the site code or device location. Text entered here will appear in the 'CPE Location' column, next to the hostname, on the monitoring platform."
- WWAN Connection Legs:** A section for specifying the number of internal LTE/5G Modems. It states "Currently there are 0 WWAN interfaces configured." and includes a text input field for "New WWAN devices count" with the value '0'.
- Backup WAN Connection Legs Monitoring:** A section explaining that the status is refreshed constantly. It includes a dropdown menu for "Check the status of Backup WAN Connection Legs:" set to "Every 1 minute" and a "Save" button.

8.1.1. WWAN Connection Legs

In this section, you can **enable and configure LTE devices** to be used as comBOX connection legs. These LTE devices can be either:

- **Internal LTE modules** built into the comBOX device, or
- **Proprietary external USB LTE modules** provided by comBOX.

By default, the number of LTE devices is set to **0 (none)**. You can increase this number based on how many LTE interfaces you wish to activate as part of your multi-WAN configuration.



This screenshot shows a zoomed-in view of the 'WWAN Connection Legs' configuration section. It includes the text: "Please specify the number of internal LTE/5G Modems. Currently there are 1 WWAN interfaces configured." and a text input field for "New WWAN devices count" with the value '1'.

For **1 LTE device**, set the **"New WWAN Devices Count:"** field to **1**.
For **2 LTE devices**, set it to **2**, and so on.

Each enabled LTE device will appear as a separate WWAN interface and can be configured independently as part of your bonded WAN setup.

Displaying status and Signal information

To **check the status** of LTE devices:

1. Navigate to the **Status** tab of the comBOX GUI.
2. Locate the **WWAN devices** which are indicated with a cellular signal icon on the right side of the corresponding **Leg ID**.
3. Click the **cellular signal icon** to view detailed information, including:

Status Information

- "Status state: 'searching' " The sim card is searching for service
- "Status state: 'enabled' " The sim card is active and working

Signal Information

- **Signal Strength (RSSI/RSRP/RSRQ/SNR)**
- **Access Tech (e.g., LTE, 5G)**

This allows for quick assessment and troubleshooting of each LTE interface.

Leg Id #1: LEG-1
Refreshes automatically

Status Information
Status state: 'enabled'

Signal Information
LTE RSSI: '-46.00' dBm
RSRQ: '-14.00' dB
RSRP: '-80.00' dBm
SNR: '2.80' dB

Dismiss

8.2. Reboot/Shutdown

This section allows you to reboot or shutdown the comBOX network appliance by pressing the corresponding button.

8.3. Backup/Restore

In this section you may choose to backup the current configuration of comBOX network appliance and save it to a file on your PC.

If you have already created a backup configuration file you may restore it by choosing the backup file from your PC and pressing the restore button

8.4. Change Password

In this section you may use the available form to change your device administration password.

In order to change the password, you need to enter your current password and confirm your new password in the corresponding fields.

8.5. Factory Defaults

If you wish to restore the configuration to factory defaults, all you need to do is press the “reset” button which is available in this section.

8.6. Product Activation

All comBOX products require a service license to be activated in order to route Internet traffic. To activate your product you need to upload the license key that was supplied to you in the corresponding field and press the “activate product” button.



Important Notice: *If your product license has expired or your product has not been activated, all Internet or VPN traffic is blocked. In that case, comBOX VLL Web Manager GUI will show a license expired notification on the top right corner of your screen.*