

8.7 Network

The page shows information about current interface status, its configurations, provides various interface, network properties configuration capabilities and contains the following subsections:

- **INTERFACES:** shows information about current interface status, allows to create new and configure them.
- **WIRELESS:** shows information about wireless radio stations, covers physical settings of the wireless hardware.
- **DHCP AND DNS:** allows management of DHCP and DNS servers.
- **HOSTNAMES:** allows management of host names.
- **STATIC ROUTES:** allows management of IPv4 and IPv6 static routes.
- **FIREWALL:** allows management of firewall zones and various firewall properties.
- **DIAGNOSTICS:** provides network diagnostics utilities.
- **GSM:** allows management of gsm modem and SIM cards.

Interfaces

INTERFACE OVERVIEW

Network	Status	Actions
<div>LAN</div> <div>br-lan</div>	<div>Uptime: 0h 20m 27s</div> <div>MAC-Address: C4:93:00:0B:F4:57</div> <div>RX: 0 B (0 Pkts.)</div> <div>TX: 0 B (0 Pkts.)</div> <div>IPv4: 192.168.1.1/24</div> <div>IPv6: fd94:746:4098::1/60</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>GSM</div> <div>wwan0</div>	<div>Uptime: 0h 20m 20s</div> <div>MAC-Address: 00:00:00:00:00:00</div> <div>RX: 256.18 KB (4425 Pkts.)</div> <div>TX: 271.71 KB (4364 Pkts.)</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>WAN</div> <div>eth1</div>	<div>Uptime: 0h 20m 22s</div> <div>MAC-Address: C4:93:00:0B:F4:56</div> <div>RX: 497.67 KB (2523 Pkts.)</div> <div>TX: 663.41 KB (1238 Pkts.)</div> <div>IPv4: 192.168.5.131/24</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>
<div>WAN6</div> <div>eth1</div>	<div>Uptime: 0h 0m 0s</div> <div>MAC-Address: C4:93:00:0B:F4:56</div> <div>RX: 497.67 KB (2523 Pkts.)</div> <div>TX: 663.41 KB (1238 Pkts.)</div>	<div>Connect/Reconnect</div> <div>Stop</div> <div>Edit</div> <div>Delete</div>

Add new interface...

Current information and status of various network interfaces (GSM, LAN, WAN).

Uptime: Current interface uptime in hours, minutes and seconds.

MAC address: Physical interface address.

RX: Received data in bytes (packet count).

TX: Transmitted data in bytes (packet count).

IPv4: Internet protocol version 4 address.

IPv6: Internet protocol version 6 address.

In addition to the network interface status, several actions may be performed:

Connect/Reconnect: Connect to configured interface network if it does not do it automatically. If it already connected to the network it will be trying to reconnect to it.

Stop: Shutdown interface. If you are connected through this interface the connection may be lost.

Edit: Edit interface settings.

Delete: Delete interface.


Add new interface: Adding new Ethernet, GSM or wireless interface with the custom name, protocol and etc.

	eth0	eth1
Type	Static	DHCP
Address	192.168.1.1	
Subnet mask	255.255.255.0	
Gateway		


 Changes will only take effect after device reboots.

Network interfaces can be configured on the common page, which can be accessed through add new interface or edit button.

Name of the new interface

 The allowed characters are: A-Z, a-z, 0-9 and _

Note: interface name length

 Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Protocol of the new interface

Static address

Create a bridge over multiple interfaces☐

Cover the following interface

☐

Ethernet Adapter: "eth0" (lan)

☐

Ethernet Adapter: "eth1" (wan, wan6)

☐

Ethernet Adapter: "wwan0" (gsm)

☐

Wireless Network: Client "WCC Lite" (lan)

☐

Custom Interface:


Back to Overview

Submit

The following options can be defined in the interface creation panel: name of the interface, protocol, coverage of a particular interface or bridging with other interfaces. After the general setup is done, more detailed settings can be set.

General SetupAdvanced SettingsPhysical SettingsFirewall Settings

Status

 **Uptime:** 0h 2m 42s
MAC-Address: CE:0A:91:C9:25:F2
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Protocol

Static address


IPv4 address

IPv4 netmask

IPv4 gateway


IPv4 broadcast

Use custom DNS servers



IPv6 assignment length


disabled

 Assign a part of given length of every public IPv6-prefix to this interface

IPv6 address

IPv6 gateway

IPv6 routed prefix

 Public prefix routed to this device for distribution to clients.

General common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot		<input checked="" type="checkbox"/>	
Use builtin IPv6-management		<input checked="" type="checkbox"/>	
Override MAC address		<input type="text" value="CE:0A:91:C9:25:F2"/>	
Override MTU		<input type="text" value="1500"/>	
Use gateway metric		<input type="text" value="0"/>	

Advanced common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces		<input type="checkbox"/> creates a bridge over specified interface(s)	
Interface		<input type="radio"/> Ethernet Adapter: "eth0" (lan) <input type="radio"/> Ethernet Adapter: "eth1" (wan, wan6) <input checked="" type="radio"/> Ethernet Adapter: "usb0" (gsm) <input type="radio"/> Wireless Network: Master "WCC Lite" (lan) <input type="radio"/> Wireless Network: Client "AP5" (wwan) <input type="radio"/> Custom Interface: <input type="text"/>	

Physical common interface setup panel.

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Create / Assign firewall-zone			
<input type="radio"/> lan: <input type="radio"/> wan: <input type="radio"/> wan6: <input type="radio"/> gsm: <input type="radio"/> wwan:		Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.	
<input type="radio"/> unspecified -or- create: <input type="text"/>			

Firewall common interface setup panel.

General Setup	Advanced Settings	IPv6 Settings
Ignore interface	<input type="checkbox"/>	? Disable DHCP for this interface.
Start	<input type="text" value="100"/>	? Lowest leased address as offset from the network address.
Limit	<input type="text" value="150"/>	? Maximum number of leased addresses.
Leasetime	<input type="text" value="12h"/>	? Expiry time of leased addresses, minimum is 2 minutes (2m).

DHCP server general setup panel.

General Setup	Advanced Settings	IPv6 Settings
Dynamic DHCP		
<input checked="" type="checkbox"/>	? Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.	
Force	<input type="checkbox"/>	? Force DHCP on this network even if another server is detected.
IPv4-Netmask	<input type="text"/>	? Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	<input type="text"/>	? Define additional DHCP options, for example "6, 192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

DHCP server advanced setup panel.


General Setup	Advanced Settings	IPv6 Settings
Router Advertisement-Service	<input type="text" value="server mode"/>	
DHCPv6-Service	<input type="text" value="hybrid mode"/>	
NDP-Proxy	<input type="text" value="hybrid mode"/>	
DHCPv6-Mode	<input type="text" value="stateless + stateful"/> ? Default is stateless + stateful	
Always announce default router	<input type="checkbox"/>	? Announce as default router even if no public prefix is available.
Announced DNS servers	<input type="text"/>	
Announced DNS domains	<input type="text"/>	

DHCP server IPv6 settings setup panel.

GSM

Interfaces - GSM

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

COMMON CONFIGURATION				
<table border="1"> <thead> <tr> <th>General Setup</th> <th>Advanced Settings</th> <th>Firewall Settings</th> </tr> </thead> </table>		General Setup	Advanced Settings	Firewall Settings
General Setup	Advanced Settings	Firewall Settings		
Status	<div>  <div> Uptime: 1h 18m 58s MAC-Address: 00:00:00:00:00:00 RX: 437.84 KB (7532 Pkts.) TX: 456.23 KB (7490 Pkts.) </div> </div>			
Protocol	<input type="text" value="wwan"/>			

General Settings Information tab. Gives you name of physical GSM interface, lets you choose protocol (not recommended!).

Note: Make sure you won't change GSM interface's protocol, which is set by default to WWAN. Changing this parameter will lead to undefined GSM modem behavior.

Interfaces - GSM

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

Bring up on boot

☒

Use builtin IPv6-management

☒

Force link

☐

Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers).

Enable IPv6 negotiation on the PPP link

☐

Modem init timeout

Maximum amount of seconds to wait for the modem to become ready

Use default gateway

☒

If unchecked, no default route is configured

Prefer PPP connection

☐

If checked, modem will prioritise PPP type connection over other types (if available)

Use gateway metric

Use DNS servers advertised by peer

☒

If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold

Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval

Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout

Close inactive connection after the given amount of seconds, use 0 to persist connection

Override MTU

Advanced Settings tab enables user to configure advanced settings for mobile communication. It includes the following options:

Bring up on boot: Checkbox to start a GSM interface on startup;

Use built-in IPv6-management: Checkbox to select if the device is going to use its own tools to manage IPv6 transport layer messages;

Force link: Specifies whether IP address, route, and gateway are assigned to the interface regardless of the link being active or only after the link has become active; when active, carrier sense events do not invoke hotplug handlers;

IPv6 support: User can select if IPv6 support is handled automatically, manually or disabled altogether;

Modem init timeout: Maximum amount of seconds before the device gives up on finishing initialization;

Use default gateway: Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured;

Prefer PPP connection: If ,the modem, supports PPP and any other communication protocol (e.g. QMI, RNDIS and etc.), prioritize PPP type connection;

Use gateway metric: The WAN configuration by default generates a routing table entry. In this field you can alter the metric of that entry. Higher metric means higher priority;

Use DNS servers advertised by peer: Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored;

LCP echo failure threshold: LCP (link control protocol) is a part of PPP (Point-to-Point Protocol) and helps to determine the quality of data transmission. If enough failures happen, LCP presumes link to be dead. 0 disables failure count checking;

LCP echo interval: Determines the period of LCP echo requests. Only effective if LCP echo failure threshold is more than zero;

Inactivity timeout: Station inactivity limit in seconds: if a station does not send anything, the connection will be dropped. A value of 0 can be used to persist connection.

Override MTU: Set custom MTU to GSM interface.

Note: If modem uses QMI connection protocol and user haven't defined custom MTU setting, the MTU on interface will be set to operator's defined MTU value.

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

Create / Assign firewall-zone



unspecified -or- create:

lan:

lan:

wan:

wan:

wan6:

gsm:



Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

GSM configuration ends with firewall settings. A user can assign an already defined firewall zone or create a new one.

Wireless

The wireless network interface parameters and configuration are described in this section.



Generic MAC80211 802.11bgn (radio0)

Channel: 11 (2.462 GHz) | Bitrate: 1 Mbit/s



0%

SSID: WCC Lite | Mode: Master

BSSID: C6:93:00:0E:C4:33 | Encryption: None



50%

SSID: AP5 | Mode: Client

BSSID: 02:1A:11:FF:87:09 | Encryption: WPA2 PSK (CCMP)

Disable

Edit

Remove

Disable

Edit

Remove

Scan
Add

Configured interfaces for the physical radio device.

Channel: Specifies the wireless channel to use.

Bitrate: Specifies transfer rate in Mbit/s.

SSID: The broadcasted service set identifier of the wireless network.

Mode: Selects the operation mode of the wireless network interface controller.

BSSID: The basic service set identification of the network, only applicable in adhoc or STA mode.

Encryption: Wireless encryption method.

	SSID	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
wlan0	AP5	02:1A:11:FF:87:09	192.168.43.1	-75 / -95 dBm	1.0 Mbit/s, 20MHz 1.0 Mbit/s, 20MHz

List of associated wireless stations.

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

General Setup

Advanced Settings



47%

Mode: Client | SSID: AP5

BSSID: 02:1A:11:FF:87:09 | Encryption: WPA2 PSK (CCMP)

Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm

Signal: -77 dBm | Noise: -95 dBm

Bitrate: 6.5 Mbit/s | Country: US

Status

Wireless network is enabled

Disable

Operating frequency

Mode

N

Channel

11 (2462 MHz)

Width

20 MHz

Transmit Power

auto



dBm

General device settings.

General Setup

Advanced Settings

Country Code

US - United States

Use ISO/IEC 3166 alpha2 country codes.

Allow legacy 802.11b rates

☒

Distance Optimization

Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Advanced device settings.

INTERFACE CONFIGURATION

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Mode

Access Point

ESSID

WCC Lite

Network

☒ lan:

☐ wan:

☐ wan6:

☐ create:

Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

Hide ESSID

☐

WMM Mode

☒

General interface settings.

INTERFACE CONFIGURATION

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Encryption

WPA2-PSK

Cipher

auto

Key

Enable key reinstallation (KRACK) countermeasures

☐

Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced robustness of key negotiation especially in environments with heavy traffic load.

Wireless security interface settings.

INTERFACE CONFIGURATION

General Setup

Wireless Security

MAC-Filter

Advanced Settings

MAC-Address Filter

disable

MAC-Filter settings.

INTERFACE CONFIGURATION

General Setup

Wireless Security

MAC-Filter

Advanced Settings

Isolate Clients

Prevents client-to-client communication

Interface name

Override default interface name

Advanced interface settings.

DHCP and DNS

DHCP server and DNS forward for NAT firewalls is described in this section.

General Settings

Resolv and Hosts Files

TFTP Settings

Advanced Settings

Domain required

Don't forward DNS-Requests without DNS-Name

Authoritative

This is the only DHCP in the local network

Local server

/lan/

Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain

lan

Local domain suffix appended to DHCP names and hosts file entries

Log queries

Write received DNS requests to syslog

DNS forwardings

/example.org/10.1.2.3

List of DNS servers to forward requests to

Rebind protection

Discard upstream RFC1918 responses

Allow localhost

Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist

ihost.netflix.com

List of domains to allow RFC1918 responses for

Local Service Only

Limit DNS service to subnets interfaces on which we are serving DNS.

Non-wildcard

Bind only to specific interfaces rather than wildcard address.


General DHCP settings.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Use /etc/ethers <input checked="" type="checkbox"/>			
Read /etc/ethers to configure the DHCP-Server			
Leasefile	<input type="text" value="/tmp/dhcp.leases"/>		
file where given DHCP-leases will be stored			
Ignore resolve file	<input type="checkbox"/>		
Resolve file	<input type="text" value="/tmp/resolv.conf.auto"/>		
local DNS file			
Ignore /etc/hosts	<input type="checkbox"/>		
Additional Hosts files	<input type="text"/>		

Resolve and hosts files settings.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Enable TFTP server <input checked="" type="checkbox"/>			
TFTP server root	<input type="text" value="/"/>		
Root directory for files served via TFTP			
Network boot image	<input type="text" value="pxelinux.0"/>		
Filename of the boot image advertised to clients			

TFTP server settings.

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Suppress logging <input type="checkbox"/> ? Suppress logging of the routine operation of these protocols			
Allocate IP sequentially <input type="checkbox"/> ? Allocate IP addresses sequentially, starting from the lowest available address			
Filter private <input checked="" type="checkbox"/> ? Do not forward reverse lookups for local networks			
Filter useless <input type="checkbox"/> ? Do not forward requests that cannot be answered by public name servers			
Localise queries <input checked="" type="checkbox"/> ? Localise hostname depending on the requesting subnet if multiple IPs are available			
Expand hosts <input checked="" type="checkbox"/> ? Add local domain suffix to names served from hosts files			
No negative cache <input type="checkbox"/> ? Do not cache negative replies, e.g. for not existing domains			
Additional servers file <input type="text"/> ? This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.			
Strict order <input type="checkbox"/> ? DNS servers will be queried in the order of the resolvfile			
Bogus NX Domain Override <input type="text" value="67.215.65.132"/>  ? List of hosts that supply bogus NX domain results			
DNS server port <input type="text" value="53"/> ? Listening port for inbound DNS queries			
DNS query port <input type="text" value="any"/> ? Fixed source port for outbound DNS queries			
Max. DHCP leases <input type="text" value="unlimited"/> ? Maximum allowed number of active DHCP leases			
Max. EDNS0 packet size <input type="text" value="1280"/> ? Maximum allowed size of EDNS.0 UDP packets			
Max. concurrent queries <input type="text" value="150"/> ? Maximum allowed number of concurrent DNS queries			

Advanced settings.

ACTIVE DHCP LEASES

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

ACTIVE DHCPV6 LEASES

Host	IPv6-Address	DUID	Leasetime remaining
?	fd74:8536:7bae::33f/128	00046836d59efa382760f3193e5ec5bf4a24	11h 54m 16s

STATIC LEASES

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host. The optional Lease time can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	IPv6-Suffix (hex)
<input type="text" value="host2"/>	<input type="text" value="f0:76:1c:3b:cb:13 (192.168.2.2)"/>	<input type="text" value="192.168.2.2"/>	<input type="text" value="10"/>	<input type="text"/>

AddDelete

List of active DHCP and static leases. It is also possible to assign fixed IP addresses to hosts on the network, based on their MAC (hardware) address.

Hostnames

HOST ENTRIES

Hostname	IP address
<input type="text" value="Host1"/>	<input type="text" value="192.168.2.35"/>

AddDelete

List of existing host names. Addition or deletion is allowed for the user.

Static routes

Routes specify over which interface and gateway a certain host or network can be reached.

STATIC IPV4 ROUTES

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Route type
	Host-IP or Network	if target is a network				
<input type="text" value="lan"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="192.168.0.254"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>

AddDelete

STATIC IPV6 ROUTES

Interface	Target	IPv6-Gateway	Metric	MTU	Route type
	IPv6-Address or Network (CIDR)				
<input type="text" value="lan"/>	<input type="text" value="0:0:0:0:ffff:c0a8:fe"/>	<input type="text" value="0:0:0:0:ffff:c0a8:fe"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>
<input type="text" value="lan"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="1500"/>	<input type="text" value="unicast"/>

AddDeleteDelete

Current IPv4 and IPv6 static routes configuration.
Interface: Lets to chose for which interface static route is created.

Target: Defines target host IP or network.
IPv4 Netmask: Defines netmask if the target is a network.
IPv4/IPv6 Gateway: Defines IPv4 or IPv6 gateway.
Metric: Specifies the route metric to use for the route.
MTU: Maximum Transmit/Receive Unit, in bytes.
Route type: All incoming packets can be: accepted, rejected, dropped.

Diagnostics

NETWORK UTILITIES

192.168.2.2

IPv4

Ping

openwrt.org

IPv4

Traceroute

openwrt.org

Nslookup

Diagnostics tools which can be used to diagnose some of the networking problems: ping, traceroute and nslookup.

Firewall

This subsection is divided into four categories: general settings, port forwards, traffic rules and custom rules.

General settings

GENERAL SETTINGS

Enable SYN-flood protection

☒

Drop invalid packets

☐

Input

accept

Output

accept

Forward

reject

General Settings for firewall can be changed in General Settings screen. These settings are defined as follows:
Input: All incoming packets can be: accepted, rejected, dropped.
Output: All outgoing packets can be: accepted, rejected, dropped.
Forward: All packets being sent to another device can be: accepted, rejected, dropped.

ZONES

Zone => Forwardings

Input

Output

Forward

Masquerading

MSS clamping

lan:

lan:

⇒

wan

accept

accept

accept

☐

☐

Edit

Delete

wan:

wan:

wan6:

gsm:

wwan:

⇒

REJECT

reject

accept

reject

☒

☒

Edit

Delete

Add

Additional zones for firewall can be created, edited or deleted.
Zone => Forwardings: Defines zones and their traffic flow.
Input: All incoming packets can be: accepted, rejected, dropped.
Output: All outgoing packets can be: accepted, rejected, dropped.
Forward: All packets being sent to another device can be: accepted, rejected, dropped.
Masquerading: Allows one or more devices in a zones network without assigned IP addresses to communicate with the Internet.
MSS clamping: Change the maximum segment size (MSS) of all TCP connections passing through this zone with MTU lower than the Ethernet default of 1500.

i Additional actions can be performed with zones: add, edit, delete.

General Settings

Advanced Settings

Name

newzone

Input

accept

Output

accept

Forward

reject

Masquerading

☐

MSS clamping

☐

Covered networks

☐ gsm:

☐ lan:

☐ wan:

☐ wan6:

☐

create:

Common properties of newly created or edited zones can be edited in this panel. The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specify which available networks are members of this zone.

General Settings

Advanced Settings

Restrict to address family

IPv4 and IPv6

Restrict Masquerading to given source subnets

0.0.0.0/0

Restrict Masquerading to given destination subnets

0.0.0.0/0

Force connection tracking

☐

Enable logging on this zone

☐

Advanced settings of new created or edited zone. Restrict to address family option defines to what IP families the zone belongs to IPv4, IPv6 or both. Restrict masquerading to given source/destination subnets defines one or more subnets for which the masquerading option is applied to. Connection tracking and logging options enable additional information gathering on the zone.

Allow forward to destination zones:

☐

lan:

lan:

☐

wan:

wan:

wan6:

gsm:

Allow forward from source zones:

☐

lan:

lan:

☐

wan:

wan:

wan6:

gsm:

Controls of the forwarding policies between new/edited zone and other zones. Destination zones cover forwarded

traffic originating from the new/edited zone. Source zones match forwarded traffic from other zones targeted at the new/edited zone. The forwarding rule is unidirectional, e.g. a forward from LAN to WAN does not imply a permission to forward from WAN to LAN as well.

Port forwards

PORT FORWARDS

Name	Match	Forward to	Enable	Sort	
4000	IPv4-tcp From any host in wan Via any router IP at port 4000	IP 192.168.2.1, port 4000 in lan	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
4001	IPv4-tcp, udp From any host in wan Via any router IP at port 4001	IP 192.168.2.1, port 4001 in lan	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
<input type="text" value="New port forward"/>	<input type="text" value="TCP+UDP"/>	<input type="text" value="wan"/>	<input type="text"/>	<input type="text" value="lan"/>	<input type="text"/>	<input type="text"/>	<div>Add</div>

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN. It is done in a way of routing network packets within a private network created by the device. Settings for the port forwarding of the device are defined as follows:

Name: The name of the port forwarding rule.

Match: Informs what port forward is matched to.

Forward to: Informs where the port is forwarded to.

Enable: Enable (checked) or disable port forward.

Sort: Allows to sort port forwarding.

The user can add, edit or delete port forwarding rules.

Traffic rules

TRAFFIC RULES

Name	Match	Action	Enable	Sort	
Allow-DHCP-Renew	IPv4-udp From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-IGMP	IPv4-igmp From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>
Allow-DHCPv6	IPv6-udp From IP range fc00::/6 in wan To IP range fc00::/6 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	▲ ▼	<div>Edit</div> <div>Delete</div>

Traffic rules which define policies for packets traveling between different zones.

Name: The name of the traffic rule.

Match: Informs what ICMP types are matched.

Action: Informs what action would be performed.

Enable: Enable (checked) or disable the rule.

Sort: Allows to sort rules.

The user can add, edit or delete traffic rules. For every rule can be defined these options: name, restrict to address family, protocol, match ICMP type, source and destination zones, source MAC, IP addresses and port, destination IP address and port, action and extra arguments, month and weekdays for which rule will apply, start/stop dates and times, time in UTC.

Name	Match	Action	Enable	Sort
This section contains no values yet				
New source NAT:				
Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="Do not rewrite"/>	<input type="text" value="Do not rewrite"/>
				<input type="button" value="Add and edit..."/>

Source NAT, which is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for the example to map multiple WAN addresses to internal subnets. The user can add, edit or delete source NAT rules. For every rule can be defined these options: name, protocol, source and destination zones, source, destination, SNAT IP addresses, ports, extra arguments, month and weekdays for which rule will apply, start/stop dates and times, time in UTC.

Custom rules

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Custom rules allow to executing arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

GSM



Note: If you have a WCC Lite without a modem, the GSM tab will still be visible, but these changes won't affect anything.

GSM

Configuration page for GSM modem

STATUS	
Active SIM	1
SIM status	READY
PIN retry count left	3
PUK retry count left	10

SIM CARDS PARAMETERS	
<div>SIM 1SIM 2</div>	
Enable	<input checked="" type="checkbox"/>
PIN code	<input type="text"/>
APN	<input type="text"/>
PAP/CHAP username	<input type="text"/>
PAP/CHAP password	<input type="text"/>
Dialnumber	*99#
Additional pppd options	<input type="text"/>

MODEM PARAMETERS	
Enable data connection	<input checked="" type="checkbox"/>
Priority SIM	1
<small>Which SIM will be prioritised when switching cards</small>	
Service Type	2G/3G/4G
<small>Choosing modem service type. For service type to come to effect, you will have restart connection.</small>	

PINGER CONFIGURATION	
Disable	<input type="checkbox"/>
Failed ping count	3
<small>Limit of failed ping requests, before pinger decides, that internet connection is lost</small>	
Reset modem	<input checked="" type="checkbox"/>
<small>Reset modem after failed pings</small>	
Switch SIM	<input checked="" type="checkbox"/>
<small>Switch SIM to non-priority after specified retry count</small>	
Priority SIM retry count	3
<small>How much blocks of failed pings will the pinger tolerate, before switching to non-priority SIM</small>	
Ping interval (minutes)	2
Primary host	google.com
Secondary host	8.8.4.4
Network interface	gsm

SIM cards parameters

Parameters for SIM card. If single SIM modem is used, there won't be "SIM 1" and "SIM 2" tabs.

Enable: Enable or disable this SIM card.

PIN code: PIN code to use on that SIM card.

APN: APN to use on that SIM card.

PAP/CHAP username: Username (optional).

PAP/CHAP password: Password (optional).

Modem parameters

Enable data connection: Enable or disable data connection through GSM modem.

Priority SIM: Primary SIM card (if Dual SIM modem is used). Mainly used for pinger configuration.

Service Type: Which radio access technology will be used when connecting to the gsm network.

Pinger configuration

Pinger is a service which pings defined hosts to check internet connection. If both of these hosts are unreachable pinger will wait and restart modem (or switch SIM card, if Dual-SIM modem is installed in WCC Lite)

Disable: Disable pinger functionality.

Failed ping count: Limit of failed ping requests, before pinger decides that internet connection is lost.

Reset modem: If checked, pinger resets gsm modem after "Failed ping count".

Switch SIM: If checked, pinger switches SIM to non-priority after "Priority SIM retry count". If internet connection is not available with non-priority SIM as well, pinger switches back to priority SIM after one failed ping attempt.


Priority SIM retry count: How many blocks of failed pings will the pinger tolerate, before switching to non-priority SIM.

Ping interval (minutes): Interval between ping requests.

Primary host: The host that will be pinged first.

Secondary host: The host that will be pinged second, if the primary host fails.

Network interface: GSM network interface name.

 GSM Pinger is used to detect the status of network connection via cellular network. This status is written to file (/var/run/board/internet-status) and can be configured to be sent to SCADAs. If pinger is disabled, status is always set equal to zero and should not be trusted to represent internet status. Additionally, this status is reflected in the "Status"->"GSM Status" window.

This is Pinger functionality described step by step:

- Pinger will ping the primary host every 2 minutes.
- If the primary host fails, pinger redirects to the secondary host immediately.
- If either primary or secondary host is responding to ping requests, pinger will continue testing connection every "Ping interval (minutes)" parameter and no further action is taken.
- If both primary and secondary hosts are unreachable, pinger will start pinging these hosts every "Ping interval (minutes) / 2" minute for "Failed ping count" times.
- If hosts are still unreachable, pinger will try to switch SIM and restart modem (if corresponding parameters are set) or will restart immediately if single SIM modem is used.
- SIM card is switched to non-priority SIM after "Priority SIM retry count" failed modem restarts with priority SIM. If a non-priority SIM fails, it is switched to priority SIM in the next pinger action.

Dual SIM start procedure

Table below shows, which card is expected on boot, when selection is made between Enable/Disable SIM cards and Primary card.

SIM 1 Enabled	SIM 2 Enabled	Priority SIM	SIM on boot
X		1	1
X		2	1
	X	1	2
	X	2	2
X	X	1	1
X	X	2	2
		1	Undefined
		2	Undefined

Layer 2 Tunneling Protocol

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Description

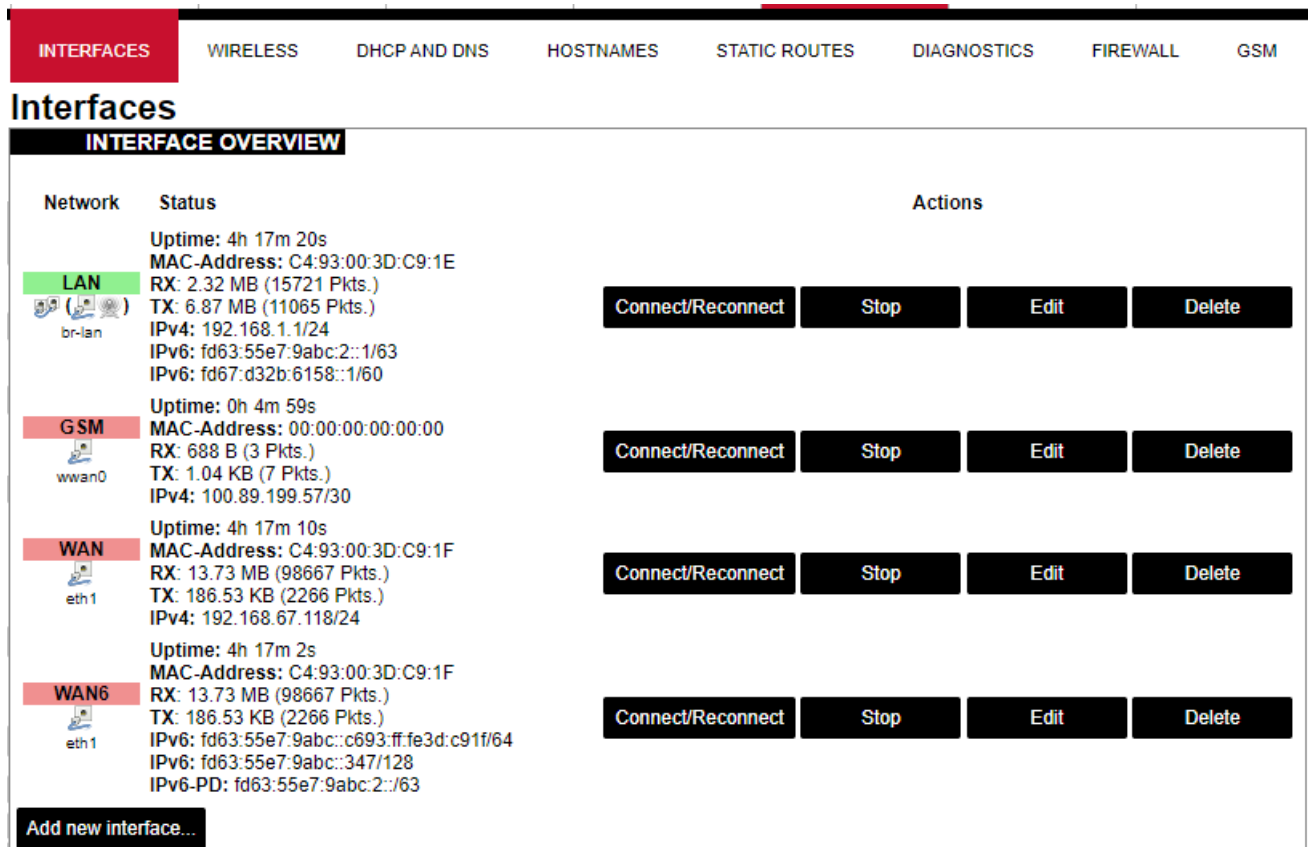
The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below). The two endpoints of an L2TP

tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LNS waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP session (or 'call') is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP. The packets exchanged within an L2TP tunnel are categorized as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel. L2TP allows the creation of a virtual private dialup network (VPDN) to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network.

Setting up L2TP interface

In order to create a L2TP tunnel following steps are required:

1. Go to **Network > Interfaces > Add new interface:**



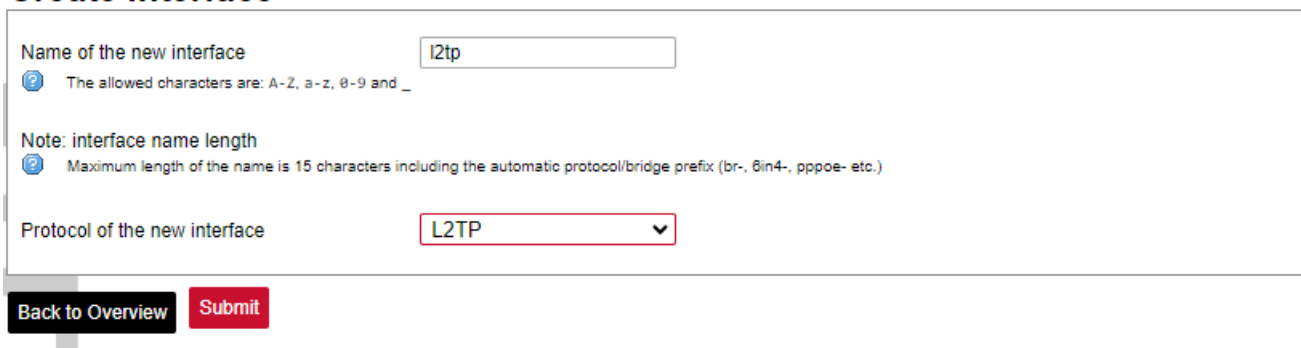
The screenshot shows the Mikrotik WinBox 'Interfaces' page. At the top, there is a navigation bar with tabs: INTERFACES, WIRELESS, DHCP AND DNS, HOSTNAMES, STATIC ROUTES, DIAGNOSTICS, FIREWALL, and GSM. Below the navigation bar, the title 'Interfaces' is displayed. Underneath, there is a section titled 'INTERFACE OVERVIEW' which contains a table of network interfaces.

Network	Status	Actions
LAN br-lan	Uptime: 4h 17m 20s MAC-Address: C4:93:00:3D:C9:1E RX: 2.32 MB (15721 Pkts.) TX: 6.87 MB (11065 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd63:55e7:9abc:2::1/63 IPv6: fd67:d32b:6158::1/60	Connect/Reconnect Stop Edit Delete
GSM wwan0	Uptime: 0h 4m 59s MAC-Address: 00:00:00:00:00:00 RX: 688 B (3 Pkts.) TX: 1.04 KB (7 Pkts.) IPv4: 100.89.199.57/30	Connect/Reconnect Stop Edit Delete
WAN eth1	Uptime: 4h 17m 10s MAC-Address: C4:93:00:3D:C9:1F RX: 13.73 MB (98667 Pkts.) TX: 186.53 KB (2266 Pkts.) IPv4: 192.168.67.118/24	Connect/Reconnect Stop Edit Delete
WAN6 eth1	Uptime: 4h 17m 2s MAC-Address: C4:93:00:3D:C9:1F RX: 13.73 MB (98667 Pkts.) TX: 186.53 KB (2266 Pkts.) IPv6: fd63:55e7:9abc::c693:ff:fe3d:c91f/64 IPv6: fd63:55e7:9abc::347/128 IPv6-PD: fd63:55e7:9abc:2::/63	Connect/Reconnect Stop Edit Delete

At the bottom of the table, there is a button labeled 'Add new interface...'.

2. Enter interface name and select L2TP protocol:

Create Interface



The screenshot shows the 'Create Interface' form in Mikrotik WinBox. It has a title bar 'Create Interface'. Below the title bar, there is a form with the following fields:

- Name of the new interface:** A text input field containing 'l2tp'. Below it, a note says: 'The allowed characters are: A-Z, a-z, 0-9 and _'.
- Note: interface name length:** A note says: 'Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)'.
- Protocol of the new interface:** A dropdown menu with 'L2TP' selected.

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

3. Enter server name and authorization parameters:

COMMON CONFIGURATION

General Setup

Advanced Settings

Firewall Settings

RX: 0 B (0 Pkts.)

TX: 0 B (0 Pkts.)

I2tp-I2tp

Status

Protocol

L2TP

L2TP Server

servername

PAP/CHAP username

username

PAP/CHAP password

.....

4. Save and apply the new configuration. A new network interface will appear.

Revision #1
★Created 11 January 2024 09:21:53 by Gabriele
✎Updated 11 January 2024 09:38:18 by Gabriele