



Configure a guest WLAN using the Luci web-interface

Guest WLAN provides internet access to your network members. It also provides firewall security rules to isolate your guest network from the rest. This recipe is based on the more comprehensive [Guest WLAN page](#), providing a more user-friendly approach through the Luci web-interface.

Note that all MAC addresses have been erased from the screenshots.

Create and configure a new wireless controller

After logging into the web-interface, manoeuvre to the **Wifi** page under **Network**. Click **Add** over the wireless controller (e.g., the 2.4 GHz radio) you want to have your guest network on. A new interface will be added as shown here:

The screenshot shows the OpenWrt Luci web-interface. The top navigation bar includes Status, System, Services, Network, Statistics, and Logout. The Network section is active, showing various sub-sections like Interfaces, Wifi, Switch, DHCP and DNS, etc. The Wifi section is selected, displaying a list of wireless controllers. Two controllers are shown: radio0 (Generic 802.11bgn) and radio1 (Generic 802.11an). Each controller has a list of associated networks with fields for SSID, BSSID, Mode, and Encryption. The radio1 controller has a network named 'OpenWrt2' with a BSSID of '00:00:00:00:00:00'. Below the controllers, the 'Associated Stations' section displays a table of connected devices.

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
OpenWrt	[redacted]	192.168.1.200	-78 dBm	-94 dBm	18.0 Mbit/s, MCS 0, 20MHz	11.0 Mbit/s, MCS 0, 20MHz
OpenWrt	[redacted]	192.168.1.124	-79 dBm	-94 dBm	13.0 Mbit/s, MCS 1, 20MHz	26.0 Mbit/s, MCS 3, 20MHz
OpenWrt2	[redacted]	192.168.1.107	-72 dBm	-95 dBm	48.0 Mbit/s, MCS 0, 20MHz	48.0 Mbit/s, MCS 0, 20MHz

As you can see, our new wireless controller is created, and we named it guest. Next up is configuring it. Choose the **Edit** option for the controller. You will need to create a new network, as you can see we named our new network guest here:

The screenshot shows the 'Wireless Network: Master "guest" (wlan0-1)' configuration page. The 'General Setup' tab is active, displaying the status of the wireless network. The network is enabled, and the mode is set to 'Access Point'. The channel is 6 (2.437 GHz) and the transmit power is 16 dBm (39 mW). The SSID is 'guest' and the encryption is WPA PSK (TKIP, CCMP). The network is associated with the 'guest' interface.

Wireless Network: Master "guest" (wlan0-1)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is 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*.

Device Configuration

General Setup | Advanced Settings

Status

Mode: Master | SSID: guest
BSSID: | Encryption: WPA PSK (TKIP, CCMP)
Channel: 6 (2.437 GHz) | Tx-Power: 15 dBm
Signal: 0 dBm | Noise: -93 dBm
Bitrate: 0.0 Mbit/s | Country: US

Wireless network is enabled Disable

Channel: 6 (2.437 GHz)

Transmit Power: 16 dBm (39 mW)

Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID: guest

Mode: Access Point

Network:

- ☒ guest:
- ☐ lan:
- ☐ wan:
- ☐ 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: ☒

Also, make sure to set up wireless security if you want to protect the connection.

Configure the new interface

Now if you manoeuvre to the Interfaces page under Network, and you should see your new interface, looking similar to this:

The screenshot shows the 'Interfaces' page in the OpenWrt Luci web interface. It displays a list of interfaces: GUEST, LAN, and WAN. Each interface has a status bar showing uptime, MAC address, RX/TX statistics, and IP address. The GUEST interface is highlighted in purple, LAN in green, and WAN in red. Each interface has a set of actions: Connect, Stop, Edit, and Delete.

Interfaces

Interface Overview

Network	Status	Actions
GUEST Master "guest"	Uptime: 0h 4m 45s MAC-Address: RX: 0.00 B (0 Pkts.) TX: 420.00 B (1 Pkts.) IPv4: 10.0.0.1/24	Connect Stop Edit Delete
LAN br-lan	Uptime: 14h 9m 46s MAC-Address: RX: 170.61 MB (680082 Pkts.) TX: 1.51 GB (1302618 Pkts.) IPv4: 192.168.1.1/24	Connect Stop Edit Delete
WAN eth1	Uptime: 14h 9m 41s MAC-Address: RX: 184.65 MB (700406 Pkts.) TX: 184.65 MB (700406 Pkts.) IPv4: 89.151.199.80/25	Connect Stop Edit Delete

Add new interface...

You will need to configure you interface before it is useful. Choose **Edit**, pick the protocol **Static address**, and fill out your chosen IPv4 address. We chose 192.168.3.1 here, but you may have different preferences. However, avoid using 192.168.1.1 or 10.0.0.1 as they may already be in use and prevent your guests from acquiring IP-addresses. Remember to set the netmask. You will also need to enable DHCP, we chose to go with the default options here except for the Leasetime wich is only one hour, suitable for environments where a large number of guests connect and leave through a day.

Notice that you have a **Firewall Settings** tab to the far right of the **General Setup** tab. Make sure you visit this tab, and create a new zone for your guest, like we have done here:

Configure the firewall

Now you are just about done. That last thing we need to do, is to open up for traffic between you guest network and WAN in the firewall. Go to the **Firewall** page under **Network**, choose **Edit** for your guest zone. Set **Input** to **REJECT** and tick wan under **Allow forward to destination zones**. Correctly configured it should look like this:

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☒

Drop invalid packets ☐

Input:

Output:

Forward:

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	<input type="text" value="accept"/>	<input type="text" value="accept"/>	<input type="text" value="reject"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: ⇒ REJECT	<input type="text" value="reject"/>	<input type="text" value="accept"/>	<input type="text" value="reject"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
guest: guest: ⇒ wan	<input type="text" value="reject"/>	<input type="text" value="accept"/>	<input type="text" value="reject"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete

[Add](#)

Remember to click **Save & Apply**. The last thing we need to do is to give our guests access to the Internet.

Right now neither DNS nor DHCP traffic will be accepted. We need to create two rules, which we can do from the **Traffic rules** tab under the **Firewall** tab. Both rules can be put in under **Open ports on router:**. We name the first one **Guest DNS** here (you can name it what you want), setting both TCP and UDP traffic and port 53:

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

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"/>	Edit Delete
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"/>	Edit Delete
Allow-DHCPv6	IPv6-UDP From IP range FE80::0:0:0:0:0:0:0:0/10 in wan with source port 547 To IP range FE80::0:0:0:0:0:0:0:0/10 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	Edit Delete
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	Edit Delete
Allow-ICMPv6-Forward	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	Edit Delete

Open ports on router:







Name	Protocol	External port
Guest DNS	TCP+UDP	53

[Add](#)

We need to configure the rule, so choose to edit it. Set **Source zone** to **guest**, and set **Destination zone** to **Device (input)** like shown here:

Firewall - Traffic Rules - Guest DNS

























This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	<input type="checkbox"/> Disable
Name	Guest DNS
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	<input type="radio"/> Any zone <input checked="" type="radio"/> guest: guest:  <input type="radio"/> lan: lan:  <input type="radio"/> wan: wan: 
Source MAC address	any
Source address	any
Source port	any
Destination zone	<input checked="" type="radio"/> Device (input) <input type="radio"/> Any zone (forward) <input type="radio"/> guest: guest:  <input type="radio"/> lan: lan:  <input type="radio"/> wan: wan: 
Destination address	any
Destination port	53
Action	accept

Similarly, create a new rule to allow DHCP for guests. We name this rule Guest DHCP, choose UDP as protocol, and set 67-68 for ports. Again edit the rule, setting **Source zone** to **guest**, and set **Destination zone** to **Device (input)**. When you are done it should look like this:

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

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"/>	   
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"/>	   
Allow-DHCPv6	IPv6-UDP From IP range FE80::0:0:0:0:0:0:0:10 in wan with source port 547 To IP range FE80::0:0:0:0:0:0:0:10 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	   
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	   
Allow-ICMPv6-Forward	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	   
Guest DNS	Any TCP, UDP From any host in guest To any router IP at port 53 on this device	Accept input	<input checked="" type="checkbox"/>	   
Guest DHCP	Any UDP From any host in guest To any router IP at ports 67-68 on this device	Accept input	<input checked="" type="checkbox"/>	