English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Contents

- 1 Introduction
- 2 DNSMasq method
- 3 23020 and later
- 4 Prior to 23020
- 5 Special Notes
    - 5.1 Guest VAP Passwords
    - 5.2 Guest Access to a Network Device
    - 5.3 Multi-radio routers
    - 5.4 VAP with no WAN

Introduction

A **Guest Network** is a separate SSID (wireless network ID) using a virtual access point (VAP) that gives guest access to the WAN (internet) while blocking them from your LAN (local network), thereby protecting your security.

DNSMasq method

This uses DNSMasq instead of DHCPd. See VAP with no WAN for setups without a WAN (e.g. WAP), as iptables (*Firewall*) rules are required for internet access (*Multiple DHCP Server* is not available with the WAN disabled). **In the DD-WRT GUI:**

- *Wireless -> Basic Settings*: Click *Add Virtual AP* under *Virtual Interfaces* and change the SSID if needed
    - Set *Network Configuration* to **Unbridged**
    - Enable the following options: *AP Isolation*, *Net Isolation*
    - Enable *Forced DNS Redirection* to prevent users from circumventing content filters (see Public DNS)
    - Set the *Optional DNS Target* (if needed), *IP Address* (e.g. 192.168.7.1), and *Subnet Mask* (255.255.255.0)
- *Wireless -> Wireless Security* set up the new "Virtual Interface" (e.g. wl1.1), preferably with WPA2-AES
- *Services -> Services -> DNSMasq*: Enable DNSMasq, but leave other options disabled
- In *Additional DNSMasq Options*, add the IP address and range for the appropriate virtual guest interface
    - Example for Broadcom (5 GHz is *wl1.1*), Atheros is *ath0.1* or *ath1.1*, **but depends on the router**:

```
interface=wl0.1
dhcp-option=wl0.1,3,192.168.7.1
```

```
dhcp-range=wl0.1,192.168.7.100,192.168.7.200,255.255.255.0,12h
```

23020 and later

Kong added easy Guest Network capability to DD-WRT starting with build 23020. See Guest WiFi + abuse control for beginners

- Firewall changes should not be needed for a normal gateway router setup

Prior to 23020

Reference: DD-WRT Guest Wireless

1. Section *Wireless -> Basic Settings* tab
    - ?Add? a ?Virtual Interface?, give this guest network a separate SSID, and ?Enable? ?AP Isolation?.
    - Click **Save**, then **Apply**
2. *Wireless Security* tab: also use a separate password, and WPA2 AES security
    - Click **Save**, then **Apply**
3. Section *Setup -> Networking* tab
    - Under ?Create Bridge? click ?Add?, name it, then set a different subnet
    - Under ?Assign to Bridge? click ?Add", select the new bridge, then assign it to the new virtual interface
    - Click **Save**, then **Apply**
4. *Networking* tab: under ?Multiple DHCP Server? click ?Add? and select the new bridge
    - Click **Save**, then **Apply**
5. Section *Administration -> Commands* tab
6. Firewall Rules to secure the private network and give the guest network internet access:
    - Copy/paste the below, then click **Save Firewall**

```
iptables -t nat -I POSTROUTING -o `get_wanface` -j SNAT --to `nvram get wan_ipaddr`
iptables -I FORWARD -i br1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i br1 -o br0 -m state --state NEW -j DROP
```

More Firewall Rules to isolate guest and restrict services' access:

- Copy/paste the below, then click **Save Firewall**

```
iptables -I FORWARD -i br0 -o br1 -m state --state NEW -j DROP
iptables -I INPUT -i br1 -p tcp --dport telnet -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport ssh -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport www -j REJECT --reject-with tcp-reset
iptables -I INPUT -i br1 -p tcp --dport https -j REJECT --reject-with tcp-reset
```

Test the guest network, reboot if not working

Special Notes

The Multiple WLANs wiki is deprecated (for old builds) and only mentioned for reference.

Guest VAP Passwords

To prevent unauthorized network access, you must use a *different wireless password* from your normal Wireless Access Point. Though isolated from the LAN, a Guest Network should have a *strong password* .

Guest Access to a Network Device

To allow the guest network access to a printer, web server, or other network device, add this rule last:

```
iptables -I FORWARD -i wl0.1 -o br0 -d {IP address} -m state --state NEW -j ACCEPT
```

- Adjusting the virtual interface, bridge, and appropriate IP address

Multi-radio routers

To have guest VAP's from multiple radios on the same subnet, create a bridge for them. Multiple interfaces would need their own entries for DNSMasq (and the firewall, if applicable), such as for both *wl0.1* and *wl1.1*. 'Net Isolation' (Networking page under br1 section) will not isolate all interfaces from the primary network.

- This may depend on the interfaces bridged via br1, so be sure to test
- To be safe, add firewall rules to block br1 from the subnet and router, but ensure the guest has DHCP & DNS:

```
iptables -I INPUT -i br1 -m state --state NEW -j REJECT
iptables -I INPUT -i br1 -p udp -m multiport --dports 53,67 -j ACCEPT
iptables -I FORWARD -i br1 -o br0 -m state --state NEW -j REJECT
```

- Copy/paste these lines to *Administration->Commands*, then click *Save Firewall*
- To allow this *br1* access to a printer, web server, or other network device, add this rule last:

```
iptables -I FORWARD -i br1 -o br0 -d {IP address} -m state --state NEW -j ACCEPT
```

VAP with no WAN

If the router is not used as a gateway (like an AP, thus WAN and DHCP are disabled, but the same subnet as the primary gateway router), firewall rules are needed for client access restrictions and internet access.

- Examples: Access Point (AP), Repeater Bridge (RB), & Dual-band Client Bridge + AP: see here
- To get internet access from the bridge:
- *Administration->Commands*: copy/paste these lines then click *Save Firewall* (**Maintain the rules order**):

```
iptables -I FORWARD -i wl0.1 -d `nvram get lan_ipaddr`/`nvram get lan_netmask` -m state --state N
iptables -t nat -I POSTROUTING -o br0 -j SNAT --to `nvram get lan_ipaddr`
```

- Note that the bridge and/or virtual interface may be different
- *Net Isolation* does not work on a WAP so keep it disabled and add this to the firewall:

```
iptables -I FORWARD -i wl0.1 -d `nvram get lan_ipaddr`/`nvram get lan_netmask` -m state --state N
```

- Also to isolate the WAP itself from the guest network: [Note: not all firmwares have the *multiport* directive]

```
iptables -I INPUT -i wl0.1 -m state --state NEW -j REJECT
iptables -I INPUT -i wl0.1 -p udp -m multiport --dports 53,67 -j ACCEPT
```

- Finally, reboot the router.

For more details on this, see this post. For more on various firewall rules' impacts, see this post.

- Settings *DNS Target* does not work on a WAP if the primary router has *Forced DNS Redirection* enabled. A workaround is if the AP is running DNSCrypt, set it to use OpenDNS "Family Shield DNS": also see Guest WiFi + abuse control for beginners.