



The secondary (client) router is unbridged in a different subnet (with NAT), while a Client Bridge is the same subnet as the host.

## Contents

- [1 Introduction](#)
- [2 Client Mode Setup](#)
- [3 Client Restrictions](#)
- [4 Troubleshooting](#)

## Introduction

This mode is NOT for WIRED connections between two routers, like an Access Point. It is a wireless connection between two routers only, usually to the primary gateway router. A Client Mode router connects to a Wireless Access Point (WAP) wireless connection as the WAN interface, and shares the internet connection only to the LAN ports, or a separate WAP for multi-radio routers. It is not seen as a WAP, nor accepts wireless connections by other client devices.

The primary (host) router is not required to be running DD-WRT firmware. The primary and secondary (DD-WRT Client Mode) routers must be on separate subnets, and NAT is used between them. Thus, when port forwarding is needed it must be configured at both routers - not just on the host router.

A Client Mode router uses its own DHCP server for IP Address, Gateway, and DNS server to connected devices. To have computers connected to both routers (main and secondary) and co-exist in the same subnet, set up DD-WRT as a Client Bridge, Repeater Bridge or use WDS. Further explanation of bridging modes is at [Linking Routers](#).

- **If using a multi-band router, do not set more than one band to CB.** The other radio(s) would normally be set as AP. For example, the 2.4GHz radio can a CB while the 5GHz is an AP, or vice versa.

## Client Mode Setup

Ensure the secondary client router is on a different subnet than the primary host router. Thus, if the primary router IP address is 192.168.A.x, you need to set the client router to an IP of 192.168.B.x. For example, if the host router uses 192.168.1.1, configure your client router to e.g. 192.168.2.x.

- Broadcom routers: read the [Peacock thread](#)

1. Recommended: reset the router
2. Connect a cable from your computer to the LAN port on your router.
3. Set your computer to a static IP address (e.g. 192.168.1.7 subnet 255.255.255.0)
4. Open a web browser and connect to 192.168.1.1 to view the DD-WRT GUI.
5. Set a username and password, if not asked for this, do a proper reset
6. Go to *Wireless->Wireless Security* and enter the *Security Mode* and other information same as Primary
7. Hit SAVE (not apply)
8. Go to the *Wireless->Basic Settings* and change the *Wireless Mode* to "Client"
9. Set the *Wireless Network Name (SSID)* to exactly match the primary router. **Check spelling and case!**
  - ◆ *If multiple routers broadcast the same SSID, to connect to a specific one (i.e. the primary router, instead of a repeater), enable MAC Filtering on the Wireless Tab, and add the specific device's MAC Address.*
  - ◆ *MAC Address can be found on the "Site Survey" page, linked from the Wireless tab in Status*
10. (Optional) If available, in *Wireless* tab (or under *Advanced*), set (or disable) the Ack Timing in meters
11. Hit SAVE (not apply)
12. Go to *Setup->Basic Setup* and change *Connection Type* to *Static IP* or "Automatic Configuration - DHCP"
  - ◆ *Static IP allows easier access remote GUI, SSH, or telnet access is enabled under Administration*
  - ◆ *If the client router is externally managed (e.g. in a college dorm), go to Setup->Basic Setup, set the WAN port protocol as needed for the AP (usually Static, DHCP, or PPPoE), and enter info provided by your ISP. This is the setting that is bonded to the wireless interface.*
  - ◆ *This is what a computer (wired or wireless) connected to the ROUTER would use to gain access to the network, not to be confused with the settings required to gain access to the WAN by the ROUTER.*
  - ◆ *The device should be in GATEWAY mode (not ROUTER), otherwise Masquerade/NAT does not happen.*
13. In *Network Setup* set the Local IP Address **to a different subnet** from the Primary (e.g. 192.168.2.1)
14. (Optional) Set your gateway to the IP address of your client router (same as the previous step)
15. (Optional) Set Static DNS servers in the Network Address Server Settings section if your WAN type does not provide them or you want to use different ones than the AP provides.
16. (Recommended) Change your Time Zone and DST to match where you are.
17. (Optional) Set a "Server IP/Name" in *Time Setting* section for NTP (blank uses a hidden default server)
18. Hit SAVE (not Apply)
19. (Optional) In *Security->Firewall*, disable *SPI Firewall* if security between AP & Client is not needed

## Client\_Mode

20. Hit Apply, then set the computer back to auto IP and DNS if needed (replug the LAN cable if not working)
21. The Client router should connect to the AP within a minute, otherwise unplug the router for 30 sec
22. Once connected and working, configure as needed (e.g. Virtual Interface for wireless connection)

## Client Restrictions

To allow internet access but prevent *192.168.1.x* clients from seeing each other on *br0*, use this firewall script (iptables):

```
iptables -I FORWARD -i br0 -d 192.168.1.0/24 -j DROP
```

## Troubleshooting

If the preceding instructions do not work, it is usually an encryption or password problem. Disable encryption on the primary router and retry the setup. Using proper encryption and the correct case-sensitive password is key. Do a reset and start over. Note: WPA2-AES (aka CCMP) *is required for 802.11N (and newer) devices.*