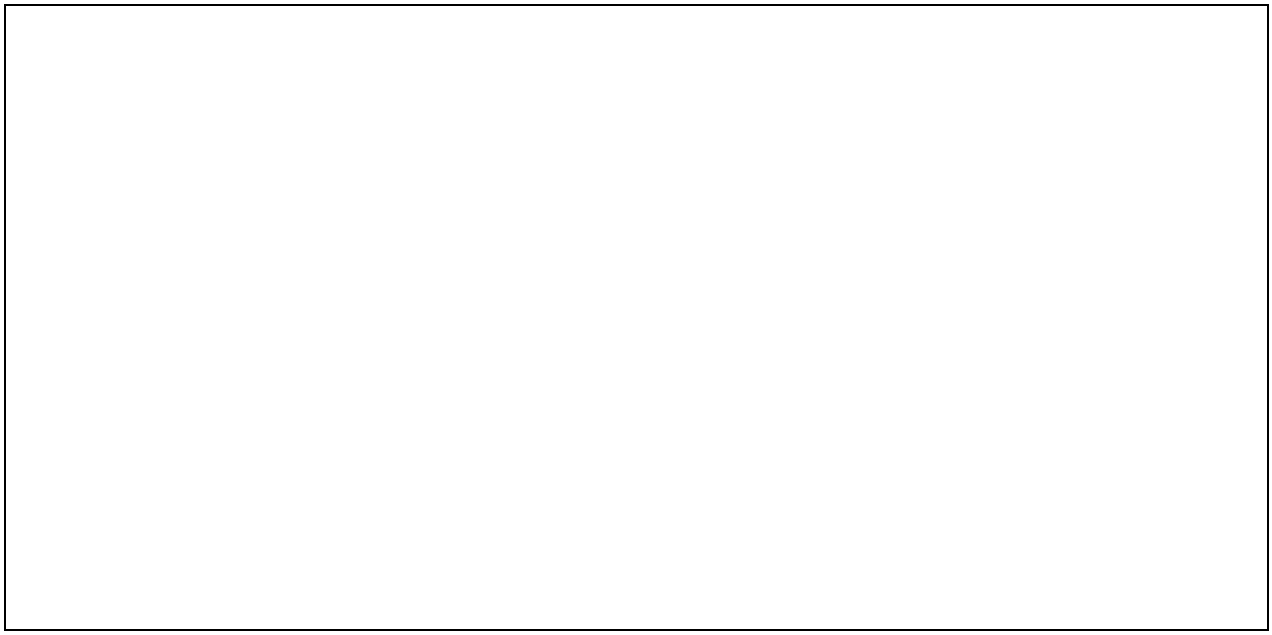
Contents

Introduction



This was tested with Broadcom (Linksys WRT54GLv1.1 & Buffalo WHR-HP-G54).

If you have a large network, for which DD-WRT is not a suitable core router, you will probably want to have wireless clients be a part of the larger network. In this case, clients would get DHCP configuration from some other DHCP server, and could be accessed by other clients on the network.

Linking routers by Ethernet cables does not require DD-WRT on any router. However, some more advanced settings are available in DD-WRT.

As an example, some colleges still allow students to have their own wireless access points (WAPs). They require that the WAPs not hand out private IP addresses (like routers with DHCP/NAT) because it makes it difficult to track down which client is causing problems (eg. virus infections, worms, etc.)

Typically, vendors such as Linksys charge more for devices which work as standalone WAPs because routers are typically used by home users and WAPs are more popular for businesses. With DD-WRT you can buy a device marketed as a router and use it as a WAP.

Secondary Router on a Separate Subnet

- This is simply a gateway router that is downstream of a primary gateway router.

If you want a secondary router to be on a separate subnet from the primary, just hard reset the router and set the router's IP to, e.g., 192.168.5.1 on the basic setup page. Then set security and SSID on the Wireless tab, hit Save then Apply, and finally plug the LAN cable from your primary to the WAN of the second router.

If you wish to be able to access your secondary router from devices on your primary LAN, enable Web GUI management in the Remote Access section of the Administration/Management page. You should then be able to access the secondary router by typing in its WAN IP. Setting up a static lease for the second router's WAN interface in Services on the first router will allow you to always know where the second one is to access it. This is the usual router/gateway mode, which is NOT the main goal of this Wiki.

Access Point (AP) instructions

A secondary router on the same subnet, so all wireless and wired network devices can access each other.

Simple Version (Same Subnet)

On the secondary access point router:

- Do a hard reset
- Disable DHCP and set the wireless channel different from the other router(s)
- Set the IP address to 192.168.1.2 (or any IP outside the gateway DHCP range that does not collide with the gateway nor any other static devices)
- Connect a LAN port from the Access Point to a LAN port on the primary router

Normal Version (Same Subnet)

Side note-If you want to have clients on one router isolated from those on the main router, you need to use IP table rules to do this fully. However, following the above "Separate Subnet" instructions will achieve this.

Now, the main how to: Pay special attention to the Review section of this article, especially if you are using an older version.

1. Hard reset the router to DD-WRT default settings
2. Connect to the router @ http://192.168.1.1
    - Note: If this router is wired to another router, there may be conflicts (both routers could have the same IP address). For the time being, disconnect this router from the main one.
3. Open the **Setup -> Basic Setup** tab
    - WAN Connection Type: Disabled
    - Local IP Address: e.g. 192.168.1.2 (same subnet as primary router but outside the DHCP range)
    - Subnet Mask: 255.255.255.0 (unless you know what you're doing)
    - DHCP Server: Disable (do not use *DHCP Forwarder*), also uncheck DNSmasq options
    - Gateway/Local DNS: IP address of primary router (unless you know what you're doing)
    - *(Recommended)* Assign WAN Port to Switch (visible when *WAN Connection Type* is Disabled)
        - This allows connection to the router's default address after a reset, to avoid colliding with the LAN
    - *(Optional)* NTP Client: Enable/Disable (if Enabled, specify Gateway/Local DNS above) Help
    - Click **Save** at the bottom, then wait for the GUI to come back
4. Open the **Setup -> Advanced Routing** tab
    - *(Recommended)* Change operating mode to: Router, then **Save**
5. Open the **Wireless -> Basic Settings** tab
    - Set the Wireless Network Name (SSID) as desired
    - *(Optional)* Sensitivity Range: The max distance (in meters) to clients * 2 (or 0 to disable), then **Save**
6. Open the **Wireless -> Wireless Security** tab
    - Note: Security is optional, but recommended! Clients must support whatever mode you select here.
    - *(Recommended)* Security Mode: WPA2
    - *(Recommended)* WPA Algorithm: AES
    - *(Recommended)* WPA Shared Key: =>8 characters, then **Save**
7. Open the **Services -> Services** tab
    - *(Optional)* DNSMasq: Disable (enable if you use additional DNSMasq settings)
    - *(Optional)* ttraff Daemon: Disable, then **Save**
8. Open the **Security -> Firewall** tab
    - Uncheck all boxes except Filter Multicast, then **Save**
    - Disable SPI firewall, then **Save**
9. Open the **Administration -> Management** tab
    - *(Recommended)* Info Site Password Protection: Enable
    - Routing: Disabled (unless you need to route between interfaces, or have other problems)
    - **Save** then **Apply Settings** and connect Ethernet cable to main router LAN port
    - Connect to the WAP's WAN port if *Assign WAN Port to Switch* is enabled
    - If not working, reboot the router to be sure all settings have been applied.
    - You may have to reboot the PC or "ipconfig /release" then "ipconfig /renew" in Windows

Review

There were three basic configuration changes you made to set up your router as a wireless access point.

Turn Off DHCP

If you did not turn off DHCP, when you plug your router into the network (after configuration), your WAP may provide IP addresses to clients on the wired network, and this may be inappropriate. Tracking down problems caused by multiple DHCP servers can be time-consuming and difficult.

Because it's so important, it is worth repeating: **Turn off DHCP before you continue!**

Set the IP address of the LAN Interface

Immediately after turning off DHCP, while your PC still has the IP address the WAP gave you, set the LAN interface of the WAP to the IP address you want it to use, e.g., if the host router is 192.168.1.1, give the WAP an IP of 192.168.1.2. Alternatively, you can use the instructions below to set the WAP's IP address via DHCP.

If you cannot connect to the WAP in order to set the LAN interface's IP address, it is probably because your computer no longer has an IP address on the same subnet. To get past this issue, simply set your computer's IP address and subnet to 192.168.1.8 and 255.255.255.0 respectively. (This assumes you are still using the default settings. If not, change the IP address and subnet as appropriate) You should now be able to point your browser at 192.168.1.1 (again assuming default settings).

LAN Uplink

There are two ways to connect your WAP to the LAN. You can either Uplink through one of the router's LAN ports, or use the WAN port that is normally connected to the cable/DSL modem.

LAN Uplink Through LAN Port

To complete the link between the two routers, connect a LAN port on the central router, to a LAN port on Linksys router (to be used as your WAP). You may need a crossover cable to do this, although many modern routers have automatic polarity sensing. To test this, connect a standard Ethernet cable between the two routers. If the LAN light comes on, the router has automatically switched the polarity and a crossover cable is not required.

LAN Uplink Through WAN Port

If you use your DD-WRT router as a WAP only, you may use your DD-WRT router's WAN port to connect it to your existing LAN. To do this, you need to disable the Internet Connection and "Assign WAN Port to Switch".

Normally, the router does Layer 3 IP routing. but by "Assigning WAN Port to Switch," your DD-WRT router will bypass that functionality and just pass on the Layer 2 ethernet packets from your wired network to the wireless network and vice versa.

Alternatively, if you have a router that supports assigning the WAN port to the switch:
Setup -> Basic Setup -> Internet Connection Type -> Connection Type = Disabled
Setup -> Basic Setup -> Network Setup -> WAN Port -> Assign WAN Port to Switch
you can connect the WAN port as your uplink to your main router. All this really buys you is an extra port (4 available instead of 3), but why not?

Roaming access

If you are installing additional Access Points to cover a broader area with Wi-Fi access, it is possible to allow clients to roam freely between them. The common method is to **use the same SSID and Security settings** on each access point. The clients control when to switch in between APs. Most clients will switch when they see a more powerful AP available but some client radios are not able to listen for a new AP when connected to an existing AP and as a result those clients will not roam to the new AP until they completely lose signal from the old one. A typical roaming transition from one AP to the other takes about 50ms if using simple authentication (open or WPA2 PSK AES)

Use a different channel on each AP. e.g. if you are in the US and installed two access points, use channels #1 and #11. Or if three access points, then use channels #1, #6, and #11 (setting the channels at least 5 apart should help keep interference between APs to a minimum). If you have a residential gateway with wireless turned on, and just one AP, then the same applies: each gets a different channel. If you are in Europe, use channels 1, 5, 9 & 13.

When using multiple Access Points, each one should be connected by **LAN to LAN uplink** as described above. They can even be attached to different switches within the same organization.

Access Point placements need to be carefully done. If the APs are too far away then there will be holes in the coverage and the clients will drop off when going from one AP to the other. If the APs are too close then clients will "stick" to one AP while moving out of its region and into another's. If the APs are too close and moving them farther apart is not practical then the transmit power on each AP can be reduced.

You can also try setting the APs to use the same channel. This will halve bandwidth when both APs are talking to clients but it may help clients that have problems sticking to one AP.

It can also be helpful to disable the slower 802.11 transfer rates with the Wl_command#rateset command for example:

```
wl down
sleep 5
wl rateset 18b 24 36 48 54
wl up
```

This sets the minimum access to 18Mbit and clients will drop off as the signal level falls below what's needed to support this.

There are additional considerations with roaming using wireless VoIP gear, and WPA Enterprise modes. These environments require additional authentication from the client that could exceed the TCP/IP TTL and cause a disconnection of a higher level application such as the VoIP client. Because of that, the IEEE 802.11r-2008 protocol, a.k.a. Fast Transition (FT), was developed. DD-WRT does not currently support 802.11r FT but there is support for it in OpenWRT. The wireless client must also support Fast Roaming for this protocol for it to work; typically it will be cell phones that support it.

How To Use DHCP to Set the WAP's IP Address

Note: This step is optional. Having the WAP's IP address set by a DHCP server is not required. It can be made static, as shown above.

*Note also that the steps below assume a DHCP server is running **outside** this DD-WRT WAP box on the LAN (e.g., in the FAI DSL box/gateway), so, keep this internal DD-WRT WAP DHCP server **disabled** as stated above, as well as all other settings.*

It is not possible to set the LAN interface to get its IP address via DHCP using the web configuration interface. You can, however, set your startup script to obtain an IP address.

Simply set your IP address to (starting DHCP client):

```
[ ! -e /tmp/udhcpc ] && ln -s /sbin/rc /tmp/udhcpc
udhcpc -i br0 -p /var/run/udhcpc.pid -s /tmp/udhcpc -H test-wrt-wireless
hostname `nslookup \`ifconfig br0 | grep 'inet addr' |cut -f 2 -d ':'\` | grep 'Name:' | awk '{pr
if test `hostname` != `nvram get wan_hostname`; then
     nvram set wan_hostname=`hostname`;
     nvram set router_name=`hostname`;
     nvram commit;
fi
```

Only the two first lines are required if you don't want your WAP to set its name based on the IP address it gets. However, if you want to save a configuration file which will apply to several WAPs, that can be a handy feature.

EDIT 2013/09/19: If you leave the "Local DNS" GUI field to 0.0.0.0, then the WAP will use the DNS supplied by DHCP. To be functional, this requires the "Gateway" is set too. So, you also wish the gateway to be assigned by DHCP too. You do it appending

```
route add default gw `nvram get wan_gateway`
```

after the udhcpc command in the script. You will leave the unused Basic/Network Setup/"Gateway" GUI field to 0.0.0.0, or, to get a GUI feedback of the currently assigned *wan_gateway* nvram value, have this field filled by the value of the nvram *lan_gateway* value by setting this last the same way as the one below for *wds_watchdog_ips*.

Then you may want the optional WDS/Connection Watchdog to ping the gateway it just got from DHCP: just enable the watchdog in the GUI, set the wanted delay to have the WAP monitor the connection to the gateway, leave the IP's field blank, append the following 4 lines after the *route add ...* command above, so that they will fill it in for you and the watchdog will help your WAP to follow any change of the gateway IP address (as long as the previous gateway IP is no longer used. You can work around the case when the previous IP is reused for another purpose with a reboot on URL ping failure **custom script** plus the cron job that triggers it in the GUI Management tab, but if the gateway loses its WAN connection, the WAP's wireless clients may lose their wireless connection at the same rhythm the WAP reboots. To prevent this, think to ping both external(s) URL(s) and internal IP(s) and make the custom script to reboot the WAP when all pings fail - this will preserve internal connections in the case the Internet is lost at the gateway WAN side).

The **if** tests below are just here to preserve the nvram service life with no rewrite when not needed on boot. Even the WAP's ip will survive over reboots thanks to a static lease - this applies to other scripts.

```
GW=`route -n|grep UG|awk '{print $2;}'`
if [ "`nvram get wds_watchdog_ips`" != "$GW" ]; then
nvram set wds_watchdog_ips="$GW"
nvram commit
fi
```

Once you have manually set the router & hostname name fields, you should set the DHCP startup script this way:

```
[ ! -e /tmp/udhcpc ] && ln -s /sbin/rc /tmp/udhcpc
udhcpc -i br0 -p /var/run/udhcpc.pid -s /tmp/udhcpc -H `nvram get wan_hostname`
route add default gw `nvram get wan_gateway`
GW=`route -n|grep UG|awk '{print $2;}'`
IP_LAN=`ifconfig br0 | grep inet | cut -d: -f2 | cut -d' ' -f1`
MSK=`ifconfig br0 | grep inet | cut -d: -f4`
if [ "`nvram get lan_ipaddr`" != "$IP_LAN" ]; then nvram set lan_ipaddr="$IP_LAN"; NC=1; fi
if [ "`nvram get lan_netmask`" != "$MSK" ]; then nvram set lan_netmask="$MSK"; NC=1; fi
if [ "`nvram get lan_gateway`" != "$GW" ]; then nvram set lan_gateway="$GW"; NC=1; fi
if [ "`nvram get wds_watchdog_ips`" != "$GW" ]; then nvram set wds_watchdog_ips="$GW"; NC=1; fi
if [ "$NC" = 1 ]; then nvram commit; reboot; fi
```

The whole ip/mask/gateway will show correctly in the Settings web GUI page.

--Bib

Related wiki links

Secure remote management for a WAP