English • <u>Deutsch</u> • <u>Español</u> • <u>Français</u> • <u>Italiano</u> • <u>???</u> • <u>Polski</u> • <u>Português</u> • <u>???????</u> • <u>Svenska</u> • <u>???(????)?</u> • <u>???(??)?</u> •

Contents

Basic Wireless Settings

Introduction

Note, if you do not see a certain setting on your router, it may be on a different screen or it is not supported. If in doubt, ask on the forums.

See: Advanced Wireless Settings for the rest of the settings not found on this page.

Regulatory Domain

Available Settings: 115+ different countries (several countries share the same regulations)

Default Setting: Germany

This determines the channels available in the list for both bands (if you have a dual band router) and the maximum EIRP "legally" allowed by the telecom authorities in the chosen country. EIRP is TX power plus antenna gain, example: * 20 dBm TX power with a 10 dBi gain antenna has an EIRP of 30 dBm.

- 24 dBm TX power with a 6 dBi gain antenna has an EIRP of 30 dBm.

Maximum EIRP varies by nation and your max TX power will be capped by the regulatory domain if you have a powerful radio. For example, Canada's max allowed EIRP is 36 dBm while its max allowed TX power is 30 dBm, with Canada selected and antenna gain at 0 dBi, the radios will never go above 30 dBm assuming they are capable of reaching that of course.

Regulatory Mode

Available Settings: Off, 802.11h Loose, 802.11h Strict, 802.11d

Default Setting: Off

Recommended Setting: Off

Here's some information on what 80211h was supposed to do:*IEEE 802.11h is the IEEE standard for Spectrum and Transmit Power Management Extensions. It solves problems like interference with satellites and radar using the same 5 GHz frequency band. It was originally designed to address European regulations but is now applicable in many other countries. The standard provides Dynamic Frequency Selection (DFS) and transmit Power Control (TPC) to the IEEE 802.11a MAC.*

TPC Mitigation Factor

Available Settings: 0 (Off), 1, 2, 3, 4

Default Setting: Off

Recommended Setting: Off

Here is what it changes:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/b_RRM_White_Paper

Wireless Physical Interface

Available Interfaces: athX (0, 1, 2 etc, varies by router as many routers have 2 or more radios in them)

If you have a dual band router ath1 will be displayed below ath0 with the same available settings. Ath0 is the 2.4GHz radio and ath1 is the 5GHz radio for most routers, for some like the TL-WDR4900 v1.3, ath0 is 5GHz & ath1 is 2.4GHz; its just the way the radios are connected on the PCB & is normal. If you create a VAP for 2.4GHz or 5GHz radio the VAPs will be labelled athX.1 & athX.1 respectively where X = the interface's number. For example, a VAP made on ath0 will be ath0.1, then ath0.2, etc. Refer to this thread for some info about VAPs with Qualcomm Atheros.

Wireless Mode

Atheros available Settings: AP, Client, Client Bridge, Adhoc, WDS Station, WDS AP**Broadcom available Settings:** AP, Client, Client Bridge, Adhoc, Repeater, Repeater Bridge**Default Setting** AP**Recommended Setting:** AP for most users, other options if you are advanced and know you need it

The help file says... * The wireless part of your router can run in different modes:

- AP mode â?? This is the default mode, also called Infrastructure mode. Your router acts as an central connection point, to which wireless clients can connect.
- Client mode â?? The radio interface is used to connect the internet-facing side of the router (i.e., the WAN) as a client to a remote access point. NAT or routing are performed between WAN and LAN, like in "normal" gateway or router mode. Use this mode, e.g., if your internet connection is provided by a remote access point, and you want to connect a subnet of your own to it.
- Client Bridged mode â?? The radio interface is used to connect the LAN side of the router to a remote access point. The LAN and the remote AP will be in the same subnet (This is called a "bridge" between two network segments). The WAN side of the router is unused and can be disabled. Use this mode, e.g., to make the router act as a "WLAN adapter" for a device connected to one of its LAN Ethernet ports.
- Ad-Hoc mode â?? This is for peer to peer wireless connections. Clients running in Ad-Hoc mode can connect to each other as required without involving central access points.
- See this page for more info on linking routers: https://www.dd-wrt.comhttp://forum.dd-wrt.com/wiki/index.php/Linking_Routers

How it works: Determines how the specific wireless interface of the router is to behave. If you want to run a normal access point which most do, AP would be your choice. Client and Client Bridge with Virtual Interfaces is the Atheros equivalent Broadcom's Repeater and Repeater Bridge settings.

Wireless Network Mode

Available Settings (2.4 GHz): Disabled, Mixed, B-Only, G-Only, BG-Mixed, NG-Mixed, N-Only (2.4 GHz)

Available Settings (5 GHz): Disabled, Mixed, A-Only, NA-Mixed, AC/N-Mixed, N-Only (5 GHz), AC-Only

Available Settings (60 GHz): Disabled, Mixed, AD-Only

Default Setting: Mixed

Recommended Setting: NG-Mixed (2.4 GHz), AC/N-Mixed (5 GHz), AD-Only (60 GHz)

Controls which 802.11 signals are being broadcast by the radio. Depending on the selected network mode your wireless channel list and maximum TX power can vary. NG-Mixed for 2.4 GHz & Mixed or AC/N-Mixed is the recommended setting for most people as your clients' NICs are able to use either (V)HT20, (V)HT40, & VHT80 "properly" with this setting. If you have any issues or do not use 802.11b clients, switch to NG-Mixed. N-Only is broken on many units for some time (both bands) & still is, try to avoid using as there is minimal performance change from NG-Mixed -> N-Only if all you use is 802.11n clients for either of them. For 802.11a/n 5 GHz radios, Mixed & NA-Mixed are the same.

Note on BCM routers, client / client bridged modes only should use straight mixed mode.

The help file says... * If you wish to exclude Wireless-G clients, choose B-Only mode. If you would like to disable wireless access, choose Disable.

Note : when changing wireless mode, some advanced parameters are susceptible to be modified ("Afterburner", "Basic Rate" or "Frame Burst").

How it works:

In Mixed mode, dd-wrt routers are able to offer various wifi network types (B, G and N) at the same time from a single 2.4GHz radio. 802.11n transmission is always embedded in an 802.11a, for 5GHz radios, or 802.11g for 2.4GHz radio transmissions. This is called Mixed Mode Format protection (also known as L-SIG TXOP Protection).

See also:

- Wireless-N Configuration - not required if recommended settings are used from this page.
- Wireless-N Throughput Testing

Wireless Channel

Available Settings (2.4 GHz): Channels 1 ~ 14 depending on your regulatory domain & channel width

Available Settings (5 GHz): Channels 34 ~ 48 (U-NII-1), 52 ~ 64 (U-NII-2), 100 ~ 144 (U-NII-2e), 149 ~ 161 (U-NII-3), 165 (ISM) depending on your regulatory domain*

Available Settings (60 GHz): Channels 1 ~ 4 depending on your regulatory domain*

Default Setting: Auto

Recommended Setting: Please actually pick a channel and try to use the cleanest channel with the least noise, most stable throughput, & lowest latency jitter. Using Channels 1, 6, or 11 assures no overlap with the adjacent channels. Using other channels will work, but may overlap with neighboring wifi which will likely be using one of the three channels above.

The help file says... * Select the appropriate channel from the list provided to correspond with your network settings (in North America between channel 1 and 11, in Europe 1 and 13, in Japan all 14 channels). All devices in your wireless network must use the same channel in order to function correctly. Try to avoid conflicts with other wireless networks by choosing a channel where the upper and lower three channels are not in use.

How it works:

IEEE 802.11 is a set of standards that are published for the purposes of carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are implemented by the IEEE LAN/MAN Standards Committee (aka "IEEE 802").

2.4GHz Channels

2.4GHz band in the 802.11 standard uses radio frequencies in the range of 2.412-2.484 GHz. 802.11 splits up the frequencies within the band into 14 radio channels, numbered 1-14. These are the 14 channels designated in the 2.4 GHz range spaced 5 MHz apart (with the exception of a 12 MHz spacing before Channel 14). The frequency range of a channel partially overlaps with the next one, so not all the channels are therefore independent. By default on a 2.4GHz band radio DD-WRT routers, channels 1, 6 and 11 have no overlap with each other; those three channels are known in the wireless community as the "standard" for wireless channel independence within the 2.4GHz band.

In North America this 2.4GHz "band" is implemented by dividing the 2.4GHz band into 13 channels each with a width of 22 MHz but also spaced only 5 MHz apart, with channel 1 centred on 2412 MHz and 13 on 2472, to which Japan adds a 14th channel 12 MHz above channel 13.

5GHz Channels

5GHz band in the 802.11 standard uses radio frequencies in the range of 4.980 GHz to 5.825 GHz. 802.11 splits up the frequencies within the band into 42 wireless radio channels, numbered 7 to 196. These are the 42 channels designated in the 5 GHz range and they are spaced 5 MHz apart. The frequency range of a channel partially overlaps with the next one, so not all the channels are therefore independent but unlike the 2.4GHz band the 5GHz band offers many more non overlapping channels.

In North America this 5GHz "band" is implemented by dividing the 5GHz band into 24 channels (36 to 165) each with a width of 22 MHz but also spaced only 5 MHz apart, with channel 36 centred on 5.180 GHz and 165 on 5.825 GHz.

NOTE - The specifics of the frequency range and how channels are allocated is regulated by each country. Usually constrained in part by how each country allocates radio spectrum to various services. For example, in

the 2.4Ghz band Japan has implemented 1 to 14 wireless channels, Europe #1-#13 and the FCC in the US decided with 1 to 11 wireless channels all within the same band. DD-WRT allows the use of all channels; this doesn't mean your client wireless adapter can support channels outside of its licensed region.

How it works in DD-WRT: To configure your radio channels in the WebGUI you browse to the "Basic Settings" under the "Wireless" page on your DD-WRT router.

If you have dual band router (ie. Two Radios inside the router) you will see two sections for configurations listed in this page with the headings as "wl0" for the 2.4GHz radio and "wl1" for the 5GHz radio.

DD-WRT has channel configuration settings that must be configured;

Wireless mode, this determines if the router will be used as an Access Point, Repeater, Client or in an Ad-hoc configuration mode. Channel options are only avalaible to a router running in AP or Ad-Hoc wireless mode.

Wireless Network mode, this setting determines what wireless protocols will be offered to the wireless clients that try to connect to the router. Depending on the wireless network mode your radio is configured for DD-WRT will have additional channel options for you to configure if you choose.

- If you want to introduce channel bonding in your wireless enviroment you should also start with "CTS Protection" set to Auto as well.

Channel Width

This determines the wireless channel width used- where higher values allow more bandwidth/throughput, but yield fewer free channels, and result in more overlapping channels. Using lower MHz channel width values yields more free non-overlapping channels but means less bandwidth/throughput is available. For a full table of possible MCS index connection rates see [1]

BEFORE DOING ANYTHING- MAKE NOTE:

1) Select your country first and YOU MUST HIT APPLY! The driver needs to reconfigure the country for the speific wifi chipset and then the router needs to get the updated channel list for your country

2) Set the Channel Width and hit Save.

3A) Select the correct WiFi "carrier" channel and concurrently go to step 3B.

3B) Set the Extension Channel UU, LL, UL, or LU .

Carrier channel is defined as the main 20Mhz channel that "carrying" the signal. Extension channels are then added to yield HT40, VHT80, and VHT160.

Available Settings (2.4 GHz): Dynamic (20/40 MHz), Wide HT40* (40 MHz), Full (20 MHz), Half (10

MHz)*, Quarter (5 MHz)*

*Note 1: You MUST have this setting on Wide HT40 (40 MHz) to allow 802.11n devices (2.4 GHz & 5 GHz) to connect at their max! *Note 2&3: Half (10MHz) and Quarter (5MHz) may not be supported on all models. It is best to just use Full (20MHz) or wider.*

Available Settings (5 GHz): VHT160*, VHT160 (80+80 MHz)*, VHT80 (80 MHz)*, Dynamic (20/40 MHz), Wide HT40 (40 MHz), Full (20 MHz)

Note: VHT80 (80 MHz), VHT160 (80+80 MHz), & VHT160 is only displayed & available for 802.11ac (5 GHz) routers that support it, & it's required to reach the max MCS link rates of 802.11ac

WARNING ABOUT USING VHT160-Using DFS channels can significantly increase 5 GHz association times because devices (STAs) can only passively scan for available APs. So instead of being able to send out a probe request and waiting for APs to reply, a STA using DFS channels must wait until an AP announces itself. You wouldn't think this would make much difference, but when switching from running 2.4 to 5 GHz tests, it took over a minute to find and associate to the router's 5 GHz SSID.

Default Settings (2.4ghz): Full (20 MHz)

Recommended Setting (2.4 GHz): Full (20 MHz)- Why? Because nearly all cell phones and tablets will limit their channel width to only 20MHz if they detect neighboring routers/wifi AP's and so 40MHZ wide communication will not be allowed; even if you enable HT40 on the router. Your mileage may vary by enabling HT40 on the router for phones and tablets. As far as Laptops/Desktops, they usually have a way to allow 40MHz wide channels in the advanced driver settings. Disable "Fat Channel Intolerant" to take advantage of 40MHz on Windows OS's. Using HT40 enables channel bonding by using 2x20 MHz wide channels together to equal 40Mhz; but, it's considered "not neighbor friendly" and discouraged by industry standards- as noted above for android & iPhone HT20 limit. Using HT40 may, **but usually doesn't**, create more interference for neighbors; it's usually not an issue unless you're in VERY packed/dense/congested wireless area like apartments- Again YMMV with HT40. HT40 allows your 802.11n devices to connect at their max rate: 300 Mbps (2x2:2 stream clients).

Note: 193mbps is not an officially recognized MCS index rate, but some devices have reported 193mbps vs 173; 173 is the maximum for 2x2:2 stream clients per 802.11ac industry standards.

Recommended Setting (5 GHz): VHT80 (80 MHz), or Wide HT40 (40 MHz). For wifi 5-wave 2 routers, VHT160 can only be taken advantage of by two/three Intel Wifi cards right now (9260/9265/AX200 2x2:2); otherwise, backhaul from one VHT160 capable router to another VHT160 capable router is the other reason to use VHT160 right now. Also to note, VHT160 operates in spectrum which requires reduced TX pwr vs. VHT80: VHT160 spectrum only allows 23dBm vs. 30dBm for VHT80 (USA and similar countries). So, use VHT160 if you know you have clients that can take advantage of it; but realize your TX distance may be worse than if you use VHT80. Also note, it may take up to a minute to find your 5ghz signal if using VHT160 mode.

Lastly, very few clients are 3x3 or 4x4 stream capable; usually only desktop wifi cards are 3x3 or 4x4 (due to space limits in tablets, phones, and laptops & cost of more antenna's). You'll obviously gain more throughput by having 3x3 or 4x4 capable routers & clients. Nearly all phones and tablets are 2x2:2 stream devices, at best, right now (limited room for 4 antenna's & cost too). AFAIK, all laptops use 2x2:2 stream cards; though, apple has a few 3x3:3 stream cards in their devices...use google to find 3x3 or 4x4 stream wifi clients.

Valid VHT80 channels are: * 36+UU

- 40+UL
- 44+LU
- 48+LL
- 52+UU
- 56+UL
- 60+LU
- 64+LL
- 100+UU
- 104+UL
- 108+LU
- 112+LL
- 116+UU
- 120+UL
- 124+LU
- 128+LL
- 132+UU
- 136+UL
- 140+LU
- 144+LL
- 149+UU
- 153+UL
- 157+LU
- 161+LL

Valid VHT160 channels are: * 36+UUU

- 64+LLL
- 100+UUU
- 128+LLL

Sensitivity Range (ACK Timing)

Available Settings: 0 ~ 999999 (meters)

Default Setting: 500 (way too short now, used to be 2000)

Recommended Setting: Try 900 first, if you have issues then try higher values like 1350 - 2250. Values over 2250 are only used when **needed** for long distance link. Use increments of 450 when making adjustments up or down.

The help file says... * Adjusts the ACK timing in Atheros typical way based on the maximum distance in meters .A value of 0 disables ACK timing completely for Broadcom firmwares. On Atheros based firmwares a value of 0 will turn into auto ACK timing mode. You can try setting ack timing to 0 and see what happens.

How it works: # AP sends a message: Everybody wait X time for a response

1. Client receives
2. Client sends a response to the AP called an ACK - Acknowledges the command waiting for X time.
3. AP sees the ACK
4. Other Clients and AP are free to send

-Ack timing adjustment is used for distance links when the time needed to transmit is greater than the amount of time the sender waits before retrying to transmit the same packet again.

-You want to set the ACK timing to 2x the distance between bridged routers measured in meters.

-If the ACK timing is too high it will not affect the throughput that much. If the ACK time is too low it can drop your throughput to the point of being unusable and can even make the system not connect.

-Recommended setting is 0 for a household network. Which for Linksys users means DD-WRT doesn't use ACK timing at all.

-Maximum theoretical ACK timeouts (not sure on thoroughness) 802.11a : 409us ~ 61km 802.11b : 744us ~ 111km 802.11g : 372us ~ 55km

Wireless Network Name (SSID)

Default Setting: ddwrt

This is where you can choose the name of your wireless network when its being broadcast to roaming clients. You can name this anything you want.

Wireless SSID Broadcast

Available Settings: Enable, disable

Default Setting: Enable

Recommended Setting: Enable

Dependent on the setting above, this controls if your SSID is being broadcast or not. When disable is selected many clients still pick up the beacon and display it as "Hidden" along with the AP's MAC address. Disabling is not recommended as it hardly does anything for security, a determined intruder can still access your network with different methods.

Network Configuration

Available Settings: Unbridged, Bridged

Default Setting: Bridged

Recommended Setting: Bridged

This setting controls if the wireless interface is "bridged" with the LAN ports. Bridged meaning a client on the wireless interface and a client on the Ethernet LAN interface are on the same network on the same subnet. Unbridged allows you to "separate" the WLAN (wireless LAN) by giving it its own subnet and even its own DHCP server. If you want a unbridged interface, you are better off creating a VAP instead of unbridging the main interface.

Wireless Security

More info, not updated: <u>Wireless Security</u>

Security Mode

Available Settings: Disabled, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, WPA2 Personal Mixed, WPA2 Enterprise Mixed, RADIUS, WEP

Default Setting: Disabled

Recommended Setting: WPA2 Personal or WPA2 Personal Mixed (inc Enterprise)

Depends on what your network security needs are, for more advanced security like RADIUS etc. Do NOT use "WPA" (aka WPA1) only or WEP, they are weak ESPECIALLY WEP! Can be cracked easily, in seconds for the latter, they also go against the IEEE 802.11n/ac specification & will usually force your link rates down to 802.11a/g speeds (54 Mbps!) This is one of the leading causes for users not knowing why they aren't getting N or AC speeds with DD-WRT.

Security from weakest --> strongest goes in the following order (not counting enterprise):

Unsecured --> WEP --> WPA+TKIP --> WPA+AES --> WPA2+AES

WPA Algorithms

Available Settings: AES, TKIP+AES, TKIP

Default Setting: Disabled

Recommended Setting: AES

The core of your wireless security strength besides having a complex password & works hand in hand with security mode, to follow IEEE 802.11n/ac spec, you MUST use WPA2 Personal or WPA2 Personal Mixed + AES (inc Enterprise) do NOT ever, ever, use TKIP or even TKIP+AES or you will be forced down to a/g speeds along with your wireless security being weak. If you have some older devices that don't support WPA2, only WPA & WEP, don't worry & do NOT use WEP! Use WPA2 Personal Mixed + AES, this still follows spec & allows full speed link rates with the best security possible. By default all wireless devices always connect using their strongest supported security, ie if your network has all WPA2 AES supported clients, but you have a PSP that only supports WPA AES, your other clients will still use WPA2 AES while the PSP uses WPA AES, no problem. **Having this set to TKIP or TKIP+AES in conjunction with incorrect security mode noted above, is THE leading cause of not getting n/ac speeds in DD-WRT.** See this link for more in depth info about AES which stands for Advanced Encryption System.

WPA Shared Key

Available Settings: Anything

Recommended Setting: Whatever you want, make it rememberable & difficult/random

This is your network password, make it complex coupled with WPA2 AES, you'll have the best security available, theres no WPA3 AES (yet)! The "unmask" checkbox toggles between hiding your password with the traditional dots, or displaying it in clear text.

Key Renewal Interval

Available Settings: 1 ~ 99999

Default Setting: 3600

Recommended Setting: 3600

In seconds, which is 1 hour by default for almost every router firmware out there including stock (3600 sec = 1 hr), is how often the wireless encryption key is changed, this is NOT your password changing, this is within the core of how wireless security functions & is a instant seamless silent event that happens with all connected clients every hour by default. Most users have no need to change this setting, its purpose is to further thwart off potential hackers & thieves by having the encryption key change frequently, WPA2 AES is extremely hard to crack & in the event a stranger in range was pulling their hair out trying to break in to your network, once the key refreshes they'll have to start all over again with a different encryption key to defeat.

WPA Algorithms   11