Contents

Introduction

This page shows the contents and descriptions of standard and advanced wireless settings for Qualcomm Atheros (QCA) based 802.11a/b/g/n/ac/ad routers. **Not every router shows every possible setting shown here as some routers will have less**. If you are a Broadcom or Mediatek (formerly Ralink) user, please refer to Advanced wireless settings for Broadcom/Mediatek wireless settings. Basic Wireless Settings apply to all routers, all of which are listed here under standard settings.

Standard Settings

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

Available Settings: AP, Client, Client Bridge (Routed), AdHoc, WDS Station, WDS AP

Default Setting: AP

Recommended Setting: AP for most users, other options if you are advanced and know you need it

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, Client Bridge (Routed), & WDS Station is the Qualcomm Atheros equivalent to Broadcom & Mediatek's Repeater and Repeater Bridge modes.

See this page for more info on linking routers: Linking Routers

---

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), Mixed or 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.

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]

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*

Default Settings: 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) and 400Mbps (2x2:2) for QAM256 enabled routers & clients. 400Mbps is very rare and was reported on an android device with custom ROM; most everything else will end up using 802.11n MCS rates of 300Mbps. HT40 yields a large throughput increase and enables Atheros Super-G* on legacy clients. However, if Full (20 MHz) is used for 802.11n clients, their max connection speed will only be **144 Mbps (2x2:2 stream clients) and 173Mbps/193Mbps* (2x2:2 stream clients) with QAM256 enabled routers & capable clients.** Legacy 802.11g clients supporting Super-G max connection speed will only be **54 Mbps**.

**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 QCA (wifi 5-wave 2) routers, VHT160 can only be taken advantage of by one Intel Wifi card right now (9260/9265 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.

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.

---

*Super-G

This is a Qualcomm Atheros technology to increase the throughput of 802.11g devices and NOT compatible with 40 MHz channel width in 802.11n. In order to utilize the Super-G feature you must have a QCA router capable of broadcasting 40 MHz wide channels which nearly all QCA routers support this feature, and a Super-G ready client. If you have a QCA router and Super-G ready client, ensure your wireless network mode is on *Mixed*, *G-Only* or "NG-Mixed" with Wide HT40 (40 MHz) as the channel width. The client should now connect at the theoretical max link rate of **108 Mbps**, doubled that of standard 802.11g 54 Mbps. This feature reaches these speeds by channel bonding, a method that bonds two 20 MHz wide channels together similar to how 802.11n does. Max throughput with Super-G should be around 75 ~ 80 Mbps depending on distance, SNR, noise, & other wireless settings. Super-G has no presence or specific controls on the user interface, its automatically on or off & is a zero config feature.

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: Use the cleanest channel with the least noise, most stable throughput, & lowest latency jitter

Controls what channel or frequency your wireless LAN (WLAN) uses. If you have packet loss, abnormally slow throughput or drop outs switch to another channel for less interference. Use site survey & experiment with using different channels, its best to use a channel thats 4 or 5 channels away from the other in use channel for zero interference from other WLANs but since thats hard in this small spectrum even just 2 or 1 channel away makes a massive difference despite there still being a partial overlap, see the images & this link for more info. All routers default to either channels 1, 6, or 11 (for 2.4 GHz) when left on the "auto" setting, it is not recommended to use these channels as most users are inexperienced, and leave them at their defaults. Most of these channels are noisy but for any reason if there isn't many APs around you using these channels, use them.

- Available channels will vary greatly by region & there is no place on Earth where every channel is available legally. Only channels 149-165 allow high TX power up to 30 dBm in most of the world, only a few countries allow 30 dBm from channel 100+, using a foreign regulatory setting to bypass your local laws is not recommended & is at your own risk. As of 2014 the FCC has announced that the lower 5 GHz band (U-NII-1) will have it's "indoor only" requirement lifted, & max power

output/EIRP increased to 24 dBm.

Extension Channel

Available Settings (40 MHz): Upper, lower

Available Settings (80 MHz): UU, LL, UL, LU

Available Settings (160 MHz): UUU, LLL, ULU, LUL, UUL, LLU

Available Settings (60 GHz): TODO

Default Setting: Auto

Recommended Setting: Any* (valid setting, observe below)

This setting is only valid when Wide HT40 (40 MHz), VHT80 (80 MHz), VHT160 (80+80 MHz) or VHT160 (160 MHz) is used for channel width. It controls the extension channel(s), which is the other channel(s) used to attain the 40 MHz width or in the case of 802.11ac, 80/160 MHz width the other 3 channels, are above &/or below the primary selected channel. Build r29974 & later have fixed the extension channel lower setting, use upper or lower depending which channel you want. Builds older than r29974 have problems with ext channel setting & channel selection list. Builds after r31277 have added full range of upper/lower & in between, options for channel widths above 40 MHz for 802.11ac.

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
    - <TODO>* ADD REMAINING VHT160 CHANNEL CONFIGS

- Of coarse this depends on the regulatory domain & client devices in use.

TurboQAM (QAM256) support

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Enable

Only valid for 2.4 GHz & for routers with QCA99xx & newer radios, this setting enables support for QAM256, which is what 802.11ac uses for its more efficient higher link rates, even at the same channel width. Since this is only an option in 2.4 GHz, full (20 mHz) or HT40 widths can be used; HT40 will yield the best MCS speeds vs Full. If the signal is strong enough, higher QAM allows more efficient use of the same spectrum space; again, for devices that support this feature.

When using a VAP (virtual access point) with a TurboQAM enabled radio, there is a minor bug which the VAP will, by default, not have TurboQAM enabled. To fix this go to the Wireless Security tab, and enter, on a seperate line, "vendor_vht=1" under the VAP's custom config box. This only works on routers that have a TurboQAM option, in the first place, for the main interface in wireless settings.

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.

Best practice is to name both 2.4GHz and 5Ghz the same SSID and use the same password for both bands. This helps "improve coverage" because your client will switch over to 2.4GHz from 5Ghz faster than if you used a separate 5GHz SSID; you're already authenticated on both radios. Using the same SSID helps reduce overhead on the router too. That said, you need to set the beacon interval carefully if you use the same SSID. Whichever radio has the lower beacon interval will result in clients "seeing" that radio first. So if you want your client to prefer 5Ghz first, then set the beacon interval lower on the 5GHz radio. That said, this is not a foolproof "fix" and many clients may struggle staying or coming back to 5GHz when in range if they venture over to 2.4GHz. This is a well known issue on phone/tablet devices. Laptops have a setting in advanced driver settings to prefer one band over the other. Most newer builds of Android wont have this band preference feature anymore. So, if you must have 5GHz, or 2.4GHz, then name the SSID's differently but know that your device will take longer to fall back to 2.4GHz because it has to re-authenticate when the 5GHz signal gets too weak.

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.

Advanced Settings

- *Builds >=r14815 have a checkbox to show or hide advanced wireless settings.*

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.

TX Power

Available Settings: 0 ~ 999

Default Setting: 16 ~ 30 dBm (varies by router)

Recommended Setting: Highest dBm your radios & local laws legally allow**

Transmit (TX) power is the amount of "current" or "juice" going to the antennas, it is NOT the output power FROM the antennas, as that is EIRP. Usually more TX power is better as it allows clients further away to "hear" your AP (assuming the clients also have near equal TX power so the AP can "hear" them back). If TX power is increased too much on older radios, excess noise can develop and reduce throughput or even range; this is an issue with most Broadcom routers. But with Qualcomm Atheros this does not seem to be much of a problem as most QCA radios work very well at their max TX power. Maximum TX power is controlled by the radios (power control*), regulatory domain, wireless channel used, & wireless channel width. The default value for most routers currently is 20 dBm. If you want to run the highest TX power possible, enter 30 dBm & the radios will use as high as their lowest limiter allows (being regulatory domain, channel, or radio EEPROM cap), most can't do 30 dBm so what's displayed on the wireless status page is what's being used. Some newer routers can get very close to or even at 30 dBm, which is the current highest allowed TX power for any regulatory domain.

***Power control**

An automatic zero config feature which controls the max TX power by the SNR & link speed. The higher the SNR, the lower the TX power will be (this action does not display on the wireless status GUI). See vendor specs/FCC documents for more info.

****Recommended Setting**

Some people believe that "high" TX power (i.e., greater than 25 dBm), may be of concern to one's health. That is not the case but each to their own. So if that's you then 22 - 25 dBm should be sufficient; any lower & range starts to significantly drop (unless you want to of course & if you have an older router than only does something like 18 dBm, no need). In case you are wondering, every 3 dBm is doubled the power, so 13 dBm is twice as much as 10 dBm, & so on; but don't worry, 30 dBm is only 1 watt.

Antenna Gain

Available Settings: 0 ~ 999

Default Setting: 0 dBi

Recommended Setting: 0 dBi

Antenna gain is amount of "gain" or "boost" of signal that the antenna provides. Its a bit complicated but remember this, antennas are **not** amplifiers. They do not magnify the signal, but instead "focus" the signal in certain directions, yes even omni-directional antennas do it. The higher the gain the better as it increases EIRP which somewhat helps extend range and significantly helps sensitivity. With high sensitivity, the AP is able to hear "faint" clients, clients that may have a low TX power or are just simply very far away. Set this to 0 as its useless, it does not function anymore & always assumes a value of 0 within the wireless drivers.

Normally it would function as so: take gain into consideration when calculating EIRP, depending on regulatory setting an example of 25 dBm EIRP (20 dBm TX power + 5 dBi gain) may be too high when the limit is lets say 22 dBm EIRP, the TX power in this case will be forced down to 17 dBm. Antenna gain setting has no effect on performance of the WLAN directly (but a physical quality high gain aftermarket antenna does!).

U-APSD (Automatic Power Save)

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Does not currently matter

U-APSD is a power-save mechanism that is an optional part of the IEEE amendment 802.11e/QoS. U-APSD is also known as WMM Power Save. It is basically a feature mode that allows your mobile devices to save more battery while connected to your wifi network. By allowing your mobile devices to enter standby or sleep mode, it conserves battery. The APSD allows smooth transition in and out of sleep mode by allowing the mobile devices to signal the router of its status.

There are two types of APSD that goes under this type of battery power saving feature.

U-APSD (Unscheduled Automatic Power Save Delivery): Your client devices signal the router to transmit any buffered data.

S-APSD (scheduled Automatic Power Save Delivery): the Access Point will send buffered data based on a predetermined schedule known to the power-saving device without any signal from the station device.

This setting is currently forcefully disabled for unknown reasons in wireless drivers/firmware and has no

functionality.

Spatial Multiplex Power Save

Available Settings: Off, Static

Default Setting: Off

Recommended Setting: Off*

The purpose of Spatial Multiplex Power Save (SM power save) is to allow a MIMO 802.11 device to power down all but one of its radios. For example, a 4×4 MIMO device with four radio chains would power down three of the four radios, thus conserving power.

SM power save defines two methods of operation:

Static, a MIMO client station powers down all the client?s radios except for one single radio. Effectively, the MIMO client station is now the equivalent of a SISO radio that is capable of sending and receiving only one spatial stream. The client uses an SM power save action frame to inform the access point that the MIMO client is using only one radio and is capable of receiving only one spatial stream from the AP.

The SM power save action frame is also used to tell the AP that the client station has powered up all of its radios and now is capable of transmitting and receiving multiple spatial streams once again.

Dynamic, a MIMO client can also power down all but one of the client?s radios but can power up the radios again much more rapidly. The client station disables all but one of the radios after a frame exchange. An access point can trigger the client to wake up the sleeping radios by sending a request-to-send (RTS) frame. The client station receives the RTS frame, powers up the sleeping radios, and sends a clear-to-send (CTS) frame back to the access point. The client can now once again transmit and receive multiple spatial streams. The client uses an SM power save action frame to inform the AP of the client?s dynamic power save state.

- There are several stations, such as a WDS setup, where their TX rates will not return to MIMO rates when under load, thus limiting throughput, so start with this off and test to see if all devices work properly with this on. If dynamic is not in the selection, it means its not supported on the the current router at this time, sadly dynamic is the better of the two.

Noise Immunity

Available Settings: Enable, Disable

Default Setting: Enable

Recommended Setting: Disable*

Controls radio sensitivity in noisy environments by tuning driver parameters from info based on but not limited to, OFDM/CCK errors, beacon RSSI levels, OFDM weak detection, FIRPWR, FIRSTEP_LEVEL, CYCPWR_THR1. The goal of noise immunity is in the name, to help make the router more "immune" to noise, its generally recommended to leave this disabled, only enable if you are an advanced user, are diagnosing various wireless issues, or it fixes a specific issue you were having. Especially if you have multiple Qualcomm Atheros routers connected to each other in any way, its highly recommended to have noise immunity enabled, or disabled on all routers, but not mixed. There has been some reports over the years that disabling noise immunity has helped stabilize the WLAN in terms of throughput &/or reducing dropouts, disabling noise immunity could also result in great or unchanged close range performance, but horrible or no throughput whatsoever, at medium ~ far range, so experiment with this setting. There is also some cases where enabling noise immunity gives abnormally low TX/RX rates & throughput, or noise immunity is simply too aggressive even in low noise, in this case, disable the feature.

**Noise Immunity is a QCA feature meant for QCA clients, so Broadcom clients may not play nice if you enable this feature. If you have a lot of iOS devices in your environment, make sure to disable noise immunity.*

QCA Q-Boost / TDMA support

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable

This setting is only available to routers with QCA99xx chipsets.

This is a completely experimental setting and has been found to significantly lower channel quality and add extra network overhead to perform TDMA. Your client must have the ability to take advantage of this feature. Right now, DON'T play with this unless you really know what you are doing; you will impact the wifi network and spectrum of other devices in the radius of the router using Q-boost. Initial testing shows this feature starts off fine, and then starts to impact wifi & spectrum in a negative fashion (Floods the network & spectrum with overhead noise). BS admits this is an experimental feature which may be removed at some point.

Protection Mode

Available Settings: None, CTS, RTS/CTS

Default Setting: None

Recommended Setting: RTS/CTS* or None for AP modes, & RTS/CTS for client modes

This setting controls whether the **r**equest **t**o **s**end/**c**lear **t**o **s**end 802.11 optional protection mechanism is enabled or disabled. When enabled, an RTS/CTS handshake must be completed before data can be transmitted from clients. Helpful in noisy &/or busy environments, it ensures all clients take turns communicating with the AP, if disabled, packet collisions may occur which causes a drop in throughput & increase in latency due

to retransmission overhead. RTS/CTS also helps negate the hidden node problem which occurs when 2 or more clients can each see the AP & vice versa, but the clients can't see eachother, this example is also good to say why RTS/CTS on an AP has no use, since from the AP's point of view, it can already see all connected clients, or they wouldn't be connected in the first place. CTS only is "CTS-to-self" which has less overhead, but is less effective in mitigating the hidden node issue, only other clients within range of the client using CTS only, will hear & honor it while RTS/CTS is the "full option" that gets passed through the AP to all clients, even if the AP has RTS/CTS disabled since RTS/CTS on the AP only applies to when the AP wants to transmit.

RTS/CTS is a setting to experiment with especially on the client mode interface of the router if you are connecting a router to another router, or if you have high error rate or high noise floor (-90 noise is good, -60 is bad) & all other options have failed. Most users should leave this set to the recommended setting above for max performance because the protection mechanism is only enabled automatically when needed, if its off when its needed, your wireless performance can plummet with errors, disconnects & low throughput, & if its no longer needed its turned off automatically on the fly.

If all that wasn't enough, protection modes also matter depending if you are using any kind of mixed modes such as mixed or NG-mixed, & if the older clients are connected or not. As well if you are using HT40 or VHT80 when there will be clients connected that don't support above HT20. In such case, you MAY want to have some protection mode, but usually with today's routers you are able to mix client types without penalty. If performance is good still without protection, continue to use none.

**Possible Tip-If you have a lot of iOS devices in your environment, make sure to enable RTS/CTS, enable RTS Threshold, and set RTS threshold value to 980.*

RTS Threshold

Available Settings: Enable, Disable

Default Setting: Disable (Enabled is @ 500 & way too low so set to 980)

Recommended Setting: Enable @ 2346 or Disable for AP modes, Enable (980 - 1500, or slightly lower if NEEDED) for client modes

Only valid if RTS/CTS or CTS is enabled, this sets the maximum packet size before the RTS/CTS protection is enabled, if you still have high packet collisions with RTS/CTS enabled and RTS Threshold is at 2346, try lowering it by 10-50 at a time. Lowering it too much can further create overhead and reduce performance as RTS/CTS frames themselves also take up air time & aren't immune to collisions, **a good limit is 980**, going any lower than 600 - 800 & you'll probably spend more air time transmitting & exchanging these frames than the actual data frame themselves, nullifying any benefit it could of provided as a large amount of the client's communication frames to the AP are <500 ~ 600 bytes at a time. Setting this to 2346 theoretically disables the RTS feature and only leaves CTS enabled as most packets don't exceed 2346 bytes.

Short Preamble

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Enable

If you have 802.11b clients in your network you can try enabling this, but if they have problems with performance or connecting, then leave it disabled. Preamble is at the head or front of the PLCP, which devices need in order to start transferring data. The long preamble ensures compatibility with legacy 802.11b devices but will slightly reduce throughput at higher data rates along with possibly introducing WLAN instability &/or overhead. Short preamble support, which is reducing the header's size by 50% down to 9 bytes, is optional for 802.11b. 802.11g & newer all support short preamble as its part of specification, so if you do not have 802.11b devices in your network, or any that you may have work fine with short preamble, leave this enabled at all times.

Short GI

Available Settings: Enable, Disable

Default Setting: Enable

Recommended Setting: Enable

The standard guard interval used in 802.11 OFDM is 0.8 ?s, to increase data rate 802.11n added optional support for a shorter 0.4 ?s guard interval which provides about a 10% increase in data rate. The shorter guard interval could (but usually doesn't) result in a higher packet error rate if timing synchronization between the transmitter and receiver is not precise. To reduce complexity, short guard interval is only implemented as a final rate adaptation step when the device is running at its highest data rate such as 72 Mbps, 144 Mbps, 300 Mbps etc, this is by design & not changeable.

Older routers & devices with Atheros AR92XX radios or older only support short GI on HT40 & not HT20, so max HT20 rates are 65 Mbps/130 Mbps/195 Mbps (1x1/2x2/3x3) instead of 72 Mbps/144 Mbps/217 Mbps respectively. **Some modern devices such as the Playstation 4 do not like the lack of short GI, & have strange performance problems, sometimes completely crippling the entire network's performance.** But the issue may also be related to hardware bugs in the AR92XX chipset, mileage may vary.

Single User Beamforming

Available Settings: Enable, Disable

Default Setting: Enable

Recommended Setting: Enable

Controls whether 802.11ac beamforming is enabled for single user, aka "regular MIMO" connected devices that support beamforming. For 2.4 GHz, beamforming is only supported & broadcasted in beacon info when TurboQAM is enabled.

Multi User Beamforming

Available Settings: Enable, Disable

Default Setting: Enable

Recommended Setting: Disable

Controls whether 802.11ac beamforming is enabled for multi user, "MU-MIMO" connected devices that support beamforming. Since MU-MIMO is a 802.11ac wave 2 feature, all wave 2 devices will support beamforming & MU-MIMO. For 2.4 GHz, beamforming is only supported & broadcasted in beacon info when TurboQAM is enabled and supported by QAM256 clients. MU-MIMO has been found to affect Broadcom clients and might limit them to only a 1x1:1 stream. Play with this at your own risk and check connection rates before and after enabling.

TX & RX Antenna Chains

Available Settings: 1, 1+2, 1+3, 1+2+3, 1+2+3+4 (varies by router)

Default Setting: Varies by router

Recommended Setting: Varies by router

This setting is critical for proper, smooth, fast Wi-Fi performance. 2x2:2 routers will either have TX/RX chains at 1+2/1+2, 1+3/1+3, 1+2/1+3, or 1+3/1+2. This can take some time to find the proper setting but its worth it, you can more easily find the correct setting by using a 802.11n client thats capable of 300 Mbps link. Note the TX/RX link rates on the wireless status page, when set incorrectly one or both of the rates will drop to a much lower speed such as 200, 170, 81 etc. This is best done with the client less than 10 feet from the AP with clear line of sight. Some routers with chains set incorrectly such as D-Link DIR-615 C1, will deny connections to clients, heavily reduce throughput, and other errors. Searching the FCC ID of your router will aid in setting the correct chain settings. Some popular routers such as the Netgear WNDR3700 v1/2/4 and D-Link DIR-825 B1/B2 require both chains set at 1+2 for proper Wi-Fi performance. **Default is not always right!***

**With builds around r21061 or later, most units have the proper defaults preset & invalid options removed, such as 1+2+3 for TX/RX on WNDR3700 v1, v2, & v4 as the router only has 2 chains each therefor only has 1 & 1+2 available to be selected. While a TL-WDR4900 v1.3 & v2 have 1+2+3 as they are 3x3:3 units. An example 4x4:4 unit is the R7800.*

AP Isolation

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable for private home Wi-Fi with trusted users, enable for public/guest Wi-Fi hotspot

AP Isolation allows clients connected to the same AP to communicate with each other or not, very much like Ad-Hoc mode. If you run a public Wi-Fi hotspot its recommended you enable this for privacy/security reasons & to help mitigate Wi-Fi snooping attacks that reveal login info such as this. If you want files to be shared from client to client in your home network, AP isolation must be disabled. This setting does not influence Wi-Fi throughput. **If this setting is enabled it will break AdHoc based play on gaming devices such as Nintendo's DS system.**

Beacon Interval

Available Settings: 15 ~ 65535

Default Setting: 100

Recommended Setting: 50 ~ 300 for 2.4 GHz & 75 ~ 250 for 5 GHz

A beacon frame, measured in milliseconds (ms), is one of the management frames in IEEE 802.11 WLANs. It contains all the information about the network & has a close relationship to the setting below it, DTIM interval. Beacon frames are transmitted periodically by the AP in an infrastructure BSS to announce the presence of a WLAN. Reducing beacon interval may help WLAN performance in noisy environments &/or with problematic clients such as some mobile tablets & phones but will decrease battery life. 100 is a typical default beacon setting but up to 250, even 300 can also work too more often than not. Increasing beacon interval would slightly reduce overhead & increase battery life, but possibly make the network more sensitive to noise & dropouts with buggy clients. "Overhead" when referring to beacon interval is airtime, beacons themselves also take up airtime which means less availability for data. For 5 GHz some routers default to 200 beacon interval such as the DIR-825 B1 stock firmware, DD-WRT default is 100 for both bands. Remember to adjust DTIM interval below, when changing beacon interval in order to keep the same DTIM period.

DTIM Interval

Available Settings: 1 ~ 255

Default Setting: 2

Recommended Setting: 2 ~ 5 (assuming default beacon interval of 100 is used)

Default being 2, the **d**elivery **t**raffic **i**ndication **m**essage (DTIM) is an element included in some beacon

frames. It notifies the client stations that are currently in low-power mode that data buffered on the access point is awaiting pickup. The DTIM interval indicates how often clients serviced by the access point should check for buffered data, the buffered data is usually multicast/broadcast data. You specify DTIM in number of beacons. If you set this value to 2, clients check for buffered data on the AP on every beacon. If you set this value to 10, clients check the access point on every 10th beacon, this is assuming beacon interval is at the default of 100. 100 beacon & 1 DTIM = every beacon that occurs every 0.1 seconds will have a DTIM with it, beacon of 50 with 2 DTIM also = every beacon that occurs every 0.1 seconds will have a DTIM with it, & so on. More beacons/DTIMs in a shorter period can help multicast performance but hurt battery, less beacons/DTIM in a longer period may harm multicast performance, but help battery. The defaults are a good medium & are commonly used by stock firmwares on cheap & expensive routers world wide, this setting will require extensive testing if you wish to alter it.

Airtime Fairness

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Enable

Airtime Fairness is a feature that boosts the overall network performance by sacrificing a little bit of network time on your slowest devices (A/B/G, even N when compared to AC). The slower Wi-Fi devices can be slow from either long physical distance, weak signal strength, or simply being a legacy device using an older standard. Example; Device A, functioning at 1 Mb/s and a faster device, B, that transmits at 5 Mb/s. If A needs to transmit 10 Mb of data, it will take 10 seconds. This means that for B to start data transmission after A, it may need to wait the full 10 seconds before A finishes it's transmission. Airtime fairness will give each device a fair amount of time. Instead of mostly or all air time to one device.

Frame Compression

Available Settings: Disabled, LZO, LZ4, LZMA

Default Setting: Disabled

Recommended Setting: Disabled (does not currently function regardless of setting)

Compresses Wi-Fi packets using any of the offered standard compression algorithms. Smaller frames over the air means less airtime which could result in more performance, but beware compression uses CPU time, weaker CPU + higher (AC+) rates will be taxing on the CPU and a CPU too slow will instead make performance &/or latency worse.

This setting is still currently broken and does not function.

WMM Support

Available Settings: Enable, Disable

Default Setting: Enable

Recommended Setting: Enable

Short for Wi-Fi Multimedia, is a Wi-Fi Alliance interoperability certification that provides a basic QoS "best effort" like function to Wi-Fi as well as other functions such as power saving, its a requirement & part of the 802.11n (& newer) specification. Disabling WMM will result in clients (ones that strictly obey specifications which is 90% of them) falling back to 802.11a/g rates (54M), the same way as using TKIP with WPA2 does.

Radar Detection

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disabled for most users. Enabled to comply with regulations where applicable.

Radar detection (AKA DFS: Dynamic Frequency Selection), if enabled, will change the frequency only when it identifies a military or doppler weather radar nearby on the same frequency. Most users shouldn't have any interference issues even those living near such locations. This applies to 5 GHz a/n/ac only.

ScanList

Default Setting: default

The frequency range in MHz, to be used by wireless radio (superchannel use requires this as they are non standard channels) & when searching for nearby APs, seperated by a dash (ie: "2600-2700" without quotes). Specially useful when using SuperChannel feature. Leave this at the default value (empty) unless you know what it does.

Sensitivity Range (ACK Timing)

Available Settings: 0 (auto ACK- athk9k only) ~ 999999 (meters)

Default Setting: 2000 (which likely defaults to 2250)

Recommended Setting: 450, or up to 1350* for both bands, greater than 2250 (default) only when **needed** for long distance link. **"0"** uses auto ACK mode on ath9k chipsets, it dynamically changes to try and settle on what the driver thinks is best, which may become too high, and may cause bad Wi-Fi performance. Using auto

ack for long distances is recommended. For indoor/home use it may cause issues due to noise and reflections. For ath10k, the chipset presently can't auto-tune the ack timing and will default to whatever is baked into the firmware by QCA: 450m. BS is still working on the code for ath10k to make it dynamically tune-able. Using **"0"** on ath10k chipsets will cause the GUI to show N/A under the wifi status window; but, the chipset is using the value baked in to the firmware: 450m.

ACK timing too low, with clients further away, causes re-transmissions which create overhead,which lowers throughput. The AP sends a packet and all clients must wait for XXX time, where XXX is the ACK timing, the client then receives that packet and responds to the AP with an ACK(nowledgement), AP sees the client then finally everyone is free to transmit again.

From BS: "Setting a too high ACK value is never a problem and its unrelated to chipsets. All chipsets use ack timing mechanisms. Just not every chipset allows you to configure it; thus, it has no compatibility issues between QCA & Broadcom chipsets. If my AP sends a packet and the packet does not get a response, within the specified ack timing (ack timing is a round trip internally), it gets re-transmitted. So, if you set a too high ack timing, but you have very bad signal conditions, it will decrease the performance a little bit since it waits longer until a re-transmission occurs. However, if you set a too low setting (important at long range links) almost every packet gets re-transmitted which leads to massive packet loss. In most cases you cannot even authenticate with wpa."

Most users want this at 450 or 900, or up to 2250, the distance used is meters and needs to be doubled the distance of the furthest client from the AP (plus some headroom). Doubled because the signal travels to the client and back, double the distance. In earlier builds with the older MADWIFI driver reducing ACK from default 2000 to 1500 gave a throughput increase of 0.5 Mbps - 1 Mbps. With the current ath9k builds, an ACK timing of **0** is now auto ACK mode, which you do not want to use for indoor/home use, use a fixed setting. But remember ACK timing too low can cause issues such as cutting off a still in progress transmission, causing a re-transmission that half way to the destination, clashes with the returning ACK of the first transmission, when the device is beyond the current set ACK range. This usually only happens with hidden nodes &/or clients that are distanced very far away/beyond ACK timing's set range but not always.

Long distance links, such as 4 KM+ will need to increase this setting accordingly. 4000m for 2km, 6000m for 3km, and so on, its good practice to add a little more ~5% or so, than the exact needed value to account for any overhead (CTS etc).

- Current ath9k firmware only uses ACK timing in 450m intervals when using **"0"** (auto ACK),: so 450, 900, 1350, 1800, 2250 & so on. You can set any value you want, but the value may not stick depending on the chipset and ath9k will revert to a multiple of 450. For Ath10k, you can set any value you want, but if you use **0** then it will use the chipset firmware default of 450, so don't use **0** for long length transmission on ath10k. For most home/indoor use, 450m (225m one way/729ft one way) should be far enough. To be safe use a higher value like 900, or up to 2250.

- 802.11g mode with a DWA-542 NIC got 21 Mbps with default 2250m on a TL-WDR4900 v1.3 with the latest build as of this posting (r27240), with ACK at 900m that rose to 22 Mbps & is mostly repeatable. Your results will vary depending on router, channel, clients & interference. Users in heavy interference areas may benefit from leaving ACK timing slightly higher (such as 900 instead of 450 etc), since there will be an increased number of clashed packets & retransmissions.

Minimum Signal for authenticate

Available Settings: -128 ~ 0

Default Setting: -128

Recommended Setting: Default for having the feature disabled, or enter any minimum value if desired

This setting is for the minimum (weakest) signal allowed with a client device to be allowed to authenticate (security check) with the router. If the signal is below (EG: -60 is weaker than -45) the specified value, the client device will be denied.

Minimum Signal for connection

Available Settings: -128 ~ 0

Default Setting: -128

Recommended Setting: Default for having the feature disabled, or enter any minimum value if desired

Exactly the same function as minimum signal for authentication, but for allowing connection, after authentication.

Poll Time for signal lookup

Available Settings: 1 ~ 3600

Default Setting: 10

Recommended Setting: Whatever suits you

This is the interval in seconds, that the router checks client device signal & compares the result to the specified minimum allowed signal to decide if the device should be kicked from the network or not.

Amount of allowed low signals

Available Settings: 1 ~ 60

Default Setting: 3

Recommended Setting: Whatever suits you

This setting specifies how many times or "strikes" a device can get, before the specified minimum signal rules are enforced. EG: If defaults are used except minimum signal is -50 for both, if a device is detected having a signal lower than -50 X number of times over the specified value for this setting, the device will be disconnected from the router. Like a "X amount of strikes and you are out" rule.

Max Associated Clients

Available Settings: 1 ~ 256

Default Setting: 128 ~ 256 (varies by router)

Recommended Setting: What suits you

Determines the maximum number of clients that can be connected to the AP at any given time. Hotspot users will find this very handy. Using a shorter DHCP lease time such as 2 ~ 12 hours instead of default 24 will also help free up IPs if you are finding 256 users is not enough for a large public hotspot.

MTik Compatibility

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable

It activates a beta WDS compatibility with Mikrotik RouterOS. It's almost useless. Only use it when you're testing stuff from DD-WRT or using Mikrotik RouterOS.

Multicast To Unicast

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable

Request that the AP will do multicast-to-unicast conversion for ARP, IPv4, and IPv6 frames. If enabled, such frames are to be sent to each station separately, with the DA replaced by their own MAC address rather than the group address. Note that this may break certain expectations of the receiver, such as the ability to drop unicast IP packets received within multicast L2 frames, or the ability to not send ICMP destination unreachable messages for packets received in L2 multicast (which is required, but the receiver can't tell the difference if this new option is enabled). Enable only if you have issues detecting devices on the network that

are connected over Wi-Fi, such as security camers, printers, and any type of "Smart" devices.

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

802.11r / Fast BSS Transition

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable*

In the early days of 802.11, handoff was a much simpler task for the mobile device. Only four messages were required for the device to establish a connection with a new access point (five if you count the optional "I'm leaving" message (deauthentication and disassociation packet) the client could send to the old access point). However, as additional features were added to the standard, including 802.11i with 802.1X authentication and 802.11e or WMM with admission control requests, the number of messages required went up dramatically. During the time these additional messages are being exchanged, the mobile device's traffic, including that from voice calls, cannot proceed, and the loss experienced by the user could amount to several seconds. Generally, the highest amount of delay or loss that the edge network should introduce into a voice call is 50 ms. This means that your wifi call would be dropped moving from AP to AP because the handshake to the new AP takes too long.

802.11r was launched to attempt to undo the added burden that security and quality of service added to the handoff process, and restore it to the original four-message exchange. In this way, handoff problems are not eliminated, but at least are returned to the status quo.

The primary application currently envisioned for the 802.11r standard is voice over IP (VOIP) via mobile phones designed to work with wireless Internet networks, instead of (or in addition to) standard cellular networks.

When you enable this feature the gui will load some new values to fill in: NAS Identifier & Mobility Domain.

NAS Identifier

The NAS ID is your router's wireless radio's MAC address without the **":"**;so 12:34:56:78:90:AA would be entered as 1234567890AA.

Mobility Domain

The Mobility domain is a 4 digit hex key you can make up. Just use 0013 for now. More research needs to go in to what these values really "should" be and why.

If the wifi is going to be on the same subnet &/or vlan, make sure to use the same mobility domain value for both radios; and, make sure the mobility domain is different from the other wifi vlan you might end up implementing.

802.11w Frame Protection

Available Settings: Enable, Disable, Auto

Default Setting: Disable

Recommended Setting: Disable

If you use 802.11r, this feature is broken and won't work. Right now don't use this feature unless you know what you are doing.

Disable EAPOL Key Retries

Available Settings: Enable, Disable

Default Setting: Disable

Recommended Setting: Disable

An AP-side workaround for key reinstallation attacks (KRACK), this option can be used to mitigate KRACK on the station side (router), to help protect client devices that no longer receive updates, or receive updates very slowly. Since many devices out there will not receive an update anytime soon (if at all), it makes sense to include this workaround. Unfortunately this can cause interoperability issues and reduced robustness of key negotiation, hence the default setting of disabled. This workaround is NOT needed on current builds (newer than r33555) & if you know that your client devices are updated to patch KRACK on them already, or if the vulnerability doesn't bother you. KRACK is already fixed in DD-WRT "properly" in both AP mode, & station mode (client/client bridge/WDS).