## Contents



# Disabled

- No encryption.

# WPA

- Implements the majority of IEEE 802.11i, but with different headers (so can operate both in same network).
- Designed to require only a firmware upgrade (full 802.11i usually requires hardward change).
- As designed, WPA uses TKIP and Michael for message integrity, based on RC4 for encryption.

## Pre-shared (personal) vs Enterprise (RADIUS)

Defines the type of authentication used.

- WPA (and WPA2) may operate in enterprise mode, using a RADIUS server to hold per-user keys. This allows individual access to be controlled in a large network.
- For a small network, e.g. home network, without a RADIUS server a pre-shared key (PSK) may be used. The same key is used by all clients, so may require more work to update.

## TKIP vs AES-based CCMP

Defines the algorithm used for message integrity and confidentiality.

- WPA was designed to be used with TKIP (and WPA2 designed to use stronger AES-based).
- However, some devices allow WPA (not WPA2) with AES (and WPA2 with TKIP).
- AES is optional in WPA; in WPA2 both AES is mandatory, but TKIP is optional.

- Note that TKIP is not directly comparable to AES; TKIP is an integrity check, AES is an encryption algorithm. In the context of wireless security this actually means TKIP vs "AES-based CCMP" (not just AES).

TKIP is a lower end encryption protocol (WEP2) and AES is a higher end (WPA2/802.11i) encryption protocol. AES is preferred.

### TKIP+AES

This is what the encryption standards are for WEP2 (TKIP) and WPA2/802.11i (AES). It will attempt to use AES if available and fall back to TKIP if not. This setting offers the most compatability but won't guarentee a higher level of encryption if a device falls back to TKIP.

## WPA2, aka 802.11i

- Fully conforms with 802.11i as it implements all mandatory features.
- Guarantees interoperability certification.
- Effectively WPA2 is Wi-Fi Alliance's brand name for 802.11i.
- Note: In some cases other optional features of 802.11i may be required, but interoperability may not be guaranteed.
- Support for AES encryption and AES-based CCMP message integrity is mandatory (is optional in WPA).
- As well as mandatory AES, WPA2 also adds PMK (Pair-wise Master Key) and Pre-authentication to help fast roaming.

### EAP options

- Authentication options for 802.11i.
- Two initial types - pre-shared key (personal) or RADIUS (enterprise), same as per WPA.
- Additional types of enterprise authentication types now available (usually not relevant for home users).

### AES-based CCMP

- WPA2 mandates AES-based CCMP for message integrity and confidentiality.
- TKIP (weaker) is optional.

### WPA2 mixed

- Mixed mode allows device to try WPA2 first, and if that fails fall-back to WPA.

# WEP

WEP was supposed to provide Confidentiality, but has found to be vulnerable and should no longer be used.

- Has been found to be vulnerable.
- Is often the default; this should be changed.
- Most devices that support WEP can be firmware/software upgraded to WPA.
- Do not use unless some devices can not be upgraded to support WPA.

WEP has been outdated for years and has better replacements. The 40-bit encryption is just not strong enough to keep data secure and can be broken rather easily. Newer encryption methods use stronger encryption and have yet to be broken while WEP can be broken in a minute according to this resource.

Use WPA where possible.

# Preference Summary

To keep things simple, the best options, in decreasing order of preference, may be:

1. WPA2 + AES
2. WPA + AES (only if all devices support it).
3. WPA + TKIP+AES (only if all devices can support it).
4. WPA + TKIP
5. WEP (will only keep out people with none or poor experience in computers)
6. Disabled (no security)

The most common two options will be WPA2 + AES and WPA + TKIP, because they match the mandatory requirements in the standards (WPA2 requires AES, WPA requires TKIP).

You can use WPA + AES for higher security than TKIP, but only if your devices support it (it is optional). For this reason it is not very common. You also do not get the improved roaming features of WPA2.

WPA + TKIP+AES provides a fallback in case AES is not supported by a device in that it switches to the more common TKIP. The disadvantage is that it might switch to TKIP unexpectedly but is more backwards compatable if needed.

Currently TKIP has no known vulnerabilities, so for broadest compatibility stick with WPA + TKIP.

The remaining combination, WPA2 + TKIP, is possible (as TKIP is optional in WPA2), but doesn't make much sense because AES is more secure and mandatory for all WPA2 devices.

*[Comment added 12/04/07 by mithrill]]*

I've created some very detailed how-to instructions for Securing Your Wireless Network on my site with lots of screen captures. I wanted to contribute to the DD-WRT community in some way in appreciation of everyone's hard work. Due to the extent of my directions, I couldn't post them on this Wiki. Hopefully these instructions will provide help to everyone in the community. Check them out at http://www.mandladventures.com/2007/04/21/securing-your-wireless-network/ but don't forget to read all of

the other great stuff already included on this Wiki.

# SSID

The SSID is what the router broadcasts as the name of the network. All wireless networking products have the option of broadcasting the SSID or not. This should not be viewed as a form of security however as wireless sniffers can detect this anyway. It might be useful to hide SSIDs for some reasons but this should always be used with a high level of encryption where possible.

# Mixed Security Modes

It seems possible (at least on the Linksys WRT160NL) to have mixed WEP and WPA security. Having mixed WEP keys does not seem to work.