hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator

hostapd is a user space daemon for access point and authentication servers. It implements IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/EAP Authenticators, RADIUS client, EAP server, and RADIUS authentication server. The current version supports Linux (Host AP, madwifi, mac80211-based drivers) and FreeBSD (net80211).

hostapd is designed to be a "daemon" program that runs in the background and acts as the backend component controlling authentication. hostapd supports separate frontend programs and an example text-based frontend, hostapd_cli, is included with hostapd.

Supported WPA/IEEE 802.11i/EAP/IEEE 802.1X features

- WPA-PSK ("WPA-Personal")
- WPA with EAP (with integrated EAP server or an external RADIUS backend authentication server) ("WPA-Enterprise")
- key management for CCMP, TKIP, WEP104, WEP40
- WPA and full IEEE 802.11i/RSN/WPA2
- RSN: PMKSA caching, pre-authentication
- IEEE 802.11r
- IEEE 802.11w
- RADIUS accounting
- RADIUS authentication server with EAP
- Wi-Fi Protected Setup (WPS)

Supported EAP methods (integrated EAP server and RADIUS authentication server)

- EAP-TLS
- EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)
- EAP-PEAP/TLS (both PEAPv0 and PEAPv1)
- EAP-PEAP/GTC (both PEAPv0 and PEAPv1)
- EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)
- EAP-TTLS/EAP-MD5-Challenge
- EAP-TTLS/EAP-GTC
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/EAP-TLS
- EAP-TTLS/MSCHAP
- EAP-TTLS/PAP
- EAP-TTLS/CHAP
- EAP-SIM
- EAP-AKA
- EAP-AKA'
- EAP-PAX
- EAP-PSK
- EAP-SAKE
- EAP-FAST
- EAP-IKEv2
- EAP-GPSK

Following methods are also supported, but since they do not generate keying material, they cannot be used with WPA or IEEE 802.1X WEP keying.

- EAP-MD5-Challenge
- EAP-MSCHAPv2
- EAP-GTC
- EAP-TNC (Trusted Network Connect; TNCS, IF-IMV, IF-T, IF-TNCCS)

More information about EAP methods and interoperability testing is available in eap_testing.txt.

Supported wireless cards/drivers

- Linux mac80211 drivers
- Linux drivers that support nl80211/cfg80211 in AP mode
- Host AP driver for Prism2/2.5/3
- madwifi (Atheros ar521x)
- BSD net80211 layer (e.g., Atheros driver) (FreeBSD 6-CURRENT)

Download

hostapd

Please see README for the current documentation.

- Release graph
- Latest release:
  - hostapd-2.10.tar.gz (PGP signature)
- ChangeLog:
  - development branch and 2.x releases
- Old releases
- Mailing list (NOTE: New server taken into use in October 2015. Subscriber list from the old server was not transferred, so you will need to subscribe again.
- New mailing list archives (10/2015-)
- Old mailing list archives (10/2002-10/2015)
- Web interface to GIT repository
- Snapshot releases from all active branches
- GIT access
- Developers' documentation for wpa_supplicant/hostapd
- Requirements for contributions to the project
- Security advisories

WPA

The original security mechanism of IEEE 802.11 standard was not designed to be strong and has proven to be insufficient for most networks that require some kind of security. Task group I (Security) of IEEE 802.11 working group has worked to address the flaws of the base standard and in practice completed its work in May 2004. The IEEE 802.11i amendment to the IEEE 802.11 standard was approved in June 2004 and published in July 2004.

Wi-Fi Alliance used a draft version of the IEEE 802.11i work (draft 3.0) to define a subset of the security enhancements that can be implemented with existing wlan hardware. This is called Wi-Fi Protected Access (WPA). This has now become a mandatory component of interoperability testing and certification done by Wi-Fi Alliance. Wi-Fi has information about WPA at its web site.

IEEE 802.11 standard defined wired equivalent privacy (WEP) algorithm for protecting wireless networks. WEP uses RC4 with 40-bit keys, 24-bit initialization vector (IV), and CRC32 to protect against packet forgery. All these choices have proven to be insufficient: key space is too small against current attacks, RC4 key scheduling is insufficient (beginning of the pseudorandom stream should be skipped), IV space is too small and IV reuse makes attacks easier, there is no replay protection, and non-keyed authentication does not protect against bit flipping packet data.

WPA is an intermediate solution for the security issues. It uses Temporal Key Integrity Protocol (TKIP) to replace WEP. TKIP is a compromise on strong security and possibility to use existing hardware. It still uses RC4 for the encryption like WEP, but with per-packet RC4 keys. In addition, it implements replay protection, keyed packet authentication mechanism (Michael MIC).

Keys can be managed using two different mechanisms. WPA can either use an external authentication server (e.g., RADIUS) and EAP just like IEEE 802.1X is using or pre-shared keys without need for additional servers. Wi-Fi calls these "WPA-Enterprise" and "WPA-Personal", respectively. Both mechanisms will generate a master session key for the Authenticator (AP) and Supplicant (client station).

WPA implements a new key handshake (4-Way Handshake and Group Key Handshake) for generating and exchanging data encryption keys between the Authenticator and Supplicant. This handshake is also used to verify that both Authenticator and Supplicant know the master session key. These handshakes are identical regardless of the selected key management mechanism (only the method for generating master session key changes).

IEEE 802.11i / RSN / WPA2

The design for parts of IEEE 802.11i that were not included in WPA has finished (May 2004) and this amendment to IEEE 802.11 was approved in June 2004. Wi-Fi Alliance is using the final IEEE 802.11i as a new version of WPA called WPA2. This included, e.g., support for more robust encryption algorithm (CCMP: AES in Counter mode with CBC-MAC) to replace TKIP, optimizations for handoff (reduced number of messages in initial key handshake, pre-authentication, and PMKSA caching).

Configuration file

hostapd is configured using a text file that lists all the configuration parameters. See an example configuration file, hostapd.conf, for detailed information about the configuration format and supported fields.

Feedback, comments, mailing list

Any comments, reports on success/failure, ideas for further improvement, feature requests, etc. are welcome at j@w1.fi. Please note, that I often receive more email than I have time to answer. Unfortunately, some messages may not get a reply, but I'll try to go through my mail whenever time permits.

Host AP mailing list can also be used for topics related to hostapd. Since this list has a broader audience, your likelihood of getting responses is higher. This list is recommended for general questions about hostapd and its development. In addition, I will send release notes to it whenever a new version is available.

The mailing list information and web archive is at http://lists.infradead.org/mailman/listinfo/hostap. Messages to hostap@lists.infradead.org will be delivered to the subscribers. Please note, that due to large number of spam and virus messages sent to the list address, the list is configured to accept messages only from subscribed addresses.

Jouni Malinen
Last modified: Sat Jan 12 18:05:23 EET 2013