IEEE 802.11s

From Wikipedia, the free encyclopedia

IEEE 802.11s is Wireless LAN standard and an IEEE 802.11 amendment for mesh networking, defining how wireless devices can interconnect to create a WLAN mesh network, which may be used for relatively fixed (not mobile) topologies and wireless ad hoc networks. The IEEE 802.11a working group taps on volunteers from universities and industries to provide specifications and possible design solutions for wireless mesh networking. As a standard, the document was iterated and revised many times prior to finalization.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac versions to provide wireless connectivity in the home, office and some commercial establishments.

Contents

Description

802.11s extends the IEEE 802.11 MAC standard by defining an architecture and protocol that supports both broadcast/multicast and unicast delivery using "radio-aware metrics over self-configuring multi-hop topologies."

Closely related standards

802.11s inherently depends on one of 802.11a, 802.11b, 802.11g or 802.11n carrying the actual traffic. One or more routing protocols suitable to the actual network physical topology are required. 802.11s requires Hybrid Wireless Mesh Protocol, or HWMP,[1] be supported as a default. However, other mesh, ad hoc (Associativity-Based Routing, Zone Routing Protocol, and location based routing) or dynamically link-state routed (OLSR, B.A.T.M.A.N.) may be supported or even static routing (WDS, OSPF). *See the more detailed description below comparing these routing protocols.*

A mesh often consists of many small nodes. When mobile users or heavy loads are concerned, there will often be a handoff from one base station to another, and not only from 802.11 but from other (GSM, Bluetooth, PCS and other cordless phone) networks. Accordingly, IEEE 802.21, which specifies this handoff between nodes both obeying 802.11s and otherwise, may be required. This is especially likely if a longer-range lower-bandwidth service is deployed to minimize mesh dead zones, e.g. GSM routing based on OpenBTS.

Mesh networking often involves network access by previously unknown parties, especially when a transient visitor population is being served. Thus the accompanying IEEE 802.11u standard will be required by most mesh networks to authenticate these users without pre-registration or any prior offline communication. *Pre-standard captive portal approaches are also common. See the more detailed description below of mesh security.*

Timeline

802.11s started as a Study Group of IEEE 802.11 in September 2003. It became a Task Group in July 2004. A call for proposals was issued in May 2005, which resulted in the submission of 15 proposals submitted to a vote in July 2005. After a series of eliminations and mergers, the proposals dwindled to two (the "SEE-Mesh" and "Wi-Mesh" proposals), which became a joint proposal in January 2006. This merged proposal was accepted as draft D0.01 after a unanimous confirmation vote in March 2006.

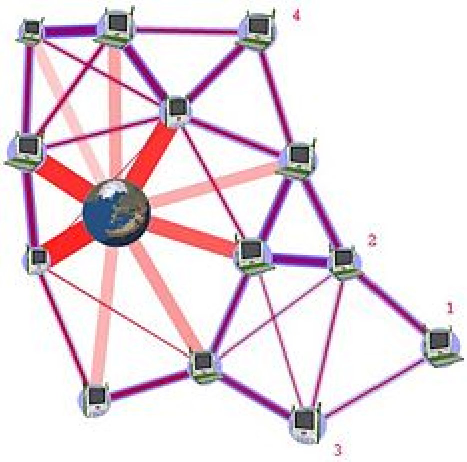
The draft evolved through informal comment resolution until it was submitted for a Letter Ballot in November 2006 as Draft D1.00. Draft D2.00 was submitted in March 2008 which failed with only 61% approval. A year was spent clarifying and pruning until Draft D3.00 was created which reached WG approval with 79% in March 2009.

The Task Groups stated goal for the May 2009 802.11 meeting is to start resolving comments from its new Letter Ballot.

In June 2011 the fifth recirculation Sponsor Ballot, on TGs Draft 12.0, was closed. The Draft met with 97.2% approval rate.[2]

The 2012 release of the 802.11 specification (802.11-2012)[3] directly incorporates Mesh Routing functionality. The IEEE page for 802.11s lists that specification as superseded.

802.11 mesh architecture



A wireless mesh network architecture allowing otherwise out-of-range nodes 1–4 to still connect to the Internet. A key characteristic is the presence of multiple-hop links and using intermediate nodes to relay packets for others.

An 802.11s wireless mesh network device is labelled as Mesh Station (mesh STA), or simply an ad hoc node. Mesh STAs form mesh links with one another, over which mesh paths can be established using an ad hoc mobile routing protocol. A key aspect of this architecture is the presence of multi-hop wireless links and routing of packets through other nodes towards the destination nodes.

Routing protocols

This should be expanded into a treatment of all the compatible routing protocols.

802.11s defines a default mandatory routing protocol (Hybrid Wireless Mesh Protocol, or HWMP),[1] yet allows vendors to operate using alternate routing protocols. HWMP is inspired by a combination of AODV (RFC 3561[4]), which uses on-demand ad hoc routing approach and tree-based routing. Examples of on-demand ad hoc routing are Dynamic Source Routing and Associativity-Based Routing. AODV route discovery and localized route repair approaches are identical to Associativity-based Routing. Prior work[5][6][7][8] has discussed and compared these various routing protocols in detail.[9]

Mesh STAs are individual devices using mesh services to communicate with other devices in the network. They can also collocate with 802.11 Access Points (APs) and provide access to the mesh network to 802.11 stations (STAs), which have broad market availability. Also, mesh STAs can collocate with an 802.11 portal that implements the role of a gateway and provides access to one or more non-802.11 networks. In both cases, 802.11s provides a proxy mechanism to provide addressing support for non-mesh 802 devices, allowing for end-points to be cognizant of external addresses.

802.11s also includes mechanisms to provide deterministic network access, a framework for congestion control and power save.

Mesh security

There are no defined roles in a mesh — no clients and servers, no initiators and responders. Security protocols used in a mesh must, therefore, be true peer-to-peer protocols where either side can initiate to the other or both sides can initiate simultaneously.

Peer authentication methods

Between peers, 802.11s defines a secure password-based authentication and key establishment protocol called "Simultaneous Authentication of Equals" (SAE). SAE is based on Diffie–Hellman key exchange using finite cyclic groups which can be a primary cyclic group or an elliptic curve.[10] The problem on using Diffie–Hellman key exchange is that it does not have an authentication mechanism. So the resulting key is influenced by a pre-shared key and the MAC addresses of both peers to solve the authentication problem.

When peers discover each other (and security is enabled) they take part in an SAE exchange. If SAE completes successfully, each peer knows the other party possesses the mesh password and, as a by-product of the SAE exchange, the two peers establish a cryptographically strong key. This key is used with the "Authenticated Mesh Peering Exchange" (AMPE) to establish a secure peering and derive a session key to protect mesh traffic, including routing traffic.

Usage

IEEE 802.11s amendment is supported by many products, mostly for smaller meshes of under 32 nodes. Some of the projects are based on earlier (draft) versions.

Linux

A reference implementation of the 802.11s draft is available as part of the mac80211 layer in the Linux kernel, starting with version 2.6.26.[11] The Linux community, with its many diverse distributions, provides a heterogenous testing ground for protocols like Hybrid Wireless Mesh Protocol.[12] OpenWrt, a Linux distribution for routers, supports mesh networking.[13] . [14]

BSD

In FreeBSD, 802.11s draft is supported starting with FreeBSD 8.0.[15]

Google Wifi

The Google Wifi router uses the 802.11s mesh networking protocol.[16]

See also

- Wireless mesh network
- Wireless ad hoc networks
- List of ad hoc routing protocols
- Mobile ad hoc network

References

1. "HWMP Protocol specification" (https://mentor.ieee.org/802.11/public/06/11-06-1778-01-000s-hwmp-specification.doc). The Working Group for WLAN Standards of the Institute of Electrical and Electronics Engineers. November 2006. Retrieved 2009-05-03.
2. "IEEE P802.11 - TASK GROUP S - MEETINGS UPDATE" (http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm). Retrieved 2012-01-02.
3. 2012 release of the 802.11 specification (802.11-2012) (http://standards.ieee.org/findstds/standard/802.11-2012.html)
4. "RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing" (http://www.ietf.org/rfc/rfc3561.txt). Mobile Ad Hoc Networking Working Group of the Internet Engineering Task Force. July 2003. Retrieved 2007-03-03.
5. "A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Network - S J Lee, et. al., 1999." (https://pdfs.semanticscholar.org/dc3f/55dcf147a71e1bfb9f1327d70b27cfda259a.pdf) (PDF).
6. "Performance Comparison of AODV, TODV, OLSR and ABR using OPNET - E. Nehra & J. Singh" (https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0358.pdf) (PDF).
7. "Compare the Performance of the Two Prominent Routing Protocols for Mobile Ad-hoc Networks" (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.6049&rep=rep1&type=pdf).
8. "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, 1999" (https://www.cs.cmu.edu/~dga/15-849/papers/royer-adhoc1999.pdf) (PDF).
9. "Routing Protocols for Ad Hoc Mobile Wireless Networks by Padmini Misra" (http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/).
10. "IEEE Xplore - Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks" (http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4622764). Retrieved 2011-10-14.
11. "Linux 2.6.26 Changes" (http://kernelnewbies.org/Linux_2_6_26#head-26b4a3f6eb606c21056e4f906a4dae88077346f5). Retrieved 2008-07-14.
12. "802.11s" (http://linuxwireless.org/en/developers/Documentation/ieee80211/802.11s). Linux Wireless.
13. "Mesh/OpenWRT" (https://sudoroom.org/wiki/Mesh/OpenWRT). Retrieved 2014-07-31.
14. BattleMesh contributors. "BattleMeshV7" (http://battlemesh.org/BattleMeshV7). Retrieved 2014-07-31.
15. "WifiMesh — FreeBSD Wiki" (http://wiki.freebsd.org/WifiMesh). Retrieved 2009-09-04.
16. "Making a 'mesh' of your Wi-Fi" (https://blog.google/products/google-wifi/making-mesh-your-wi-fi/). Retrieved 2016-11-16.

External links

- Status of 802.11s
- Open80211s.org
- WifiMesh - FreeBSD Wiki

Retrieved from "https://en.wikipedia.org/w/index.php?title=IEEE_802.11s&oldid=799430170"

- This page was last edited on 7 September 2017, at 17:53.
-