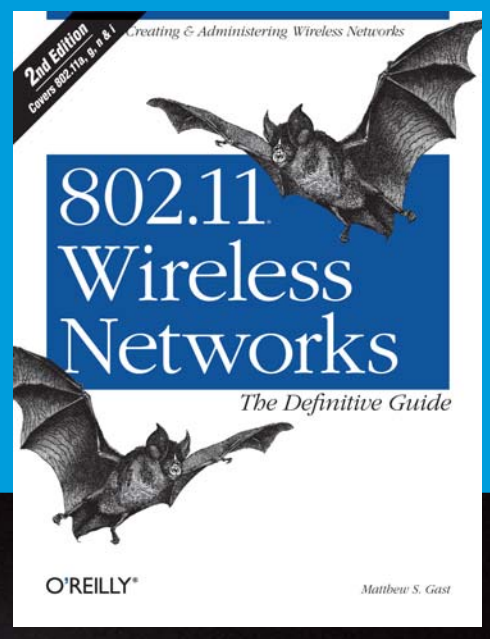
Matthew Gast's 802.11 Protocol Map



802.11 Wireless Networks: The Definitive Guide, 2nd Edition
By Matthew Gast
ISBN 0-596-10052-3, $44.95

Back End Databases

EAP-SIM, EAP-AKA: Mobile Telephone Networks
Token Card: PAP, EAP-GTC
PKI: X.509 Certificate Validation
Active Directory NT Domain: MS-CHAP-V2
LDAP Directory: PAP, EAP-GTC
Billing and Record Keeping
Local Database
RADIUS accounting RFC 2866
Radius Proxy RFC 2865 section 2, RFC 2607-policy

Remote Authentication Dial-In User Service (RADIUS)
802.1X-RADIUS guidelines-RFC 3580
RADIUS-RFC 2865

Tunneled TLS (TTLS) Internet-Draft: attribute/value pair (AVP) exchange; TLS
Protected EAP (PEAP) Internet-Draft: inner EAP exchange; TLS
EAP-RFC 3748
EAP-TLS RFC 2716 (Based On TLS, RFC 2246)

EAP-Method Interface

802.1X Extensible Authentication Protocol (EAP) Over LAN (EAPOL)
EAPoL-802.1X clause 7

Key Derivation from TLS Master Secret

TCP/IP Protocol Suite
Ethertypes
0x0800 (IP), 0x0806(ARP), 0x86DD (IPv6)

Other network protocols

RFC 1042 Encapsulation

IPX Protocol Suite Ethertype 0x8137
AppleTalk ARP Ethertype 0x80F3
802.1H Bridge-Tunnel Encapsulation

802.2
Logical Link Control (LLC) /
Sub-Network Access Protocol (SNAP)

AP Bridging and Frame Translation
Ethernet Network 802.3, etc. 802.1Q

Medium Access Control (MAC)

Services - 802.11 clause 6
Framing - 802.11 clause 7
Functions - 802.11 clause 9
Management - 802.11 clause 11
Security - 802.11 clause 8

Key hierarchy- 802.11i, clause 8.5.1

Pairwise Master Key (PMK)
Pairwise Transient Key (PTK): Temporal Key(TK); Message Integrity Check (MK) Key
Group Master Key (GMK)
Group Transient Key (GTK): Temporal Key(TK); Message Integrity Check (MK) Key

Key distribution, 802.11i, clause 8.5

Wired Equivilent Privacy (WEP) 802.11 clause 8.2
Initialization Vector (IV); Key; Frame
RC4
Encrypted Frame + Integrity Check Value (ICV)

Temporal Key Integrity Protocol (TKIP) 802.11i Clause 8.3.2
TKIP Sequence (TSC); Temporal key; Frame; MIC Key; Frame
Key Mixing
Per-Frame Key
Michael Integrity Check
Frame + MIC
WEP
Encrypted and Authenticated Frame

Counter with CBC MAC Protocol (CCMP) 802.11i clause 9.3.3
Packet Number (PN); Temporal Key; Frame
Counter with CBC-MAC (CCM) Mode RFC 3610
AES FIPS PUB 197
Encrypted and Authenticated Frame

Physical Layer Convergence Procedure (PLCP)

Frequency-Hopping Spread Spectrum (FHSS)	Direct Sequence Spread Spectrum (DSSS)	High-Rate Direct Sequence Spread Spectrum (HR/DSSS)	Extended Rate PHY (ERP)	Proposed: High-Throughput MIMO PHY	OFDM PHY
802.11 Clause 14	802.11b Clause 18 Barker Encoding	802.11b Clause 18 Complimentary Code Keying	802.11g Clause 19 Coded OFDM	Future 802.11n	802.11a/j Clause 17 Coded OFDM

Spectrum Management Services
Transmit Power Control-802.11h Clause 11.5
Dynamic Frequency Selection-802.11h Clause 11.6
(Optional in Some Regulation Domains)

Regulatory Compliance
United States - Federal Communications Commission, *fcc.gov*
Europe - European Telecommunications Standards Institute, *etsi.org*
- European Radiocommunications, *ero.dk*
Japan - Ministry of Internal Communications, *soumu.go.jp*
802.11 d Regulatory Extensions
Rules Set by Regulators

2.4 GHz ISM Band
2.412 Ghz-2.484 GHz

5 GHz Unlicensed Bands 4.920 GHz-5.825 GHz

4.920-4.980 GHz	5.040-5.080 GHz	5.150-5.250 GHz	5.250-5.235 GHz	5.470-5.725 GHz Worldwide *Harmonized* Band	5.725-5.825 GHz
Channels 240-252	Channels 8-16	Channels 34-46 (Japan) Channels 36-48 (U.S.)	Channels 52-64	Channels 100-140	Channels 149-161
		United States Lower U-NII band FCC 15.407	United States Mid U-NII Band FCC 15.407	United States FCC 03-287	United States Upper U-NII Band FCC 15.407
				Europe ERC/DEC/(99)23 ETSI EN 301 893	
Japan Equipment Ordinance Articles 7, 49.20, 49.21	Japan Equipment Ordinance Articles 7, 49.20, 49.21	Japan Equipment Ordinance Articles 7, 49.20, 49.21			

The Standards

Institute of Electrical and Electronics Engineers [IEEE]: *http://www.ieee.org*
Standards download from Get IEEE802: *http://standards.ieee.org/getieee802/*

802.11 Standards

802.11 – Wireless LAN MAC and PHY 802.11 FHSS PHY and 802.11 DSSS PHY: 1 and 2 Mbpsin the 2.4 GHz band
802.11a – OFDM PHY: up to 54 Mbps in the 5 GHz band
802.11b – HR/DSSS PHY: 5.5 Mbps and 11 Mbps in the 2.4 GHz band
802.11d – Regulatory domain extensions
802.11F – Inter-Access Point Protocol recommendations
802.11g – Extended Rate PHY: up to 54 Mbps in the 2.4 GHz band
802.11h – Spectrum and Transmit Power Management Extensions
802.11i – Security enhancements
802.11j – 4.9 - 5 GHz operation in Japan

802.11 Working Group Standards

Task Group e – Quality of Service (QoS) enhancements
Task Group k – Radio resource management
Task Group n – High throughput (>100 Mbps) PHY
Task Group p – Wireless access in vehicular environments (WAVE)
Task Group r – Roaming enhancements
Task Group s – Multihop/mesh extensions
Task Group T – Performance measurements
Task Group u – Interoperability and handoff between different types
Task Group v – Network management enhancements

Related IEEE Standards

802.1X – Port-based access control
802.1H – MAC bridging and bridge/tunnel encapsulation
802.1D – IEEE 802 MAC bridging
802.1Q – Virtual bridged local area networks
802.1p – Priority bits
802.2 – Logical Link Control and SNAP encapsulation
802.3af – Power over Ethernet

Internet Engineering Task Force (IETF) *www.ietf.org*

Standards – downloaded from *www.ietf.org/rfc.html* or *http://rfc-editor.org/*
Draft Standards – (Internet-Drafts) down loaded from *www.ietf.org/ID.html*

Authentication Standards

RFC 2865 – Remote Authenticated Dial-In User Service (RADIUS)
RFC 2868 – RADIUS tunnel support
RFC 2866 – RADIUS accounting
RFC 2867 – RADIUS tunnel accounting
RFCs 2869 and 3579 – RADIUS extensions (including EAP)
RFC 3748 – Extensible Authentication Protocol
RFC 3580 – RADIUS & 802.1X
RFC 2716 – EAP-TLS

I-D: Protected EAP (PEAP)
I-D: Tunneled TLS (TTLS)
I-D: EAP-FAST
I-D: EAP-SIM – authentication using mobile telephone subscriber identity module
I-D: EAP-AKA – authentication using UMTS (3G) authentication and key agreement

Related Standards

RFC 2246 – Transport Layer Security
RFC 1042 – IP encapsulation on IEEE 802 networks

Regulators

United States – Federal Communications Commission, *fcc.gov*
Europe – European Telecommunications Standards Institute, *etsi.org*
European Radiocommunications Office, *ero.dk*
Japan – Ministry of Internal Communications, *soumu.go.jp*

Europe, Middle East, and Africa

European Telecommunications Standards Institute, *http://www.etsi.org*
European Radiocommunications Office, *http://www.ero.dk*
European Conference of Postal and Telecommunications Administrations, *http://www.cept.org*

Austria – Rundfunk & Telekom Regulierungs, *http://www.tkc.at/*
Belgium – Institut Belge des services postaux et des télécommunications, *http://www.ibpt.be/*
Czech Republic – Český telekomunikační úřad (Czech Telecommunication Office), *http://www.ctu.cz/*
Denmark – IT- og Telestyrelsen (National IT and Telecom Agency), *http://www.tst.dk/*
Finland – Ministry of Transport and Communications, *http://www.mintc.fi/*
France – Autorité de Régulation des Télécommunications, *http://www.art-telecom.fr/*
Germany – Regulierungsbehörde für Telekommunikation und Post, *http://www.regtp.de/*
Greece – Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (National Telecommunications and Post Commission), *http://www.eett.gr/*
Ireland – Commission for Communications Regulation, *http://www.odtr.ie/*
Italy – Autorità per le garanzie nelle comunicazioni, *http://www.agcom.it/*
Netherlands – OPTA, *http://www.opta.nl/*
Norway – Post-og Teletilsynet, *http://www.npt.no/*
Poland – Urząd Regulacji Telekomunikacji i Poczty (URTiP), *http://www.urtip.gov.pl/*
Portugal – Autoridade Nacional de Comunicações (Anacom), *http://www.anacom.pt/*
Switzerland – Bundesamt für Kommunikation (Bakom), *http://www.bakom.ch/*
United Kingdom – Office of Communications, *http://www.ofcom.org.uk/*
Israel – Ministry of Communications, *http://www.moc.gov.il/*
South Africa – Independent Communications Authority of South Africa, *http://www.icasa.org.za/*

Asia/Pacific Rim

Australia – Australian Communications Authority, *http://www.aca.gov.au/*
China – Ministry of Information Industries, *http://www.mii.gov.cn/*
Hong Kong – Office of the Telecommunications Authority, *http://www.ofta.gov.hk/*
India – Ministry of Communications and Information Technology, *http://www.mit.gov.in/*
Indonesia – Directorate General of Post and Telecommunication, *http://www.postel.go.id/*
Japan – Ministry of Internal Affairs and Communications, *http://www.soumu.go.jp/*
Korea – Ministry of Information & Communication, *http://www.mic.go.kr*
Malaysia – Ministry of Energy, Communications, and Multimedia, *http://www.ktkm.gov.my/*
New Zealand – Ministry of Economic Development, *http://www.med.govt.nz/*
Philippines – National Telecommunications Commission, *http://www.ntc.gov.ph*
Singapore – Infocomm Development Authority, *http://www.ida.gov.sg/*
Taiwan – Directorate General of Telecommunications, *http://www.dgt.gov.tw/*
Thailand – Post and Telegraph Department, *http://www.ptd.go.th/*
Vietnam – Department General of Posts & Telecommunications, *http://www.vnpt.com.vn/DGPT*

Americas

Brazil – Anatel, *http://www.anatel.gov.br/*
Canada – Industry Canada, *http://www.ic.gc.ca/*
Chile – Subsecretaria de Telecomunicaciones, *http://www.subtel.cl/*
Mexico – Secretariat of Communications and Transport, *http://www.sct.gob.mx/*
Peru – Ministry of Transportation and Communications, *http://www.mtc.gob.pe/*

Related International Organizations

International Telecommunications Union – *http://www.itu.int/*

Vendors

Supplicants

Cisco – Aironet Client Software, *cisco.com*
Funk – Odyssey client, *funk.com*
Meetinghouse – AEGIS client, *mtghouse.com*
Microsoft – Windows XP/Windows 2000 built-in supplicants, *microsoft.com*

RADIUS servers

Cisco – CiscoSecure ACS, *cisco.com*
Funk – Steel Belted RADIUS, Odyssey Server, *funk.com*
Interlink – *interlinknetworks.com*
Open Systems Consultants – Radiator, *open.com.au*
Lucent – NavisRadius, *lucent.com*
Meetinghouse – AEGIS Server, *mtghouse.com*
Microsoft – Internet Authentication Server, *microsoft.com*

Access Points

3Com – *3com.com*
Accton – (reference design), *accton.com*
Apple – *apple.com*
Aruba – *arubanetworks.com*
Avaya – *avaya.com*
Buffalo – *buffalotech.com*
Cisco – *cisco.com*
D-Link – *d-link.com*
Enterasys – *enterasys.com*
Extreme – *extremenetworks.com*
Foundry – *foundry.com*
Hewlett-Packard – *hp.com*
Netgear – *netgear.com*
Proxim – *proxim.com*
SMC – *smc.com*
Symbol – *symbol.com*
Trapeze – *trapezenetworks.com*

Chip Vendors

Agere – *agere.com*
Airgo – *airgo.com*
Atheros – *atheros.com*
Broadcom – *broadcom.com*
Conexant – *conexant.com*
Intel – *intel.com*
Marvell – *marvell.com*
Texas Instruments – *ti.com*

Analysis tools

AirMagnet – *airmagnet.com*
Berkeley Varitronics – YellowJacket, *bvsystems.com*
Network Instruments – Observer, *networkinstruments.com*
Sniffer – Sniffer Wireless, *sniffer.com*
WildPackets – AiroPeek, *wildpackets.com*

Open Source Projects

Ethereal – network protocol analyzer, *ethereal.com*
HostAP & wpa_supplicant – access point & supplicant, *hostap.epitest.fi*
xsupplicant (Open1X) – supplicant, *open1x.org*
FreeRADIUS – RADIUS server, *freeradius.org*
SecureW2 – TTLS plug-in for the Windows supplicant, *securew2.com*
wEAP – EAP plug-ins for Windows, *weap.sourceforge.net*

O'REILLY®

© 2005 Matthew S. Gast O'Reilly logo is a registered trademark of O'Reilly Media, Inc. All other trademarks are property of their respective owners. 04/05 Part #50055