استاندارد ایران-آی تریپل ای
۸۰۲/۱۱
چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

ISIRI-IEEE
802.11
1st. edition
Identical with:
IEEE 802.11:2007

مخابرات- فن‌آوری اطلاعات- مبادله مخابراتی و اطلاعاتی بین سامانه‌ها- شبکه‌های محلی و شهری- الزامات ویژه- قسمت ۱۱: ویژگی‌های کنترل دسترسی رسانه (MAC) و لایه فیزیکی (PHY) در شبکه‌های محلی بی‌سیم

IEEE standard for information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements - Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications

ICS: 33.040

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین‌ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسهٔ استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آنها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

" مخابرات- فن‌آوری اطلاعات- مبادله مخابراتی و اطلاعاتی بین سامانه‌ها- شبکه‌های محلی و شهری- الزامات ویژه- قسمت ۱۱: ویژگی‌های کنترل دسترسی رسانه (MAC) و لایه فیزیکی (PHY) در شبکه‌های محلی بی‌سیم "

رئیس:	**سمت و/ یا نمایندگی**
محسن زاده، علی‌اکبر (فوق لیسانس مهندسی برق-مخابرات)	مشاور مرکز تحقیقات مخابرات ایران
دبیر:	
سلطانی حقیقت، الهه (لیسانس مهندسی برق-مخابرات)	کارشناس شرکت آگاهان ارتباط آریا
اعضا: (اسامی به ترتیب حروف الفبا)	
پارسایی، زهرا (لیسانس مهندسی برق- الکترونیک)	کارشناس شرکت ارتباطات سیار
حسام محسنی، علیرضا (دکترای مهندسی کامپیوتر-سخت افزار)	عضو هیأت مدیره شرکت بسامد
حسینی سرشکی، سیدمحمد (فوق لیسانس مهندسی برق-مخابرات)	مدیر عامل شرکت رایان الکترونیک
راحمی، بیژن (دکترای مهندسی برق-مخابرات)	عضو هیأت علمی دانشگاه صنعتی شریف
رستم فرودی، ماندانا (لیسانس مهندسی برق-الکترونیک)	پژوهشگر مرکز تحقیقات مخابرات ایران و ناظر پروژه

شیخ عطار، محمدرضا (فوق لیسانس مهندسی برق-الکترونیک)	پژوهشگر مرکز تحقیقات مخابرات ایران و ناظر پروژه
موسوی مدنی، فریبرز (دکترای مهندسی برق- مخابرات)	عضو هیأت علمی دانشگاه الزهرا
میرزاباقی، منصور (فوق لیسانس مهندسی برق-مخابرات)	پژوهشگر مرکز تحقیقات مخابرات ایران و ناظر پروژه

فهرست مندرجات

پیش گفتار

استاندارد " مخابرات- فن‌آوری اطلاعات- مبادله مخابراتی و اطلاعاتی بین سامانه‌ها- شبکه‌های محلی و شهری- الزامات ویژه- قسمت ۱۱: ویژگی‌های کنترل دسترسی رسانه (MAC) و لایه فیزیکی (PHY) در شبکه‌های محلی بی‌سیم " که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات مخابرات ایران، بر مبنای روش تنفیذ مورد اشاره در **راهنمای ISO/IEC Guide21-1 (پذیرش منطقه‌ای یا ملی استانداردهای "بین‌المللی/منطقه‌ای" و دیگر مدارک استاندارد)** به عنوان استاندارد ملی ایران، تهیه شده و در هفتاد و ششمین اجلاسیه کمیتهٔ ملی استاندارد مخابرات مورخ ۱۳۸۸/۱۲/۱۰مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

این استاندارد ملی بر اساس پذیرش استاندارد بین‌المللی به شرح زیر است:

IEEE 802.11:2007, IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

مخابرات- فن‌آوری اطلاعات- مبادله مخابراتی و اطلاعاتی بین سامانه‌ها- شبکه‌های محلی و شهری- الزامات ویژه- قسمت ۱۱: ویژگی‌های کنترل دسترسی رسانه (MAC)[1] و لایه فیزیکی (PHY)[2] در شبکه‌های محلی بی‌سیم

۱ هدف و دامنه کاربرد

این استاندارد ملی، بر اساس پذیرش استاندارد بین‌المللی IEEE Std 802.11:2007 تدوین شده است.
هدف از تدوین این استاندارد، تعیین و تعریف مشخصات یک کنترل دسترسی رسانه (MAC)و چندین لایه فیزیکی (PHY) برای اتصالات بی‌سیم ایستگاه (STA)[3] های ثابت[4]، قابل حمل[5] و متحرک در یک ناحیه محلی[6] است. این استاندارد اتصالات بی‌سیم را برای دستگاه‌های خودکار، تجهیزات، یا ایستگاه‌هایی که نیازمند استقرار سریع هستند و ممکن است قابل حمل با دست یا سوار بر خودروهای متحرک، در حال حرکت در یک ناحیه محلی باشند، فراهم می‌نماید. بعلاوه در این استاندارد سازمان‌های تنظیم مقررات به عنوان وسیله‌ای برای استانداردسازی دسترسی به یک یا چند باند فرکانسی به منظور تحقق اهداف ارتباطات محلی، ارائه می‌شود. این استاندارد به ویژه به انجام وظایف زیر می‌پردازد:

الف- شرح کارکردها و سرویس‌های مورد نیاز توسط تجهیزات منطبق بر استاندارد IEEE 802.11، برای عملکرد در شبکه‌های Ad hoc[7] و زیرساخت و نیز جنبه‌های تحرک ایستگاه (گذار) در این شبکه‌ها.

ب- تعریف رویه‌های MAC برای پشتیبانی سرویس‌های تحویل واحد داده سرویس MAC (MSDU)[8] ناهمزمان.

پ- تعریف فنون مختلف سیگنالینگ PHY و کارکردهای واسطی که توسط IEEE 802.11 MAC کنترل می‌شوند.

ت- اجازه عملکرد تجهیزات منطبق بر استاندارد IEEE 802.11 در شبکه محلی بی‌سیم (WLAN)[9] که ممکن است در کنار چندین IEEE 802.11 WLAN هم‌پوشان[10] قرار داشته باشند.

---

1 - Medium Access Control

MAC مربوط به اصطلاح دیگری نیز هست که در بند ۳-۸۴ استفاده شده است.

2 - Physical layer
3 - Stations
4 - Fixed
5 - Portable
6 - Local area

۷ - شبکه‌هایی که به صورت موقت برای انجام کارهای خاص تشکیل می‌شوند.

8 - MAC Service Data Unit
9 - Wireless Local Area Netwok
10 - Overlapping

ث- شرح الزامات و رویه‌ها برای فراهم نمودن محرمانگی داده برای آنکه اطلاعات کاربر از طریق رسانه بی‌سیم (WM)[1] و تصدیق هویت تجهیزات منطبق بر استاندارد IEEE 802.11 منتقل شوند.
ج- شرح سازوکارهای انتخاب پویای فرکانس (DFS)[2] و کنترل توان انتقال (TPC)[3] که ممکن است جهت برآورده کردن نیازهای تنظیمی برای عملکرد در باند ۵ گیگاهرتز استفاده شوند.
چ- تعریف رویه‌های MAC برای پشتیبانی کاربردهای شبکه محلی (LAN)[4] با الزامات کیفیت سرویس (QoS)[5] ، شامل انتقال صوت، صدا و ویدئو.

این استاندارد در تعیین مشخصات یک MAC و چندین لایه فیزیکی برای اتصالات بی‌سیم ایستگاه‌های ثابت، قابل حمل و متحرک در یک ناحیه محلی کاربرد دارد.

۲ مراجع الزامی

مدارک زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.
در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.
استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ETSI EN 301 893, Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Part 2: Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive.
2-2 FIPS PUB 180-1-1995, Secure Hash Standard.
2-3 FIPS PUB 197-2001, Advanced Encryption Standard (AES).
2-4 IEEE Std 802®-2001, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.
2-5 IEEE Std 802.1X™-2004, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control.
2-6 IEEE Std C95.1™-1991 (Reaff 1997), IEEE Standard Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.
2-7 IETF RFC 1321, The MD5 Message-Digest Algorithm, April 1992 (status: informational).
2-8 IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, H. Krawczyk, M. Bellare, R. Canetti, February 1997 (status: informational).
2-9 IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad, R. Housley, September 2002 (status: informational).

1 - Wireless Medium
2 - Dynamic Frequency Selection
3 - Transmit Power Control
4 - Local Area Network
5 - Quality of Service

2-10 IETF RFC 3610, Counter with CBC-MAC (CCM), D. Whiting, R. Housley, N. Ferguson, September 2003 (status: informational).
2-11 IETF RFC 4017, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, D.Stanley, J. Walker, B. Aboba, March 2005 (status: informational).
2-12 ISO/IEC 3166-1, Codes for the representation of names of countries and their subdivisions—Part 1: Country codes.
2-13 ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.
2-14 ISO/IEC 8802-2:1998, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.
2-15 ISO/IEC 8824-1:1995, Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation.
2-16 ISO/IEC 8824-2:1995, Information technology—Abstract Syntax Notation One (ASN.1): Information object specification.
2-17 ISO/IEC 8824-3:1995, Information technology—Abstract Syntax Notation One (ASN.1): Constraint specification.
2-18 ISO/IEC 8824-4:1995, Information technology—Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.
2-19 ISO/IEC 8825-1:1995, Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
2-20 ISO/IEC 8825-2:1996, Information technology—ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).
2-21 ISO/IEC Technical Report 11802-5:1997(E), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 5: Medium Access Control (MAC) Bridging of Ethernet V2.0 in Local Area Networks (previously known as IEEE Std 802.1H-1997 [B13]).
2-22 ISO/IEC 14977:1996, Information technology—Information technology. Syntactic Metalanguage. Extended BNF.
2-23 ISO/IEC 15802-1:1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.
2-24 ISO/IEC 15802-3, Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges.
2-25 ITU Radio Regulations, volumes 1–4.
2-26 ITU-T Recommendation V.41 (11/88), Code-independent error-control system.
2-27 ITU-T Recommendation Z.100 (03/93), CCITT specification and description language (SDL).
2-28 ITU-T Recommendation Z.105 (03/95), SDL combined with ASN.1 (SDL/ASN.1).
2-29 ITU-T Recommendation Z.120 (2004), Programming Languages—Formal Description Techniques (FDT)—Message Sequence Chart (MSC).

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود[۱]:

۱-۳

دسته دسترسی (AC) [۲]

برچسبی برای مجموعه مشترک از پارامترهای دسترسی کانال توزیع شده ارتقاء یافته (EDCA)[۳] است که توسط یک ایستگاه با کیفیت سرویس به منظور رقابت بر سر تصاحب کانال، جهت انتقال واحدهای داده سرویس MAC با اولویت‌هایی خاص استفاده می‌شود.

۲-۳

کنترل دسترسی

ممانعت از استفاده غیر مجاز از منابع است.

۳-۳

نقطه دسترسی (AP) [۴]

هستاری[۵] است که عملکردهای ایستگاه (STA) را داراست و دسترسی به سرویس‌های توزیعی را از طریق رسانه بی‌سیم (WM) برای ایستگاه‌های مرتبط فراهم می‌کند.

۴-۳

داده تصدیق هویت اضافی (AAD)[۶]

داده‌ای است که رمزنگاری نشده ولی بصورت رمزی محافظت شده است.

۵-۳

شبکه Ad hoc

اغلب به عنوان اصطلاحی برای مجموعه سرویس پایه مستقل (IBSS)[۷] استفاده می‌شود.

۶-۳

کنترل پذیرش[۸]

آلگوریتمی است که برای اطمینان از این امر استفاده می‌شود که پذیرش یک جریان جدید توسط شبکه‌ای با منبع محدود، موجب نقض کردن تعهدات سرویس به جریان‌های پذیرفته شده قبلی نمی‌شود.

۱- مرجع اصطلاحاتی که در اینجا تعریف نشده اند عبارت است از:
The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition

2 - Access Category
3 - Enhanced Distributed Channel Access
4 - Access Point
5 - Entity
6 - Additional authentication data
7 - Independent Basic Service Set
8 - Admission control

۷-۳

زمانبندی تجمیعی[1]

تجمیع زمان‌بندی‌های تحویل و/یا سرکشی که توسط نقطه دسترسی کیفیت سرویس، در یک دوره سرویس (SP)[2] واحد، برای یک ایستگاه کیفیت سرویس غیر نقطه دسترسی خاص انجام می‌شود.

۸-۳

همبستگی[3]

سرویسی است که برای نگاشت نقطه دسترسی/ایستگاه (AP/STA)[4] و ایجاد امکان احضار سرویس‌های سامانه توزیع (DSSs)[5] استفاده می‌شود.

۹-۳

تصدیق هویت[6]

سرویسی است که برای شناسایی یک ایستگاه به عنوان عضوی از مجموعه ایستگاه‌های مجاز به ارتباط با سایر ایستگاه‌ها استفاده می‌شود.

۱۰-۳

مجموعه تصدیق هویت و مدیریت کلید (AKM)[7]

مجموعه‌ای از یک یا چند آلگوریتم است که برای تصدیق هویت و مدیریت کلید، بصورت مجزا یا در ترکیب با آلگوریتم‌های لایه بالاتر تصدیق هویت و مدیریت کلید که خارج از محدوده این استاندارد هستند، طراحی شده است.

۱۱-۳

سرویس‌ده تصدیق هویت (AS)[8]

هستاری است که یک سرویس تصدیق هویت را برای یک تصدیق کننده هویت[9] فراهم می‌کند. این سرویس، سرویس، با استفاده از اعتبارنامه‌های فراهم شده توسط متقاضی، تعیین می‌کند که آیا متقاضی مجاز به دسترسی به سرویس‌های فراهم‌شده توسط تصدیق کننده هویت هست یا خیر (به استاندارد IEEE 802.1X: 2004 مراجعه شود).

۱۲-۳

تصدیق کننده هویت

هستاری در یک انتهای یک قسمت LAN نقطه به نقطه است که تصدیق هویت هستار متصل به انتهای دیگر پیونده را مقدور می‌کند (به استاندارد IEEE 802.1X: 2004 مراجعه شود).

---

1 - Aggregated schedule
2 - Service Period
3 - Association
4 - Access Point/Station
5 - Distribution System Services
6 - Authentication
7 - Authentication and Key Management
8 - Authentication Server
9 - Authenticator

۱۳-۳

آدرس تصدیق کننده هویت (AA)[1]

آدرس MAC تصدیق کننده هویت IEEE 802.1X است.

۱۴-۳

مجاز[2]

مجاز بودن به صورت صریح و روشن.

۱۵-۳

ناحیه سرویس پایه (BSA)[3]

ناحیه‌ای متشکل از اعضای یک مجموعه سرویس پایه است که ممکن است شامل اعضای BSSهای دیگر هم باشد.

۱۶-۳

مجموعه سرویس پایه (BSS)

مجموعه‌ای از ایستگاه‌هایی است که با استفاده از اولیه‌های[4] سرویس و یک ایستگاه که از اولیه START استفاده کرده است بصورت موفقیت آمیز همزمان شده‌اند. عضویت در یک BSS بدان معنا نیست که ارتباط بی‌سیم با تمام اعضای دیگر این BSS امکان پذیر است.

۱۷-۳

انتهای پرارزش[5]

در بردارنده این مفهوم است که برای یک نمایش عددی چند هشتایی[6] خاص، باارزش‌ترین هشتایی، کوچکترین آدرس را دارد.

۱۸-۳

آدرس پخش همگانی[7]

یک آدرس چندپخشی یگانه است که تمام ایستگاه‌ها را مشخص می‌کند.

۱۹-۳

کانال

نمونه‌ای از رسانه ارتباطی است که برای عبور PDUها بین دو یا چند ایستگاه استفاده می‌شود.

۲۰-۳

فاصله‌گذاری کانال[8]

---

1 - Authenticator Address
2 - Authorized
3 - Basic Service Area
4 - Primitives
5 - Big Endian
6 - Multi-octet
7 - Broadcast address
8 - Channel spacing

تفاوت بین فرکانس‌های مرکزی دو کانال غیر هم‌پوشان و مجاور فرستنده رادیویی است.

۲۱-۳

مجموعه رمزنگاری[1]

مجموعه‌ای از یک یا چند آلگوریتم است که برای تدارک محرمانگی داده، اعتبار یا دست نخوردگی داده و/یا حفاظت از پخش مجدد طراحی شده است.

۲۲-۳

کارکرد سنجش کانال شفاف (CCA)[2]

این کارکرد منطقی در لایه فیزیکی، وضعیت جاری استفاده از رسانه بی‌سیم را تعیین می‌کند.

۲۳-۳

دوره بدون رقابت (CFP)[3]

دوره زمانی در جریان عملیات یک کارکرد هماهنگی نقطه‌ای (PCF)[4] است که در آن حق ارسال تنها توسط یک هماهنگ کننده نقطه‌ای (PC)[5] به ایستگاه‌ها داده می‌شود، تا مبادلات قاب بین اعضاء BSS بدون رقابت رقابت برسر تصاحب رسانه بی‌سیم انجام گیرد.

۲۴-۳

دوره رقابت (CP)[6]

دوره زمانی خارج از دوره بدون رقابت (CFP) در یک BSS با هماهنگ کننده نقطه‌ای است. در BSS ای که هماهنگ کننده نقطه‌ای وجود ندارد، این دوره تمام زمان عملکرد BSS را در بر می‌گیرد.

۲۵-۳

فاز دسترسی کنترل شده (CAP)[7]

یک دوره زمانی است که در آن هماهنگ کننده مختلط (HC)[8]، پس از بدست آوردن دسترسی رسانه که با حس کردن آزاد بودن کانال در یک دوره زمان بین قاب PCF (PIFS)[9] انجام شده، کنترل رسانه را در اختیار اختیار دارد. این دوره ممکن است طی چندین فرصت انتقال (TXOP)[10] متوالی باشد و امکان دارد شامل TXOPهای سرکشی شده باشد.

۲۶-۳

تابع هماهنگی[11]

تابعی منطقی است که زمانی را که یک ایستگاه عمل کننده در یک BSS، مجاز به ارسال PDUها از طریق

---

1 - Cipher suite
2 - Clear Channel Assessment
3 - Contention-Free Period
4 - Point Coordination Function
5 - Point Coordinator
6 - Contention Period
7 - Controlled Access Phase
8 - Hybrid Coordinator
9 - Point Coordination Function (PCF) Interframe Space
10 - Transmission Opportunity
11 - Coordination Function

رسانه بی‌سیم است، تعیین می‌کند. تابع هماهنگی در یک BSS ممکن است دارای یک تابع هماهنگی مختلط (HCF)[1]، یا دارای یک HCF و یک PCF و یک تابع هماهنگی توزیع شده (DCF)[2]باشد. یک QoS BSS دارای یک DCF و یک HCF است.

۲۷-۳

سرکشی بدون رقابت[3]

ایستگاهی است که قادر به پاسخ به یک سرکشی CF در قاب داده است، البته اگر چنین قابی صف‌بندی شده و قابل تولید باشد.

۲۸-۳

حالت شمارنده با کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمزنگاری (CCM)[4]

حالتی از بلوک رمزنگاری با کلید متقارن است که محرمانگی را با استفاده از حالت شمارنده (CTR)[5] و اعتبار اعتبار منبع داده را با استفاده از کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمزنگاری (CBC-MAC)[6] فراهم می‌کند.

یادآوری- به استاندارد IETF RFC 3610 مراجعه شود.

۲۹-۳

کپسوله کردن رمزنگاری[7]

عملیات ایجاد پی‌بار[8] رمزنگاری از داده متن ساده است که شامل متن رمز شده و هر وضعیت رمزنگاری مربوطه است که توسط گیرنده داده مورد نیاز است، برای مثال بردارهای مقداردهی اولیه (IVs)[9]، اعداد توالی، کدهای دست‌نخوردگی پیام (MICs)[10] و شناسه‌های کد از این دسته‌اند.

۳۰-۳

محرمانگی داده[11]

یک خاصیت اطلاعات است که از افشاء آن برای اشخاص، هستارها یا پردازش‌های غیر مجاز جلوگیری می‌کند.

۳۱-۳

سرویس ابطال تصدیق هویت[12]

---

1 - Hybrid Coordination Function
2 - Distributed Coordination Function
3 _ Contention Free pollable
4 - Counter mode with Cipher-block chaining Message authentication code
5 - Counter mode
6 - Cipher-block chaining message authentication code
7 - Cryptographic encapsulation
8 - Payload
9 - Initialization Vectors
10 - Message Integrity Codes
11 - Data confidentiality
12 - Deauthentication service

سرویسی است که یک همبستگی تصدیق هویت موجود را باطل می‌کند.

۳۲-۳

حذف کردن کپسول[1]

به حالت اولیه درآوردن یک قاب حفاظت نشده از یک قاب حفاظت شده است.

۳۳-۳

حذف کپسول[2]

عملیات ایجاد داده متنی ساده با حذف کردن کپسول از یک قاب کپسوله شده است.

۳۴-۳

دسته دسترسی با امکان تحویل[3]

یک دسته دسترسی نقطه دسترسی کیفیت سرویس است که در آن نقطه دسترسی قادر به استفاده از EDCA برای تحویل ترافیک از دسته دسترسی به یک ایستگاه کیفیت سرویس غیر نقطه دسترسی (non-AP)[4] در یک دوره سرویس زمانبندی نشده آغاز شده توسط ایستگاه است.

۳۵-۳

قاب هدایت شده[5]

به تعریف قاب تک پخشی[6] مراجعه شود.

۳۶-۳

پیونده مستقیم[7]

یک پیونده دو طرفه از یک ایستگاه non-AP QoS به یک ایستگاه non-AP QoS دیگر است که در همان زیر ساخت QoS BSS فعالیت می‌کند و از یک QoS AP عبور نمی‌کند. به محض آنکه یک پیونده مستقیم برقرار شود، همه قاب‌ها بین دو ایستگاه non-AP QoS بطور مستقیم مبادله می‌شوند.

۳۷-۳

سرویس عدم همکاری[8]

سرویسی است که یک ارتباط موجود را حذف می‌کند.

۳۸-۳

تابع هماهنگی توزیع شده (DCF)[9]

---

1 - Decapsulate
2 - Decapsulation
3- Delivery-enabled access category
4 - Non-Access Point
5 - Directed frame
6 - Unicast
7 - Direct link
8 - Disassociation service
9 - Distributed Coordination Function

رده‌ای از تابع هماهنگی است که در آن هنگام عملکرد شبکه، منطق تابع هماهنگی یکسانی در همه ایستگاه‌های BSS فعال است.

۳۹-۳

سرویس توزیع[1]

سرویسی است که با استفاده از اطلاعات ارتباط، MSDUهای MAC را در سامانه توزیع (DS)[2] تحویل می‌دهد.

۴۰-۳

سامانه توزیع (DS)

سامانه‌ای است که برای اتصال متقابل یک مجموعه از BSSها و LANهای یکپارچه، جهت ایجاد یک مجموعه سرویس گسترش یافته (ESS)[3] استفاده می‌شود.

۴۱-۳

رسانه سامانه توزیع (DSM)[4]

رسانه یا مجموعه‌ای از رسانه‌ها است که توسط یک سامانه توزیع برای ارتباط بین نقاط دسترسی و درگاه‌های یک ESS استفاده می‌شود.

۴۲-۳

سرویس سامانه توزیع (DSS)

مجموعه‌ای از سرویس‌هایی است که توسط سامانه توزیع فراهم شده است و از طریق یک نمونه واحد از رسانه بی‌سیم، MAC را قادر به انتقال MSDUها بین ایستگاه‌هایی که دارای ارتباط مستقیم با یکدیگر نیستند می‌کند. این سرویس‌ها شامل این موارد است:

انتقال MSDUها بین نقاط دسترسی BSSها در یک ESS، انتقال MSDUها بین درگاه‌ها و BSSها در یک ESS، و انتقال MSDUها بین ایستگاه‌های موجود در BSS یکسان در حالت‌هایی که MSDU دارای یک آدرس مقصد چند پخشی یا پخش همگانی است یا مقصد، یک آدرس منفرد بوده و ایستگاه با یک AP در ارتباط است. DSS ها بین زوج‌هایMAC IEEE 802.11 فراهم می‌شوند.

۴۳-۳

پیونده فروسو[5]

یک پیونده یک طرفه بین یک نقطه دسترسی و یک یا چند ایستگاه non-AP است.

۴۴-۳

انتخاب پویای فرکانس (DFS)[6]

---

1 - Distribution service
2 - Distribution System
3 - Extended Service Set
4 - Distribution System Medium
5 - Downlink
6 - Dynamic Frequency Selection

تسهیلات مقرر شده برای تحقق الزامات در برخی قلمروهای تنظیم کننده برای آشکارسازی رادار و پخش یکپارچه کانال در باند فرکانسی ۵ گیگاهرتز است. این تسهیلات ممکن است برای اهداف دیگری مانند تخصیص خودکار فرکانس نیز استفاده شوند.

۴۵-۳

انتخاب‌گر پویای فرکانس[1]

ایستگاهی در یک IBSS است که مسئولیت انتخاب کانال بعدی را پس از آنکه رادار فعالیت کننده در یک کانال آشکار شود، بر عهده دارد. به دلیل طبیعت IBSSها، نمی‌توان تضمین کرد که در هر زمان خاص یک انتخاب‌گر DFS واحد وجود داشته باشد و پروتکل به این موضوع تأکید دارد.

۴۶-۳

کلید تأیید کلید پروتکل تصدیق هویت قابل گسترش در شبکه‌های محلی (EAPOL)[2] (KCK)[3]

کلیدی است که برای بررسی دست نخوردگی در قاب کلید EAPOL استفاده می‌شود.

۴۷-۳

کلید رمزنگاری کلید EAPOL (KEK)[4]

کلیدی است که برای رمزنگاری فیلد داده کلید[5] در یک قاب کلید EAPOL استفاده می‌شود.

۴۸-۳

توان تابشی همه جهته موثر (EIRP)[6]

توان معادل یک سیگنال ارسال شده از یک تابنده همه جهته است. EIRP معادل حاصل‌ضرب توان فرستنده در بهره آنتن (کاهش یافته با هر نوع اتلاف تزویج بین فرستنده و آنتن) است.

۴۹-۳

کپسوله کردن[7]

ساختن یک قاب حفاظت شده از یک قاب حفاظت نشده است.

۵۰-۳

عملیات کپسوله کردن[8]

عملیات ایجاد یک قاب محافظت شده توسط کپسوله کردن داده متنی ساده است.

۵۱-۳

دسترسی کانال توزیع شده ارتقاء یافته (EDCA)[9]

---

1 - Dynamic Frequency Selection owner
2 - Extensible Authentication Protocol over LANs (IEEE Std 802.1X-2004)
3 - EAPOL-Key Confirmation Key
4 - EAPOL-Key Encryption Key
5 - Key Data Field
6 - Effective Isotropic Radiated Power
7 - Encapsulate
8 - Encapsulation
9 - Enhanced Distributed Channel Access

سازوکار دسترسی چندگانه تشخیص حامل با اجتناب از برخورد (CSMA/CA)[1] بصورت اولویت‌بندی شده است که توسط ایستگاه‌های کیفیت سرویس در یک QoS BSS استفاده می‌شود. این سازوکار دسترسی توسط QoS AP نیز استفاده می‌شود و با دسترسی کانال کنترل شده HCF (HCCA)[2] بصورت هم‌زمان کار می‌کند.

۵۲-۳

کارکرد دسترسی کانال توزیع شده ارتقاء یافته (EDCAF)[3]

یک کارکرد منطقی در یک ایستگاه کیفیت سرویس است که در مورد استفاده از EDCA، زمانی‌که یک قاب در صف ارسال با AC مرتبط، مجاز به انتقال از طریق رسانه بی‌سیم است، تصمیم‌گیری می‌کند. در هر AC یک EDCAF وجود دارد.

۵۳-۳

ناحیه سرویس گسترش یافته (ESA)[4]

ناحیه‌ای است که در آن اعضای یک ESS ممکن است ارتباط برقرار کنند. یک ESA بزرگ‌تر یا مساوی یک BSA است و ممکن است درگیر چندین BSS با پیکربندی هم‌پوشان، گسسته یا هر دو باشد.

۵۴-۳

مجموعه سرویس گسترش یافته (ESS)

مجموعه‌ای از یک یا چند BSS با اتصال متقابل است که برای هر ایستگاه مرتبط با یکی از آن BSSها، به عنوان یک BSS واحد برای لایه کنترل پیوندهٔ منطقی (LLC)[5] ظاهر می‌شود.

۵۵-۳

دست‌دهی چهار طرفه[6]

یک پروتکل مدیریت کلید زوجی تعریف شده در این استاندارد است. این دست‌دهی، مالکیت دوطرفه یک شاه کلید جفتی (PMK)[7] را توسط دو طرف تأیید می‌کند و یک کلید موقت گروهی (GTK)[8] را توزیع می‌کند.

۵۶-۳

دست‌دهی کلید موقتی پیوندهٔ ایستگاه به ایستگاه چهار طرفه (STK)[9]

یک پروتکل مدیریت کلید بین دو طرف است که مالکیت دوطرفه یک شاه کلید پیوندهٔ ایستگاه به ایستگاه چهار طرفه (SMK)[10] را تأیید می‌کند و یک STK را توزیع می‌کند.

---

1 - Carrier Sense Multiple Access with Collision Avoidance
2 - Hybrid Coordination Function (HCF) Controlled Channel Access
3 - Enhanced Distributed Channel Access Function
4 - Extended Service Area
5 - Logical Link Control
6 - 4-Way Handshake
7 - Pairwise Master Key
8 - Group Temporal Key
9 - 4-Way Station-to-Station Link (STSL) Transient Key (STK)
10 - 4-Way Station-to-Station Link (STSL) Master Key

۵۷-۳

تکه تکه کردن[1]

عملیات تقسیم یک MSDU یا واحد داده پروتکل مدیریت MAC (MMPDU)[2] به یک توالی از واحدهای داده پروتکل MAC (MPDUs)[3] کوچکتر پیش از ارسال است. عملیات الحاق مجموعه‌ای از MPDUهای کوچک و تشکیل یک MSDU یا MMPDU پیوند تکه‌ها[4] نام دارد (جهت اطلاعات کامل در مورد این عملیات، به بند ۵-۸-۱-۹ استاندارد ISO/IEC 7498-1: 1994 مراجعه شود).

۵۸-۳

جابجایی گوسی فرکانس (GFSK)[5]

یک نوع مدولاسیون است که در آن داده ابتدا توسط یک فیلتر گوسی، در باند پایه فیلتر شده و سپس با استفاده از مدولاسیون فرکانسی ساده، مدوله می‌شود.

۵۹-۳

گروه

هستارهایی در یک شبکه بی‌سیم مانند یک نقطه دسترسی و ایستگاه‌های مرتبط با آن، یا همه ایستگاه‌ها در یک شبکه IBSS است.

۶۰-۳

دست‌دهی کلید گروهی[6]

یک پروتکل مدیریت کلید گروهی است که در این استاندارد تعریف شده است و فقط برای صدور یک کلید موقت گروهی (GTK)[7] جدید به همتاهایی که ایستگاه محلی قبلاً با آنها ارتباطات امنیتی ایجاد کرده است، استفاده می‌شود.

۶۱-۳

شاه کلید گروهی (GMK)[8]

یک کلید کمکی است که ممکن است برای استنتاج یک GTK استفاده شود.

۶۲-۳

کلید موقت گروهی (GTK)

یک عدد تصادفی اختصاص یافته توسط منبع پخش همگانی/چند پخشی است، که برای حفاظت از MPDUهای پخش همگانی/چند پخشی از آن منبع استفاده می‌شود. GTK ممکن است از یک GMK منتج شود.

---

1 - Fragmentation
2 - MAC Management Protocol Data Unit
3 - MAC Protocol Data Units
4 - Defragmentation
5 - Gaussian Frequency Shift Keying
6 - Group key handshake
7 - Group Temporal Key
8 - Group Master Key

۶۳-۳

همبستگی امنیتی کلید موقت گروهی (GTKSA) [1]

شرایطی است که از مبادله موفقیت‌آمیز توزیع یک GTK توسط یک دست‌دهی کلید گروهی یا یک دست‌دهی چهار طرفه ایجاد می‌شود.

۶۴-۳

ایستگاه پنهان [2]

ایستگاهی است که یک ایستگاه دوم نمی‌تواند با استفاده از تشخیص حامل (CS)[3] آن را آشکار کند، در حالیکه انتقالات آن با انتقالات ایستگاه دوم به ایستگاه سوم تداخل دارد.

۶۵-۳

تابع هماهنگی مختلط (HCF) [4]

یک کارکرد هماهنگی است که برای ایستگاه‌های بی‌سیم با کیفیت سرویس، دسترسی کیفیت سرویس اولویت بندی شده و پارامترگذاری شده را به همراه ادامه پشتیبانی از ایستگاه‌های non-QoS با بهترین امکان انتقال فراهم می‌کند. HCF شامل عملکردهای فراهم شده توسط EDCA و HCCA است. HCF با DCF و PCF سازگار است. HCF یک مجموعه یکپارچه از قالب‌های قاب و توالی‌های مبادله‌ای که ایستگاه ممکن است در حین دوره رقابت یا دوره بدون رقابت استفاده کند، را پشتیبانی می‌کند.

۶۶-۳

هماهنگ‌کننده مختلط (HC) [5]

یک نوع هماهنگ‌کننده است که به عنوان بخشی از امکان کیفیت سرویس، توالی مبادله‌های قاب و قوانین مدیریت MSDU تعریف شده توسط HCF را پیاده‌سازی می‌کند. HC در هر دو دوره با رقابت و بدون رقابت عمل می‌کند. HC مدیریت پهنای باند به همراه تخصیص TXOPها به ایستگاه‌های کیفیت سرویس را انجام می‌دهد. HC در کنار نقطه دسترسی کیفیت سرویس قرار دارد.

۶۷-۳

دسترسی کانال کنترل شده HCF (HCCA) [6]

سازوکار دسترسی کانال است که توسط HC جهت هماهنگ کردن استفاده بدون رقابت رسانه توسط ایستگاه کیفیت سرویس، برای تک‌پخشی پیونده فروسو، پیونده فراسو و انتقالات پیونده مستقیم استفاده می‌شود.

۶۸-۳

تصدیق هویت IEEE 802.1X

تصدیق هویت پروتکل تصدیق هویت قابل گسترش (EAP)[7] است که توسط پروتکل IEEE 802.1X انتقال

---

1 - Group Temporal Key Security Association
2 - Hidden station
3 - Carrier Sense
4 - Hybrid Coordination Function
5 - Hybrid Coordinator
6 - Hybrid Coordination Function (HCF) Controlled Channel Access
7 - Extensible Authentication Protocol

می‌یابد.

۶۹-۳

مجموعه سرویس پایه مستقل (IBSS)

یک مجموعه سرویس پایه است که یک شبکه مستقل را شکل می‌دهد و در آن هیچگونه دسترسی به سامانه توزیع (DS)[1] قابل دسترس نیست.

۷۰-۳

آدرس مجزا[2]

به تعریف آدرس تک‌پخشی مراجعه شود.

۷۱-۳

زیرساخت[3]

زیرساخت شامل رسانه سامانه توزیع (DSM)، نقطه دسترسی (AP)، و هستارهای درگاهی است و همچنین محل منطقی کارکردهای سرویس توزیع و یکپارچگی یک ESS است. یک زیرساخت شامل سامانه توزیع به همراه یک یا چند AP و صفر یا چند درگاه است.

۷۲-۳

سرویس یکپارچه[4]

سرویسی است که تحویل MSDUها را بین سامانه توزیع و یک شبکه محلی غیر IEEE 802.11 (از طریق یک درگاه) ممکن می‌کند.

۷۳-۳

شمارنده کلید[5]

یک شمارنده ۲۵۶ بیتی (۳۲ هشتایی) است که در تابع شبه تصادفی (PRF)[6] برای ایجاد IVها استفاده می‌شود. یک شمارنده کلید واحد برای هر ایستگاه وجود دارد که برای آن ایستگاه جهانی است.

۷۴-۳

کپسوله کردن داده کلید (KDE)[7]

قالبی برای داده‌ها غیر اطلاعاتی در فیلد داده کلید EAPOL است.

۷۵-۳

سرویس مدیریت کلید[8]

سرویسی برای توزیع و مدیریت کلیدهای رمزنگاری در یک شبکه کاملاً امن (RSN)[1] است.

---

1 - Distribution System
2 - Individual address
3 - Infrastructure
4 - Integration service
5 - Key counter
6 - Pseudo-Random Function
7 - Key Data Encapsulation
8 - Key management service

۷۶-۳

پیوند[۲]

در یک هستار IEEE 802.11 MAC، یک مسیر فیزیکی شامل دقیقاً یک پیمایش از رسانه بی‌سیم است که برای انتقال یک MSDU بین دو ایستگاه استفاده می‌شود.

۷۷-۳

حاشیه پیوند[۳]

نسبت توان سیگنال دریافت‌شده به حداقل توان مطلوب ایستگاه است. ایستگاه ممکن است اطلاعات نرخ و شرایط کانال را به همراه تداخل در محاسبه حاشیه پیوند منظور کند. آلگوریتم خاص برای محاسبه حاشیه پیوند، وابسته به پیاده‌سازی است.

۷۸-۳

انتهای کم‌ارزش[۴]

مفهومی برای نمایش عددی چند هشتایی است، بطوریکه کم‌ارزش‌ترین هشتایی، کوچکترین آدرس را دارد.

۷۹-۳

زنده بودن[۵]

نشانگر این نکته است که واقعاً همتا در این نمونه از ارتباطات شرکت دارد.

۸۰-۳

کلید نشست اصلی (MSK)[۶]

کلیدی است که بین همتاهای EAP استنتاج شده و با روش EAP به AS صادر می‌شود. طول این کلید حداقل ۶۴ هشتایی است.

۸۱-۳

واحد داده پروتکل مدیریت MAC (MMPDU)

واحدی از داده‌های ردوبدل شده بین دو هستار همتای MAC است که از سرویس‌های لایه فیزیکی برای پیاده‌سازی پروتکل مدیریت MAC استفاده می‌کند.

۸۲-۳

واحد داده پروتکل MAC (MPDU)

واحدی از داده‌های ردوبدل شده بین دو هستار همتای MAC است که از سرویس‌های لایه فیزیکی استفاده می‌کند.

---

1 - Robust Security Network
2 - Link
3 - Link margin
4 - Little endian
5 - Liveness
6 - Master Session Key

۸۳-۳

واحد داده سرویس MAC (MSDU)

اطلاعاتی است که به عنوان یک واحد بین نقاط دسترسی سرویسMAC مبادله می‌شود.

۸۴-۳

کد دست‌نخوردگی پیام (MIC) [1]

عدد تولید شده توسط یک تابع رمزنگار است. اگر داده ورودی تغییر کند، مقدار جدید نمی‌تواند بدون اطلاع از کلید(های) رمزنگاری استفاده شده توسط تابع رمزنگار، بصورت صحیح محاسبه شود. این مقدار، کد تصدیق هویت پیام (MAC)[2] نامیده می‌شده است، اگرچه اختصار MAC در این استاندارد برای مفهوم دیگری در نظر گرفته شده است.

۸۵-۳

مایکل[3]

کد دست نخوردگی پیام (MIC) برای پروتکل دست نخوردگی کلید موقت (TKIP)[4] است.

۸۶-۳

ایستگاه سیار[5]

نوعی ایستگاه است که از ارتباطات شبکه در هنگام حرکت استفاده می‌کند.

۸۷-۳

چندپخشی[6]

زمانی این اصطلاح برای یک MSDU به کار می‌رود، که آدرس مقصد آن یک آدرس چندپخشی باشد و زمانی این اصطلاح برای یک MPDU یا قاب کنترل به کار می‌رود که آدرس گیرنده آن یک آدرس چندپخشی باشد.

۸۸-۳

آدرس چندپخشی[7]

یک آدرس MAC است که بیت گروه آن "۱" شده است.

۸۹-۳

آدرس گروهی چندپخشی[8]

یک آدرس MAC مرتبط با پیمانی سطح بالاتر استکه متشکل از گروهی از ایستگاه‌هایی است که بصورت

---

1 - Message Integrity Code

2 - Message Authentication Code

دقت شود که در اکثر متن MAC کوته واژه مربوط به Media Access Control است.

3 - Michael

4 - Temporal Key Integrity Protocol

5 - Mobile station

6 - Multicast

7 - Multicast address

8 - Multicast-group address

منطقی با هم مرتبط هستند.

۹۰-۳

بردار تخصیص شبکه (NAV) [1]

نشانگری نگهداری شده توسط هر ایستگاه از دوره‌های زمانی است که ارسال به محیط بی‌سیم توسط ایستگاه آغاز نخواهد شد مستقل از اینکه تابع ارزیابی کانال پاک (CCA)[2] ایستگاه، محیط بی‌سیم را اشغال تشخیص تشخیص بدهد یا خیر.

۹۱-۳

ایستگاه کیفیت سرویس غیر نقطه دسترسی (non-AP QoS STA) [3]

ایستگاهی است که تسهیلات کیفیت سرویس را پشتیبانی می‌کند اما یک AP نیست. یک ایستگاه non-AP دارای یک HC نیست و از QoS AP برای سرویس‌های سامانه توزیع (DSSs) استفاده می‌کند.

۹۲-۳

بی بدیل[4]

یک مقدار عددی است که در عملیات رمز نگاری مرتبط با یک کلید رمزنگاری خاص استفاده می‌شود و نباید مجدداً با آن کلید استفاده شود که این شامل تمام مقداردهی‌های مجدد سامانه در تمام دفعات است.

۹۳-۳

نقطه دسترسی بدون کیفیت سرویس (non-QoS AP)

یک نقطه دسترسی است که تسهیلات کیفیت سرویس را پشتیبانی نمی‌کند.

۹۴-۳

مجموعه سرویس پایه بدون کیفیت سرویس (non-QoS BSS)

یک BSS است که تسهیلات کیفیت سرویس را پشتیبانی نمی‌کند.

۹۵-۳

ایستگاه بدون کیفیت سرویس (non-QoS STA)

ایستگاهی است که امکانات کیفیت سرویس را پشتیبانی نمی‌کند.

۹۶-۳

جفتی[5]

به دو هستار (یا یک ویژگی آنها) اطلاق می‌شود که به هم مرتبط هستند، که یک AP و یک ایستگاه مرتبط با آن، یا دو ایستگاه در یک شبکه IBSS مثال‌هایی از آن هستند. این اصطلاح به نوعی از سلسله مراتب کلید رمزنگاری اشاره دارد که به کلیدهای به اشتراک گذاشته شده توسط تنها دو هستار مربوط است.

---

1 - Network Allocation Vector
2 - Clear Channel Assessment
3 - Non-AP QoS STA
4 - Nonce
5 - Pairwise

۹۷-۳

شاه کلید جفتی (PMK) [۱]

کلیدی است که دارای بالاترین مرتبه در این استاندارد است. PMK ممکن است از یک کلید ایجاد شده با روش EAP منتج شود یا مستقیماً از یک کلید از پیش به اشتراک گذاشته شده (PSK)[۲] به دست آید.

۹۸-۳

همبستگی امنیتی شاه کلید جفتی (PMKSA) [۳]

حالتی حاصل از مبادله موفقیت‌آمیز تصدیق هویت IEEE 802.1X بین همتا و AS یا ایجاد یک PSK است.

۹۹-۳

کلید موقتی جفتی (PTK) [۴]

مقداری است که از PMK، AA، آدرس متقاضی (SPA)[۵]، بی بدیل تصدیق کننده هویت (Anonce)[۶] و بی بدیل متقاضی، با استفاده از PRF متنج شده است و تا ۵ کلید قابل تقسیم است: کلید رمزنگاری موقتی، دو کلید MIC موقتی، KEK و کلید تأیید کلید EAPOL (KCK)[۷].

۱۰۰-۳

همبستگی امنیتی کلید موقتی جفتی (PTKSA) [۸]

حالتی است که از یک دست‌دهی موفقیت‌آمیز چهار طرفه بین همتا و تصدیق کننده هویت ایجاد می‌شود.

۱۰۱-۳

کیفیت سرویس پارامترگذاری شده[۹]

رفتاری از MPDUها است که بستگی به پارامترهای مربوط به MPDUها دارد. کیفیت سرویس پارامترگذاری شده اصولاً از طریق سازوکار HCCA فراهم می‌شود، اما ممکن است توسط سازوکار EDCA زمانیکه مشخصات ترافیک (TSPEC)[۱۰] برای کنترل پذیرش استفاده می‌شود، نیز فراهم گردد.

۱۰۲-۳

رمز عبور[۱۱]

یک رشته متنی سری است که برای اثبات هویت کاربر استفاده می‌شود.

۱۰۳-۳

دست‌دهی کلید همتا[۱۲]

---

1 - Pairwise Master Key
2 - Preshared Key
3 - Pairwise Master Key Security Association
4 - Pairwise Transient Key
5 - Supplicant Address
6 - Authenticator nonce
7 - EAPOL-Key Confirmation Key
8 - Pairwise Transient Key Security Association
9 - Parameterized Quality of Service
10 - Traffic Specification
11 - Pass-phrase
12 - PeerKey handshake

یک پروتکل مدیریت کلید است که از دست‌دهی SMK و دست‌دهی STK تشکیل شده است و برای ایجاد همبستگی‌های امنیتی SMK (SMKSAs)[1] و همبستگی‌های امنیتی STK (STKSAs)[2]جدید جهت ایمن ایمن کردن STSLها استفاده می‌شود.

۱۰۴-۳

کلید رمزنگاری برای هر قاب[3]

یک کلید رمزنگاری یگانه برای هر MPDU است که توسط برخی پروتکل‌های امنیتی IEEE 802.11 به کار برده می‌شود.

۱۰۵-۳

شمارنده توالی برای هر قاب[4]

برای TKIP، شمارنده‌ای است که به عنوان بی بدیل در استنتاج کلید رمزنگاری برای هر قاب استفاده می‌شود. برای پروتکل حالت شمارنده با کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمز (CCMP) [5]، IV برای هر قاب است.

۱۰۶-۳

سواری دادن[6]

افزونی بار یک قاب داده است که با یک تأییدیه رسیدنMPDU از قبل و/یا یک سرکشی از ایستگاهی که قاب‌ها به آن ارسال می‌شوند، انجام می‌شود.

۱۰۷-۳

هماهنگ کننده نقطه‌ای (PC) [7]

هستاری داخل ایستگاه در یک AP است که کارکرد هماهنگی مرکزی را انجام می‌دهد.

۱۰۸-۳

کارکرد هماهنگی نقطه‌ای (PCF) [8]

رده‌ای از کارکردهای هماهنگی ممکن است که در آن منطق کارکرد هماهنگی در تمام مواقع فعالیت شبکه فقط در یک ایستگاه موجود در یک BSS، فعال است.

۱۰۹-۳

ایستگاه قابل حمل[9]

نوعی ایستگاه است که ممکن است از محلی به محل دیگر حرکت کند، اما تنها هنگامی‌که در یک محل ثابت

---

1 -SMK Security Association
2 - STK Security Association
3 - Per-frame encryption key
4 - Per-frame sequence counter
5 - Counter mode with Cipher-block chaining Message authentication code Protocol
6 - Piggyback
7 - Point Coordinator
8 - Point Coordination Function
9 - Portable station

است، از ارتباطات شبکه استفاده می‌کند.

۱۱۰-۳

درگاه[1]

نقطه‌ای منطقی است که در آن سرویس یکپارچه فراهم شده است.

۱۱۱-۳

همبستگی شبکه امنیتی پیش از خدشه ناپذیری (pre-RSNA)[2]

نوعی ارتباط است که توسط دو ایستگاه بکار گرفته می‌شود، به شرطی که رویه تصدیق هویت و همکاری بین آنها دست‌دهی چهار طرفه نباشد.

۱۱۲-۳

تجهیزات همبستگی شبکه امنیتی پیش از خدشه ناپذیری (pre-RSNA)

تجهیزاتی است که قادر به ایجاد RSNA نیست.

۱۱۳-۳

کلید از پیش به اشتراک گذاشته شده (PSK)

کلیدی ایستا است که با روشی خارج از دامنه این استاندارد و در واقع توسط روش‌هایی خارج از باند، به واحدهای سامانه توزیع می‌شود.

۱۱۴-۳

کیفیت سرویس اولویت بندی شده[3]

ارائه سرویسی است که در آن MPDUهای دارای اولویت بالاتر، با رفتاری متفاوت و ممتاز نسبت به MPDUهای دارای اولویت پایین‌تر برخورد می‌شود. کیفیت سرویس اولویت بندی شده از طریق سازوکار EDCA فراهم می‌شود.

۱۱۵-۳

سازوکار حفاظت[4]

رویه‌ای است که سعی در به‌روزرسانی NAVهای تمام ایستگاه‌های گیرنده، پیش از ارسال یک قاب دارد که ممکن است در هستارهای لایه فیزیکی آن ایستگاه‌های گیرنده، به عنوان فعالیت معتبر شبکه شناخته شود یا نشود.

۱۱۶-۳

قاب سازوکار حفاظت[5]

قابی است که به عنوان بخشی از یک رویه سازوکار حفاظت ارسال می‌شود.

---

1 - Portal
2 - Pre-Robust Security Network Association
3 - Prioritized Quality of Service
4 - Protection mechanism
5 - Protection mechanism frame

۱۱۷-۳

تابع شبه تصادفی (PRF)

تابعی است که ورودی‌های مختلف را در هم می‌ریزد تا یک مقدار شبه تصادفی استنتاج نماید. برای تضمین بقای یک ارتباط که در آن از مقدار شبه تصادفی استفاده می‌شود، یک بی بدیل به عنوان یکی از ورودی‌های تابع استفاده می‌شود.

۱۱۸-۳

نقطه دسترسی کیفیت سرویس (QoS AP)

نقطه دسترسی‌ای است که تسهیلات کیفیت سرویس را پشتیبانی می‌کند. کارکردهای QoS AP ابرمجموعه کارکردهای یک non-QoS AP است و بنابراین یک QoS AP قادر است مشابه یک non-QoS AP برای ایستگاه‌های non-QoS عمل کند.

۱۱۹-۳

مجموعه سرویس پایه کیفیت سرویس (QoS BSS)

BSS ای است که تسهیلات QoS را فراهم می‌کند. یک زیرساخت QoS BSS شامل یک QoS AP است.

۱۲۰-۳

تسهیلات کیفیت سرویس[1]

مجموعه‌ای از کارکردهای ارتقاء یافته، قوانین دسترسی به کانال، قالب‌های قاب، توالی‌های مبادله قاب و اشیاء مدیریت شده است که برای تدارک کیفیت سرویس اولویت بندی شده و پارامترگذاری شده استفاده می‌شود.

۱۲۱-۳

مجموعه سرویس پایه مستقل کیفیت سرویس (QoS IBSS)

IBSS ای است که در آن یک یا چند ایستگاه، تسهیلات کیفیت سرویس را پشتیبانی می‌کنند.

۱۲۲-۳

ایستگاه کیفیت سرویس (QoS STA)

ایستگاهی است که تسهیلات کیفیت سرویس را پیاده‌سازی می‌کند. یک ایستگاه QoS زمانی‌که با یک non-QoS BSS ارتباط دارد، مشابه یک ایستگاه non-QoS عمل می‌کند.

۱۲۳-۳

سرویس همبستگی مجدد[2]

سرویسی است که یک ارتباط برقرار شده بین نقطه دسترسی و ایستگاه را قادر به انتقال از یک AP به AP دیگر (یا همان AP) می‌کند.

۱۲۴-۳

توان دریافتی[1]

---

1 - Quality of Service facility
2 - Reassociation service

میانگین توان اندازه‌گیری شده در اتصال‌دهنده[2] آنتن است.

۱۲۵-۳

نشانگر توان دریافتی (RPI)[3]

یک درجه بندی از سطح توان دریافتی از دید اتصال‌دهنده آنتن است.

۱۲۶-۳

شبکه کاملاً امن (RSN)

شبکه‌ای امنیتی است که فقط تولید RSNAها را مقدور می‌کند. یک RSN می‌تواند با استفاده از نشانه عنصر اطلاعاتی RSN از قاب‌های راهنما[4] که مجموعه رمز گروه، از نوع حریم خصوصی معادل باسیم (WEP)[5] نیست، شناسایی شود.

۱۲۷-۳

همبستگی شبکه کاملاً امن (RSNA)[6]

نوعی ارتباط است که اگر رویه تصدیق هویت استقرار یا ارتباط بین یک جفت ایستگاه، شامل دست‌دهی چهار طرفه باشد، توسط این دو استفاده می‌گردد. متذکر می‌شود که صرف وجود یک RSNA برای یک جفت از تجهیزات، باعث تأمین امنیت کامل نمی‌شود. امنیت کامل زمانی فراهم می‌شود که تمام تجهیزات شبکه از RSNAها استفاده کنند.

۱۲۸-۳

تجهیزاتی با قابلیت RSNA[7]

ایستگاهی است که قادر به ایجاد RSNAها است. چنین تجهیزاتی به دلیل پیکربندی می‌توانند از pre-RSNAها استفاده کند. متذکر می‌شود که داشتن قابلیت RSNA، جهت برآورده کردن وضعیت پیروی پیاده‌سازی پروتکل (PICS)[8] RSNA کافی نیست. تجهیزات پیشین که به TKIP ارتقاء یافته‌اند، می‌توانند دارای قابلیت RSNA باشند، اما اگر CCMP را نیز پشتیبانی نکنند، با PICS منطبق نخواهند بود.

۱۲۹-۳

تجهیزات دارای امکان RSNA[9]

ایستگاهی است که RSNA-capable است و dot11RSNAEnabled آن، برابر صحیح (“True”) تنظیم شده است.

---

1 - Receive power
2 - Connector
3 - Received Power Indicator
4 - Beacon
5 - Wired Equivalent Privacy
6 - Robust Security Network Association
7 - Robust Security Network Association- (RSNA-) capable equipment
8 - Protocol Implementation Conformance Statement
9 - Robust Security Network Association- (RSNA-) enable equipment

۱۳۰-۳

مدیریت کلید RSNA [1]

مدیریت کلیدی است که شامل دست‌دهی چهار طرفه ، دست‌دهی کلید گروهی، و دست‌دهی کلید همتا است.

۱۳۱-۳

دوره سرویس زمان‌بندی شده [2]

دوره سرویسی است که توسط نقطه دسترسی کیفیت سرویس زمان‌بندی شده است. دوره سرویس زمان‌بندی شده در بازه‌های ثابت زمانی آغاز می‌شود.

۱۳۲-۳

شبکه امنیتی [3]

BSS ای است که در آن ایستگاه آغازگر BSS، اطلاعات قابلیت‌های امنیتی و پیکربندی BSS را با اضافه کردن عنصر اطلاعاتی RSN در قاب‌های راهنما فراهم می‌کند.

۱۳۳-۳

انتخابگر [4]

موردی است که مشخص‌کننده یک لیست تشکیل‌دهنده در یک عنصر اطلاعاتی پیام مدیریت IEEE 802.11 است.

۱۳۴-۳

بازه زمانی سرویس (SI) [5]

بازه زمانی بین آغاز دو دوره سرویس زمان‌بندی شده متوالی است.

۱۳۵-۳

دوره سرویس (SP)

یک زمان پیوسته است که در حین آن یک یا چند قاب تک‌پخشی پیونده فروسو به یک ایستگاه کیفیت سرویس ارسال می‌شوند و/یا یک یا چند TXOP به ایستگاه یکسانی داده می‌شود. دوره‌های سرویس ممکن است زمان‌بندی شده با غیر زمان‌بندی شده باشند. برای یک ایستگاه non-AP، در هرزمان حداکثر یک دوره سرویس فعال می‌تواند وجود داشته باشد.

۱۳۶-۳

ایستگاه (STA)

تجهیزاتی است که شامل یک MAC و واسط لایه فیزیکی (PHY)منطبق بر IEEE 802.11 با محیط بی‌سیم است.

---

1 - Robust Security Network Association- (RSNA-) key management
2 - Scheduled service period
3 - Security network
4 - Selector
5 - Service Interval

۱۳۷-۳

سرویس ایستگاه (SS) [1]

مجموعه‌ای از سرویس‌هایی است که انتقال MSDUها را بین ایستگاه‌های داخل یک BSS پشتیبانی می‌کند.

۱۳۸-۳

پیونده ایستگاه به ایستگاه (STSL) [2]

یک پیونده مستقیم برقرارشده بین دو ایستگاه است که به یک نقطه دسترسی مشترک مرتبط شده‌اند. این اصطلاح به یک سازوکار عام اطلاق می‌شود که ممکن است جهت ایجاد ارتباط مستقیم ایستگاه به ایستگاه در حالت زیر ساخت، پیاده‌سازی شود. برقراری این نوع پیونده شامل یک مرحله مقداردهی اولیه است. STSL با رویه‌های خاص قطع ارتباط تحت شرایط تعیین شده در این استاندارد، خاتمه می‌پذیرد. مثال جدید این رویه، پیونده مستقیم توسط برقراری پیونده مستقیم (DSL)[3] است.

۱۳۹-۳

شاه کلید پیونده ایستگاه به ایستگاه (SMK) [4]

یک مقدار تصادفی است که توسط یک AP در حین یک دست‌دهی SMK ایجاد می‌شود و برای استنتاج یک STK استفاده می‌شود.

۱۴۰-۳

دست‌دهی SMK [5]

یک پروتکل مدیریت کلید بین دو طرفی است که یک SMK جدید را تولید می‌کنند.

۱۴۱-۳

همبستگی امنیتی SMK (SMKSA)

حالتی است که ناشی از یک دست‌دهی موفقیت‌آمیز SMK است.

۱۴۲-۳

کلید موقتی پیونده ایستگاه به ایستگاه (STK)

مقداری است که از SMK، آدرس MAC آغازگر (MAC_I)[6]، آدرس MAC همتا (MAC_P)، بی بدیل آغازگر (Inonce)[7] و بی بدیل همتا (PNounce)[8] ، با استفاده از تابع شبه تصادفی (PRF) منتج می‌شود. این این مقدار تاتا ۵ کلید قابل تقسیم است: کلید رمزنگاری موقتی، دو کلید MIC موقتی، KEK و KCK.

---

1 - Station Service
2 - Station-to-Station Link
3 - Direct-Link Setup
4 - Station-to-station link Master Key
5 - Station-to-station link Master Key (SMK) handshake
6 - Initiator MAC Address
7 - Initiator nonce
8 - Peer Nonce

۱۴۳-۳

همبستگی امنیتی STK (STKSA)

حالتی است که ناشی از یک مبادله موفقیت‌آمیز STK است.

۱۴۴-۳

متقاضی[1]

هستاری در یک انتهای یک قسمت LAN نقطه به نقطه است که توسط یک تصدیق‌کننده هویت متصل به انتهای دیگر آن پیوندە، تصدیق هویت می‌شود (IEEE std 802.1X:2004).

۱۴۵-۳

آدرس درخواست‌کننده (SPA)

آدرس MAC درخواست‌کننده IEEE 802.1X است.

۱۴۶-۳

کلید رمزنگاری موقتی[2]

بخشی از یک PTK یا GTK است که به‌طور مستقیم یا غیرمستقیم برای رمزنگاری داده‌های MPDU استفاده می‌شود.

۱۴۷-۳

کلید موقتی[3]

ترکیب کلید رمزنگاری موقتی و کلید کد دست‌نخوردگی پیام موقتی است.

۱۴۸-۳

کلید موقتی کد دست نخوردگی پیام

بخشی از یک کلید موقتی است که برای اطمینان از دست نخوردگی MSDUها یا MPDUها استفاده می‌شود.

۱۴۹-۳

واحد زمانی (TU) [4]

زمانی معادل ۱۰۲۴ میکروثانیه است.

۱۵۰-۳

دسته‌بندی ترافیکی (TC) [5]

برچسبی برای MSDUهایی است که از دید هستارهای لایه بالاتر، اولویت کاربر (UP)[6] متمایزی نسبت به سایر MSDUهای ارائه شده جهت ارسال بر روی همان پیونده را دارند. این دسته‌بندی‌های ترافیکی تنها

1 - Supplicant
2 - Temporal encryption key
3 - Temporal key
4 - Time Unit
5 - Traffic Category
6 - User Priority

برای هستارهای MAC که کیفیت سرویس را در سرویس داده MAC پشتیبانی می‌کنند، معنادار هستند. این هستارهای MAC، اولویت کاربر را برای MSDUهای متعلق به یک دسته ترافیکی خاص، با استفاده از مقدار اولویت فراهم شده توسط آن MSDUها در نقطه دسترسی سرویس MAC (MAC_SAP) [1]، تعیین می‌کنند.

۱۵۱-۳

رده‌بندی ترافیک (TCLAS) [2]

مشخصات مقادیر پارامتر خاص برای شناسایی MSDUهای متعلق به یک جریان ترافیکی (TS) [3] خاص است. فرآیند رده‌بندی، که بالای MAC_SAP ، در یک QoS AP انجام می‌شود، از مقادیر پارامتر برای یک TS خاص استفاده می‌کند تا MSDU ورودی را بررسی نموده و تعیین نماید که آیا این MSDU متعلق به آن TS هست یا خیر. TCLAS ممکن است در ایستگاه non-AP QoS با چندین جریان نیز رخ دهد. چنین رده‌بندی‌هایی خارج از حیطه این استاندارد است.

۱۵۲-۳

شناسه ترافیک (TID) [4]

هر یک از شناسه‌های مورد استفاده هستارهای بالاتر جهت تشخیص MSDUها از هستارهای MACای است که کیفیت سرویس را در سرویس داده MAC پشتیبانی می‌کنند. ۱۶مقدار TID ممکن است؛ هشت TC شناسایی، و هشت TS شناسایی پارامترگذاری شده دیگر. TID در لایه‌های بالای MAC به یک MSDU اختصاص می‌یابد.

۱۵۳-۳

مشخصات ترافیک (TSPEC) [5]

مشخصات کیفیت سرویس یک جریان داده به و/یا از یک ایستگاه non-AP QoS است.

۱۵۴-۳

جریان ترافیک (TS)

مجموعه‌ای از MSDUهاست که تحت مقادیر پارامتر کیفیت سرویس فراهم شده توسط MAC در یک TSPEC خاص، باید تحویل داده شوند. TSها تنها برای هستارهای MAC که کیفیت سرویس را در سرویس داده MAC پشتیبانی می‌کنند، معنی‌دار هستند. این هستارهای MAC، TSPEC قابل اجرا برای تحویل MSDUهای متعلق به یک TS خاص را با استفاده از مقدار TSID فراهم شده توسط MSDUهای موجود در MAC_SAP تعیین می‌کنند.

۱۵۵-۳

شناسه جریان ترافیک (TSID) [1]

---

1 - MAC Service Access Point
2 - Traffic Classification
3 - Traffic Stream
4 - Traffic Identifier
5 - Traffic Specification

عبارت است از شناسه‌های مورد استفاده توسط هستارهای لایه بالاتر برای تشخیص MSDUها از هستارهای MAC برای کیفیت سرویس پارامترگذاری شده (جریان ترافیک در یک مشخصات ترافیک خاص) در سرویس داده MAC. TSID در لایه‌های بالای MACبه یک MSDU اختصاص می‌یابد.

۱۵۶-۳

شبکه امنیت عبوری (TSN) [۲]

شبکه امنیتی است که ایجاد RSNAها و pre-RSNAها را مقدور می‌سازد. یک TSN می‌تواند با نشانه موجود در عنصر اطلاعات RSN از قاب‌های راهنما که مجموعه رمز گروه مورد استفاده، WEP است شناسایی شود.

۱۵۷-۳

فرصت ارسال (TXOP) [۳]

یک بازه زمانی است که در آن ایستگاه کیفیت سرویس اجازه دارد توالی‌های تبادل قاب به رسانه بی‌سیم را آغاز کند. یک TXOP ، با یک نقطه شروع و یک حداکثر دوره تعریف می‌شود. TXOP یا توسط ایستگاه و با رقابت موفقیت‌آمیز بر سر کانال بدست می‌آید و یا توسط HC تخصیص داده می‌شود.

۱۵۸-۳

دارنده فرصت ارسال [۴]

ایستگاه کیفیت سرویسی است که یک TXOP را توسط HC صاحب شده یا با رقابت موفقیت‌آمیز آن را به دست آورده است.

۱۵۹-۳

توان ارسالی [۵]

توان موثر منتشره همه جهته‌ای (EIRP) [۶] است که به عملیات لایه فیزیکی همتافتگری تقسیم فرکانسی متعامد (OFDM) [۷] IEEE 802.11 پنج گیگاهرتز، در کشوری که آن را تصویب کرده است، مربوط می‌شود.

۱۶۰-۳

دسته دسترسی با امکان تحریک (AC) [۸]

یک دسته دسترسی ایستگاه کیفیت سرویس non-AP است که قاب‌های زیرگروه QoS Data و QoS Null از ایستگاه non-AP که به AC نگاشت می‌شوند، در صورتی‌که دوره سرویسی در جریان نباشد، یک دوره سرویس زمان‌بندی نشده را آغاز می‌کنند.

---

1 - Traffic Stream Identifier
2 - Transition Security Network
3 - Transmission Opportunity
4 - Transmission Opportunity (TXOP) holder
5 - Transmit power
6 - Effective Isotropic Radiated Power
7 - Orthogonal Frequency Division Multiplexing
8 - Trigger-enabled Access Category

۱۶۱-۳

افشاء غیرمجاز[1]

فرآیند در دسترس قرار دادن اطلاعات برای اشخاص، هستارها و پردازش‌های غیرمجاز است.

۱۶۲-۳

استفاده غیرمجاز از منابع[2]

استفاده از منابع به صورت ناسازگار با خط‌مشی امنیتی تعریف شده است.

۱۶۳-۳

تک‌پخشی[3]

اگر برای یک MSDU بکار برده شود، MSDUای است که به عنوان آدرس مقصد (DA)، یک آدرس گیرنده واحد دارد. اگر برای MPDU یا قاب کنترل استفاده شود، MPDU یا قاب کنترلی است که به عنوان آدرس گیرنده (RA)، یک آدرس گیرنده واحد دارد.

۱۶۴-۳

آدرس تک‌پخشی[4]

آدرس هدایت شده[5]

آدرس انفرادی[6]

یک آدرس MAC است که بیت گروه آن "۱" نشده است.

۱۶۵-۳

گسترش یکنواخت[7]

مقرراتی برای سازوکار انتخاب کانال است که استفاده یکنواختی را از طریق حداقل مجموعه کانال‌ها در محدوده مقررات فراهم می‌کند.

۱۶۶-۳

دوره سرویس زمان‌بندی نشده[8]

دوره‌ای است که با ارسال یک قاب تحریک[9] از یک ایستگاه کیفیت سرویس non-AP به نقطه دسترسی QoS آغاز می‌شود.

۱۶۷-۳

پیونده فراسو[10]

---

1 - Unauthorized disclosure
2 - Unauthorized resource use
3 - Unicast
4 - Unicast address
5 - Directed address
6 - Individual address
7 - Uniform spreading
8 - Unscheduled service period
9 - Trigger frame
10 - Uplink

یک پیونده یک طرفه از یک ایستگاه غیر نقطه دسترسی به یک نقطه دسترسی است.

۱۶۸-۳

اولویت کاربر (UP)

مقداری مرتبط با یک MSDU است که نشان می‌دهد چگونه MSDU باید مدیریت شود. UP در لایه‌های بالای MAC به یک MSDU اختصاص می‌یابد.

۱۶۹-۳

حریم خصوصی معادل باسیم (WEP)

یک آلگوریتم محرمانگی داده رمزنگاری (تأیید نشده) است که توسط استاندارد IEEE Std 802.11 مشخص شده است و ممکن است برای فراهم کردن محرمانگی داده استفاده شود که از نظر موضوعی با یک شبکه محلی باسیم که از فنون رمزنگاری برای ارتقاء محرمانگی داده استفاده نمی‌کند، معادل است.

۱۷۰-۳

سامانه توزیع بی‌سیم (WDS)[1]

سازوکاری برای ارتباط بی‌سیم است که از یک قالب قاب چهار آدرسی که در این استاندارد مشخص شده است، استفاده می‌کند. این استاندارد، چنین قالب قابی را شرح می‌دهد، اما چگونگی استفاده از چنین سازوکار یا قالب داده‌ای را توضیح نمی‌دهد.

۱۷۱-۳

سامانه شبکه محلی بی‌سیم (WLAN)

سامانه‌ای شامل DS، APها و هستارهای درگاه و همچنین مکان منطقی کارکردهای توزیع و یکپارچگی یک ESS است. یک سامانه WLAN علاوه بر DS، شامل یک یا چند AP و صفر یا چند درگاه است.

۱۷۲-۳

رسانه بی‌سیم (WM)

رسانه‌ای است که برای پیاده‌سازی انتقال PDUها بین هستارهای لایه فیزیکی همتای یک شبکه محلی بی‌سیم استفاده می‌شود.

1 - Wireless Distribution System

۴ فهرست اصطلاحات معادل

معادل فارسی	اصطلاح انگلیسی
دست‌دهی چهار طرفه	4-Way Handshake
شاه کلید پیونده ایستگاه به ایستگاه چهار طرفه	4-Way Station-to-Station Link (STSL) Master Key
دست‌دهی کلید موقتی پیونده ایستگاه به ایستگاه چهار طرفه	4-Way Station-to-Station Link (STSL) Transient Key (STK)
دسته دسترسی	Access Category
نقطه دسترسی	Access Point
نقطه دسترسی/ایستگاه	Access Point/Station
شبکه خاص	Ad hoc network
داده تصدیق هویت اضافی	Additional authentication data
کنترل پذیرش	Admission control
زمانبندی تجمیعی	Aggregated schedule
همبستگی	Association
تصدیق هویت	Authentication
مجموعه تصدیق هویت و مدیریت کلید	Authentication and Key Management
سرویس‌ده تصدیق هویت	Authentication Server
تصدیق کننده هویت	Authenticator
آدرس تصدیق کننده هویت	Authenticator Address
بی بدیل تصدیق کننده هویت	Authenticator nonce
مجاز	Authorized
ناحیه سرویس پایه	Basic Service Area
راهنما	Beacon
انتهای پرارزش	Big Endian
آدرس پخش همگانی	Broadcast address
تشخیص حامل	Carrier Sense
دسترسی چندگانه تشخیص حامل با اجتناب از برخورد	Carrier Sense Multiple Access with Collision Avoidance
فاصله‌گذاری کانال	Channel spacing
مجموعه رمزنگاری	Cipher suite

Cipher-block chaining message authentication code	کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمزنگاری
Clear Channel Assessment	کارکرد سنجش کانال شفاف
Clear Channel Assessment	ارزیابی کانال پاک
Connector	اتصال‌دهنده
Contention Free pollable	سرکشی بدون رقابت
Contention Period	دوره رقابت
Contention-Free Period	دوره بدون رقابت
Controlled Access Phase	فاز دسترسی کنترل شده
Coordination Function	تابع هماهنگی
Counter mode	حالت شمارنده
Counter mode with Cipher-block chaining Message authentication code	حالت شمارنده با کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمزنگاری
Counter mode with Cipher-block chaining Message authentication code Protocol	پروتکل حالت شمارنده با کد تصدیق هویت پیام با زنجیره‌ای از بلوک رمز
Cryptographic encapsulation	کپسوله کردن رمزنگاری
Data confidentiality	محرمانگی داده
Deauthentication service	سرویس ابطال تصدیق هویت
Decapsulate	حذف کردن کپسول
Decapsulation	حذف کپسول
Defragmentation	تکه‌ها
Delivery-enabled access category	دسته دسترسی با امکان تحویل
Direct link	پیونده مستقیم
Directed address	آدرس هدایت شده
Directed frame	قاب هدایت شده
Direct-Link Setup	برقراری پیونده مستقیم
Disassociation service	سرویس عدم همکاری
Distributed Coordination Function	تابع هماهنگی توزیع شده
Distribution service	سرویس توزیع
Distribution System	سامانه توزیع
Distribution System	سامانه توزیع
Distribution System Medium	رسانه سامانه توزیع
Distribution System Services	سرویس‌های سامانه توزیع

Downlink	پیونده فروسو
Dynamic Frequency Selection	انتخاب پویای فرکانس
Dynamic Frequency Selection owner	انتخاب‌گر پویای فرکانس
EAPOL-Key Confirmation Key	کلید تأیید کلید پروتکل تصدیق هویت قابل گسترش در شبکه‌های محلی
EAPOL-Key Confirmation Key	کلید تأیید کلید EAPOL
EAPOL-Key Encryption Key	کلید رمزنگاری کلید EAPOL
Effective Isotropic Radiated Power	توان تابشی همه جهته موثر
Effective Isotropic Radiated Power	توان موثر منتشره همه جهته
Encapsulation	کپسوله کردن
Enhanced Distributed Channel Access	دسترسی کانال توزیع شده ارتقاء یافته
Enhanced Distributed Channel Access Function	کارکرد دسترسی کانال توزیع شده ارتقاء یافته
Entity	هستار
Extended Service Area	ناحیه سرویس گسترش یافته
Extended Service Set	مجموعه سرویس گسترش یافته
Extensible Authentication Protocol	پروتکل تصدیق هویت قابل گسترش
Extensible Authentication Protocol over LANs	پروتکل تصدیق هویت قابل گسترش در شبکه‌های محلی
Fixed	ثابت
Fragmentation	تکه تکه کردن
Gaussian Frequency Shift Keying	جابجایی گوسی فرکانس
Group Key Handshake	دست‌دهی کلید گروهی
Group Master Key	شاه کلید گروهی
Group Temporal Key	کلید موقت گروهی
Group Temporal Key Security Association	همبستگی امنیتی کلید موقت گروهی
Hidden Station	ایستگاه پنهان
Hybrid Coordination Function	تابع هماهنگی مختلط
Hybrid Coordination Function (HCF) Controlled Channel Access	دسترسی کانال کنترل شده تابع هماهنگی مختلط
Hybrid Coordinator	هماهنگ‌کننده مختلط
Independent Basic Service Set	مجموعه سرویس پایه مستقل
Individual address	آدرس مجزا

Individual address	آدرس انفرادی
Infrastructure	زیرساخت
Initialization Vectors	بردارهای مقداردهی اولیه
Initiator MAC Address	آدرس MAC آغازگر
Initiator Nonce	بی بدیل آغازگر
Integration Service	سرویس یکپارچه
Key counter	شمارنده کلید
Key Data Encapsulation	کپسوله کردن داده کلید
Key Data Field	فیلد داده کلید
Key management service	سرویس مدیریت کلید
Link	پیوند
Link margin	حاشیه پیوند
Little Endian	انتهای کم‌ارزش
Liveness	زنده بودن
Local area	ناحیه محلی
Local Area Network	شبکه محلی
Logical Link Control	کنترل پیوند منطقی
MAC Management Protocol Data Unit	واحد داده پروتکل مدیریت MAC
MAC Protocol Data Units	واحدهای داده پروتکل MAC
MAC Service Access Point	نقطه دسترسی سرویس MAC
MAC Service Data Unit	واحد داده سرویس MAC
Master Session Key	کلید نشست اصلی
Medium Access Control	کنترل دسترسی رسانه
Message Authentication Code	کد تصدیق هویت پیام
Message Integrity Code	کد دست‌نخوردگی پیام
Michael	مایکل
Mobile station	ایستگاه سیار
Multicast	چندپخشی
Multicast address	آدرس چندپخشی
Multicast-group address	آدرس گروهی چندپخشی
Multi-octet	چند هشتایی
Network Allocation Vector	بردار تخصیص شبکه
Non-Access Point	غیر نقطه دسترسی

Non-AP QoS STA	ایستگاه کیفیت سرویس غیر نقطه دسترسی
Nonce	بی بدیل
Orthogonal Frequency Division Multiplexing	همتافتگری تقسیم فرکانسی متعامد
Overlapping	هم‌پوشان
Pairwise	جفتی
Pairwise Master Key	شاه کلید جفتی
Pairwise Master Key Security Association	همبستگی امنیتی شاه کلید جفتی
Pairwise Transient Key	کلید موقتی جفتی
Pairwise Transient Key Security Association	همبستگی امنیتی کلید موقتی جفتی
Parameterized Quality of Service	کیفیت سرویس پارامترگذاری شده
Pass-phrase	رمز عبور
Payload	پی‌بار
Peer Nonce	بی بدیل همتا
PeerKey Handshake	دست‌دهی کلید همتا
Per-frame encryption key	کلید رمزنگاری برای هر قاب
Per-frame sequence counter	شمارنده توالی برای هر قاب
Physical layer	لایه فیزیکی
Piggyback	سواری دادن
Point Coordination Function	کارکرد هماهنگی نقطه‌ای
Point Coordination Function (PCF) Interframe Space	دوره زمان بین قاب PCF
Point Coordinator	هماهنگ کننده نقطه‌ای
Portable	قابل حمل
Portable Station	ایستگاه قابل حمل
Portal	درگاه
Pre-Robust Security Network Association	همبستگی شبکه امنیتی پیش از خدشه ناپذیری
Preshared Key	کلید از پیش به اشتراک گذاشته شده
Primitives	اولیه‌ها
Prioritized Quality of Service	کیفیت سرویس اولویت بندی شده
Protection mechanism	سازوکار حفاظت
Protection mechanism frame	قاب سازوکار حفاظت
Protocol Implementation Conformance Statement	وضعیت پیروی پیاده‌سازی پروتکل

Pseudo-Random Function	تابع شبه تصادفی
Quality of Service	کیفیت سرویس
Quality of Service facility	تسهیلات کیفیت سرویس
Reassociation service	سرویس همبستگی مجدد
Receive power	توان دریافتی
Received Power Indicator	نشانگر توان دریافتی
Robust Security Network	شبکه کاملاً امن
Robust Security Network Association	همبستگی شبکه کاملاً امن
Robust Security Network Association-(RSNA-) capable equipment	تجهیزاتی با قابلیت RSNA
Robust Security Network Association-(RSNA-) key management	مدیریت کلید RSNA
Scheduled service period	دوره سرویس زمان‌بندی شده
Security network	شبکه امنیتی
Selector	انتخابگر
Service Interval	بازه زمانی سرویس
Service Period	دوره سرویس
SMK Security Association	همبستگی‌های امنیتی SMK
Station	ایستگاه
Station Service	سرویس ایستگاه
Station-to-station Link	پیونده ایستگاه به ایستگاه
Station-to-station link Master Key	شاه کلید پیونده ایستگاه به ایستگاه
Station-to-station link Master Key (SMK) Handshake	دست‌دهی شاه کلید پیونده ایستگاه به ایستگاه
STK Security Association	همبستگی‌های امنیتی STK
Supplicant	متقاضی
Supplicant Address	آدرس متقاضی
Temporal Encryption Key	کلید رمزنگاری موقتی
Temporal key	کلید موقتی
Temporal Key Integrity Protocol	پروتکل دست نخوردگی کلید موقت
Time Unit	واحد زمانی
Traffic Category	دسته‌بندی ترافیکی
Traffic Classification	رده‌بندی ترافیک

Traffic Identifier	شناسه ترافیک
Traffic Specification	مشخصات ترافیک
Traffic Stream	جریان ترافیکی
Traffic Stream Identifier	شناسه جریان ترافیک
Transition Security Network	شبکه امنیت عبوری
Transmission Opportunity	فرصت انتقال
Transmission Opportunity	فرصت ارسال
Transmission Opportunity (TXOP) holder	دارنده فرصت ارسال
Transmit power	توان ارسالی
Transmit Power Control	کنترل توان انتقال
Trigger frame	قاب تحریک
Trigger-enabled Access Category	دسته دسترسی با امکان تحریک
Unauthorized disclosure	افشاء غیرمجاز
Unauthorized resource use	استفاده غیرمجاز از منابع
Unicast	تک پخشی
Unicast address	آدرس تک‌پخشی
Uniform spreading	گسترش یکنواخت
Unscheduled service period	دوره سرویس زمان‌بندی نشده
Uplink	پیونده فراسو
User Priority	اولویت کاربر
Wired Equivalent Privacy	حریم خصوصی معادل باسیم
Wireless Distribution System	سامانه توزیع بی‌سیم
Wireless Local Area Netwok	شبکه محلی بی‌سیم
Wireless Medium	رسانه بی‌سیم

۵ تغییرات

در پذیرش این استاندارد به عنوان استاندارد ملی، عنوان استاندارد از IEEE standard for information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements - Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications به عنوان روی جلد تغییر یافت.

کلیه بندهای استاندارد بین‌المللی IEEE Std 802.11:2007 در مورد این استاندارد معتبر و الزامی است.