Ратифицированные стандарты

IEEE 802.11d

В связи с большим распространением технологии потребовалось согласование ее работы в 6 регулирующих доменах: США, Канада, Евросоюз, Япония, Испания и Франция.

Введенные расширения позволяют точке доступа доставлять необходимые параметры радио-канала радио-клиенту, что автоматически задает радио-частоту для функционирования, соответствующую нормам разных стран.

Кадр-маячок стандарта расширен информацинными полями о стране, параметрах частоты передачи и таблице параметров частоты передачи. Информация о стране: номер первого допустимого канала, число каналов, максимально допустимый уровень мощности передачи. Частотные параметры транляции: число разрешенных для трансляции (хопа) каналов, основание для расчета хопа из таблицы параметров передачи. Таблица параметров частоты передачи: информация, необходимая для формирования последовательности пеердач, разрешенной в стране. Множественные последовательности передач можно хранить в одной таблице.

IEEE 802.11e

Задача обеспечить QoS появилась из-за необходимости передачи VoWLAN-траффика. QoS сети обеспечат видео- и аудио-траффик по требованию, а также высокоскоростной доступ в Интернет.

802.11e задает 4 класса траффика и использует временные параметры на MAC-уровне для приоритезации траффика. Механизм EDCA (Enhanced Distributed Channel Access) маркирует кадры, используя IETF DCSP (Differentiated Services Code Points), и задает следующие категории доступа:

- **Voice:** VoIP использует DSCP 6 или 7 для передачи с малой задержкой (латентностью).
- **Video:** Видео-потоки используют DSCP 4 или 5.
- **Best Effort:** Интерактивные приложения и приложения с большой латентностью используют DSCP 0 или 3. Все станции, не поддерживающие 802.11e, классифицируются в эту категорию.
- **Backgroud:** Поддерживающий траффик использует DSCP 1 или 2.

С каждым классом сассоциирована своя очередь кадров.

802.11e также по-разному задает параметры окна между кадрами: траффик с большим приоритетом имеет меньший параметр ожидания (InterFrame Spacing) для передачи очередного кадра. Точно также отсрочка передачи из-за конфликтов в сети (Contenstion Window, Random Backoff Wait) меньше для траффика с большим приоритетом.

Полная миграция на 802.11e потребует перепрошивки аппаратуры/драйверов, а не замены аппаратного обеспечения.

IEEE 802.11F

В стандарте не описаны варианты реализации, чтобы оставить возможность построения совершенно разных распределенных систем. тандарт обеспечивает большую гибкость в проектировании, но это привело к тому, что точки доступа разных производителей вряд ли смогут взаимодействоватт друг с другом, особенно когда они рассчитаны сразу и на беспровдную, и на проводную связь.

IEEE 802.11e задает протокол IAPP (Inter-AP Protocol), обеспечивающий взаимодействие точек доступа от разных производителей, а также динамическую передачу криптографических ключей между AP (Access Point).

IAPP реализуется поверх сетевого уровня (link layer), а потому не является IEEE стандартом. Скорее это рекомендуемый набор практик, который включает:

- сервисные точки доступа (SAP),
- сервисные примитивы (в том числе сервис передачи криптографических ключей),
- набор функций,
- протокол взаимодействия точек доступа в единой распределенной системе, опирающийся на UDP.

Функции IAPP:

- **сервисы распределенной системы**,
  - формирование и поддержка,
- **отображение адресов беспроводной сети на адреса распределенной системы**,
  - отображение MAC-адресов беспроводной среды на адреса распределенной системы,
- ограничение каждой станции одной ассоциацией (с точкой доступа?) в любой момент времени,
- сервис реассоциации, включающий передачу криптографических ключей,
- поддержка аутентификации и секретности 802.11, включая контроль доступа по 802.1x.

IEEE 802.11i

Стандарт был создан для улучшения безопасности на MAC-уровне и называется теперь Enhanced Security Network (ESN). Видение безопасности WLAN состоит из следующих подходов:

- Wired Equivalent Privacy (WEP) protocol,
- Temporal Key Integrity Protocol (TKIP) - исправляет уязвимости, обнаруженные в WEP протоколе и Rivest Cipher 4 (RC4) алгоритме,
- Advanced Encryption Standard (AES),
- IEEE 802.1x для аутентификации и инициализации криптографическимх ключей, а также управления ими,
- использование AES со 128-битным ключом на MAC-уровне, т.к. RC4 кажется недостаточно надежным.

Стандарт потребует изменений в аппаратной части (новые беспроводные NIC) особенно на

старых медленных компьютерах, так как AES обладает высокой вычислительной дороговизной.