Беспроводные локальные сети: Wireless LAN (WLAN)

Сравнительная таблица стандартов беспроводной связи

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11a	WLAN	до 54 Мбит/с	до 100 метров	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 и 450 Мбит/с (в перспективе до 600 Мбит/с)	до 100 метров	2,4 — 2,5 или 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбит/с	6-10 км	1,5-11 ГГц
WiMax	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2.3-13.6 ГГц
WiMax	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	н/д (стандарт в разработке)	н/д (стандарт в разработке)
Bluetooth v1.1.	802.15.1	WPAN	до 1 Мбит/с	до 10 метров	2,4 ГГц
	802.15.3	WPAN	от 11 до 55 Мбит/с	до 100 метров	2,4 ГГц
Bluetooth v3.0 + HS	802.11	WPAN	от 3 Мбит/с до 24 Мбит/с	до 100 метров	2,4 ГГц
UWB	802.15.3a	WPAN	110-480 Мбит/с	до 10-3 метров	7,5 ГГц
ZigBee	802.15.4	WPAN	от 20 до 250 Кбит/с	1-100 м	2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал)
Инфракрасный порт	IrDA	WPAN	до 16 Мбит/с	от 5 до 50 сантиметров, односторонняя связь — до 10 метров	

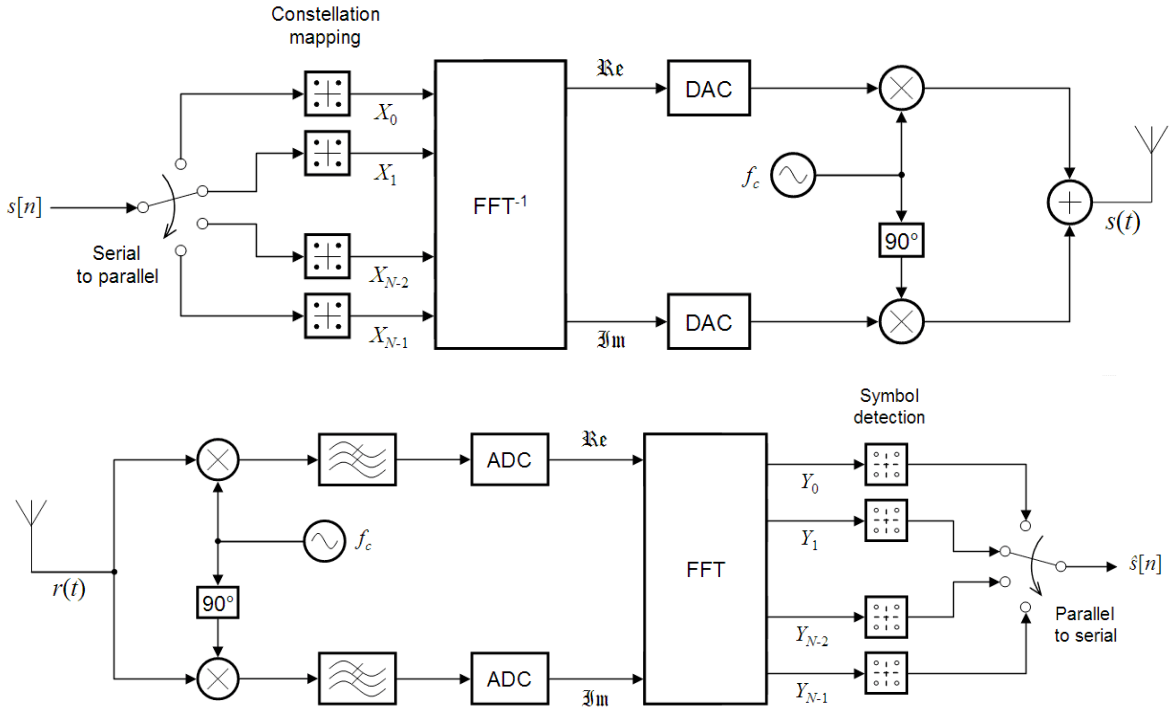
Топология сетей: 1) Infrastructure mode, 2) Ad-hoc

Методы расширения спектра

- Псевдослучайная перестройка рабочей частоты (ППРЧ) (FHSS — Frequency Hopping Spread Spectrum). Перестройка несущей частоты по псевдослучайному закону.
- Расширение спектра методом прямой последовательности (ПРС) (DSSS — Direct Sequence Spread Spectrum). Каждому символу передаваемого сообщения ставится в соответствие псевдослучайная последовательность (ПСП) с соответствующим увеличением тактовой частоты.
- Расширение спектра методом линейной частотной модуляции (ЛЧМ) (CSS — Chirp Spread Spectrum). Перестройка несущей частоты по линейному закону.

IEEE 802.11a

Модуляция сигнала: OFDM (Orthogonal frequency-division multiplexing) — ортогональное частотное разделение каналов с мультиплексированием)



IEEE 802.11b

Модуляция HR/DSSS - High Rate Direct Sequence Spread Spectrum - высокоскоростное расширение спектра методом прямой последовательности. На скоростях 1 Мб/с и 2 Мб/с каждый «единичный» передаваемый бит кодируется 11-битовой последовательность кода Баркера, а «нулевой» бит – инверсной последовательностью. Используются 3 неперекрывающихся канала шириной 22 . На скорости 11 Мб/с – кодирование дополнительными ортогональными последовательностями (CCK – Complementary Code Keying).

IEEE 802.11g

На скорости передачи 11 Мбит/с используется метод DSSS – CCK кодирование , на больших скоростях (до 54 Мбит/с) – OFDM модуляция.

IEEE 802.11n

Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с применяя передачу данных сразу по четырьмя антеннам. По одной антенне, до 150 Мбит/с. Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

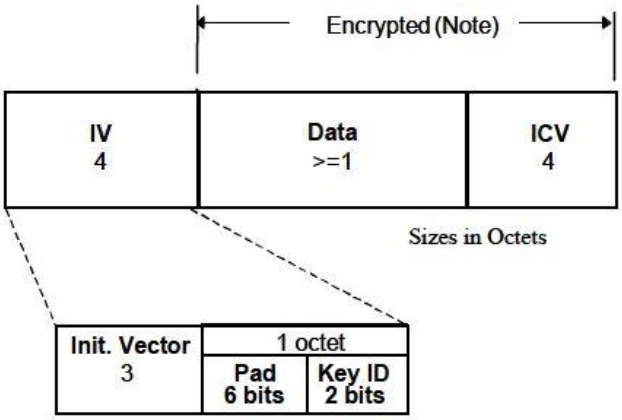
Кроме того, устройства 802.11n могут работать в трёх режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
- «чистом» режиме — 802.11n (максимальная скорость и увеличенная дальность передачи за счет технологии MIMO - многоканальный вход/выход).

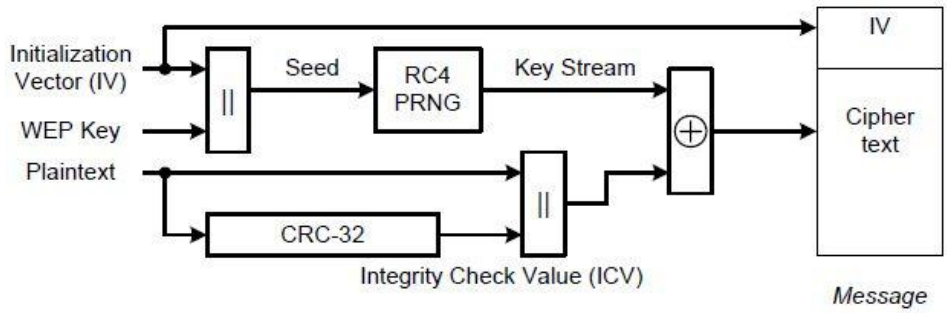
Технологии защиты беспроводных сетей

Wired Equivalent Privacy (WEP)

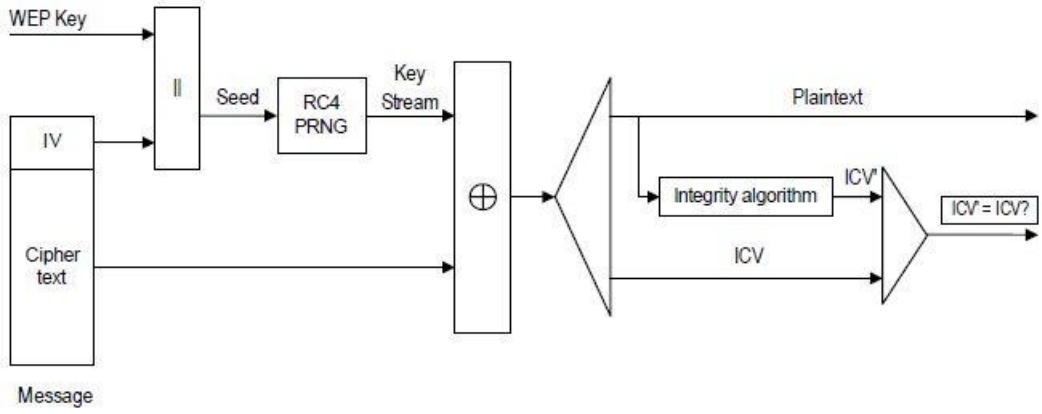
WEP-40 и WEP-104 имеют длину ключей 40 и 104 бита и 24-битовый вектор инициализации.
Используются два типа ключей: ключи по умолчанию (4) и назначенные ключи (1).



Инкапсуляция WEP



Декапсуляция WEP



WPA (**Wi-Fi Protected Access**) WPA = 802.1X + EAP + TKIP + MIC

EAP (Extensible Authentication Protocol) - расширяемый протокол аутентификации. Условием аутентификации является предъявление пользователем сертификата (мандата) серверу аутентификации (серверу RADIUS - Remote Authentication in Dial-In User Service).

TKIP (Temporal Key Integrity Protocol) — протокол целостности временного ключа. В TKIP используется алгоритм RC4 и 48-битовый вектор инициализации, для каждого блока данных (пакета) генерируется новый 128-битовый ключ.

MIC (Message Integrity Check) – проверка целостности сообщения (64-разрядный хэш).

WPA-PSK (Pre-Shared Key) - упрощенный WPA (пароль вместо сертификата для каждого отдельного узла).

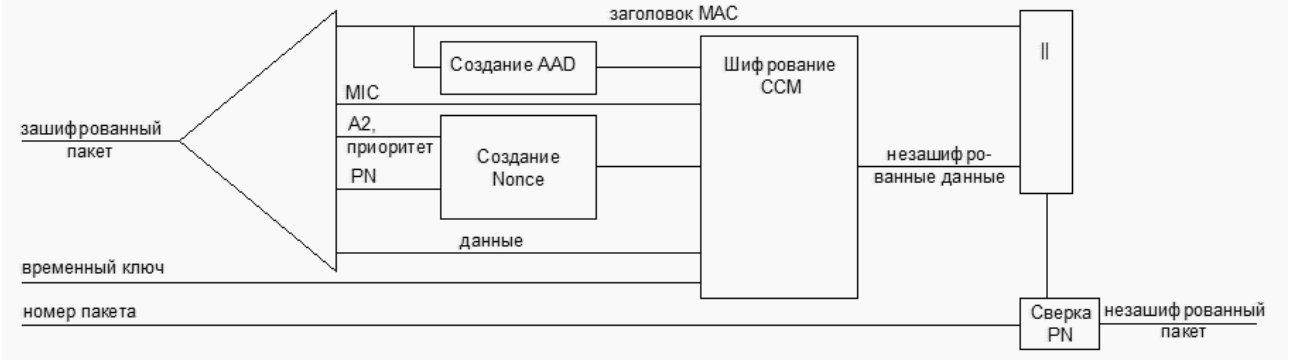
WPA2 (Стандарт IEEE 802.11i)

AES (Advanced Encryption Standard) - усовершенствованный стандарт шифрования со 128-битовым ключом и 128-разрядными блоками данных.

CCMP — Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – протокол аутентификации сообщений в режиме сцепления блоков с использованием счетчика пакетов.

Схема шифрования по алгоритму CCMP

Схема расшифрования по алгоритму CCMP



AAD – Additional Authentication Data – дополнительные данные аутентификации из заголовка MPDU (MAC Protocol Data Unit)

Поле управления кадра (FCF)	После-доват. номер	Адрес	Данные (кадр LLC Уровня)	FCS (Frame Check sequence)

Последовательность генерации ключей:

1. MK – Master Key – мастер-ключ
2. PMK – Pairwise Master Key – парный MK
3. PTK – Pairwise Transient Key – парный временный ключ

PTK = KCK + KEK + TK

KCK – Key Confirmation Key – применяется для шифрования очередного PMK

KEK – Key Encryption Key - используется для генерации GTK –Group Transient Key,

TK – Temporary Key – Temporary Key – используется для шифрования данных