Учебный центр компьютерного обучения «СПЕЦИАЛИСТ» при МГТУ им. Н.Э.Баумана

ОСНОВЫ СЕТЕЙ И СЕТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Часть III

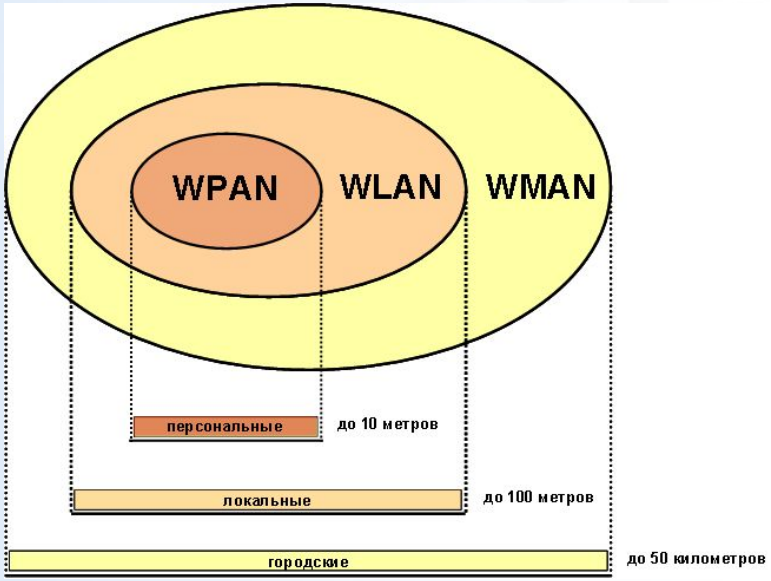
Сети Wi-Fi

Беспроводные компьютерные сети (WLAN)

Wireless LAN (*Wireless Local Area Network*; WLAN) — беспроводная локальная вычислительная сеть.

Беспроводные компьютерные сети — это технология, позволяющая создавать вычислительные сети без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона.

По дальности действия можно выделить:



- **Беспроводные персональные сети (WPAN — Wireless Personal Area Networks). Пример технологии — Bluetooth.**
- **Беспроводные локальные сети (WLAN — Wireless Local Area Networks). Пример технологии — Wi-Fi.**
- **Беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks). Пример технологии — WiMAX.**

Wi-Fi

Wi-Fi (*Wireless Fidelity* — «беспроводная точность») — беспроводная технология создания сетей. Под технологией Wi-Fi подразумеваются все стандарты семейства IEEE 802.11, определенные организацией Wi-Fi Alliance.

Сферы применения беспроводных сетей

- **Внутриофисные сети**
- **Домашние сети**
- **Выставочные комплексы и конференц-залы**
- **Доступ к Интернет в гостиницах, кафе, библиотеках, студенческих городках и т.д. – “hot spot”**
- **Сети провайдеров Интернет: подключение клиентов там, где нет возможности протянуть кабель**
- **«Гостевой» доступ к корпоративной сети для клиентов и партнеров**

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- быстрота и легкость развертывания (нет кабелеукладочных работ);
- легкость подключения новых пользователей;
- пользователи мобильных устройств могут легко перемещаться в пределах действующих зон покрытия сети;
- простота и легкость переноса сети на новую территорию;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей:

- меньшая скорость передачи информации;
- подверженность влиянию электро-магнитных помех;
- зависимость скорости связи от расположения пользователей и наличия препятствий (стен и перегородок)
- простота подключения требует использования более сложных схем обеспечения безопасности передаваемой информации

ОСНОВНЫЕ ЭЛЕМЕНТЫ WI-FI СЕТИ.

Беспроводная сеть состоит из точек доступа и клиентских устройств (настольных компьютеров, ноутбуков, PDA), оснащенных беспроводными адаптерами.

Точка доступа (access point, AP) – это приемо-передающее радиоустройство, обеспечивающее связь между беспроводными устройствами и их подключение к проводной локальной сети.

Беспроводной адаптер предоставляет клиентскому устройству подключение к сети через точку доступа, либо выполняет прямое подключение к другому адаптеру.

Способы объединения устройств в WI-FI сеть

Ad Hoc (в переводе «к случаю») – независимая конфигурация (IBSS – Independent Basic Service Set)

Компьютеры оснащены беспроводными сетевыми адаптерами и соединяются напрямую друг с другом - одноранговое взаимодействие по типу «точка-точка». Точки доступа не нужны.

Достоинства режима Ad Hoc (точка – точка).

- нужны только адаптеры
- развернуть такую сеть максимально просто
- низкая цена

Недостатки режима Ad Hoc (точка – точка).

- малый радиус действия сети
- низкая помехозащищенность
- малое число пользователей
- затрудненность подключения сети к internet
- низкая скорость передачи информации

Инфраструктурный – с использованием точки доступа

Беспроводные клиенты взаимодействуют друг с другом через точку доступа.

Точку доступа можно рассматривать как беспроводной *концентратор.*

ТД также может обеспечивать подключение беспроводных устройств к существующей проводной сети.

Basic Service Set, BSS) – это группа станций, связывающихся одна с другой по беспроводной связи.

Режим инфраструктуры (или клиент-сервер). Достоинства:

- большая мощность передатчика у AP (отсюда – большая дальность и надежность)
- лучший контроль за подключениями
- возможность простого объединения разных сетей – проводных и безпроводных

Режим инфраструктуры (или клиент-сервер). Недостатки:

- более сложная настройка (необходимо настраивать AP)
- стоимость сети несколько повышается (для маленьких сетей – значительно)
- отказ точки доступа приведет к остановке всей сети

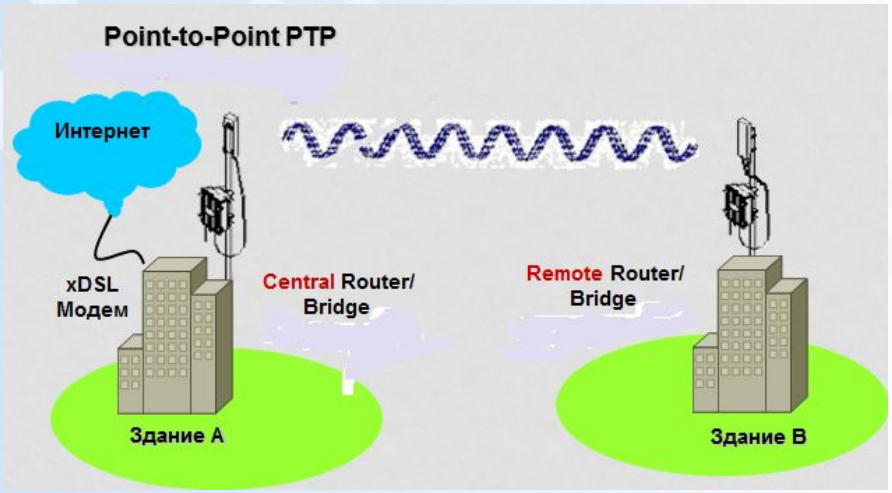
Режимы работы *точки доступа.*

Режим «точка доступа» (Access Point)

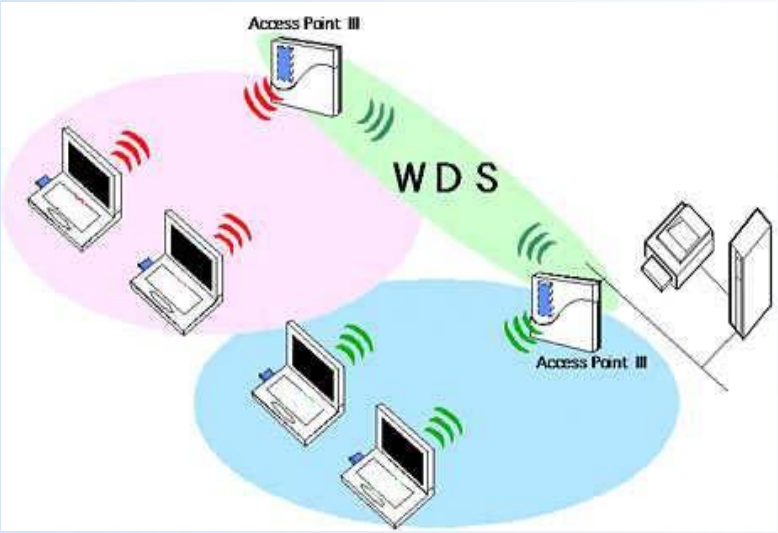
Беспроводные клиенты взаимодействуют друг с другом через точку доступа. ТД также может обеспечивать подключение беспроводных устройств к существующей проводной сети.

Режим беспроводный мост «точка-точка»

Используется для объединения двух проводных сегментов LAN, находящихся на расстоянии до нескольких км.



WDS **(Wireless Distribution System) - распределённая беспроводная система. В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение.**



WDS with AP **(WDS with Access Point) – распределённая беспроводная система, включая точку доступа. С помощью этого режима можно организовать не только мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры**

Режим беспроводный мост «точка-многоточка»

Используется для объединения двух и более проводных сегментов LAN, находящихся на расстоянии до нескольких км.

Режим беспроводный клиент

Режим можно применять при подключении к беспроводной сети устройств с портом Ethernet, но без возможности установки беспроводного адаптера.

Семейство стандартов беспроводных сетей IEEE 802.11

Группа стандартов IEEE 802.11 входит в серию стандартов IEEE 802.X, относящихся к сетям и коммуникациям, сюда также входят такие стандарты, как 802.3 Ethernet, 802.5 Token Ring и т.д.

Семейство стандартов IEEE 802.11 определяет компоненты и характеристики сети на физическом уровне передачи данных и на уровне доступа к середе.

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

Общедоступность беспроводной сети требует реализации дополнительных механизмов для:

- ***аутентификации абонентов (проверка подлинности) с целью предотвращения несанкционированного доступа к сетевым ресурсам;***
- **обеспечения *конфиденциальности данных (шифрование) с целью обеспечения целостности и защиты при передаче по общедоступному радиоканалу.***

Основными стандартами аутентификации в беспроводных сетях являются стандарты

IEEE 802.11, WPA, WPA2 и 802.1x.

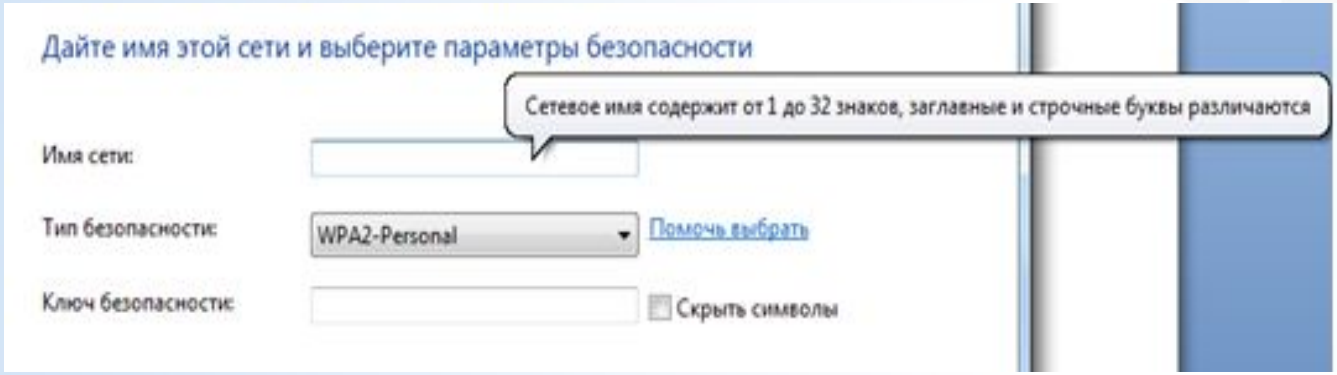
Стандарт IEEE 802.11 предусматривает два механизма аутентификации беспроводных абонентов: *открытую аутентификацию (open authentication) и аутентификацию с общим ключом (shared key authentication).*

Также широко используются два других механизма, а именно назначение идентификатора беспроводной ЛВС (Service Set Identifier, SSID) и аутентификация абонента по его MAC-адресу (MAC address authentication).

Идентификатор беспроводной ЛВС (Service Set Identificator, SSID)

SSID представляет собой атрибут беспроводной ЛВС, позволяющий логически отличать сети друг от друга. В общем случае, абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной ЛВС.

SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной ЛВС.



Аутентификация по MAC-адресу (MAC Address Authentication)

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных ЛВС.

При аутентификация по MAC-адресу происходит сравнение MAC-адреса абонента либо со списком разрешенных либо со списком запрещенных адресов, хранящихся локально или на сервере аутентификации (рис. 7).

Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.

RADIUS (Remote Authentication Dial-In User Server) – сервер аутентификации (проверки подлинности) удаленных клиентов. Он обеспечивает аутентификацию пользователей.

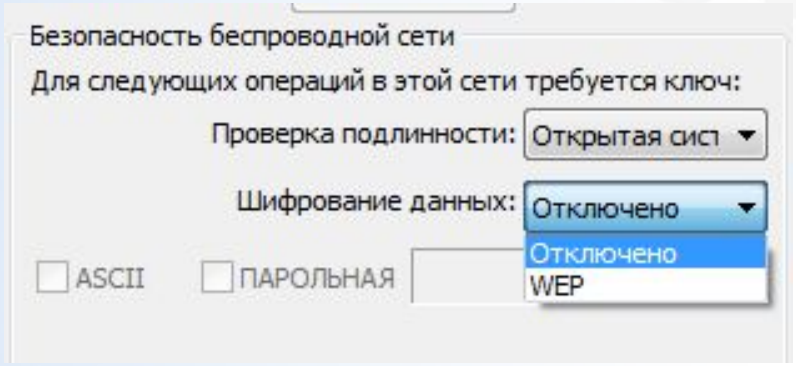
Открытая аутентификация (Open Authentication)

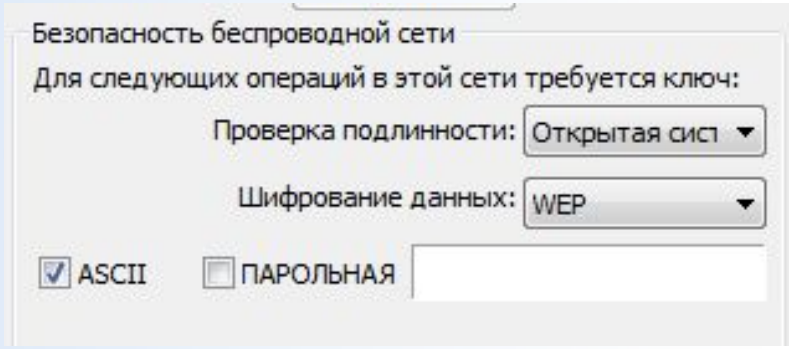
Открытая аутентификация по сути не является алгоритмом аутентификации в привычном понимании.

Если в беспроводной сети не используется шифрование, то любой абонент, знающий идентификатор SSID точки радиодоступа, получит доступ к сети.

При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа.

Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку доступа, ни расшифровывать данные, переданные точкой доступа





МЕХАНИЗМ ШИФРОВАНИЯ WEP

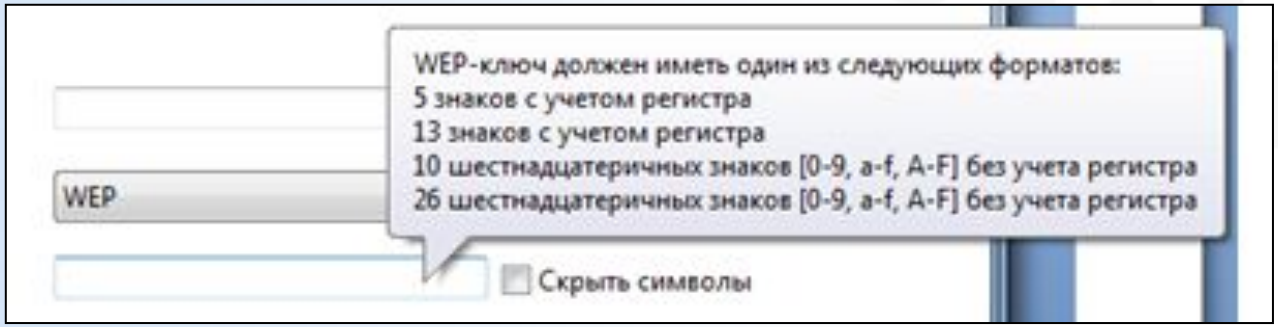
Шифрование WEP (Wired Equivalent Privacy) - секретность на уровне проводной связи.

Для обмена данными ключи шифрования у абонента и точки доступа должны быть идентичными.

Алгоритм шифрования WEP использует ключи длиной 64 или 128 бит.

При настройках шифрования в оборудовании:

- Ключ 64 бит (40 бит длина ключа + 24 бита вектор инициализации) - вводятся 5 байтовых ASCII-символов (5·8=40) или 10 шестнадцатеричных чисел (10·4=40)
- Ключ 128 бит (104 бит длина ключа + 24 бита вектор инициализации) - вводятся 13 байтовых ASCII-символов (13·8=104) или 26 шестнадцатеричных чисел (26·4=104).



Вектор инициализации имеет длину 24 бита и суммируется с 40- или 104-битовым базовым ключом шифрования WEP, таким образом на вход алгоритма шифрования подается 64- или 128-битовый ключ. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале.

Аутентификация с общим ключом (Shared Key Authentication)

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11.

Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует рис.

1.Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.

2.Точка радиодоступа посылает подтверждение аутентификации , содержащее challenge text.

3.Абонент шифрует challenge text своим статическим WEP-ключом, и посылает точке радиодоступа запрос аутентификации.

4.Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем challenge text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

Протокол безопасности WPA (Wi-Fi Protected Access, защищенный доступ Wi-Fi).

WPA был разработан для обеспечения улучшенного шифрования данных и аутентификации пользователей, по сравнению с WEP.

В WPA предусмотрены улучшенные средства аутентификации и шифрования передаваемых данных.

В WPA используется механизм шифрования TKIP *временный протокол целостности ключа (Temporal Key Integrity* Protocol, TKIP).

WPA может работать в двух режимах:

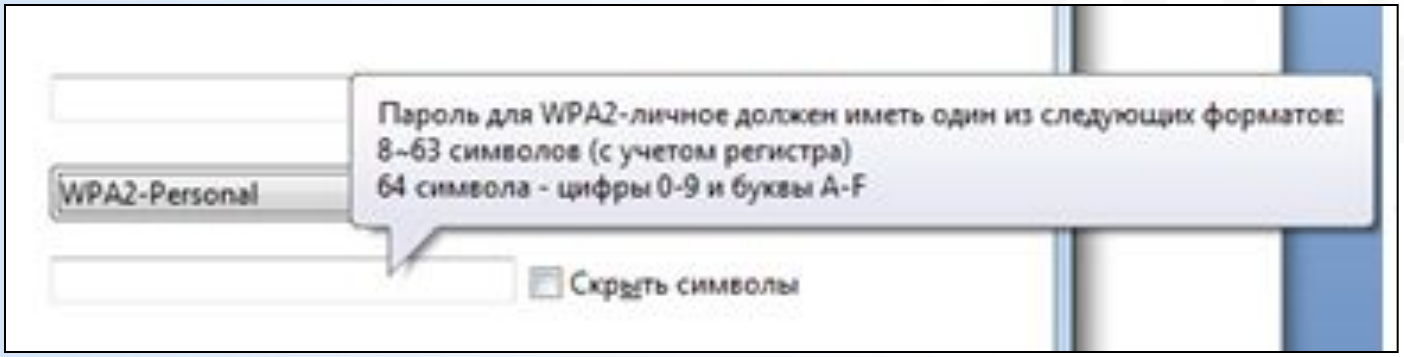
- WPA-PSK - *Pre-Shared Key (*персональный) - предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). До тех пор пока пароли совпадают, клиенту будет разрешен доступ в сеть (подход с использованием пароля делает WPA-PSK уязвимым для атаки методом подбора)
- WPA-Enterprise (корпоративный) - хранение базы данных и проверка аутентичности по стандарту 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего RADIUS (Remote Authentication Dial-In User Service) .

Стандарт 802.11i (WPA2)

В июне 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях — 802.11i, также известный как WPA2.

802.11i по умолчанию использует шифрование AES (Advanced Encryption Standard), но для совместимости со старыми версиями может задействовать TKIP.

WPA2, так же как и WPA, может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key (персональный).*



Стандарты беспроводных сетей - IEEE 802.11b

- Работает на частоте 2,4 ГГц
- Используется метод прямой последовательности с разнесением сигнала по широкому диапазону (DSSS)
- Поддерживает скорость соединения 1, 2, 5.5, 11 Мбит/с (*реальная скорость передачи данных от 4 до 6 Мбит/с*), автоматический или фиксированный выбор скорости
- Защита данных при помощи шифрования WEP

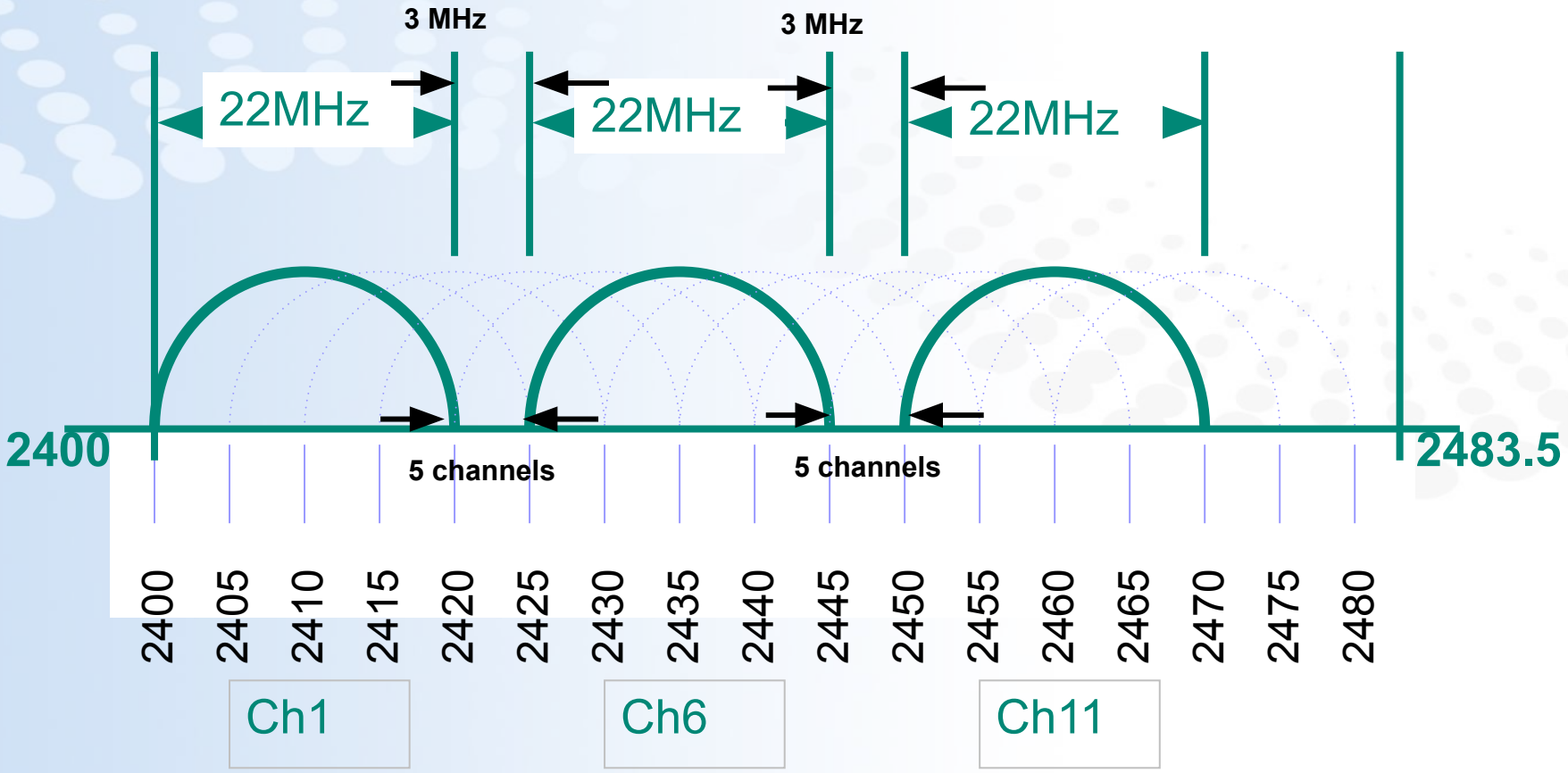
Стандарты беспроводных сетей - IEEE 802.11a

- Более сложная передовая технология
- Работает на частоте 5 ГГц
- Используется метод мультиплексирования с ортогональным делением частот (OFDM)
- Поддерживает скорость соединения до 54 Мбит/с (48, 36, 24, 18, 12, 9 и 6 Мбит/с), *реальная скорость передачи данных от 22 до 24 Мбит/с*
- 12 одновременно доступных для работы каналов
- Защита данных при помощи шифрования WEP

Стандарты беспроводных сетей - IEEE 802.11g

- Обратная **совместимость с устройствами стандарта IEEE 802.11b**
- Работает на частоте 2.4 ГГц
- Используется метод прямой последовательности с разнесением сигнала по широкому диапазону (DSSS) и метод мультиплексирования с ортогональным делением частот (OFDM)
- Скорость соединения до 54 Мбит/с, автоматический или фиксированный выбор скорости
- **Защита данных при помощи WPA** (Wi Fi Protected Access), 802.1x

Частоты каналов



Стандарты беспроводных сетей - IEEE 802.11n

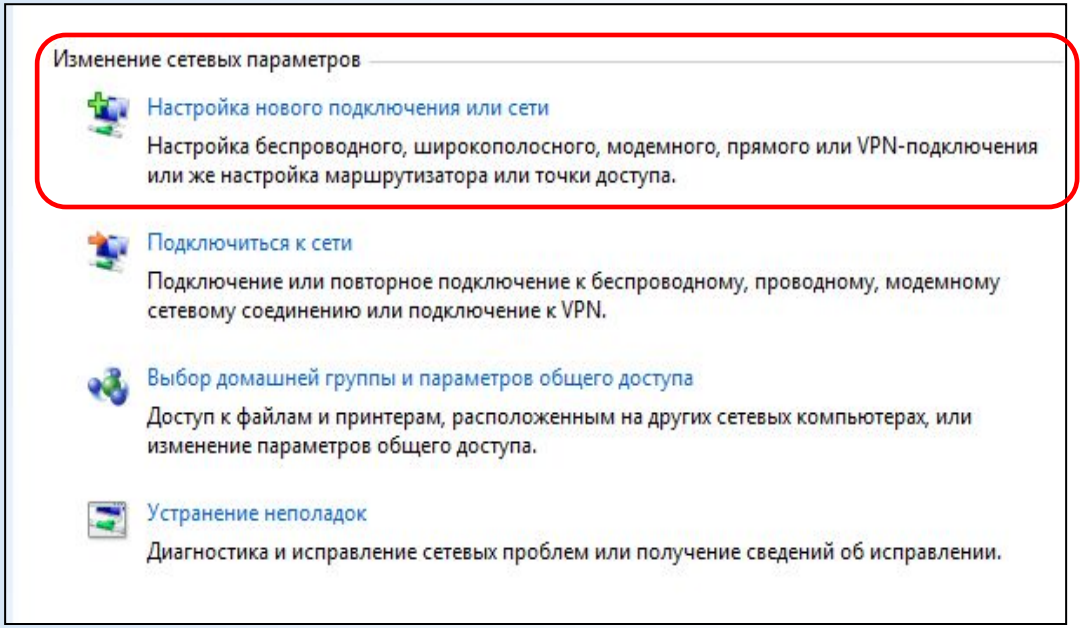
- Этот стандарт был утверждён 11 сентября 2009.
- Устройства 802.11n работают в диапазонах частот 2,4—2,5 или 5,0 ГГц.
- Поддерживает скорость соединения до 600 Мбит/с.
- Поддерживается совместимость с устройствами стандарта 802.11b или 802.11g в диапазоне 2,4 ГГц и с устройствами 802.11a — в диапазоне 5 ГГц.

Стандарт IEEE	Частотный диапазон, ГГц	Год ратификации WiFi альянсом	Теоретическая пропускная способность, Мбит/с	Реальная скорость передачи данных, Мбит/с
802.11 b	2,4	1999	11	5
802.11 a	5	2001	54	20
802.11 g	2,4	2003	54	20
802.11 n	2,4 и 5	2009	300	50-120

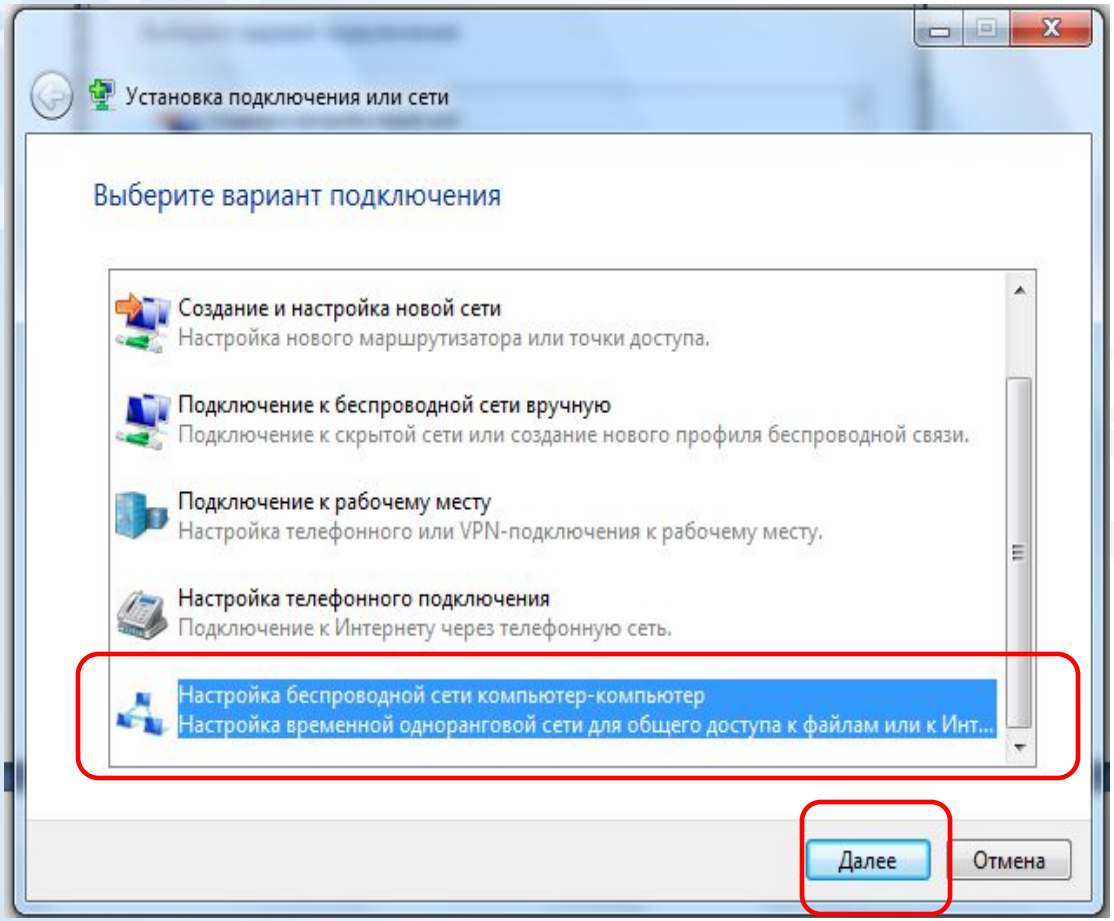
Настройка сети Ad Hoc (компьютер-компьютер) с помощью встроенной службы Windows

Основное достоинство данного режима – простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.
Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования.
Реальная скорость обмена данных будет ниже, и составит не более 11/N Мбит/с, где N – число устройств в сети.

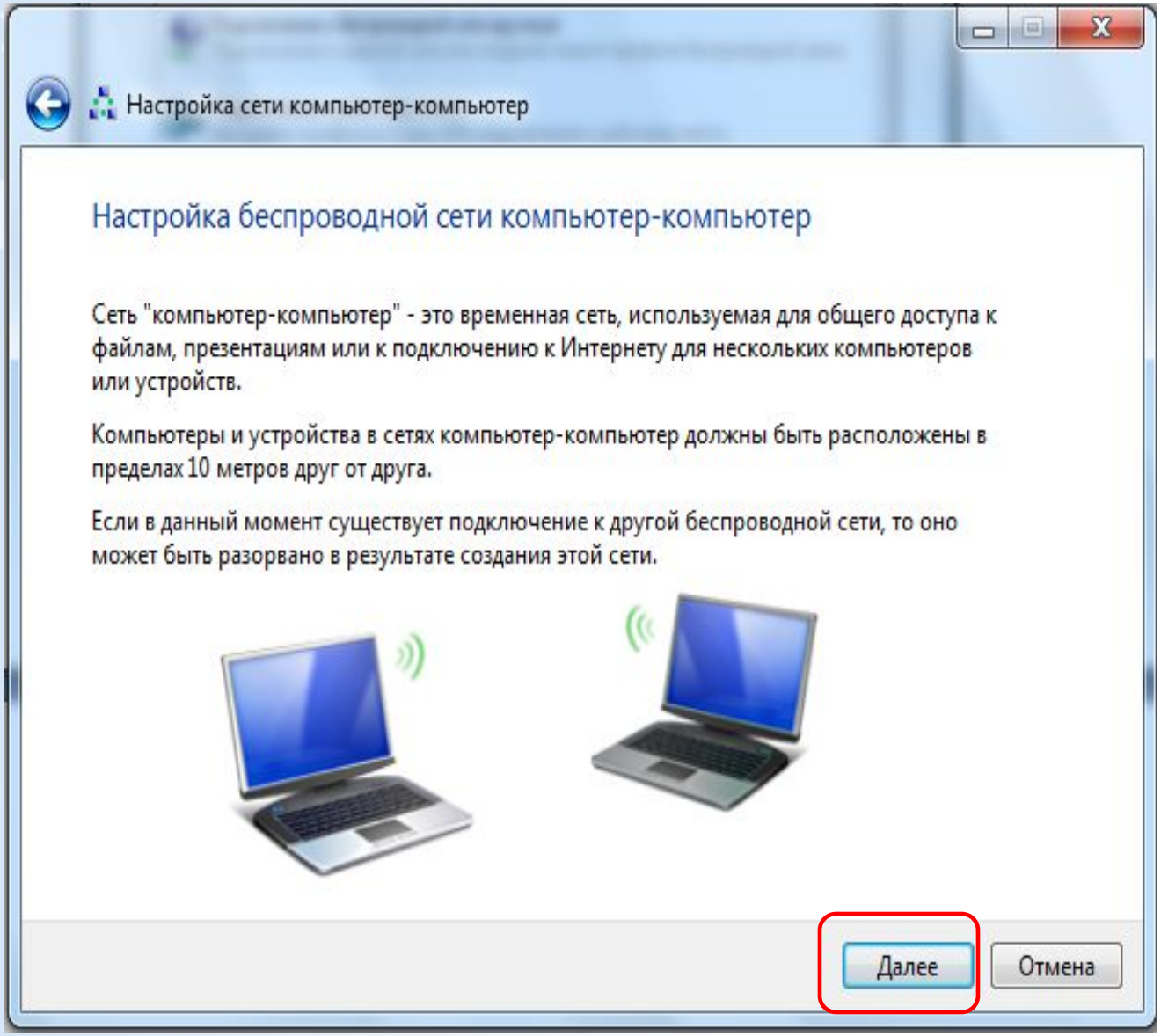
- Откройте Центр управления сетями и общим доступом.
- Щелкните пункт Настройка нового подключения или сети.

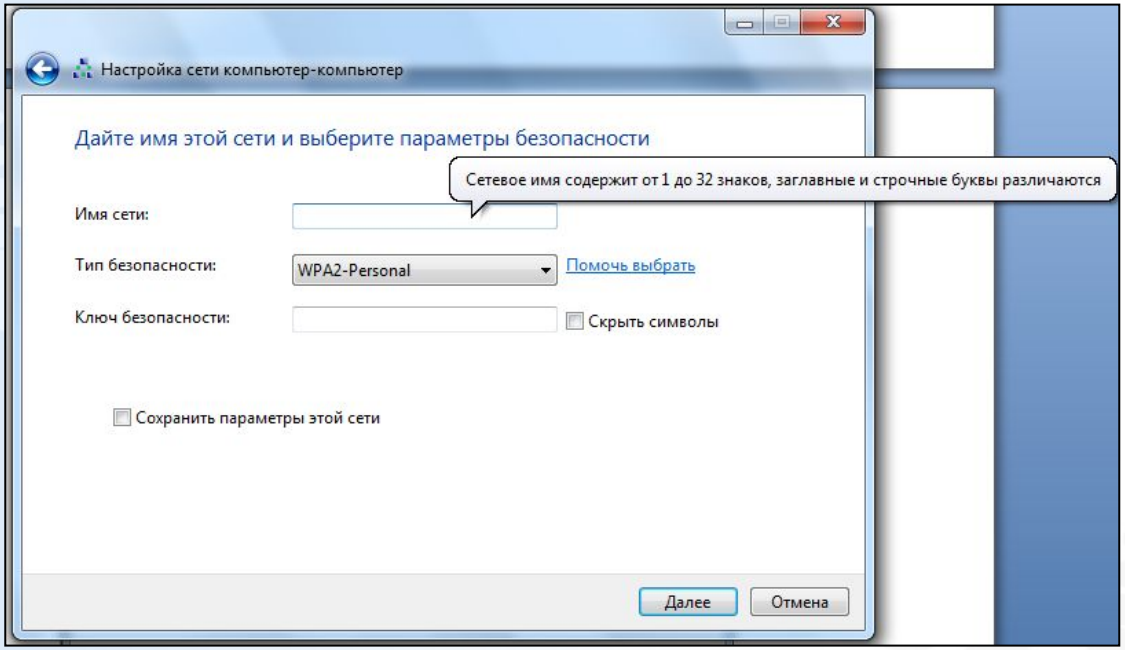


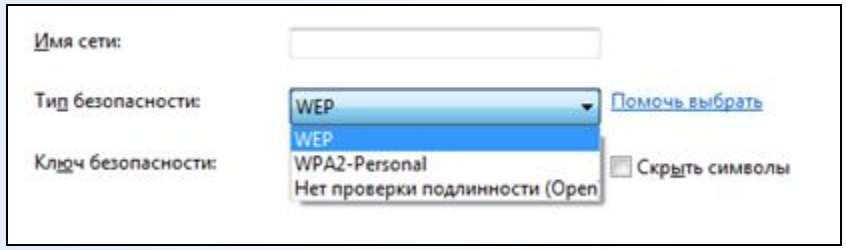
- Щелкните Настройка беспроводной сети компьютер-компьютер и нажмите кнопку Далее

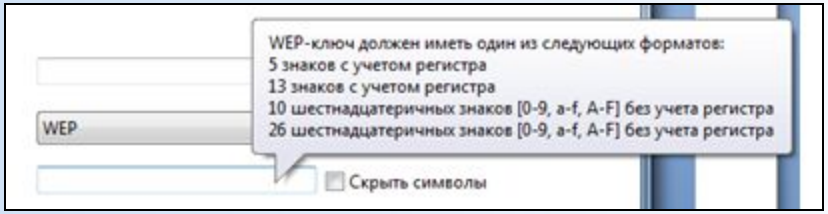


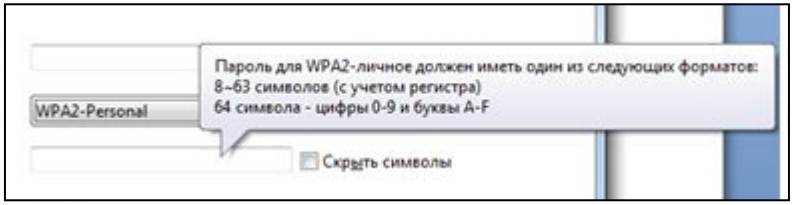
- Нажмите кнопку Далее

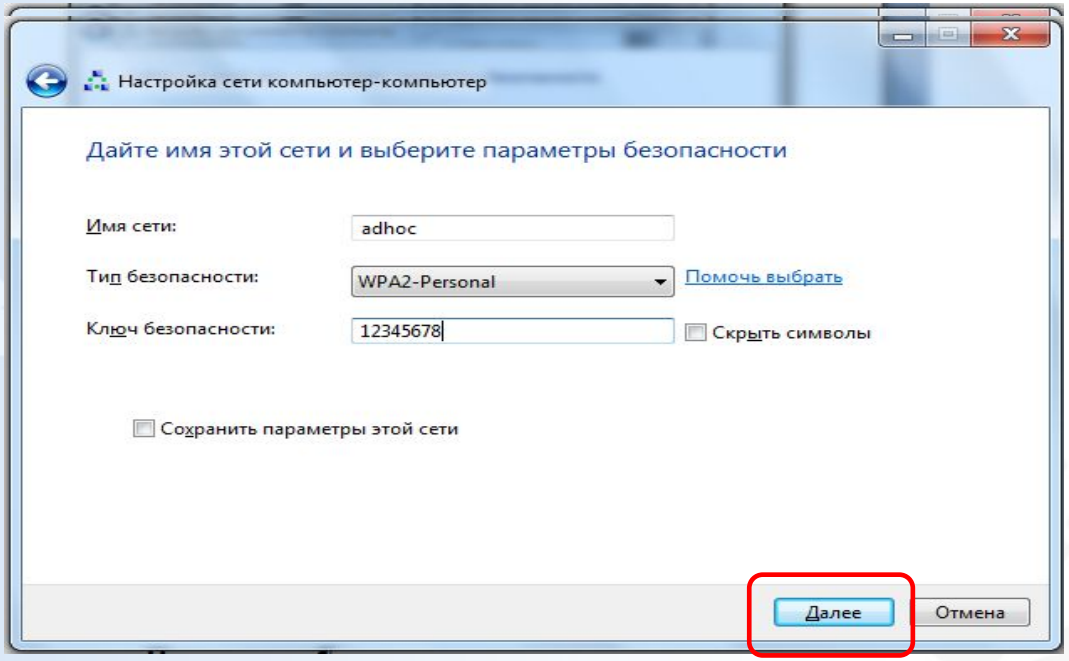


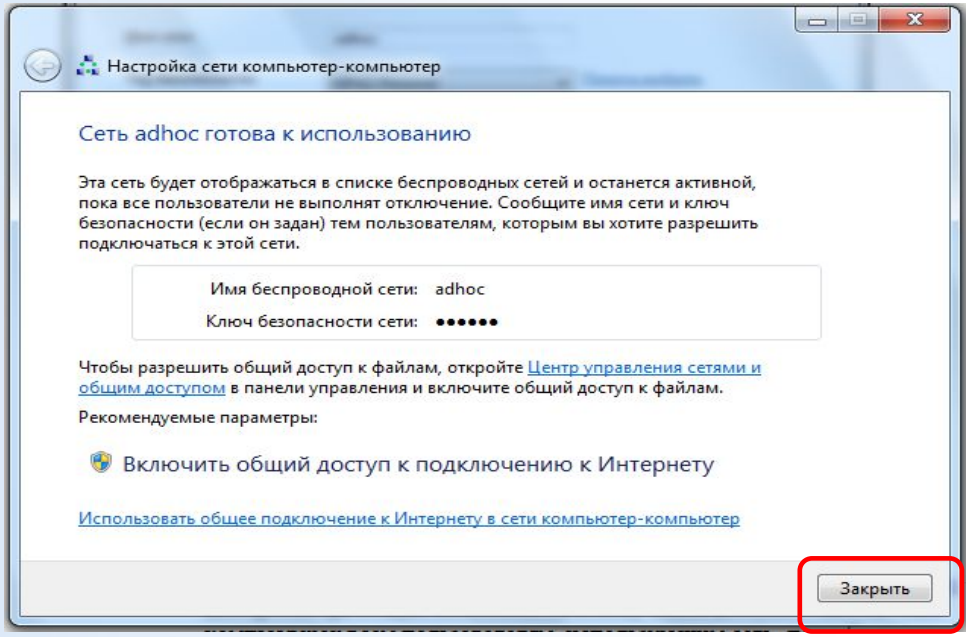


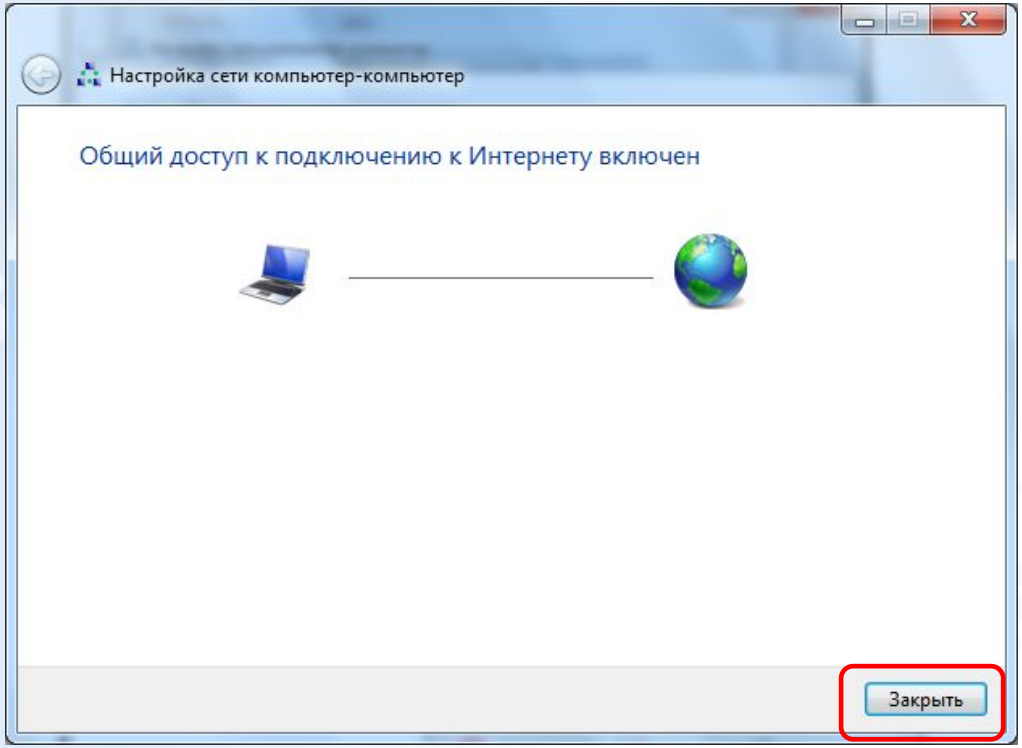


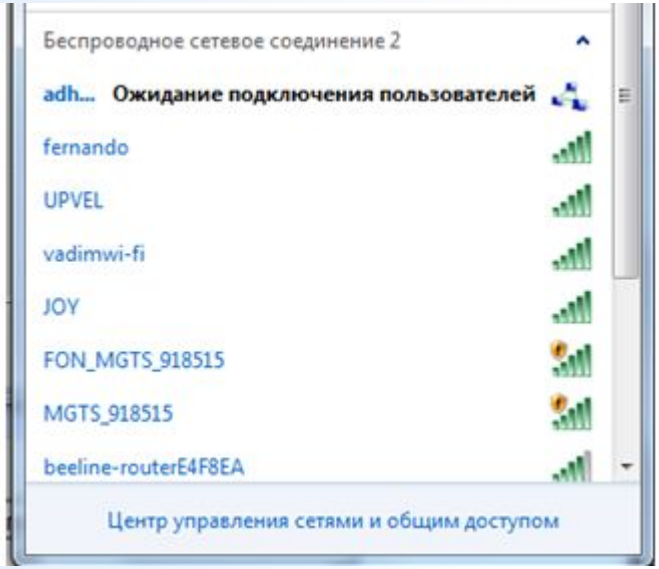




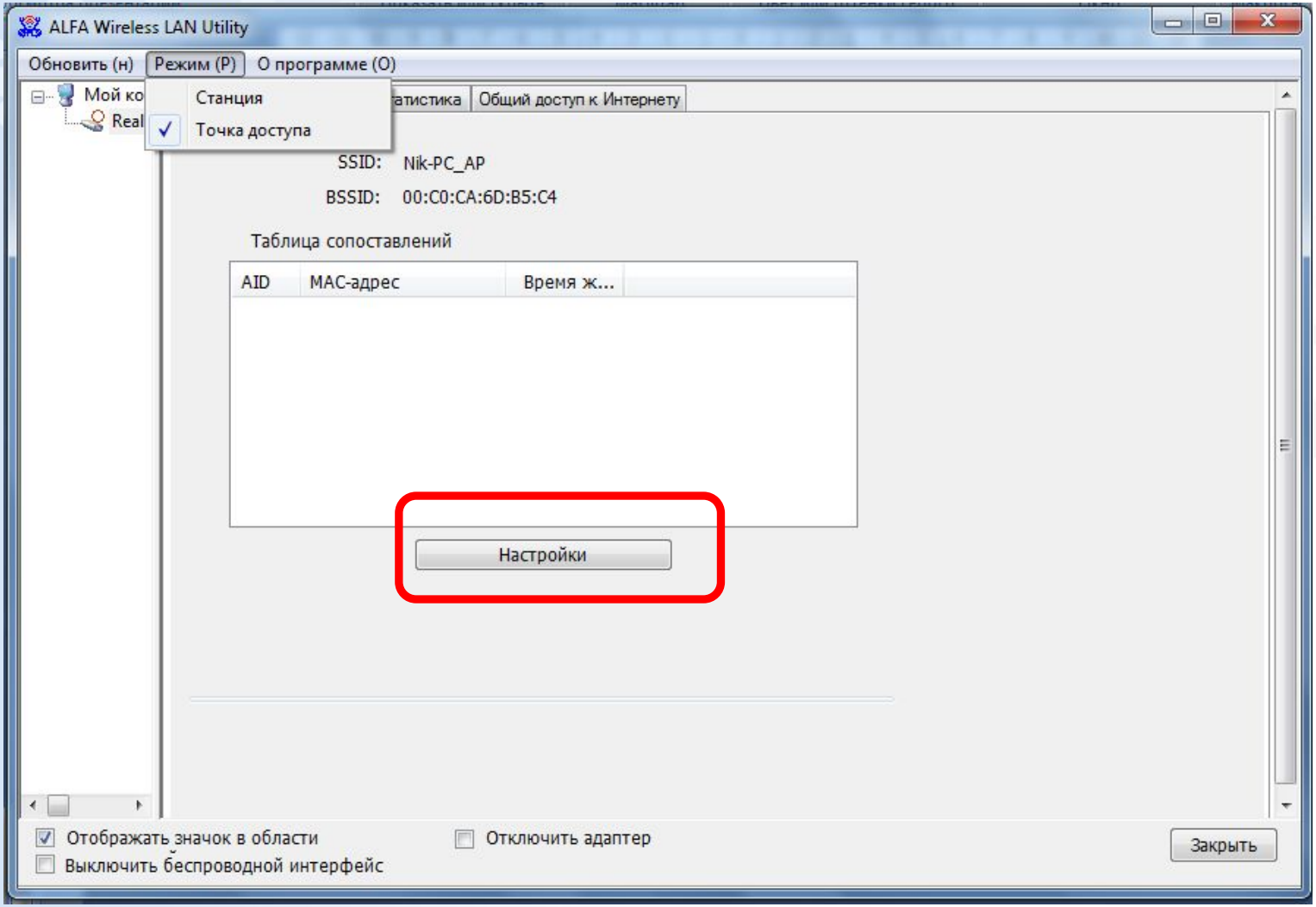




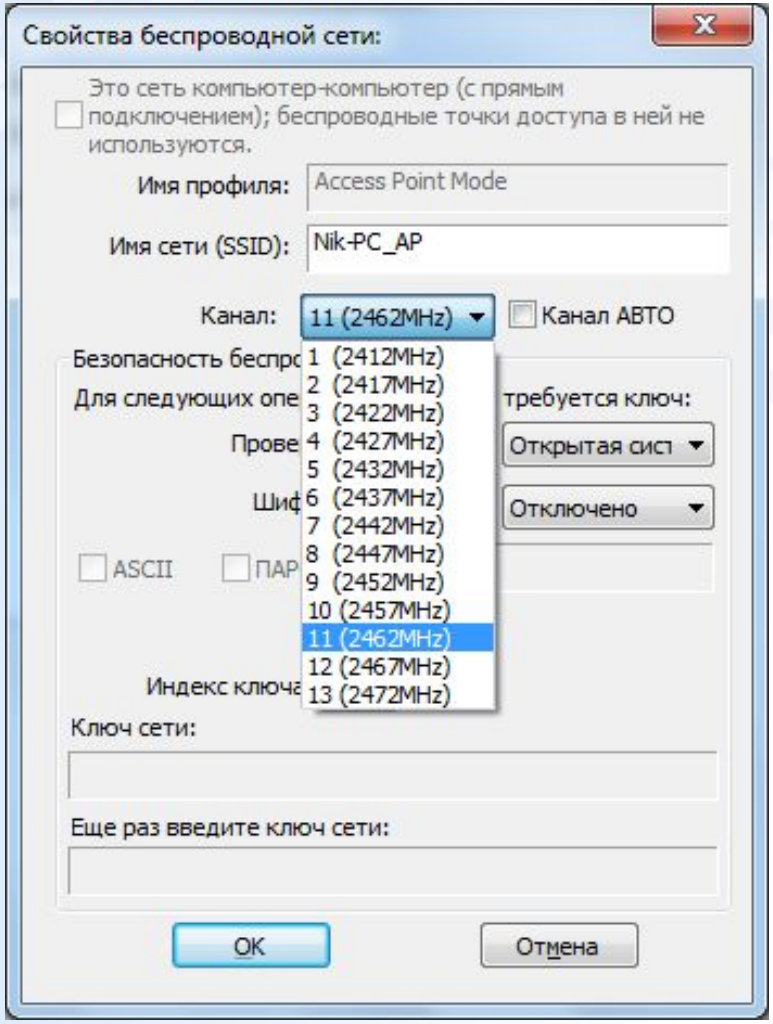




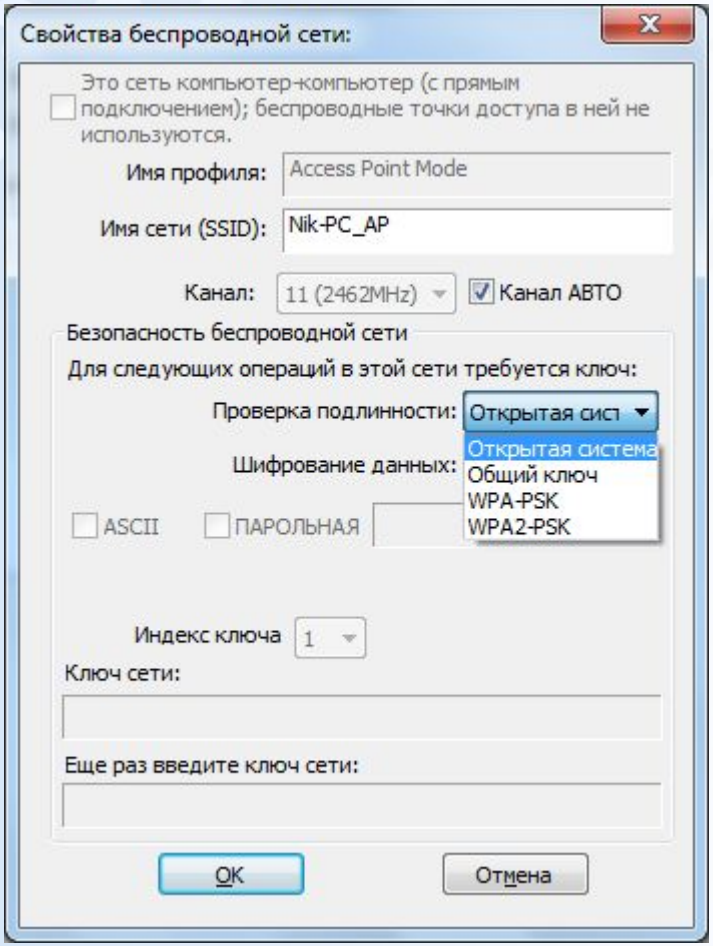
Настройка точки доступа



Выбор канала

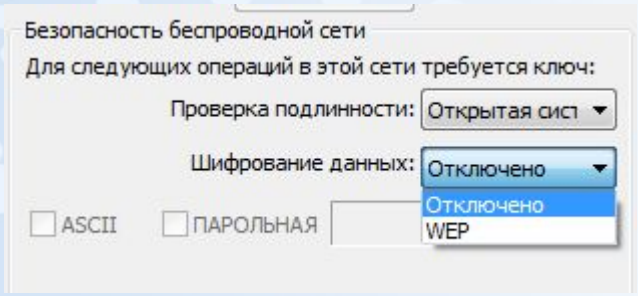


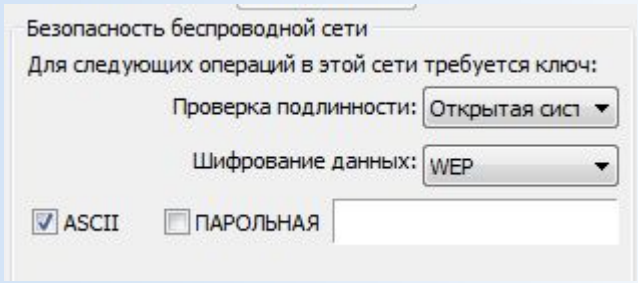
Проверка подлинности

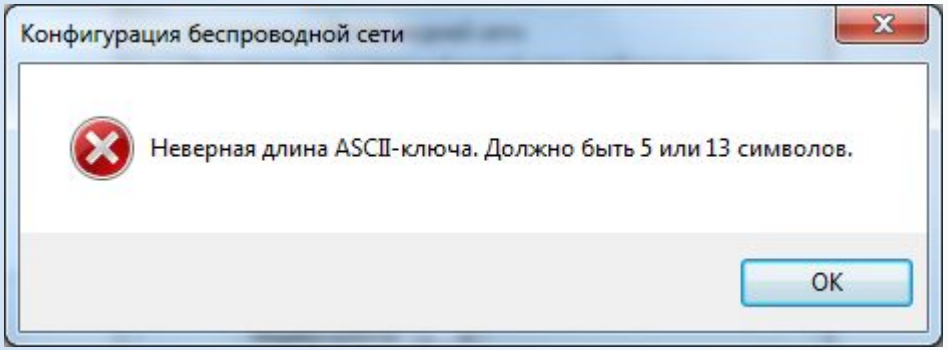


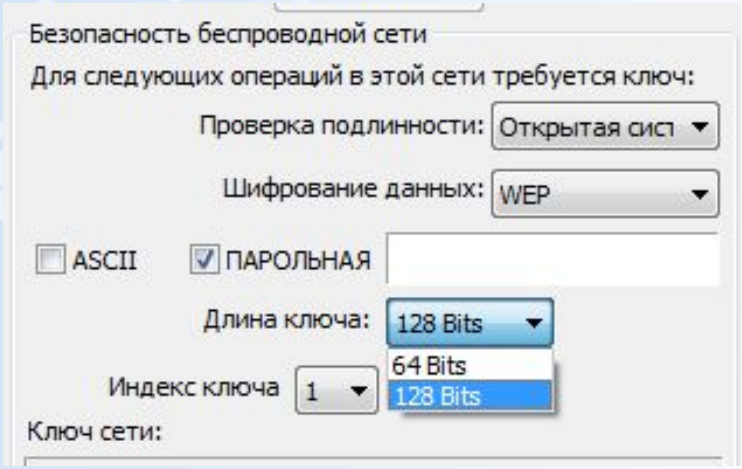
Authentication Type (Проверка подлинности)	Encryption Type (Шифрование)
Открытая система (Open)	NONE, WEP
Общий ключ (Shared)	WEP
WPA-PSK/ WPA2-PSK	TKIP, AES

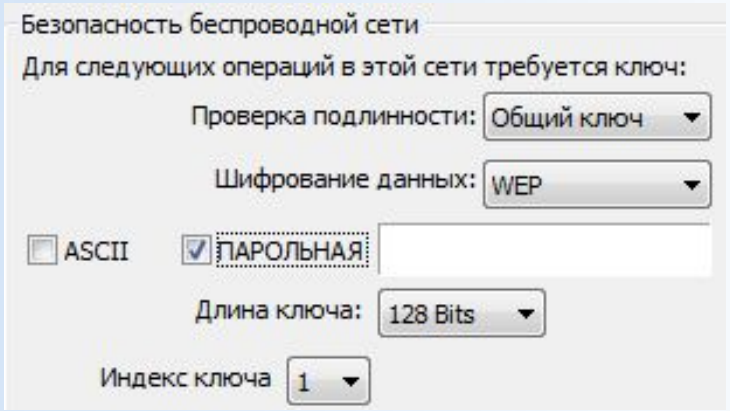
Шифрование

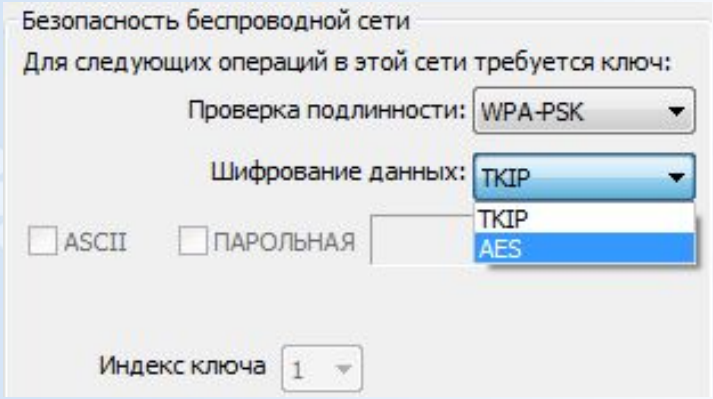

Безопасность беспроводной сети
Для следующих операций в этой сети требуется ключ:
Проверка подлинности:
Открытая сист
Шифрование данных:
Отключено
Отключено
WEP
ASCII
ПАРОЛЬНАЯ

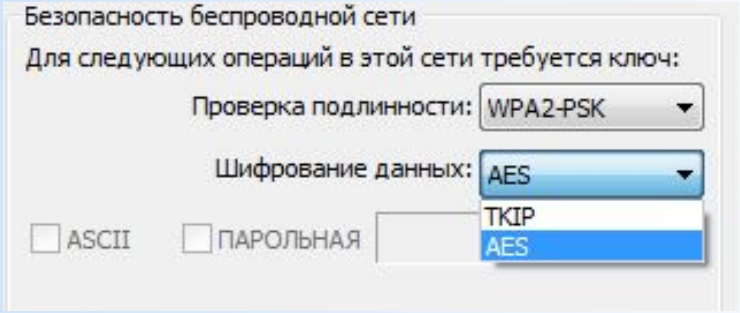

Безопасность беспроводной сети
Для следующих операций в этой сети требуется ключ:
Проверка подлинности:
Открытая сист
Шифрование данных:
WEP
ASCII
ПАРОЛЬНАЯ

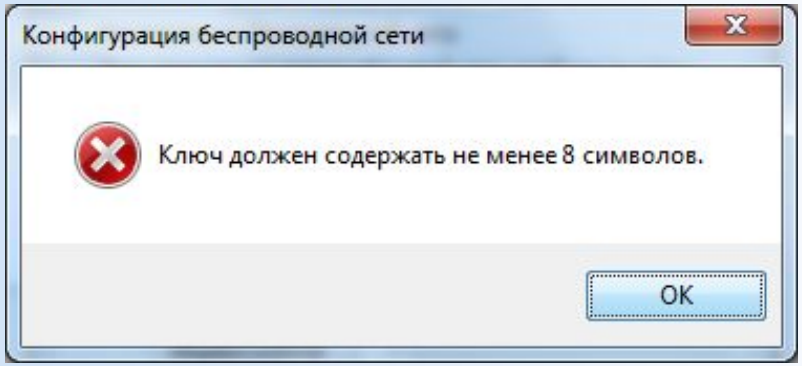

Конфигурация беспроводной сети
Неверная длина ASCII-ключа. Должно быть 5 или 13 символов.
OK



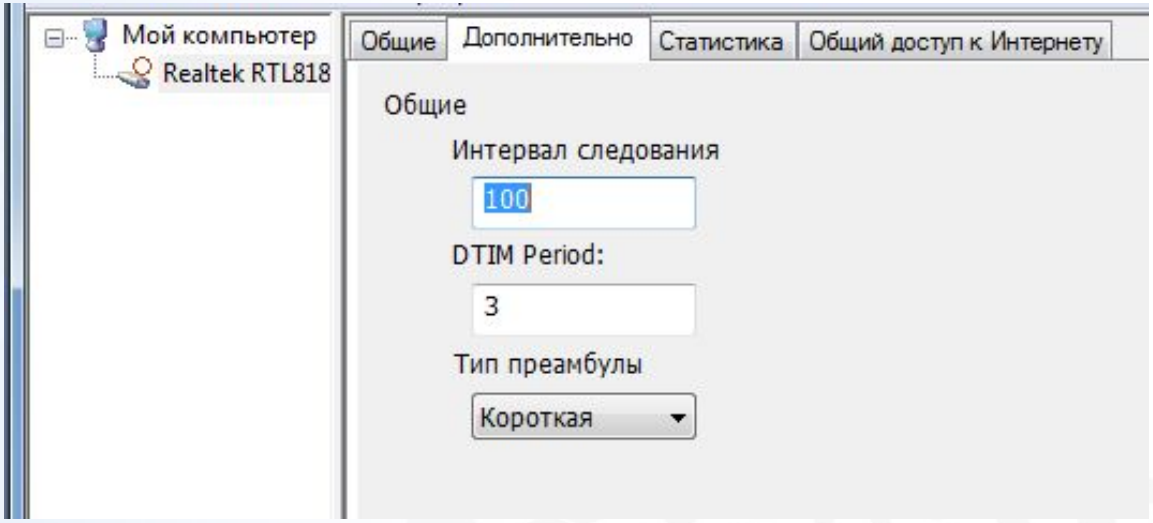






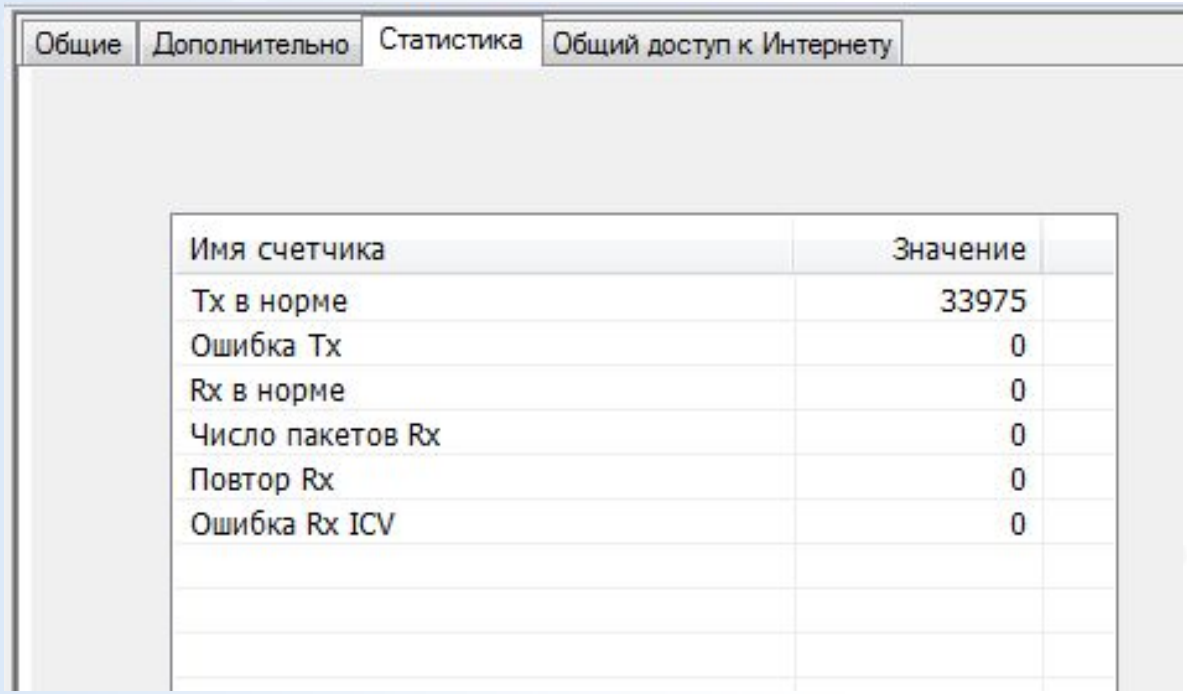


Дополнительные настройки



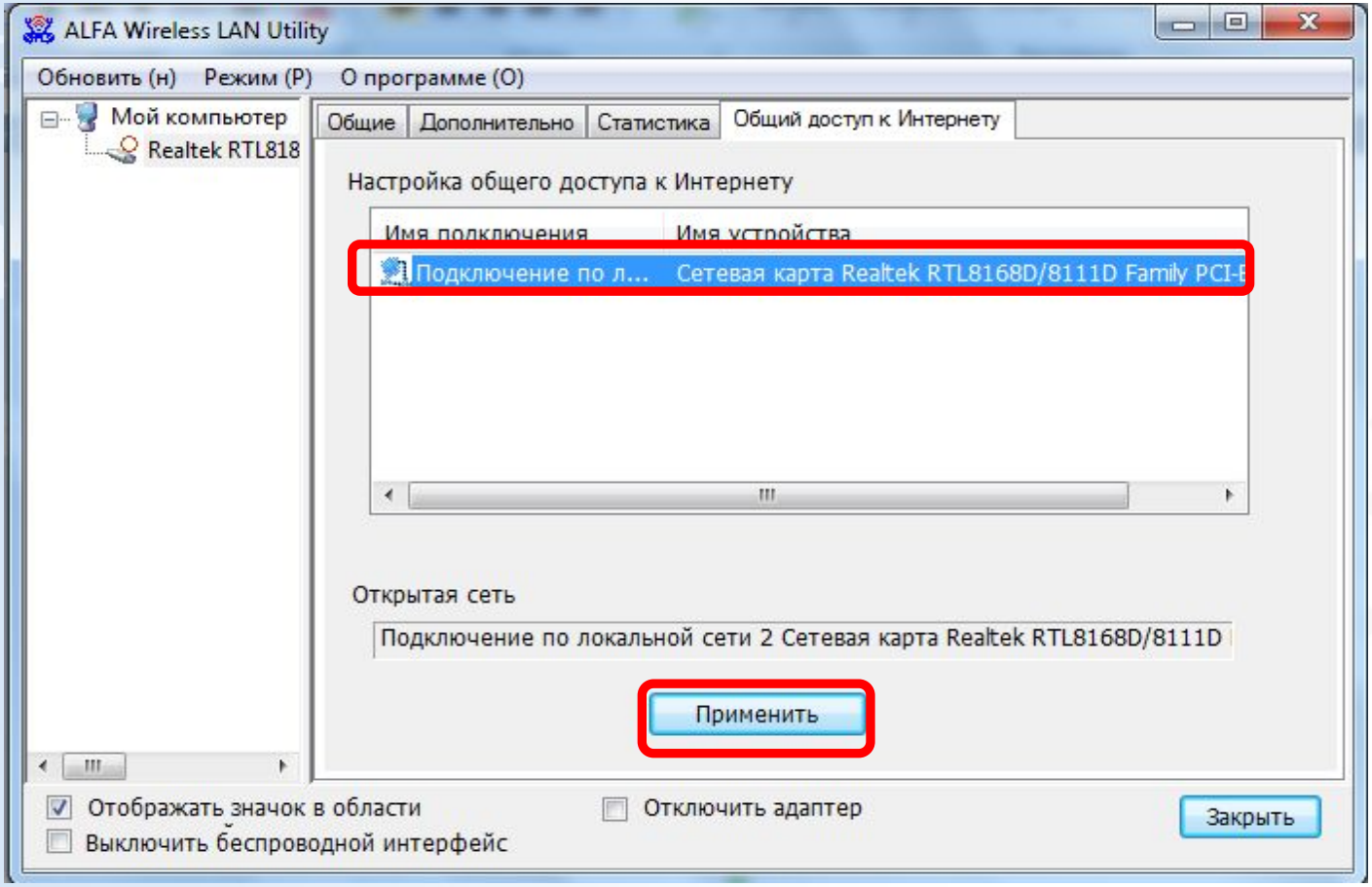
- **Интервал следования (Beacon Interval -** Интервал маяка): Временной интервал между передачами маяка. Маяк - это периодический импульс, передаваемый беспроводным устройством и информирующий сеть о том, что он по-прежнему активен. Это значение должно быть установлено в диапазоне от 1 до 1000 миллисекунд. Интервал маяка по умолчанию составляет 100 мс.
- **DTIM Period**: Интервал отправки сообщения Delivery Traffic Indication Message по умолчанию равен 3. DTIM - это обратный счетчик, уведомляющий клиентов о необходимости прослушивания широковещательных и многоадресных сообщений. С помощью этого параметра настраивается временной интервал, по истечении которого широковещательные и многоадресные пакеты, помещенные в буфер, будут доставлены беспроводным клиентам. При работе с приложениями, которые для доставки данных используют широковещательные и многоадресные фреймы, следует использовать интервал сообщений, регламентирующих доставку трафика (DTIM), равный 1, чтобы минимизировать задержку трафика в реальном времени, например многоадресных потоков аудио- и видеоданных.
- **Preamble** (Преамбула): это последовательность двоичных битов, которые используются для синхронизации приемников и подготовки приема переданных данных .
  Если в сети не используются никакие устройства стандарта 802.11b, для обеспечения оптимальной производительности в качестве типа преамбулы можно указать значение **Short** (Короткая). Тип преамбулы **Long** (Длинная) используется при наличии в сети устройств и 802.11g, и 802.11b.

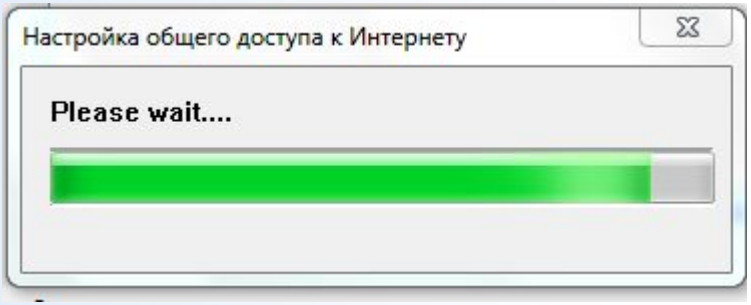
Статистика



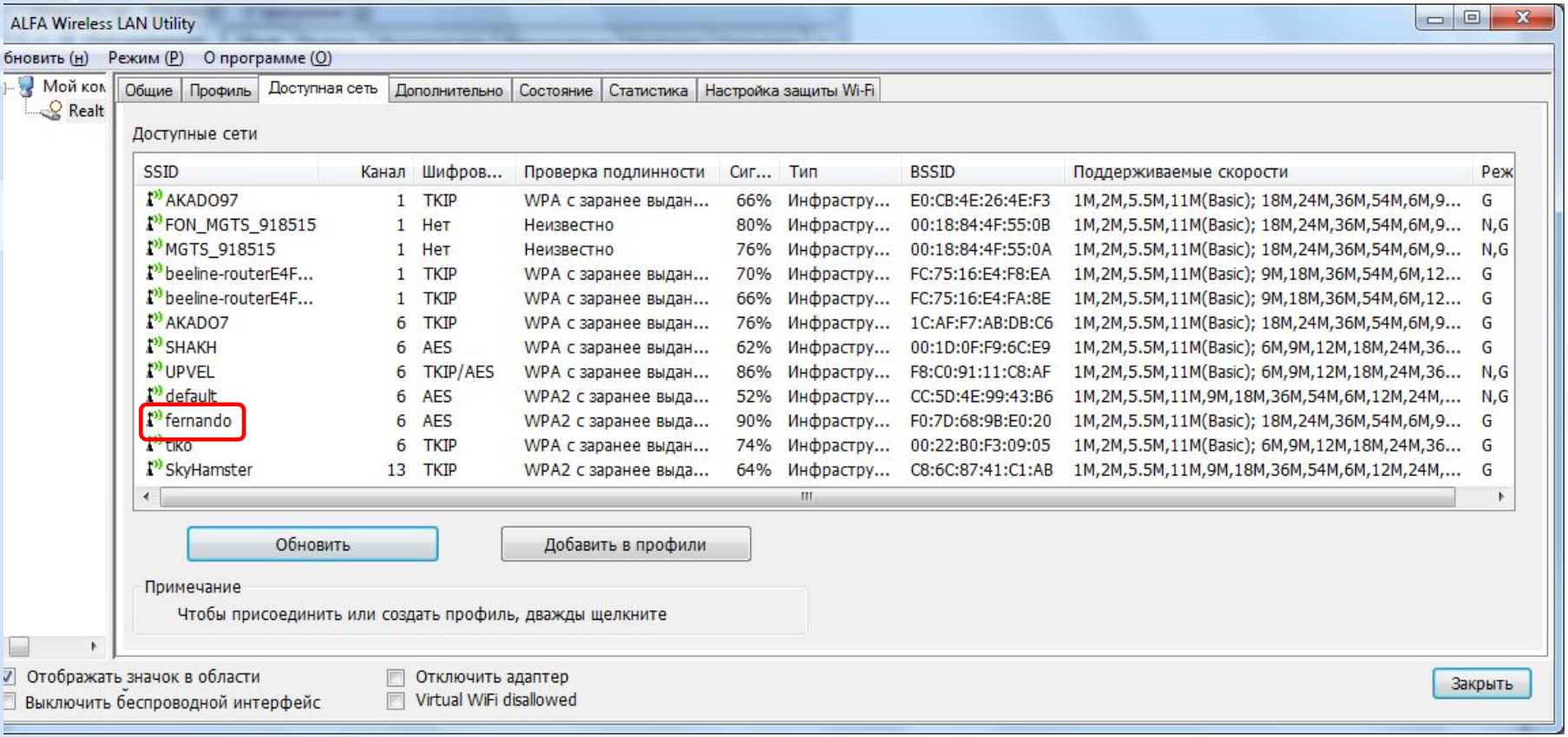
ICV (Integrity Check Value) (Код контроля целостности) - простая контрольная сумма, вычисляемая для фрейма 802.11 перед началом шифрования – это четырехбайтовая контрольная сумма, используемая в WEP- и WPA-шифрованных пакетах для сверки результата дешифрации. Принимающая сторона вычисляет значение ICV принятого пакета и сравнивает вычисленное значение с полученным. Если значения не совпадают, дешифрация считается неудавшейся.

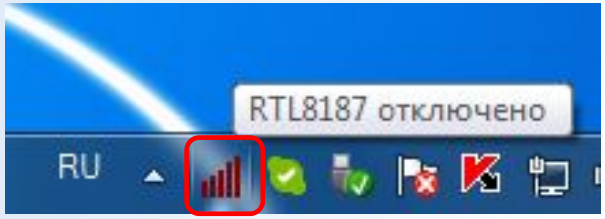
Настройки общего доступа к Интернету

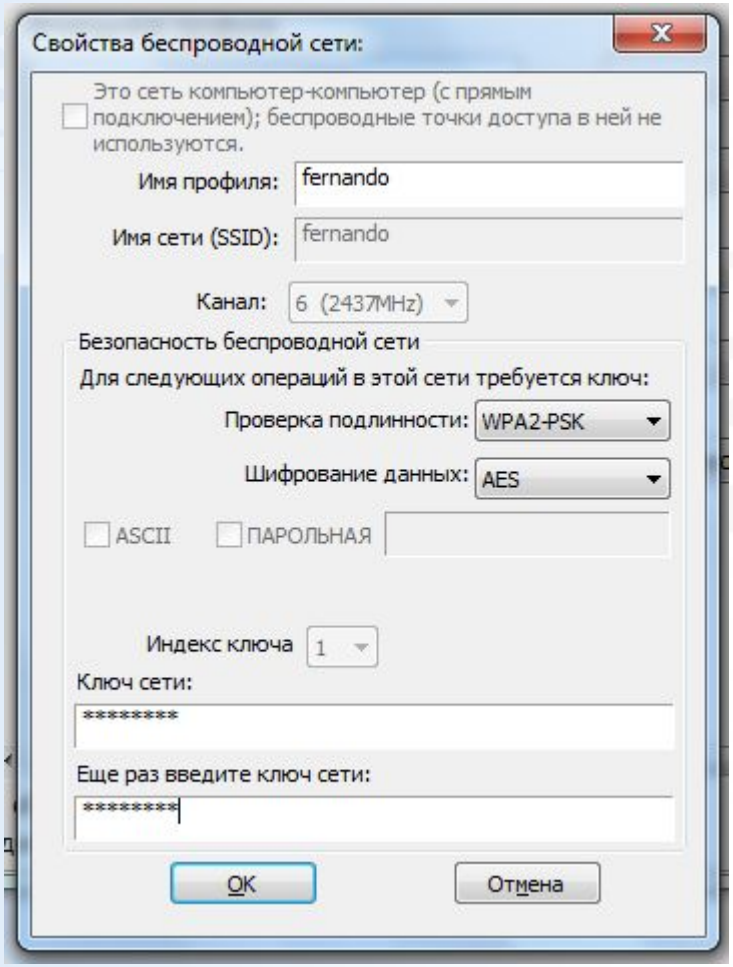


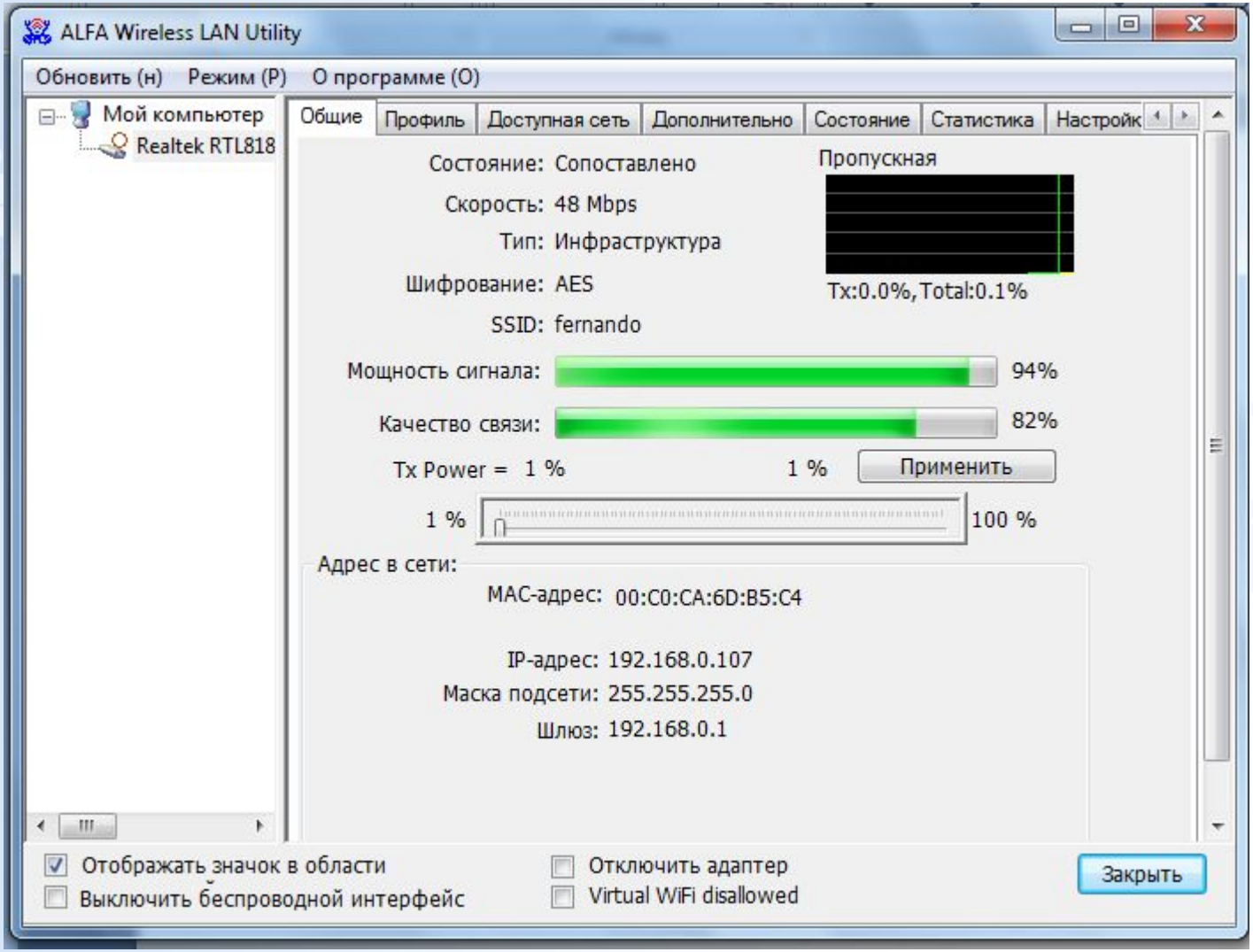


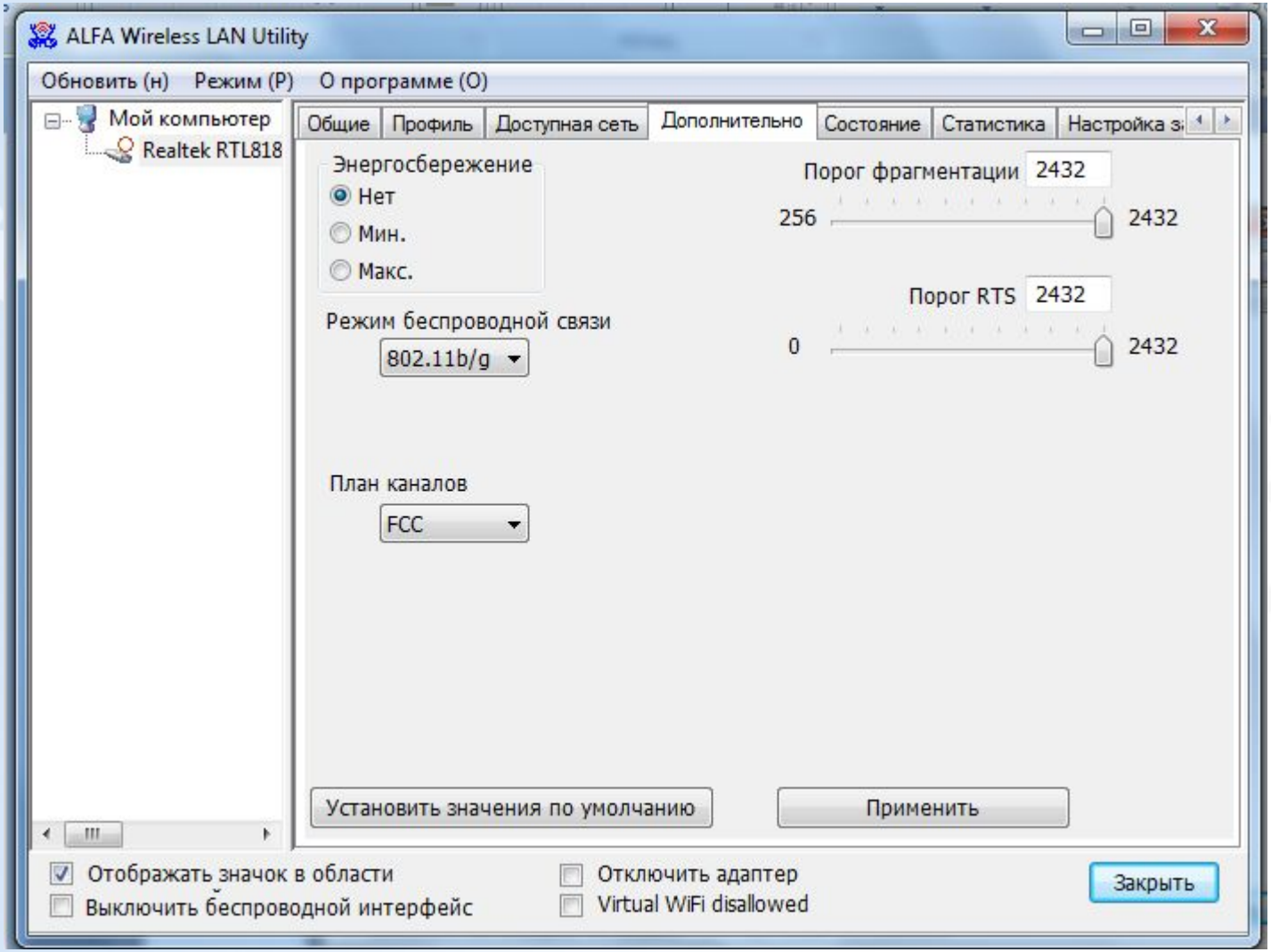
Подключение к сети Wi-Fi








ALFA Wireless LAN Utility
Обновить (н)
Режим (Р)
О программе (О)
Мой компьютер
Realtek RTL818
Общие
Профиль
Доступная сеть
Дополнительно
Состояние
Статистика
Настройк
Состояние: Сопоставлено
Скорость: 48 Mbps
Тип: Инфраструктура
Шифрование: AES
SSID: fernando
Пропускная
Tx:0.0%,Total:0.1%
Мощность сигнала:
94%
Качество связи:
82%
Tx Power = 1 %
1 %
Применить
1 %
100 %
Адрес в сети:
MAC-адрес: 00:C0:CA:6D:B5:C4
IP-адрес: 192.168.0.107
Маска подсети: 255.255.255.0
Шлюз: 192.168.0.1
Отображать значок в области
Выключить беспроводной интерфейс
Отключить адаптер
Virtual WiFi disallowed
Закрыть



Порог RTS (RTS Threshold) — определяет пороговое значение RTS. Другими словами, это минимальное число байт, для которого может действовать механизм соединения по каналу с использованием сигналов готовности к передаче/готовности к приему (RTS/CTS). В сети с высоким уровнем радиочастотных помех или большим числом беспроводных устройств, использующих один и тот же канал, снижение значения RTS Threshold может способствовать сокращению числа потерянных фреймов. Пороговое значение RTS по умолчанию составляет 2347 байт.

Порог фрагментации (**Fragmentation threshold)** — определяет максимальное значение, доступное для устройства при отправке информации в пакетах, прежде чем пакеты будут разбиты на фрагменты. Обычно причинами проблем, возникающих при отправке информации, является наличие другого сетевого трафика и конфликты передаваемых данных. Их можно устранить, разбив информацию на фрагменты. Чем ниже установленный порог фрагментации, тем меньше размер пакета, который не будет разбиваться на фрагменты. При максимальном значении 2346 фрагментация практически отключается.

Country	Channel Range	Country	Channel Range
USA	CH1 ~ CH11	FRANCE	CH10 ~ CH13
CANADA	CH1 ~ CH11	JAPAN	CH1 ~ CH14
ETSI	CH1 ~ CH13	ISRAEL	CH1 ~ CH13
SPAIN	CH10 ~ CH11		