Обеспечение безопасности беспроводной локальной сети

Владимир Борисович Лебедев

ТТИ ЮФУ

Программа

- Почему атакуют беспроводные локальные сети (WLAN)
- Ограничение доступа в сети WLAN
- Аутентификация в сети WLAN
- Шифрование в сети WLAN
- Фильтрация трафика в сети WLAN

Почему атакуют беспроводные локальные сети (WLAN)

Одним из главных преимуществ беспроводных сетей является удобство в подключении устройств. Но оборотной стороной удобства подключения и возможности передачи информации без проводов является уязвимость вашей сети для перехвата информации и атак со стороны злоумышленников.

Взломщику не требуется физического подключения к вашему компьютеру или к любому другому устройству для получения доступа в вашу сеть. Злоумышленник может настраиваться на сигналы вашей беспроводной сети точно так же как на волну радиостанции.

Взломщик может получить доступ в вашу сеть из любой точки в пределах действия беспроводной связи. Получив доступ к вашей сети, злоумышленники смогут бесплатно воспользоваться вашими Интернет-сервисами, а также получить доступ к компьютерам в сети и повредить файлы, либо украсть персональную или конфиденциальную информацию.

Для защиты от этих уязвимостей беспроводной связи необходимы специальные функции обеспечения безопасности и методы защиты беспроводной локальной сети (WLAN) от внешних атак. Для этого достаточно выполнить несколько несложных операций в процессе исходной настройке беспроводного устройства, а также настроить дополнительные параметры обеспечения безопасности.

Почему атакуют беспроводные локальные сети (WLAN)

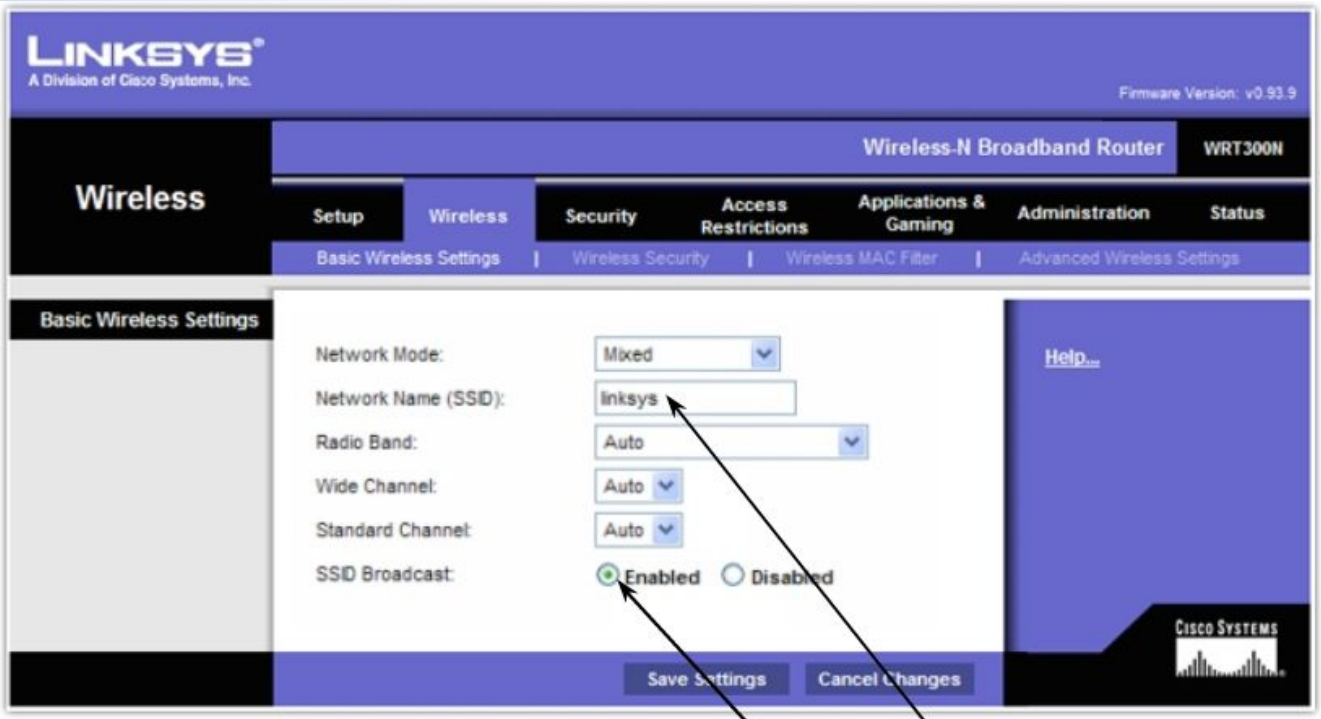
Вардрайвинг — это процесс передвижения на автомобиле по некоторой области с одновременным поиском беспроводных ЛВС. После обнаружения точки доступа к беспроводной ЛВС она регистрируется и открывается в общий доступ. Цель вардрайвинга — привлечение внимания к незащищенности большинства беспроводных сетей, а также демонстрация широкого распространения и использования технологии беспроводной ЛВС.
Процесс, подобный вардрайвингу, известен как war-walking (боевая ходьба), в котором некоторое лицо перемещается по некоторой области пешком в целях обнаружения точки беспроводного доступа. После обнаружения точки доступа в месте обнаружения делается отметка мелом, чтобы обозначить состояние беспроводного соединения.

Почему атакуют беспроводные локальные сети (WLAN)

Один из простейших способов доступа в беспроводную сеть - использовать имя сети или SSID.

Все компьютеры, подключенные к беспроводной сети, должны использовать ее SSID. По умолчанию, беспроводные маршрутизаторы и точки доступа рассылают идентификаторы SSID всем компьютерам в пределах действия беспроводной сети. Если функция рассылки SSID активирована, то любой беспроводной клиент сможет обнаружить сеть и подключиться к ней, если не настроены другие функции обеспечения безопасности.

Функцию рассылки SSID можно отключать. Если она отключена, то сведения о доступности сети уже не являются общедоступными. Любой компьютер, подключаемый в сеть, должен использовать ее SSID.



Для SSID и широковещательного SSID заданы значения по умолчанию

Почему атакуют беспроводные локальные сети (WLAN)

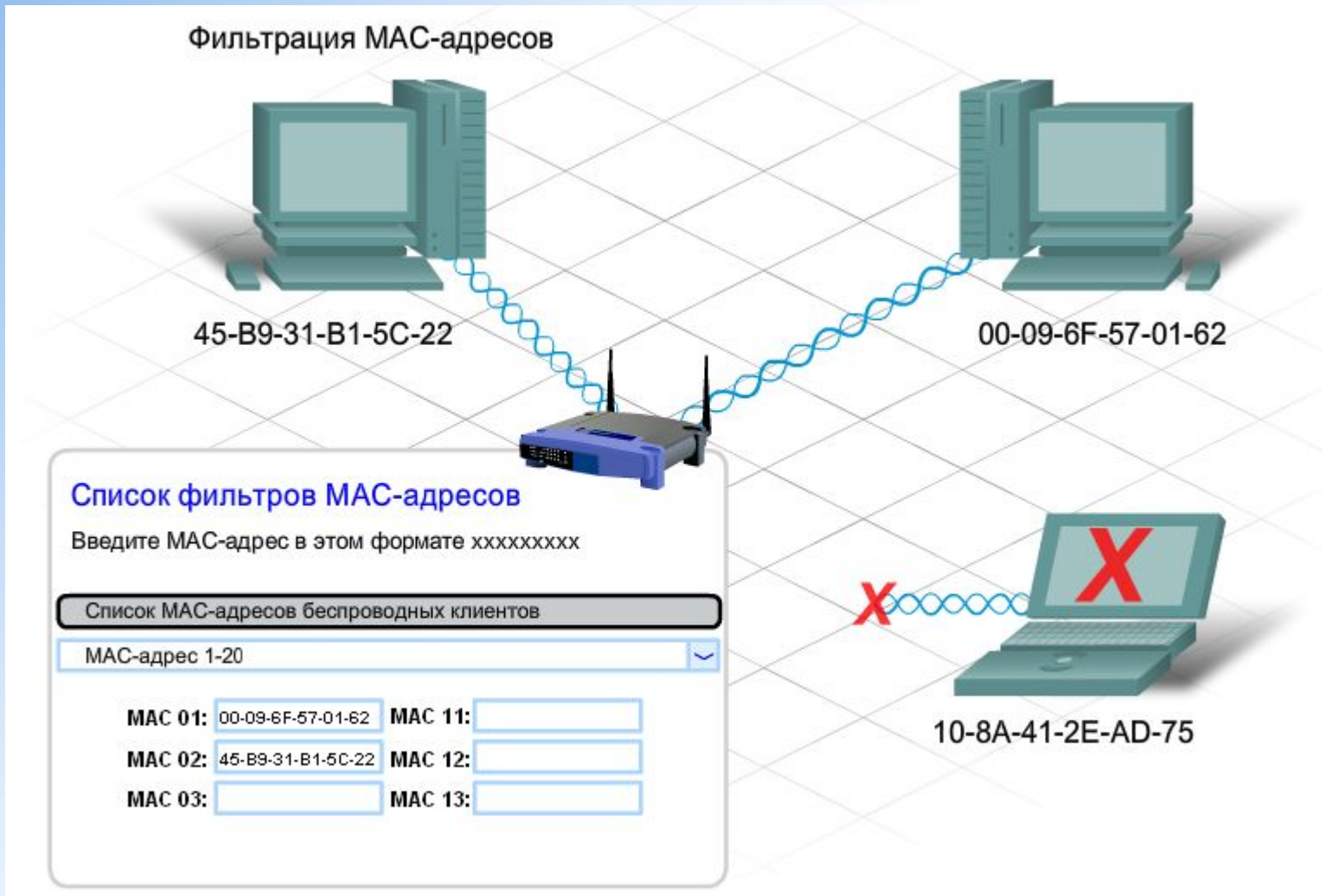
В качестве дополнительной меры защиты настоятельно рекомендуется изменить настройки, заданные по умолчанию. Беспроводные устройства поставляются с предварительно настроенными SSID, паролями и IP-адресами. Используя настройки по умолчанию, злоумышленник сможет легко идентифицировать сеть и получить доступ.

Даже если отключена рассылка SSID, существует вероятность проникновения в сеть, если злоумышленнику стал известен SSID, заданный по умолчанию. Если не изменить другие настройки по умолчанию, а именно пароли и IP-адреса, то взломщики могут проникнуть в точку доступа и внести изменения в ее конфигурацию. Настройки, заданные по умолчанию, должны быть изменены на более безопасные и уникальные.

Эти изменения сами по себе еще не гарантируют безопасности вашей сети. Например, SSID передаются открытым текстом. Но сегодня имеются устройства для перехвата беспроводных сигналов и чтения сообщений, составленных открытым текстом. Даже если функция рассылки SSID отключена и значения по умолчанию изменены, взломщики могут узнать имя беспроводной сети с помощью таких устройств. Используя эту информацию, они смогут подключиться к сети. Для обеспечения безопасности беспроводной локальной сети (WLAN) следует использовать комбинацию из нескольких методов защиты.

Ограничение доступа в сети WLAN

Один из способов ограничения доступа в беспроводную сеть – определить устройствам разный уровень привилегий доступа в сеть.
Для этого применяется фильтрация MAC-адресов.

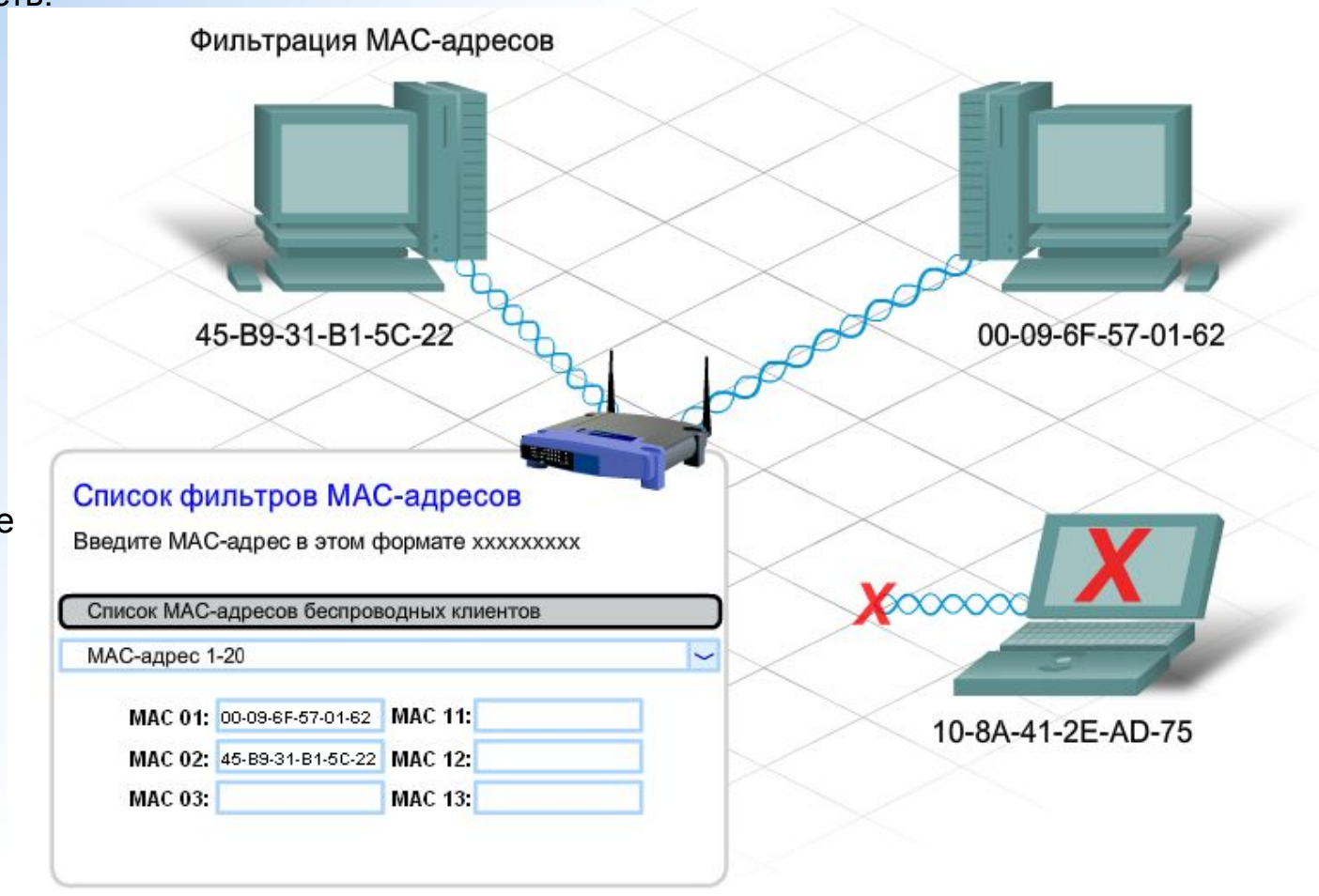


Фильтрация MAC-адресов

Фильтрация MAC-адресов позволяет задать перечень устройств, имеющим разрешение на соединение с беспроводной сетью, с помощью их MAC-адресов. При каждой попытке беспроводного клиента установить соединение или ассоциироваться с точкой доступа он должен передать свой MAC-адрес. Если включена функция **фильтрация по MAC-адресам**, то беспроводной маршрутизатор или точка доступа выполнит поиск MAC-адреса этого устройства по своему предварительно заданному списку. Разрешение на соединение получат только те устройства, чьи MAC-адреса были заранее прописаны в базе данных маршрутизатора.

Если MAC-адрес не найден в базе данных, устройству будет отказано в установлении соединения или в доступе в беспроводную сеть.

Такой тип обеспечения безопасности имеет некоторые недостатки. Например, он предполагает, что MAC-адреса всех устройств, которым должен быть предоставлен доступ в сеть, включены в базу данных до того, как будет выполнена попытка соединения. Устройство, не распознанное по базе данных, не сможет выполнить соединение. При этом взломщик может создать клон MAC-адреса устройства, имеющего доступ в сеть.



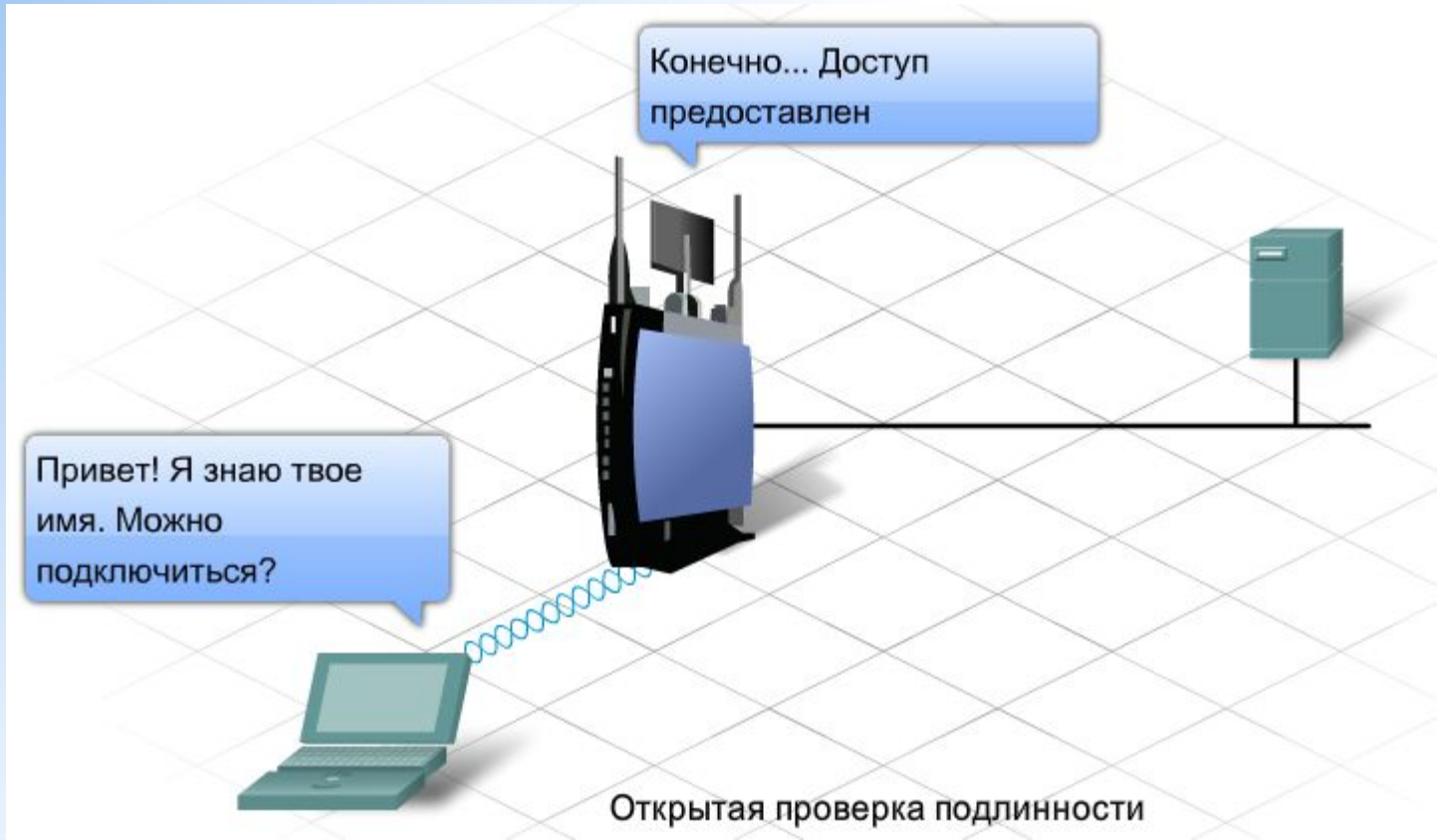
Аутентификация в сети WLAN

Другой способ администрирования доступа - аутентификация.
Аутентификация – это предоставление разрешения на вход в сеть по результатам проверки подлинности набора учетных данных.
Ее цель - выяснить, является ли устройство, пытающееся установить соединение, доверенным устройством.

Наиболее распространена аутентификация по имени пользователя и паролю. В беспроводной среде аутентификация позволяет выполнить проверку подлинности подключенного узла, но процесс проверки выполняется несколько по-другому.
Если включена функция аутентификации, то она должна быть выполнена до того, как клиенту будет предоставлено разрешение на подключение к сети WLAN. Существует три группы методов аутентификации беспроводных сетей: **обрыв аутентификация**, **PSK** и **EAP**.

Открытая аутентификация

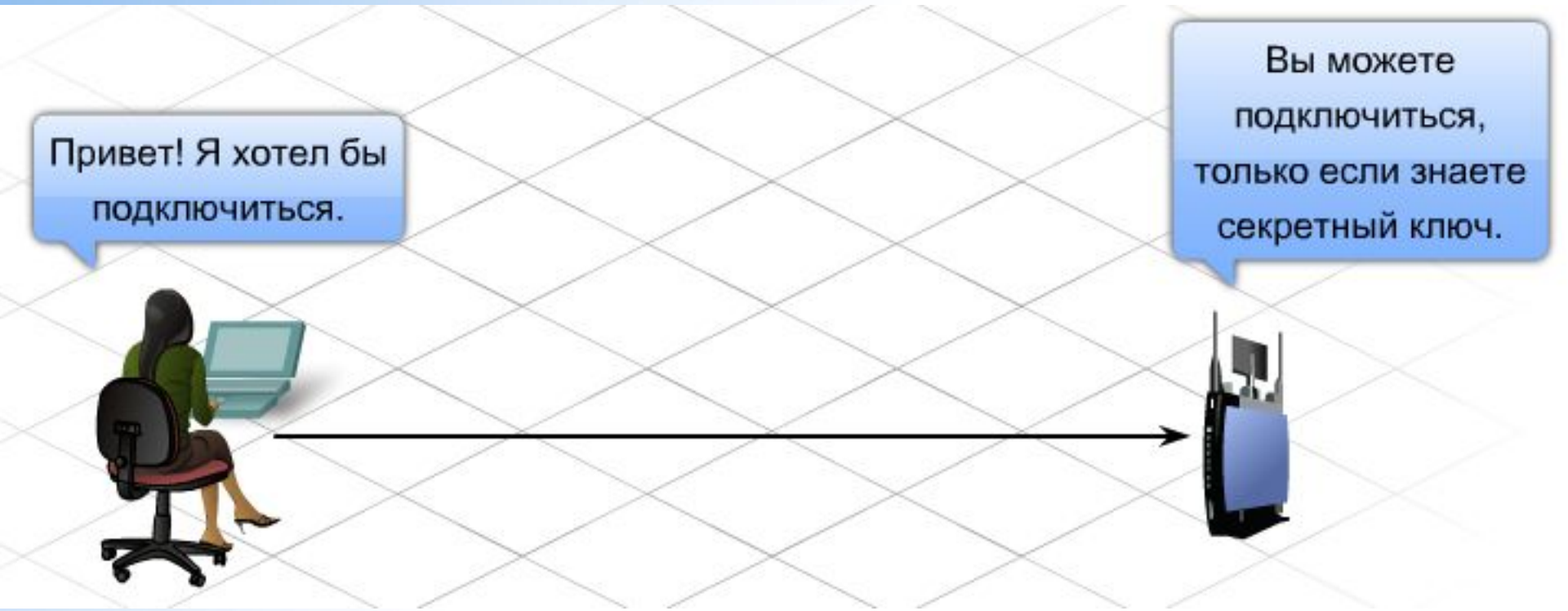
По умолчанию для беспроводных устройств аутентификация не требуется. Всем устройствам разрешено устанавливать соединения независимо от их типа и принадлежности. Это называется открытой аутентификацией. Открытая аутентификация должна использоваться только в общедоступных беспроводных сетях, например, в школах и Интернет-кафе (ресторанах). Она может использоваться в сетях, где аутентификация будет выполняться другими средствами после подключения к сети.



Режим предварительных ключей (Pre-shared keys, PSK)

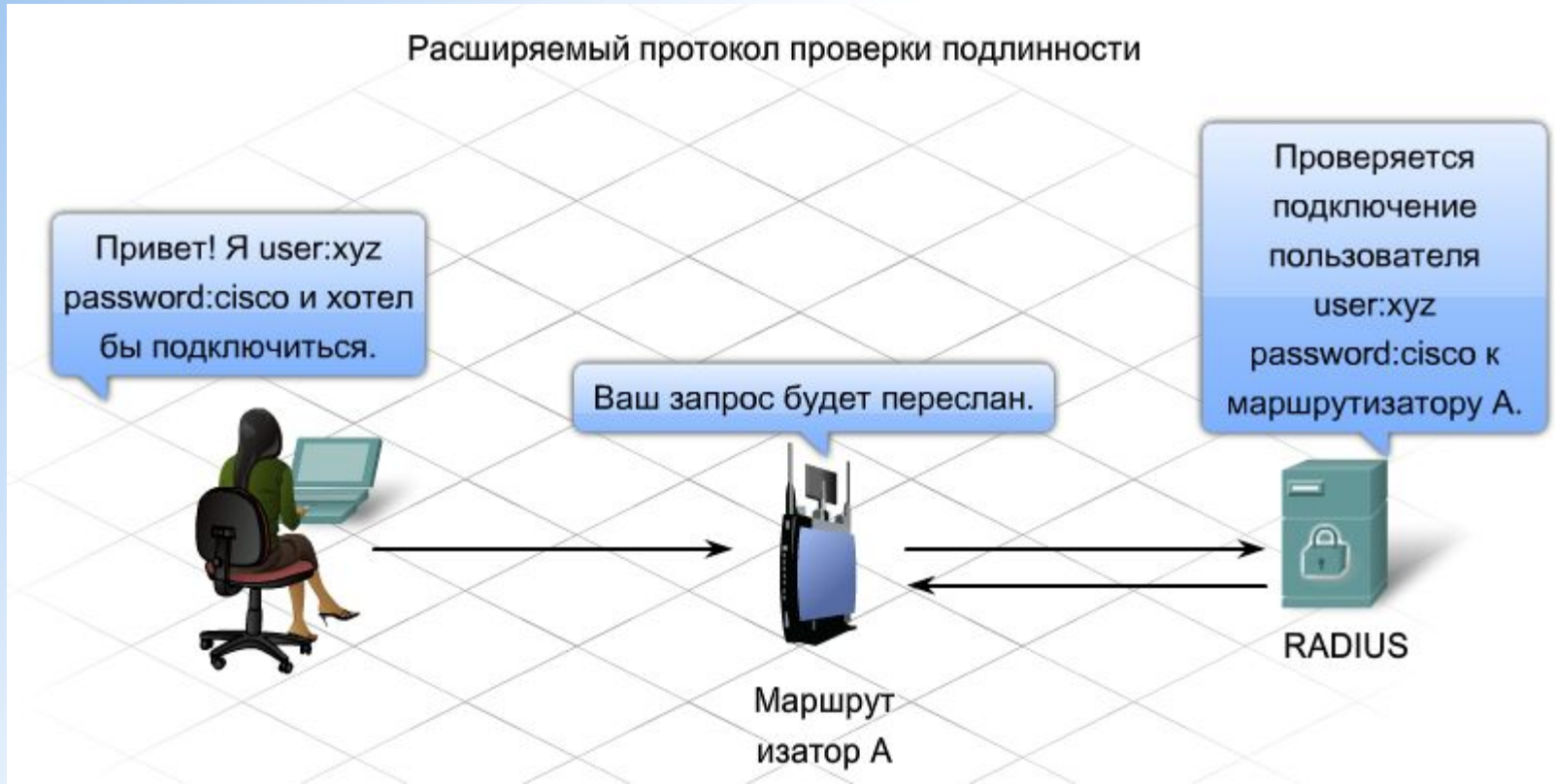
При использовании режима PSK точка доступа и клиент должны использовать общий ключ или кодовое слово. Точка доступа отправляет клиенту случайную строку байтов. Клиент принимает эту строку, шифрует ее (или скремблирует), используя ключ, и отправляет ее обратно в точку доступа. Точка доступа получает зашифрованную строку и для ее расшифровки использует свой ключ. Если расшифрованная строка, принятая от клиента, совпадает с исходной строкой, отправленной клиенту, то клиенту дается разрешение установить соединение.

PSK выполняет одностороннюю аутентификацию, то есть, точка доступа проверяет подлинность подключаемого узла. PSK не подразумевает проверки узлом подлинности точки доступа, а также не проверяет подлинности пользователя, подключающегося к узлу.



Расширяемый протокол проверки подлинности (Extensible Authentication Protocol, EAP)

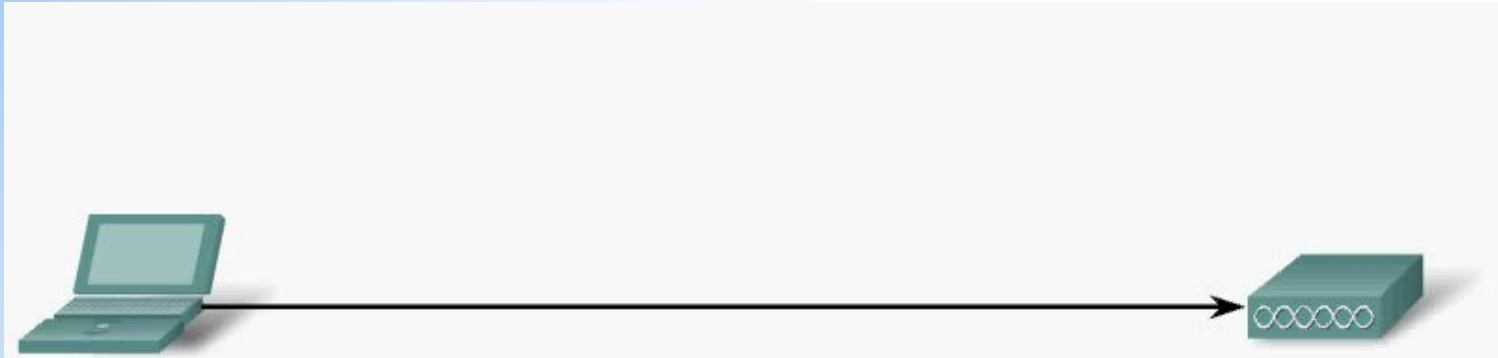
EAP обеспечивает взаимную или двухстороннюю аутентификацию, а также аутентификацию пользователя. Если на стороне клиента установлено программное обеспечение EAP, клиент взаимодействует с внутренним сервером аутентификации, таким как сервер дистанционной аутентификации мобильного пользователя коммутируемой сети (**RADIUS**). Этот обслуживающий сервер работает независимо от точки доступа и ведет базу данных пользователей, имеющих разрешение на доступ в сеть. При применении EAP пользователь, а не только узел, должен предъявить имя и пароль, которые затем проверяются по базе данных сервера RADIUS. Если предъявленные учетные данные являются допустимыми, пользователь рассматривается как прошедший проверку подлинности.



Аутентификация в сети WLAN

Если функция аутентификации включена, то независимо от применяемого метода клиент должен успешно пройти аутентификацию до того, как ему будет предоставлено разрешение на вход в точку доступа. Если включены функции аутентификации и фильтрации MAC-адресов, то в первую очередь выполняется аутентификация.

Если аутентификация прошла успешно, точка доступа затем проверяет MAC-адрес по таблице MAC-адресов. После выполнения проверки точка доступа добавляет MAC-адрес этого узла в свою таблицу узлов. Таким образом, предполагается, что клиент ассоциирован с точкой доступа и имеет разрешение на подключение к сети.



mov

Шифрование в сети

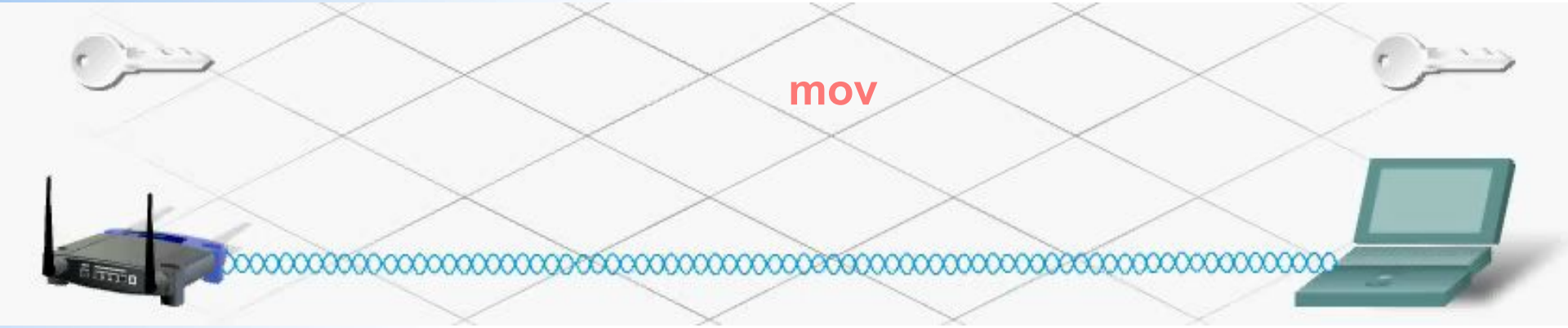
Аутентификация и фильтрация MAC-адресов могут блокировать взломщику доступ в беспроводную сеть, но не смогут предотвратить перехват передаваемых данных. Поскольку не существует четких границ беспроводных сетей и весь трафик передается без проводов, то взломщик может легко перехватывать или прочитать кадры данных беспроводной сети. Шифрование – это процесс преобразования данных таким образом, что даже перехват информация оказывается бесполезным.

Протокол конфиденциальности, эквивалентной проводной связи – Wired Equivalency Protocol (WEP)

Протокол WEP – это усовершенствованный механизм безопасности, позволяющий шифровать сетевой трафик в процессе передачи. В протоколе WEP для шифрования и расшифровки данных используются предварительно настроенные ключи.

WEP-ключ вводится как строка чисел и букв длиной 64 или 128 бит. В некоторых случаях протокол WEP поддерживает 256-битные ключи. Для упрощения создания и ввода этих ключей во многих устройствах используются фразы-пароли. Фраза-пароль – это простое средство запоминания слова или фразы, используемых при автоматической генерации ключа.

Для эффективной работы протокола WEP точка доступа, а также каждое беспроводное устройство, имеющее разрешение на доступ в сеть, должны использовать общий WEP-ключ. Без этого ключа устройства не смогут распознать данные, передаваемые по беспроводной сети.



Шифрование в сети WLAN

Протокол WEP – это эффективное средство защиты данных от перехвата. Тем не менее, протокол WEP также имеет свои слабые стороны, одна из которых заключается в использовании статического ключа для всех устройств с поддержкой WEP. Существуют программы, позволяющие взломщику определить WEP-ключ. Эти программы можно найти в сети Интернет. После того, как взломщик получил ключ, он получает полный доступ ко всей передаваемой информации.

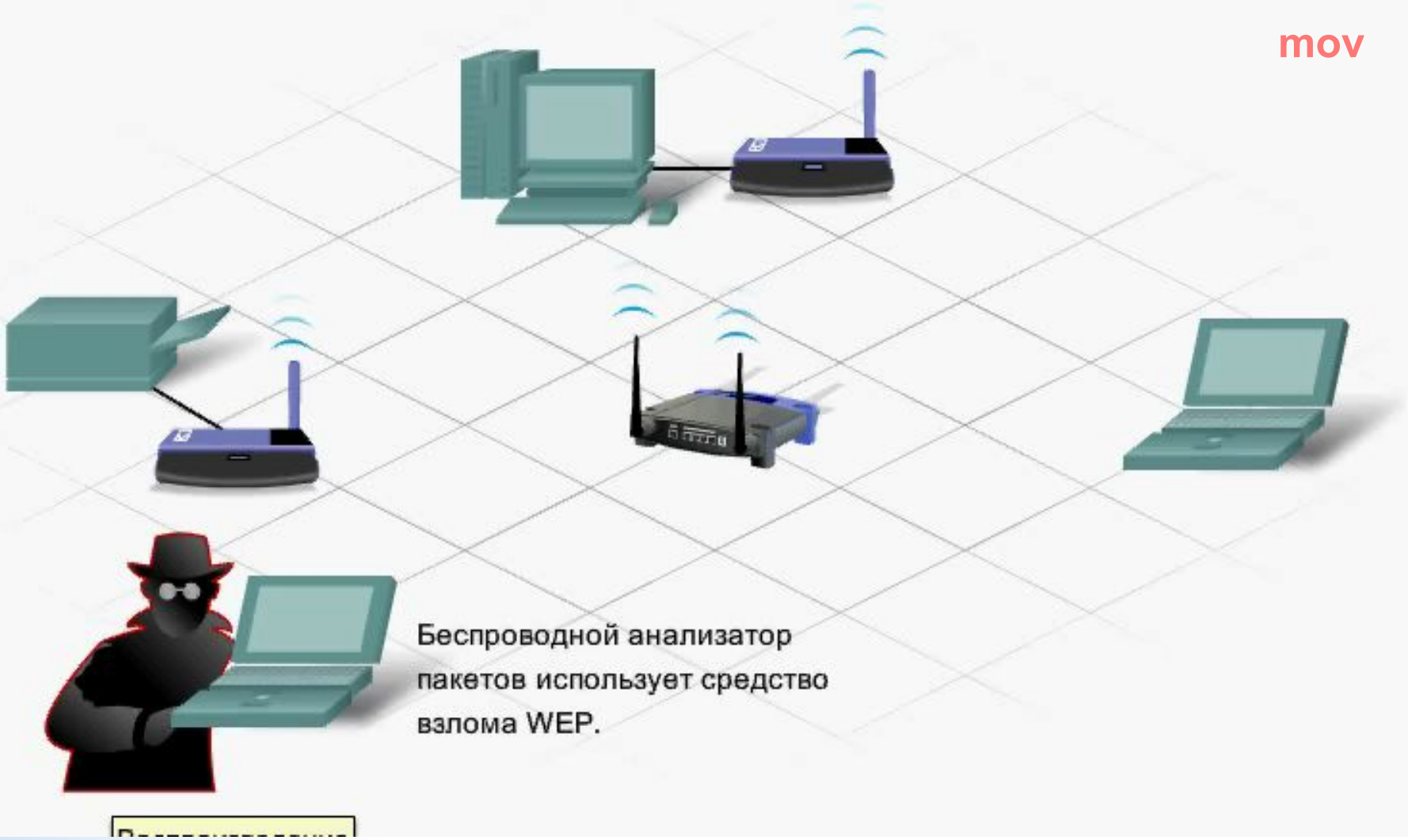
Одним из средств защиты от такой уязвимости является частая смена ключей. Существует усовершенствованное и безопасное средство шифрования – протокол защищенного доступа Wi-Fi (Wi-Fi Protected Access, (**WPA**)).

Защищенный доступ к Wi-Fi (WPA)

В протоколе WPA используются ключи шифрования длиной от 64 до 256 бит. При этом WPA, в отличие от WEP, генерирует новые динамические ключи при каждой попытке клиента установить соединение с точкой доступа. По этой причине WPA считается более безопасным, чем WEP, так как его значительно труднее взломать.

Беспроводный анализатор пакетов

mov

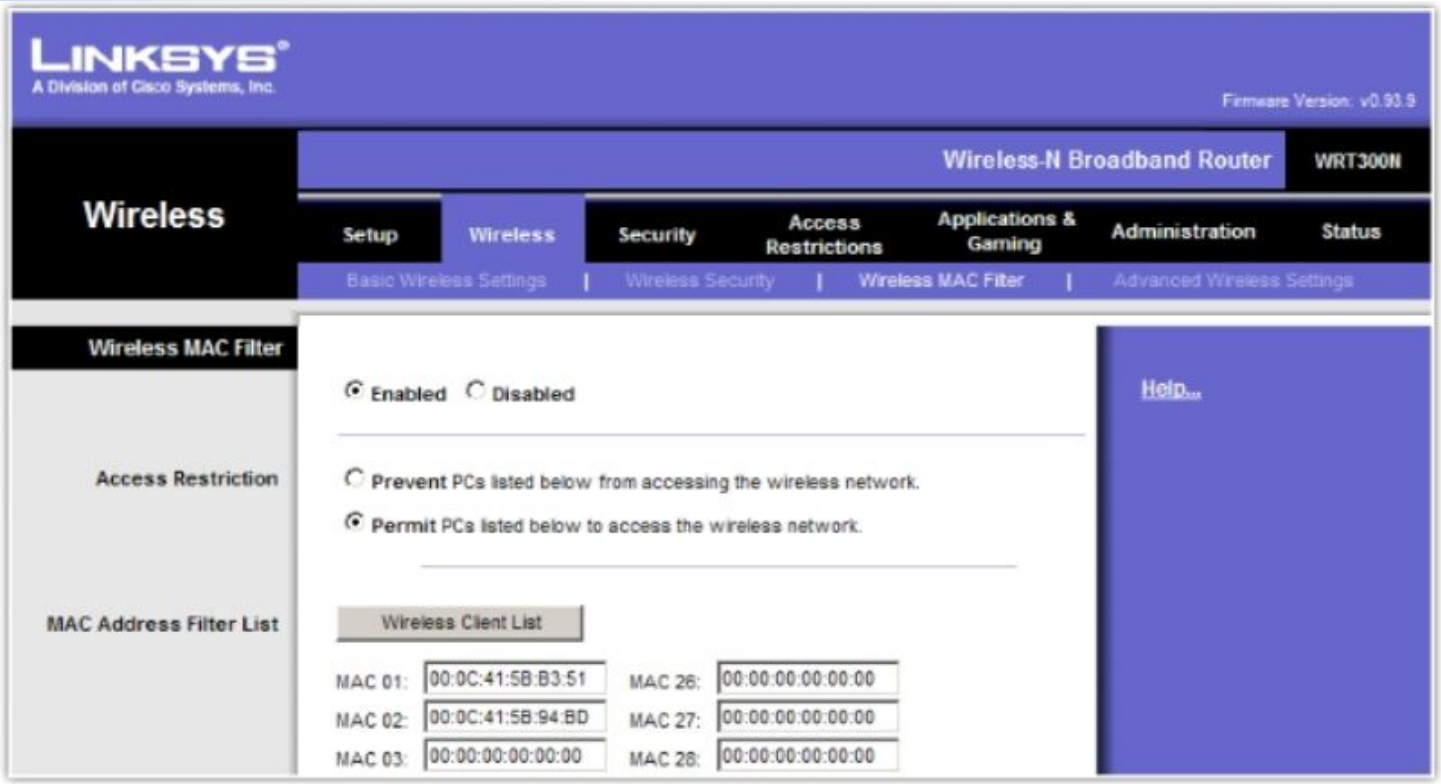


Беспроводной анализатор пакетов использует средство взлома WEP.

Фильтрация трафика в сети

Помимо управления доступом в сеть WLAN и администрирования прав на использование передаваемых данных, необходимо также управлять трафиком, передаваемым по сети WLAN. Для этого применяется фильтрация трафика.

Фильтрация позволяет блокировать вход и выход нежелательного трафика из сети. Фильтрацию выполняет точка доступа по мере прохождения трафика через нее. Это средство позволяет исключать или ограничивать трафик отдельных MAC-адресов или IP-адресов. Кроме того, фильтрация трафика позволяет блокировать отдельные программы по номерам портов. Исключение нежелательного и подозрительного трафика из сети позволяет повысить пропускную способность передачи более важных данных и тем самым увеличить производительность сети WLAN. Например, с помощью фильтрации можно заблокировать весь telnet-трафик, поступающий на отдельную машину, например, сервер аутентификации. Любые попытки проникновения на сервер аутентификации с помощью telnet, будут блокироваться как подозрительные.



Вопросы&Ответы

Обеспечение безопасности беспроводной локальной сети

ТТИ ЮФУ