Доступ к беспроводным сетям и безопасность сетей стандарта 802.1X: мифы и факты

Открытость беспроводных сетей может вводить в заблуждение пользователей и администраторов сети. Администратор сети стремится ограничить доступ к сети только авторизированными пользователями, а последним нужна уверенность в том, что он подключаются к нужной сети. В этом документе описывается типичный процесс регистрации клиентов в беспроводной локальной сети, а также процессы аутентификации 802.1X и EAP.

FLUKE networks

Содержание

Доступ к беспроводным сетям и безопасность сетей стандарта 802.1X: мифы и факты

Сетевые администраторы и пользователи озабочены вопросами доступа к сети и обеспечения безопасности. Сетевой администратор хочет быть уверен в том, что клиент, запрашивающий доступ к сети, является авторизированным пользователем, а не злоумышленником. Пользователь в свою очередь хочет получить гарантию того, что при помощи своего ноутбука с беспроводным доступом он подключается к нужной, а не ложной сети, запущенной хакером для перехвата пользовательской информации. Отношения сетевого администратора и пользователя выстраиваются на основе доверия.

Некоторые из первых систем безопасности и обеспечения конфиденциальности, разработанных для обеспечения доверия, оказались уязвимыми к нападению хакеров. Среди них 802.11 Wired Equivalent Privacy (WEP). Для создания надёжной сетевой среды современный сетевой администратор использует стандарт 802.1X. Последняя версия 802.1X оправдывает все его надежды.

13 декабря 2004 г. IEEE представил новый стандарт 802.1X, «Протокол управления доступом к сети на основании портов». Он доступен по адресу http://standards.ieee.org/getieee802/802.1.html. Стандарт 802.1X позволяет производить аутентификацию и авторизацию устройств, пытающихся подключиться к локальной сети, и отказывает им в доступе, если аутентификация или авторизация не проходят.

Администраторы беспроводных локальных сетей одними из первых внедрили стандарт 802.1X. В отличие от обычных проводных кабельных сетей беспроводные локальные сети нельзя «защитить» стенами и закрытыми дверями, поэтому они более уязвимы к нападениям. Сейчас стандарт 802.1X всё чаще применяется в кабельных сетях в качестве дополнительной меры защиты.

Стандарт IEEE 802.1X эволюционировал из протокола Point-to-Point (PPP) и расширенного протокола аутентификации (Extensible Authentication Protocol, или EAP). PPP чаще всего используется для подключения к Интернет по телефонной линии. Он основан на механизме аутентификации, включающем ввод имени пользователя и пароля. Стандарт EAP разработан для создания более надёжного механизма защиты. EAP используется вместе с протоколом аутентификации PPP и предоставляет общую структуру разных методов аутентификации. EAP описан в IETF RFC 3748, доступном по адресу http://www.ietf.org/rfc. Стандарт IEEE 802.1X описывает использование EAP в проводных и беспроводных локальных сетях. 802.1X не использует PPP; скорее EAP сообщения будут упакованы в Ethernet фреймы. Этот метод инкапсуляции пакетов EAP известен как «EAP over LANs», или EAPOL.

IEEE 802.1X определяет три главные роли для выполнения процесса аутентификации. Аутентификатор — это сетевое устройство (например, точка доступа, коммутатор), которое осуществляет аутентификацию перед предоставлением доступа. Запрашивающая сторона — это сетевое устройство (например, клиентский ПК, КПК), которому требуется доступ. Сервер аутентификации – зачастую это сервер RADIUS – осуществляет аутентификацию, необходимую для проверки регистрационных данных запрашивающей стороны от имени аутентификатора, и указывает, допускается ли запрашивающая сторона к услугам аутентификатора. Несмотря на то, что возможно объединить роли аутентификатора и сервера аутентификации в одном устройстве, обычно используются два отдельных устройства. Это особенно полезно при разработке беспроводных сетей, в которых основной объём работы производится запрашивающей стороной (беспроводным ноутбуком), а сервер аутентификации и аутентификатор (точка доступа) может быть меньше и обладать меньшей вычислительной мощностью и памятью.

Рис. 1: Роли 802.1X

Далее осуществляется типичный успешный процесс аутентификации 802.1X. Он инициируется, как только запрашивающая сторона обнаруживает действующее соединение (например, ПК связывается с точкой доступа).

Отправ.	Получат.	EAP, содержание пакета	Цель
		Начало EAP	Запрос запуска процесса аутентификации EAP.
		EAP – запрос/ идентификационные данные	Запрос аутентификации перед предоставлением доступа.
		EAP – ответ/ идентификационные данные	Ответ на запрос с идентификационными данными.
		EAP – ответ/ идентификационные данные	Передача запроса серверу аутентификации.
		Вызов	Отправка запроса для получения идентификационных данных. Существует несколько разных версий EAP, поэтому вызов может отличаться (например, имя пользователя/пароль, сертификат пользователя).
		Вызов	Инкапсуляция вызова с EAPOL и отправка его запрашивающей стороне.
		Ответ на вызов	Отправка ответа на вызов.
		Ответ на вызов	Декодирование ответа и отправка его на сервер.
		Сообщение о соединении и ключ для сессии	Сообщение о соединении и ключ для сессии будут отправлены только в том случае, если запрашивающая сторона отправила верный ответ и сервер смог проверить идентификационные данные.
		Сообщение о соединении	Запрашивающая сторона успешно аутентифицирована.
		Обмен ключами	Создание ключей шифрования с помощью ключей для сессии.
		Ответ обмена ключами	Набор ключей шифрования.

Существует множество версий EAP. Они обычно отличаются сложностью и степенью безопасности выполняемого процесса. Некоторые процессы обработки запроса на аутентификацию выполняются клиентом, в то время как другие предусматривают двустороннюю аутентификацию клиента и сети. Некоторые используют шифрование запросов и ответов. Самые распространённые типы EAP – это те, которые встроены в коммутаторы, маршрутизаторы и операционные системы, поскольку их легче всего внедрить. В приведённой ниже таблице приведены некоторые из наиболее распространённых типов EAP, используемых с 802.1X.

Тип EAP	Имя	Тип локальной сети
EAP-TLS	Безопасность EAP на уровне передачи	Беспроводная Проводная
EAP-GTC	Карта EAP Generic Token Card	Проводная
EAP-MD5	EAP Message Digest 4	Проводная
EAP-MS-CHAP-V2	EAP Microsoft Challenge Handshake Authentication Protocol, версия 2	Проводная
EAP-FAST	Гибкая аутентификация EAP посредством безопасного туннелирования	Беспроводная
LEAP	Легкий EAP	Беспроводная
PEAP-GTC	Защищённая карта EAP Generic Token Card	Беспроводная Проводная
PEAP-MD5	Защищённое решение EAP Message Digest 5	Беспроводная Проводная
PEAP-MS-CHAP-V2	Защищённый EAP Microsoft Challenge Handshake Authentication Protocol, версия 2	Беспроводная Проводная
PEAP-TLS	Защищённый уровень передачи EAP	Беспроводная Проводная
TTLS-PAP	Протокол аутентификации при помощи пароля для безопасности туннелированной передачи	Беспроводная Проводная
TTLS-CHAP	Протокол Handshake Authentication Protocol для безопасности туннелированной передачи	Беспроводная Проводная
TTLS-MS-CHAP	Протокол Microsoft Challenge Handshake Authentication Protocol для безопасности туннелированной передачи	Беспроводная Проводная
TTLS-MS-CHAP-V2	Протокол Microsoft Challenge Handshake Authentication Protocol, версии 2 для безопасности туннелированной передачи	Беспроводная Проводная
TTLS-EAP-MD5	Message Digest 5 для безопасности туннелированной передачи	Беспроводная Проводная
TTLS-EAP-MS-CHAP-V2	Протокол Message Digest 5 Microsoft Challenge Handshake Authentication Protocol для безопасности туннелированной передачи, версия 2	Беспроводная Проводная
TTLS-EAP-TLS	Безопасность туннелированной передачи	Беспроводная Проводная

Далее следуют примеры процессов аутентификации для некоторых наиболее используемых типов EAP: EAP-TLS, LEAP и PEAP-MSCHAP-V2. В первом примере мы добавляем процесс подключения к беспроводной локальной сети и процесс получения IP адреса, поскольку они вместе с процессом аутентификации составляют типичный процесс регистрации клиента при подключении к сети.

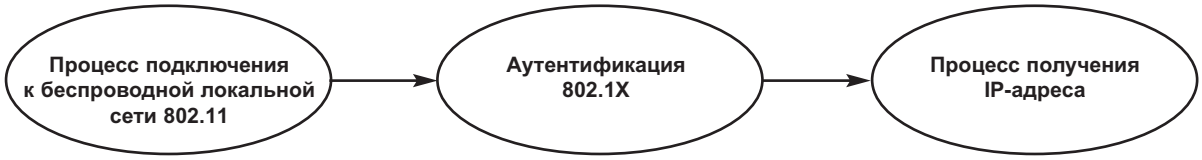
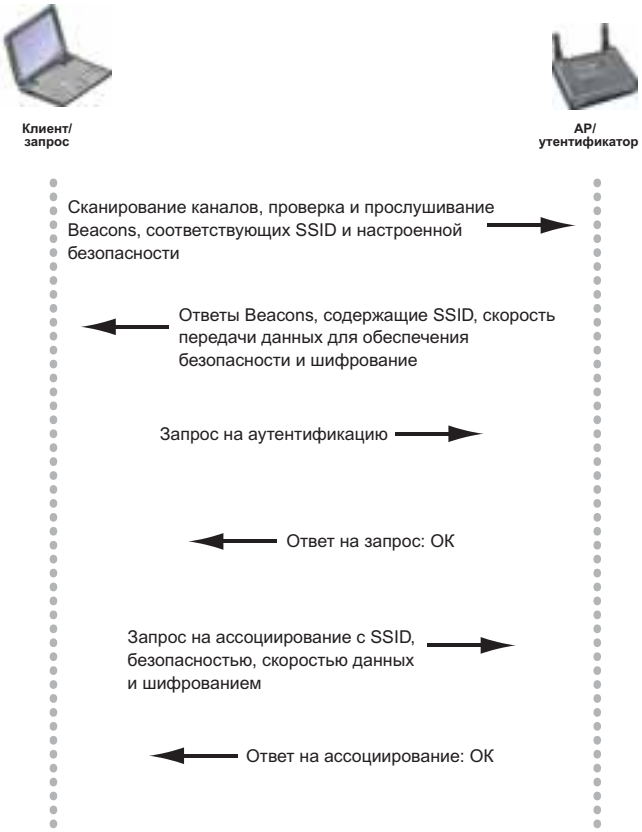


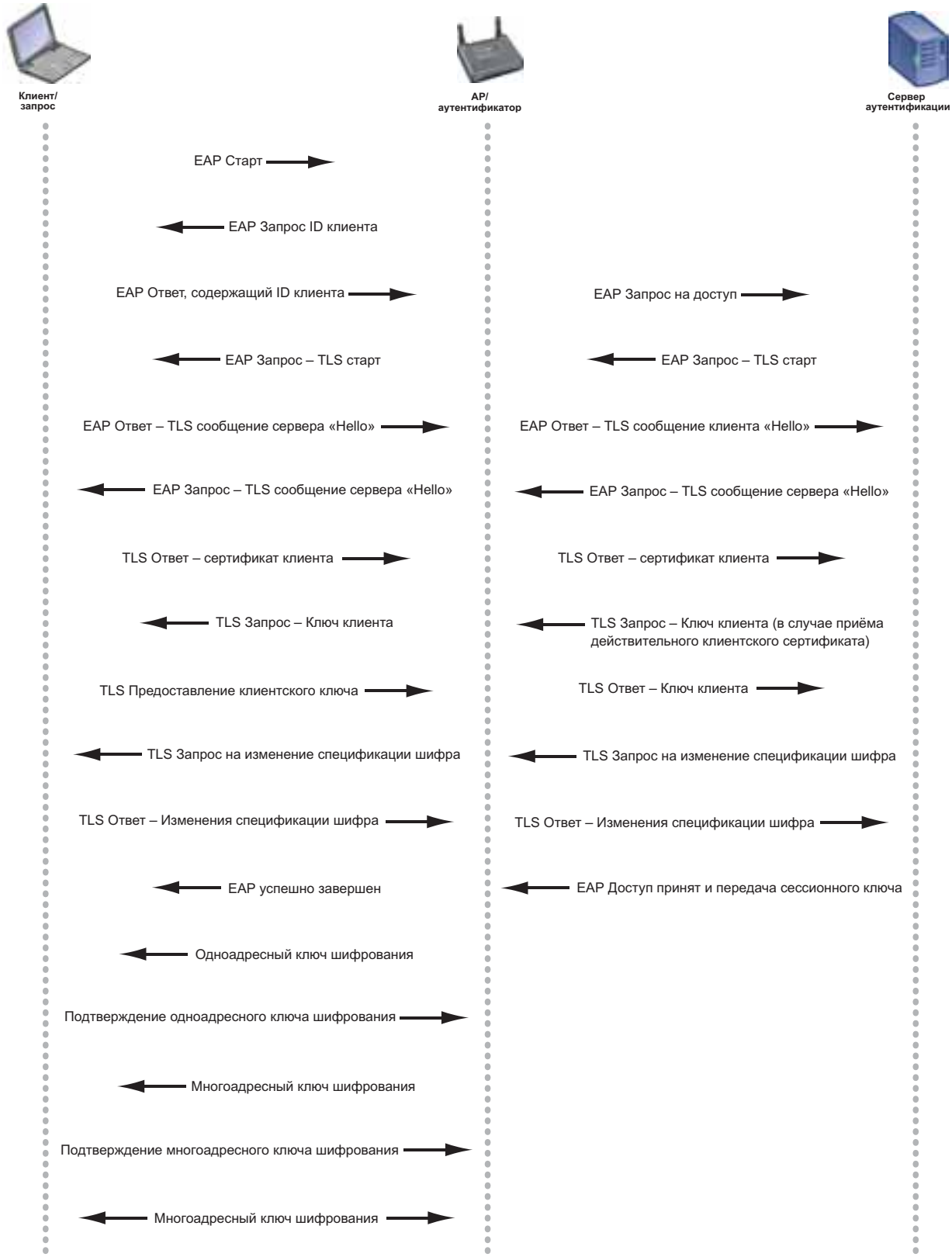
Рис. 2: Обычный процесс регистрации клиента в локальной беспроводной сети

Пример 1: процесс подключения к беспроводной локальной сети с аутентификацией EAP TLS.

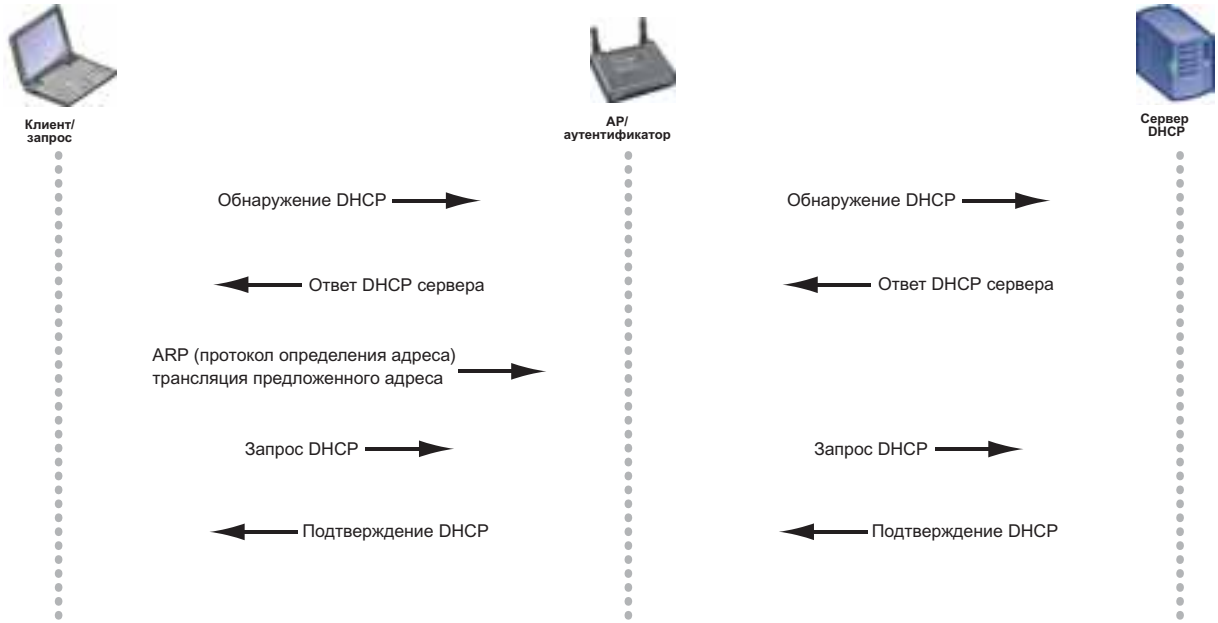
Подключение по протоколу 802.11



Процесс аутентификации 802.1X EAP-TLS

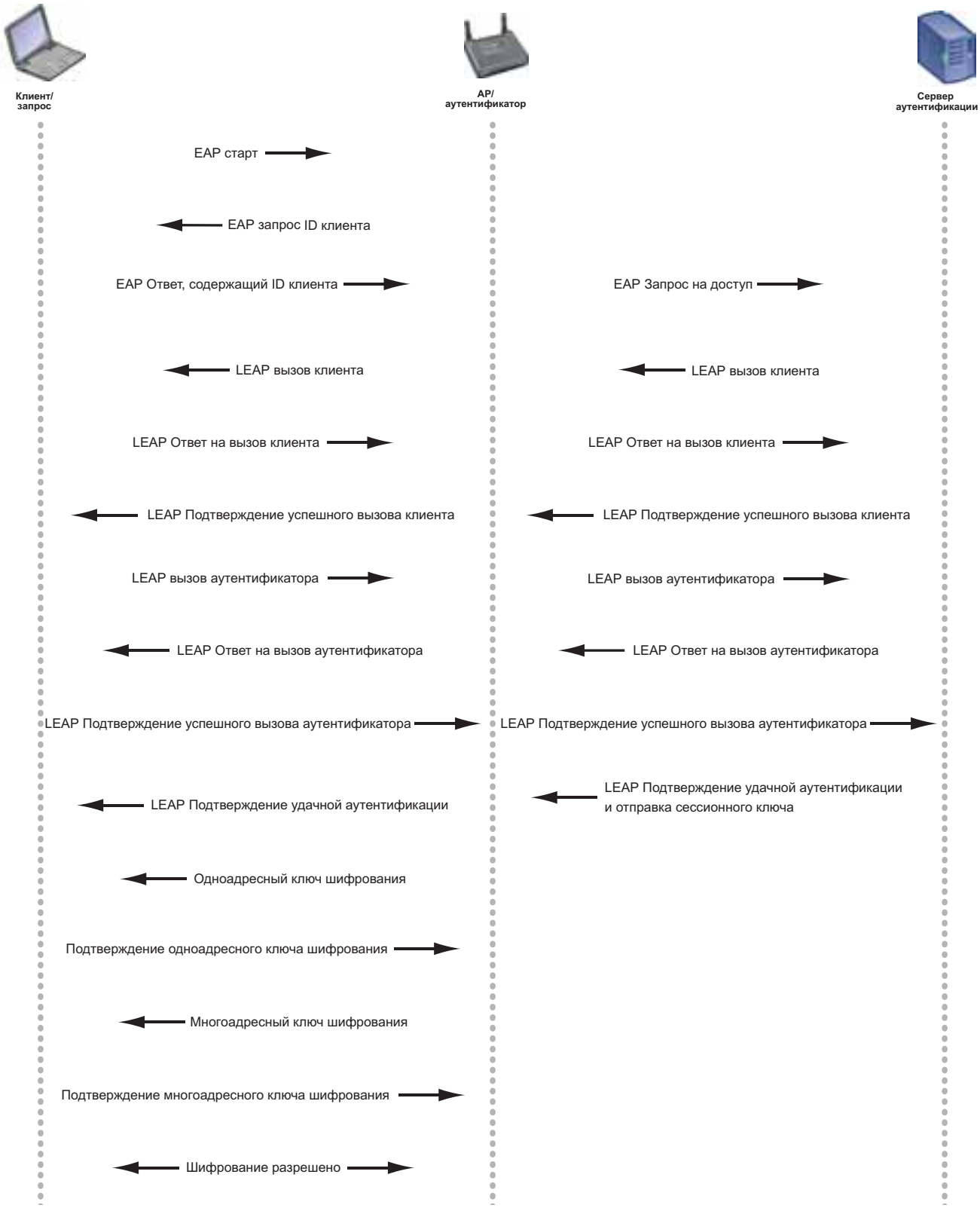


Процесс получения IP адреса от DHCP



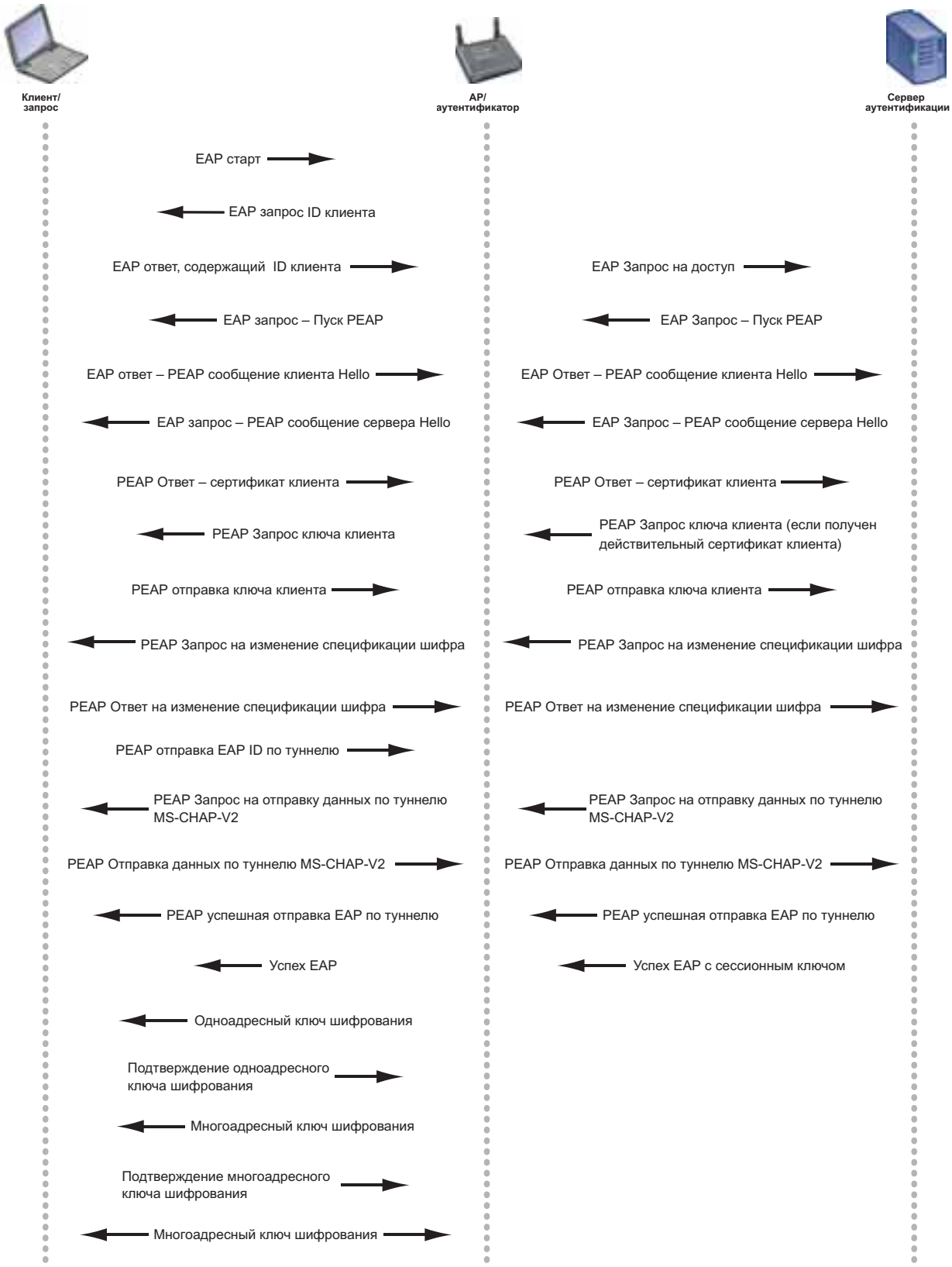
Пример 2: аутентификация 802.1X LEAP

В этом примере мы документируем только процесс аутентификации LEAP. Подключение к беспроводной локальной сети и взаимодействие с DCHP сервером не изменены.



Пример 3: процесс аутентификации 802.1X PEAP-MS-CHAP-V2

В этом примере мы документируем только процесс аутентификации PEAP-MS-CHAP-V2. Подключение к беспроводной локальной сети и взаимодействие с DCHP сервером не изменены.



Итоги

Понимание особенностей подключения, аутентификации и получения IP-адреса поможет решить проблемы регистрации клиентов. Средства анализа сетей позволяют отслеживать и документировать весь процесс регистрации клиентов в сети. В случае если действительный пользователь не может получить доступ к сети, подключите сетевой анализатор и пронаблюдайте весь процесс регистрации. Вы сможете определить, на каком моменте процесс приостанавливается. Определив проблему посредством наблюдения, Вы узнаете, что неисправно и что необходимо отладить в процессе.

Аутентификация, процесс проверки идентификационных данных, является основным компонентом обеспечения безопасности сети. При внедрении аутентификации IEEE 802.1X сетевые администраторы получают эффективное средство управления и контроля доступа к сети. Есть несколько видов EAP: одни разработаны как для проводных, так и для беспроводных сетей, другие – только для одной категории сетей. Перед выбором следует изучить каждый из них, так как у каждого типа есть свои преимущества и недостатки. Понимание процессов аутентификации и регистрации помогает решить проблемы пользовательского доступа. Кроме того, учёт возможных угроз для безопасности — это лучший способ установить доверие в Ваших сетях.

Ссылки

IEEE Std 802.1X-2004, стандарт IEEE для локальных и городских сетей, Протокол управления доступом к сети на основании портов.

IETF RFC 3748, расширенный протокол проверки (EAP), Бланк Л. (Blunk, L.), Фольбрехт Дж. (Vollbrecht, J.), Абоба Б. (Aboba, B.), Карлсон Дж. (Carlson, J.), Левковец Х. (Levkowetz, H.), июнь 2004 г.

Гейер Джим (Geier Jim). «802.1X обеспечивает аутентификацию и управление ключами.» Wi-Fi Planet 7 мая 2002 г.

Шнайдер Джоэл (Snyder Joel). «Что такое 802.1X?» Network World Fusion 6 мая 2002 г.

«802.1X – управление доступом к беспроводной сети на основании портов.» Wi-Fi Planet.com 5 сентября 2003 г.

«Развёртывание 802.1X для беспроводных локальных сетей: типы EAP.» Wi-Fi Planet.com 10 сентября 2003 г.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA, США 98206-0777

Fluke Networks работает более чем в 50 странах мира. За информацией о местных дистрибьюторах и представительствах обращайтесь на сайт **www.flukenetworks.com/contact**.

Отпечатано в США. 04/2006 3036913 A-RUS-N ред. A