Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)

Содержание

Введение

Настоящий документ содержит пример конфигурации беспроводного контроллера LAN (WLC) для аутентификации EAP (протокол расширенной аутентификации) с помощью внешнего сервера RADIUS. Данным сервером может быть сервер ACS (сервер управления доступом) Cisco Secure в качестве внешнего сервера RADIUS для проверки учетных данных пользователя.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Владение основными знаниями о конфигурации "облегченных" точек доступа (AP) и контроллеров Cisco WLC.
- Основные сведения о протоколе облегченных точек доступа (LWAPP).
- Знакомство со способами настройки внешнего сервера RADIUS аналогично Cisco Secure ACS.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Aironet легковесный AP серии 1232AG
- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 5.1
- Cisco Secure ACS, который выполняет версию 4.1
- Адаптер клиента Cisco Aironet 802.11 a/b/g
- Утилита Cisco Aironet Desktop Utility (ADU), которая выполняет микропрограммное обеспечение 4.2

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Для настройки устройства для аутентификации EAP выполните следующие действия:

1. Конфигурация WLC для основной операции и регистрация "облегченных" AP на контроллере.
2. Конфигурация WLC для аутентификации RADIUS через внешний сервер RADIUS.
3. Конфигурация параметров WLAN.
4. Конфигурация Cisco Secure ACS в качестве сервера RADIUS и создание базы данных пользователей для аутентификации клиентов.

Схема сети

В этой настройке WLC Cisco 4400 и Легковесный AP связаны через концентратор. Внешний сервер RADIUS (Cisco Secure ACS) также подключается к данному концентратору. Все устройства находятся в пределах одной подсети. AP изначально зарегистрирована на

контроллере. Необходимо настроить WLC и AP для аутентификации с использованием LEAP (упрощенный расширяемый протокол аутентификации). Клиенты, которые подключаются к AP, используют аутентификацию LEAP для связи с AP. Необходимо использовать Cisco Secure ACS, чтобы выполнить аутентификацию RADIUS.

Конфигурация WLC для основной операции и регистрация "облегченных" AP на контроллере

Используйте мастер запуска конфигурации в интерфейсе командной строки (CLI) для настройки WLC в основном режиме. Также можно использовать GUI для настройки WLC. В данном документе описана конфигурация на WLC, выполняемая с помощью мастера запуска конфигурации в CLI.

После первоначальной загрузки WLC, он напрямую подключается к мастеру запуска конфигурации. Используйте мастер запуска конфигурации для настройки основных параметров. Можно запустить мастер в CLI или GUI. Эти выходные данные отображают пример мастера запуска конфигурации в CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.77.244.204 Management Interface Netmask: 255.255.255.224 Management Interface Default Router:
10.77.244.220 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 10.77.244.220 AP Manager Interface IP
Address: 10.77.244.205 AP-Manager is on Management subnet, using same values AP Manager
Interface DHCP Server (10.77.244.220): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group
Name: Test Network Name (SSID): Cisco123 Allow Static IP Addresses [YES][no]: yes Configure a
RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS
server. Please see documentation for more details. Enter Country Code (enter 'help' for a list
of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configuration saved!
Resetting system with new configuration..
```

Данные параметры используются, чтобы настроить WLC для выполнения основных операций. В этом примере конфигурации WLC использует **10.77.244.204** в качестве IP-адреса интерфейса управления и **10.77.244.205** как IP-адрес интерфейса менеджера точки доступа.

Перед настройкой других функций на контроллерах WLC необходимо зарегистрировать "облегченные" AP в WLC. В данном документе предполагается, что "облегченная" AP зарегистрирована на контроллере WLC. См. регистрацию облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC) для получения дополнительной информации о том, как Легковесные AP регистрируются в WLC.

Конфигурация WLC для аутентификации RADIUS через внешний сервер RADIUS

Необходимо настроить WLC для переадресации на внешний сервер RADIUS учетные данные пользователя. Внешний сервер RADIUS проверяет учетные данные пользователя и предоставляет доступ беспроводным клиентам.

Чтобы настроить WLC для внешнего сервера RADIUS, выполните следующие действия:

1. **Выберите Security и RADIUS Authentication в контроллере GUI, чтобы открыть страницу**

RADIUS Authentication Servers. Чтобы определить сервер RADIUS, нажмите New.

2. Определите параметры сервера RADIUS в RADIUS Authentication Servers > New page. В их числе: RADIUS Server IP Address, Shared Secret, Port Number и Server Status.Флажки Network User и Management определяют, просит ли основанная на RADIUS аутентификация управление WLC и пользователей сети. Данный пример использует Cisco Secure ACS в качестве сервера RADIUS с IP-адресом 10.77.244.196.
3. Сервер RADIUS может теперь использоваться WLC для аутентификации. Можно найти сервер RADIUS перечисленным при выборе **Security> Radius> Authentication**.RFC 3576 поддерживается на сервере RADIUS регистратора доступа Cisco CNS (CAR), исключая сервер Cisco Secure ACS версии 4.0 и более ранних версий.Чтобы аутентифицировать пользователей, можно также использовать функцию локального сервера RADIUS. Локальный сервер RADIUS был введен в коде версии 4.1.171.0. У контроллеров WLC, использующих предыдущие версии, нет функции локального сервера RADIUS. Локальный EAP – это способ аутентификации, который позволяет пользователям и беспроводным клиентам выполнять аутентификацию локально. Он разработан для работы в удаленных офисах, которым необходимо поддерживать подключение к беспроводным клиентам, если нарушена связь с внутренней системой, или внешний сервер аутентификации перестал работать. Чтобы выполнить аутентификацию пользователя, локальный EAP извлекает учетные данные пользователя из локальной базы данных пользователя или внутренней базы данных LDAP. Локальный EAP поддерживает LEAP, EAP-FAST с концентратором доступа PPTP (PAC), EAP-FAST с сертификатами и аутентификацию EAP-TLS между контроллером и беспроводным клиентом.Локальный EAP разработан в качестве резервной системы аутентификации. Если серверы RADIUS настроены на контроллере, данный контроллер сначала выполняет попытки аутентификации беспроводных пользователей с помощью серверов RADIUS. Локальный EAP выполняет попытку аутентифицировать пользователей, только если серверы RADIUS не обнаружены, устарели или не настроены.См. Локальную EAP-аутентификацию на Контроллере беспроводной локальной сети с EAP-FAST и Примером конфигурации Сервера LDAP для получения дополнительной информации о том, как настроить Локальный EAP на Контроллерах беспроводной локальной сети.

Настройка параметров WLAN

Далее настройте WLAN, которую клиенты используют для подключения к беспроводной сети. Настроив основные параметры для WLC, можно настроить SSID для WLAN. Можно использовать данный SSID для WLAN или создать новый SSID. В данном примере вы создаете новый SSID.

Примечание: На контроллере можно настраивать до 16 сетей WLAN. С помощью решения Cisco WLAN можно контролировать до 16 сетей WLAN для "облегченных" AP. Каждому WLAN можно назначить уникальная политика безопасности. С помощью "облегченных" AP транслируются все активные идентификаторы SSID WLAN решения Cisco WLAN и включаются политики, определенные для каждой WLAN.

Чтобы настроить новую WLAN и связанные параметры, выполните следующие действия:

1. **Выберите WLANs в GUI контроллера, чтобы открыть страницу WLANs.**На данной странице отобразится список сетей WLAN на данном контроллере.

2. **Чтобы создать новую WLAN, выберите New.** Введите Имя профиля и SSID WLAN для WLAN и нажмите **Apply**. В данном примере SSID – Cisco.
3. После создания новой WLAN появляется страница WLAN > Edit для новой WLAN. На этой странице можно определить различные параметры, определенные для этого WLAN, который включает Общую политику, Политику безопасности, политики QoS и другие Усовершенствованные параметры.Выберите соответствующий Интерфейс из раскрывающегося меню. Другие параметры могут быть изменены на основе требования сети WLAN.Установите флажок **Статуса** в соответствии с Общей политикой для включения WLAN.
4. Нажмите **Вкладку Безопасность** и выберите **Layer 2 Security**. От раскрывающегося меню безопасности уровня 2 выберите **802.1x**. В параметрах 802.1x выберите размер Ключа WEP. Данный пример использует 128-разрядный Ключ WEP, который является the104-разрядным Ключом WEP плюс 24-разрядный Вектор инициализации.
5. Выберите вкладку **AAA Servers**. От Серверов проверки подлинности (RADIUS) раскрывающееся меню выберите соответствующий сервер RADIUS. Этот сервер используется для аутентификации беспроводных клиентов.
6. **Нажмите Apply, чтобы сохранить данную конфигурацию.**

Конфигурация Cisco Secure ACS в качестве сервера RADIUS и создание базы данных пользователей для аутентификации клиентов

Чтобы создать базу данных пользователей и включить аутентификацию EAP в Cisco Secure ACS, выполните следующие действия:

1. **В ACS GUI выберите User Setup, введите имя пользователя и нажмите Add/Edit. В данном примере пользователь – ABC.**
2. Когда откроется страница User Setup, определите все параметры, которые относятся к данному пользователю. В данном примере параметры Username, Password и Supplementary User Information настроены, так как они необходимы только для аутентификации EAP.**Щелкните Submit и повторите то же действие, чтобы добавить пользователей в базу данных.** По умолчанию всех пользователей группируют под группой по умолчанию и назначают та же политика, как определено для группы. Дополнительные сведения о назначении определенных пользователей различным группам см. в разделе Управление группой пользователей документа Руководство пользователя по Cisco Secure ACS сервера Windows версии 3.2.
3. На сервере ACS определите контроллер в качестве клиента AAA. **В ACS GUI нажмите Network Configuration.**Когда страница Network Configuration появится, определите название WLC, IP-адреса, общего секретного ключа и метода аутентификации (RADIUS Airespace Cisco). Сведения о серверах аутентификации, отличной от ACS, см. в документации от производителя.**Примечание:** Общий секретный ключ на WLC и сервере ACS должны совпадать. При вводе общего секретного ключа необходимо учитывать регистр.
4. **Выберите System Configuration и Global Authentication Setup, чтобы убедиться, что сервер аутентификации настроен для выполнения необходимого способа аутентификации EAP.** В параметрах конфигурации EAP выберите соответствующий способ аутентификации EAP. В данном примере используется аутентификация LEAP. **По завершении нажмите Submit.**

Настройте клиента

Клиент должен также быть настроен для соответствующего типа EAP. Клиент предлагает тип EAP серверу во время процесса согласования EAP. Если поддержки сервера, что тип EAP, это подтверждает тип EAP. Если тип EAP не поддерживается, он передает Отрицательное подтверждение, и клиент снова выполняет согласование с другим методом EAP. Этот процесс продолжается, пока о поддерживаемом типе EAP не выполняют согласование. Данный пример использует LEAP в качестве типа EAP.

Выполните эти шаги для настройки LEAP на клиенте со служебной программой рабочего стола Aironet.

1. Двойное нажатие на значке **Утилиты Aironet** для открытия его.
2. Нажмите вкладку **Profile Management**.
3. Щелкните по профилю и выберите **Modify**.
4. Под Вкладкой Общие выберите *Profile Name*. Введите **SSID** WLAN.**Примечание:** SSID учитывает регистр, и он должен точно совпасть с SSID, настроенным на WLC.
5. Под **Вкладкой Безопасность** выберите *802.1x*. Выберите тип EAP в качестве **LEAP** и нажмите **Configure**.
6. Выберите **Use Temporary Username and Password**, который побуждает вас вводить пользователя cerdentials каждый раз перезагрузки компьютера.Проверьте одну из этих трех опций, данных здесь. Данный пример использует **Автоматически Быстрый для Имени пользователя и пароля**, которое требует, чтобы вы ввели учетные данные *Пользователя LEAP* в дополнение к *Имени пользователя в Windows и Паролю*, перед входом в систему к окнам.Проверьте флажок **Always Resume the Secure Session** наверху окна, если вы хотите, чтобы соискатель LEAP всегда попытался возобновить предыдущий сеанс без потребности побудить вас повторно вводить свои учетные данные каждый раз, когда клиентский адаптер перемещается и повторно связывается к сети.**Примечание:** См. Настройку раздел Клиентского адаптера документа Cisco Aironet 802.11a/b/g Клиентские адаптеры беспроводной сети (CB21AG и PI21AG) Руководство по установке и конфигурированию для получения дополнительной информации другие опции.
7. Под **Вкладкой Дополнительно** можно настроить Преамбулу, Расширение Aironet и другие опции 802.11, такие как Питание, Частота и т.д.
8. **Нажмите кнопку ОК.** Клиент теперь пытается связаться с настроенными параметрами.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Попытайтесь связать беспроводного клиента с "облегченной" AP с помощью аутентификации LEAP, чтобы убедиться в исправной работе конфигурации.

Примечание: В данном документе предполагается, что профиль клиента настроен для аутентификации LEAP. Дополнительные сведения о конфигурации беспроводной сетевой карты 802.11 a/b/g для аутентификации LEAP см. в разделе Использование аутентификации EAP.

Если профиль беспроводного клиента активирован, пользователь получит запрос

предоставить имя пользователя/пароль для аутентификации LEAP. Например:

"Облегченная" AP, а потом и WLC, поступают в учетные данные пользователя на сервере RADIUS (Cisco Secure ACS) для проверки учетных данных. Сервер RADIUS сравнивает данные с базой данных пользователя и предоставляет доступ к беспроводному клиенту (если учетные данные пользователя являются допустимыми) для проверки учетных данных пользователя. В отчете Passed Authentication на сервере ACS отображаются сведения о том, что клиент прошел аутентификацию RADIUS. Например:

При успешном завершении аутентификации клиент подключится к беспроводной LAN.

Это может также быть проверено под вкладкой **Monitor** GUI WLC. Выберите **Monitor> Clients** и проверка для MAC-адреса клиента.

Устранение неполадок

Чтобы устранить неполадки данной конфигурации, выполните следующие действия:

1. **Чтобы проверить регистрацию AP в WLC используйте команду debug lwapp events enable.**
2. Проверьте получение и подтверждение сервером RADIUS запроса на аутентификацию от беспроводного клиента. Проверьте IP-АДРЕС NAS - дата и время, чтобы проверить, смог ли WLC достигнуть сервера RADIUS.Чтобы выполнить данное действие, проверьте отчеты Passed Authentications и Failed Attempts на сервере ACS. Данные отчеты доступны в Reports и Activities на сервере. Ниже приведен пример ошибки аутентификации сервера RADIUS:**Примечание:** Сведения об устранении неполадок и получении данных об отладке в Cisco Secure ACS см. в разделе Получение номера версии Cisco Secure ACS для Windows и сведений об отладке AAA.
3. **Чтобы устранить неполадки аутентификации AAA, можно также использовать команды debug:debug aaa all enable – настраивает отладку сообщений AAA.debug dot1x packet enable – активирует отладку всех пакетов dot1x.**Вот пример выходных данных от **команды debug 802.1x aaa enable**:`(Cisco Controller) >debug dot1x aaa enable *Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8, id=2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43 .....ABC *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f ....B:... *Sep 23 15:15:43.799: 00000010: 41 42 43 ABC *Sep 23 15:15:43.799:`

00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed ...#......[2.e.. *Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13 ..O...5..k..WP.. *Sep 23 15:15:43.904: 00000020: 41 42 43 ABC *Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 **AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05** *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907: 00000000: 03 03 00 04 .... *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1, length=19, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae ....)#...l.. *Sep 23 15:15:43.915: 00000010: 41 42 43 ABC *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **AAA response 'Success'** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **Returning AAA response** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 **AAA Message 'Success' received for mobile 00:40:96:ac:dd:05** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8, vendorId 0, valueLen 4 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79, vendorId 0, valueLen 35 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2, length=35,id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c ...#.....f,j...L *Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6 ..i.....).V...`. *Sep 23 15:15:43.918: 00000020: 41 42 43 ABC *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1, vendorId 9, valueLen 16 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25, vendorId 0, valueLen 21 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80, vendorId 0, valueLen 16 Примечание: Некоторые линии в выходных данных отладки были обернуты из-за пространственных ограничений.

4. Просмотрите журнал регистрации на WLC, чтобы проверить получение учетных данных сервером RADIUS. Нажмите Monitor для проверки журналов от GUI WLC. Из меню левой стороны нажмите Statistics и сервер RADIUS щелчка из списка опций.Это важно, так как в некоторых случаях сервер RADIUS не получает учетные данные

пользователя, если конфигурация сервера RADIUS на WLC является неверной.Если параметры RADIUS настроены неверно, то журнал регистрации на WLC выглядит следующим образом:**Можно использовать совокупность команд show wlan summary, чтобы определить, какие из сетей WLAN используют аутентификацию сервера RADIUS. Затем можно просмотреть выходные данные команды show client summary, чтобы увидеть, какие MAC-адреса (клиенты) успешно аутентифицированы в сетях RADIUS WLAN.** Также можно сопоставить эту информацию с журналами регистрации успешных и неудачных попыток аутентификации Cisco Secure ACS.

Советы по поиску и устранению неполадок

- , RADIUS active, standby disabled.
- Используйте **команду ping**, чтобы проверить, достижим ли сервер RADIUS от WLC.
- Необходимо, чтобы сервер RADIUS был выбран в раскрывающемся меню WLAN (SSID).
- Во время использования WPA необходимо установить последнее исправление Microsft WPA для Windows XP SP2. Также необходимо обновить драйвер для запрашивающего устройства клиента в соответствии с последней версией.
- Если используется PEAP, например сертификаты с XP, SP2, в котором карты управляются с помощью утилиты Microsoft wireless-0, необходимо получить исправление KB885453 от Microsoft.**Если необходимо использовать нулевую конфигурацию Windows/запрашивающее устройство клиента, отключите параметр Enable Fast Reconnect. Для этого выберите Wireless Network Connection Properties > Wireless Networks > Preferred networks. Потом выберите SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect.** Далее можно найти нужный параметр для включения или отключения в конце окна.
- При наличии карт Intel 2200 или 2915 сведения об известных связанных с ними проблемах см. на веб-сайте Intel:Intel® PRO/Беспроводное сетевое подключение 2200BGIntel® PRO/Беспроводное сетевое подключение 2915ABGЗагрузите текущие драйверы Intel, чтобы избежать проблем. Можно загрузить драйверы Intel с сайта http://downloadcenter.intel.com/
- aggressive failover WLC, AAA "not responding" . Но это действие не является необходимым, так как сервер AAA, возможно, не отвечает только данному конкретному клиенту, если установлен режим silent discard. Он может отвечать другим действительным клиентам (с действительными сертификатами). WLC AAA not responding not functional.Чтобы избежать этого, отключите функцию aggressive failover. **Для этого введите команду config radius aggressive-failover disable из GUI контроллера.** Если эта функция отключена, то контроллер будет переключаться на следующий сервер AAA, если три клиента подряд не смогут получить ответ от сервера RADIUS.

Управление таймерами EAP

Во время аутентификации 802.1x пользователь мог бы видеть сообщение об ошибках `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: MAX EAPOL-Key M1 retransmissions reached for mobile xx:xx:xx:xx:xx`.

Это сообщения об ошибках указывают, что клиент вовремя не ответил на контроллер во время WPA (802.1x) согласование ключа. Контроллер устанавливает таймер для ответа во время ключевого согласования. Как правило, когда вы видите это сообщение, это происходит из-за проблемы с соискателем. Удостоверьтесь, что вы выполняете последние

версии Драйверов клиента и микропрограммного обеспечения. На WLC существует несколько таймеров EAP, которыми можно манипулировать для помощи с аутентификацией клиента. Эти таймеры EAP включают:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Прежде чем можно будет манипулировать этими значениями, необходимо понять то, что они делают, и как изменение их повлияет на сеть:

- **Таймаут ИДЕНТИФИКАЦИОННОГО ЗАПРОСА EAP:**Этот таймер влияет, сколько времени вы ждете между Идентификационными Запросами EAP. По умолчанию это - одна секунда (4.1 и ниже) и 30 секунд (4.2 и больше). Причина для этого изменения состояла в том, потому что некоторым клиентам, рука helds, телефоны, сканеры и т.д., пришлось, нелегко ответив достаточно быстро. Устройства как портативные ПК, обычно не требуйте манипулирования этими значениями. Доступное значение от 1 до 120.Так, что происходит, когда этот атрибут установлен в значение 30? Когда клиент сначала соединяется, это передает EAPOL, Запускаются к сети, и WLC передает вниз пакет EAP, запрашивая Личность пользователя или машины. Если WLC не получает Идентификационный Ответ, он отправляет другой Идентификационный Запрос спустя 30 секунд после первого. Когда клиент перемещается, это происходит на первоначальном подключении, и.Когда мы увеличиваем этот таймер, что происходит? Если все хорошо, нет никакого влияния. Однако, если существует проблема в сети (включая клиентов выдал, проблемы AP или проблемы RF), это может вызвать задержки сетевого подключения. Например, при установке таймера в максимальное значение 120 секунд WLC ждет 2 минуты между Идентификационными Запросами. Если клиент бродит, и Ответ не получен WLC, то мы создали, как минимум, простой two-minute для этого клиента.Рекомендации для этого таймера равняются *5*. В это время нет никакой причины разместить этот таймер в его максимальном значении.
- **Максимальные числа попыток ИДЕНТИФИКАЦИОННОГО ЗАПРОСА EAP:**Значение Максимальных чисел попыток является числом раз, WLC отправит Идентификационный Запрос клиенту, прежде, чем удалить его запись из MSCB. Однажды Максимальные числа попыток достигнут, WLC передает кадр de-аутентификации клиенту, вынуждая их перезапустить процесс EAP. Доступное значение равняется 1 - 20. Затем, мы посмотрим на это более подробно.Максимальные числа попыток работают с Идентификационным Таймаутом. Если вам установили ваш Идентификационный Таймаут в 120 и ваши Максимальные числа попыток к 20, сколько времени делает он берет 2400 (или 120 * 20). Это означает, что потребовалось бы 40 минут для клиента, чтобы быть удаленным и запустить процесс EAP снова. Если вы установите Идентификационный Таймаут в 5 со значением Максимальных чисел попыток 12, то он возьмет 60 (или 5 * 12). В отличие от предыдущего примера, существует одна минута, пока клиент не удален и должен запустить EAP.Рекомендации для Максимальных чисел попыток равняются *12*.
- **Ключевой для EAPOL таймаут:**Для Ключевого для EAPOL Значения таймаута по умолчанию составляет 1 секунду или 1000 миллисекунд. Это означает, что, когда ключами EAPOL обмениваются между AP и клиентом, AP передаст ключ и дождется к 1 секунде по умолчанию для клиента для ответа. После ожидания значения заданного

времени AP повторно передаст ключ снова. Можно использовать **config advanced eap eapol-key-timeout** команда *<time>* для изменения этой установки. В то время как коды до 6.0 обеспечивают значения между 1 и 5 секундами, доступные значения в 6.0 между 200 и 5000 миллисекунд. Следует иметь в виду, что, если у вас есть клиент, который не отвечает на ключевую попытку, расширяя таймеры, может дать им немного больше времени для ответа. Однако это могло также продлить время, которое это берет для WLC/AP к deauthenticate клиента для целого процесса 802.1x для начала снова.

- **Ключевые для EAPOL максимальные числа попыток:**Для Ключевого для EAPOL значения Максимальных чисел попыток по умолчанию равняется 2. Это означает, что мы повторим исходную ключевую попытку клиенту дважды. Эта установка может быть изменена с помощью **config advanced eap eapol-key-retries** команда *<retries>*. Доступные значения между 0 и 4 повторными попытками. Если клиент не отвечает на начальную ключевую попытку, Использование значения по умолчанию для Ключевого для EAPOL Таймаута (т.е. 1 секунда) и значения по умолчанию для Ключевой для EAPOL Повторной попытки (2) процесс пошел бы следующим образом:AP передает ключевую попытку клиенту.Это ждет одна секунда ответа.Если нет никакого ответа, то первая Ключевая для EAPOL Повторная попытка передается.Это ждет одна секунда ответа.Если нет никакого ответа, то вторая Ключевая для EAPOL Повторная попытка передается.Если нет все еще никакого ответа от клиента, и значение повтора встречено, то клиент является deauthenticated. Снова, как с Ключевым для EAPOL Таймаутом, расширяя Ключевое для EAPOL значение повтора, при некоторых обстоятельствах, могло быть выгодным. Однако установка его к максимуму может снова быть вредной, поскольку было бы продлено deauthenticate сообщение.

Извлечение файла пакета с сервера ACS RADIUS для устранения неполадок

При использовании ACS в качестве внешнего сервера RADIUS, этот раздел может использоваться для устранения проблем конфигурации. Package.cab – это файл Zip, в котором содержатся все необходимые файлы для устранения неполадок в ACS. Можно использовать утилиту CSSupport.exe, чтобы создать package.cab, или можно объединить данные файлы вручную.

Дополнительные сведения о создании и извлечении файла пакета из WCS см. в разделе Создание файла package.cab документа Получение номера версии Cisco Secure ACS для Windows и сведений об отладке AAA.

Дополнительные сведения

- Пример конфигурации при отказе контроллера WLAN для "облегченных" точек доступа
- Обновление программного обеспечения контроллера беспроводной локальной сети
- Справочник по командам контроллера беспроводной локальной сети Cisco
- Cisco Systems – техническая поддержка и документация