Подсказки по устранению неполадок инструмента обновления LWAPP

Содержание

Введение

В данном документе обсуждаются некоторые из основных проблем, которые могут возникнуть при использовании средства обновления при обновлении автономных точек доступа для использования облегченного режима. В нем также содержатся рекомендации по решению этих проблем.

Предварительные условия

Требования

До начала обновления на точке доступа необходимо установить программное обеспечение Cisco IOS® версии 12.3(7)JA или выше.

В контроллерах Cisco должно быть установлено программное обеспечение версии не ниже 3.1.

В системе контроля беспроводной сети Cisco (если она используется) должно использоваться ПО версии не ниже 3.1.

Утилита модернизации поддерживается на платформах Windows 2000 и Windows XP. Необходимо использовать одну из этих версий операционной системы Windows.

Используемые компоненты

Сведения в этом документе основываются на этих точках доступа и Контроллерах беспроводной локальной сети.

AP, которые поддерживают эту миграцию:

- Все 1121G точки доступа
- Все точки доступа 1130AG
- Все точки доступа 1240 AG
- Все точки доступа серии 1250
- Для всех основанных на IOS модульных платформ точек доступа серий 1200 (модернизация программного обеспечения 1200/1220 Cisco IOS, точки доступа 1210 и 1230) эта возможность зависит от наличия радиомодулей:–если поддерживается 802.11G, MP21G и MP31G–если поддерживается 802.11G, RM21A и RM22AТочки доступа серий 1200 можно модернизировать при наличии любой комбинации поддерживаемых радиомодулей: только G, только A или и G, и A. Для точки доступа, которая содержит двойные радио, если одно из этих двух радио является поддерживаемым LWAPP радио, инструмент обновления все еще выполняет обновление. Программное средство добавляет предупреждающее сообщение к подробному журналу, который указывает, какое радио является неподдерживаемым.
- Все точки доступа 1310 AG
- Карта беспроводного мобильного интерфейса (WMIC) Cisco C3201**Примечание:** Второе поколение 802.11a радио содержит два номера изделия.

Точки доступа должны выполнить Cisco IOS Release 12.3 (7) JA или позже прежде чем можно будет выполнить обновление.

Для Cisco C3201WMIC точки доступа должны выполнить Cisco IOS Release 12.3 (8) JK или позже прежде чем можно будет выполнить обновление.

Модернизация автономных точек доступа до упрощенного режима поддерживается следующими контроллерами Cisco Wireless LAN:

- контроллеры серий 2000
- Контроллеры серии 2100
- контроллеры серий 4400
- Модули беспроводных служб (Cisco WiSM) для коммутаторов серии Cisco Catalyst 6500
- Сетевые модули контроллеров в маршрутизаторах с интегрированными службами серии Cisco 28/37/38xx
- Коммутаторы с интегрированным контроллером беспроводной сети Catalyst 3750G

В контроллерах Cisco должно быть установлено программное обеспечение версии не ниже 3.1.

Требуется версия Cisco Wireless Control System (WCS) не ниже 3.1. Утилита модернизации поддерживается на платформах Windows 2000 и Windows XP.

Можно загрузить последнюю версию утилиты обновления от страницы Cisco Software Downloads.

Условные обозначения

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

Обзор процесса модернизации

Пользователь запускает утилиту модернизации, которая принимает входной файл, содержащий список точек доступа и их идентификационных данных. Сервисные telnet к точкам доступа во входном файле серия Команд Cisco IOS для подготовки точки доступа к обновлению, которое включает команды для создания подписанных сертификатов. Также отправляется команда контроллеру запрограммировать устройство для разрешения авторизации определенных точек доступа с помощью самостоятельно подписанных сертификатов. Это тогда загружает программное обеспечение Cisco IOS версии 12.3 (11) JX1 на точку доступа так, чтобы это могло присоединиться к контроллеру. После того, как точка доступа присоединяется к контроллеру, она загружает завершенную версию Cisco IOS от него. Утилита модернизации создает выходной файл, включающий список точек доступа и соответствующих значений хэша ключей для самостоятельно подписанных сертификатов. Этот список можно импортировать в программное обеспечение управления WCS. Программа WCS затем может отправить эту информацию другим контроллерам в сети.

См. дополнительные сведения в разделе Процедура обновления в документе Обновление автономных точек доступа Cisco Aironet до облегченного режима.

Средство обновления – основные действия

Это средство обновления используется для обновления автономных точек доступа до облегченного режима при условии, что точка доступа совместима с таким обновлением. Инструмент модернизации выполняет основные задачи, необходимые для модернизации из автономного до упрощенного режима. Выполняются следующие действия:

- Проверка основных условий—Проверяет, поддерживается ли точка доступа, используется ли на ней программное обеспечение минимальной версии и поддерживается ли тип радиоканала.
- Удостоверьтесь, что AP настроен как Root.
- Подготовка автономной точки доступа для обновления—Добавляет конфигурацию инфраструктуры открытого ключа (PKI) и иерархию сертификатов, чтобы выполнить аутентификацию точки доступа для контроллеров Cisco и сформировать для точки доступа самостоятельно подписанные сертификаты (сертификаты SSC). Если на точке доступа имеются установленные производителем сертификаты (сертификат MIC), то

сертификаты SSC не используются.
- Загружает образ обновления из автономного в облегченный режим (например, 12.3(11)JX1 или 12.3(7)JX.), который позволяет установить беспроводное соединение между точкой доступа и контроллером. После успешной загрузки происходит перезагрузка точки доступа.
- Генерирует файл выходных данных, содержащий MAC-адреса точки доступа, тип сертификата и безопасный хеш-ключ, а затем автоматически обновляет контроллер. Выходной файл можно импортировать в программу WCS и экспортировать в другие контроллеры.

Важные примечания

Прежде чем вы будете использовать эту утилиту, будете рассматривать эти важные замечания:

- Точки доступа, преобразованные с этим программным средством, не соединяются с 40xx, 41xx, или 3500 контроллеров.
- Нельзя выполнить модернизацию точек доступа только с радиомодулями 802.11b или с радиомодулями 802.11a первого поколения.
- Если вы хотите сохранить статический IP - адрес, маску подсети, имя хоста и шлюз по умолчанию точек доступа после преобразования и перезагрузки, необходимо загрузить один из этих автономных образов на точках доступа перед вами тайный точки доступа к LWAPP:12.3 (7) JA12.3 (7) JA112.3 (7) JA212.3 (7) JA312.3 (7) JA412.3 (8) JA12.3 (8) JA112.3 (8) JA212.3 (8) JEA12.3 (8) JEA112.3 (8) JEA212.3 (8) JEB12.3 (8) JEB112.4 (3-граммовый) JA12.4 (3-граммовый) JA1
- При обновлении точек доступа к LWAPP от одного из этих автономных образов преобразованные точки доступа не сохраняют свой статический IP - адрес, маску подсети, имя хоста и шлюз по умолчанию:12.3 (11) JA12.3 (11) JA112.3 (11) JA212.3 (11) JA3
- Когда процесс обновления завершен, инструмент обновления LWAPP не освобождает ресурсы памяти операционной системы Windows. Ресурсы памяти освобождены только после выхода из инструмента обновления. При обновлении нескольких групп точек доступа необходимо выйти из программного средства промежуточные группы для выпуска ресурсов памяти. Если вы не выходите из программного средства промежуточные группы, производительность станции обновления быстро ухудшается из-за потребления избыточного использования памяти.

Типы сертификатов

Существует два вида точек доступа:

- Точки доступа с сертификатом MIC
- Точки доступа, для которых необходим сертификат SSC

Заводские сертификаты обозначаются термином MIC (сокращение от Manufacturing Installed Certificate — сертификат производителя). Точки доступа Cisco, поставленные до 18 июля 2005 г., не имеют сертификата MIC, поэтому создают собственные сертификаты при модернизации до упрощенного режима. Контроллеры запрограммированы для работы с самостоятельно подписанными сертификатами для аутентификации определенных точек

доступа.

Необходимо рассматривать точки доступа Cisco Aironet MIC, использующие протокол Lightweight Access Point Protocol (например, точки доступа Aironet 1000) и устранять неисправности соответствующим образом. Другими словами, проверьте подсоединение по протоколу IP, произведите отладку блока состояний LWAPP, а затем проверьте шифрование.

Журнал средства обновления содержит сведения о том, использует ли точка доступа протокол MIC или SSC. Ниже приведен пример подробного журнала средства обновления:

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO 172.16.1.60 MIC is already configured in the AP 2006/08/21 16:59:07
INFO 172.16.1.60 Hardware is PowerPC405GP Ethernet, address is 0015.63e5.0c7e (bia
0015.63e5.0c7e) 2006/08/21 16:59:08 INFO 172.16.1.60 Inside Shutdown function 2006/08/21
16:59:10 INFO 172.16.1.60 Shutdown the Dot11Radio1 2006/08/21 16:59:11 INFO 172.16.1.60 Shutdown
the Dot11Radio0 2006/08/21 16:59:12 INFO 172.16.1.60 Updating the AP with Current System Time
2006/08/21 16:59:13 INFO 172.16.1.60 Saving the configuration into memory 2006/08/21 16:59:13
INFO 172.16.1.60 Getting AP Name 2006/08/21 16:59:58 INFO 172.16.1.60 Successfully Loaded the
LWAPP Recovery Image on to the AP 2006/08/21 16:59:58 INFO 172.16.1.60 Executing Write Erase
Command 2006/08/21 17:00:04 INFO 172.16.1.60 Flash contents are logged 2006/08/21 17:00:06 INFO
172.16.1.60 Environmental Variables are logged 2006/08/21 17:00:06 INFO 172.16.1.60 Reloading
the AP 2006/08/21 17:00:08 INFO 172.16.1.60 Successfully executed the Reload command
```

В этом журнале в выделенной строке указано, что на точке доступа установлен сертификат MIC. См. дополнительные сведения о сертификатах и процессе обновления в разделе Обзор процедуры обновления в документе Обновление автономных точек доступа Cisco Aironet до облегченного режима.

В случае если точки доступа используют сертификат SSC, на контроллере сертификат не создается. Средство обновления подает на точку доступа команду на генерацию пары ключей Rivest, Shamir и Adelman (RSA), используемой для подписи самостоятельно сгенерированного сертификата (сертификата SSC). Средство обновления добавляет запись к списку аутентфикации контроллера, в которой содержится MAC-адрес точки доступа и открытый хеш-ключ. Открытый хеш-ключ используется контроллером для проверки подписи SSC.

Если такая запись не была добавлена к контроллеру, проверьте файл CSV выходных данных. В нем должны быть записи для каждой точки доступа. Если такая запись найдена, импортируйте этот файл на контроллер. **При использовании интерфейса командной строки контроллера (с использованием команды config auth-list) или веб-коммутатора необходимо импортировать одни файл за раз.** При использовании системы контроля беспроводной сети можно импортировать весь файл CSV как шаблон.

Кроме того, проверьте регуляторный домен.

Примечание: Если у вас есть AP LAP, но вы хотите функциональность Cisco IOS, необходимо загрузить автономный Образ Cisco IOS на ней. С другой стороны, если вы имеете автономный AP и хотите преобразовать его в LWAPP, можно установить образ для восстановления LWAPP по автономному IOS.

Можно выполнить шаги для изменения образа AP с **командами archive download** CLI или

кнопкой MODE. См. Устранение проблем для получения дополнительной информации о том, как использовать повторную загрузку изображения кнопки РЕЖИМА, которая работает с автономным IOS или образом для восстановления, названным к имени файла использованной модели точки доступа по умолчанию.

Следующий раздел обсуждает некоторые обычно замечаемые проблемы в операции обновления и шагах для решения этих вопросов.

Проблема

Признак

Беспроводное соединение между точкой доступа и контроллером не устанавливается. В разделе Решения данного документа предложены причины в порядке уменьшения их вероятности.

Решения

Используйте этот раздел для решения проблемы.

Причина 1

Точка доступа не может обнаружить контроллер с использованием механизма обнаружения LWAPP или не может с ним соединиться.

Устранение неполадок

Выполните следующие действия:

1. **Введите в командной строке контроллера команду debug lwapp events enable.**Найдите последовательность ответных реакций (LWAPP discovery > discovery response > join request > join). Отсутствие ответной реакции на LWAPP discovery означает, что точка доступа не может найти или не находит контроллер.Ниже приведен пример успешного ответа от контроллера беспроводной локальной сети на попытку подсоединения, полученного на точке доступа, преобразованной для использования облегченного режима. **Команда debug lwapp events enable приводит к отображению следующих выходных данных:**Thu May 25 06:53:54 2006: **Received LWAPP DISCOVERY REQUEST from AP** 00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1' Thu May 25 06:53:54 2006: **Successful transmission of LWAPP Discovery-Response to AP** 00:15:63:e5:0c:7e on Port 1 Thu May 25 06:53:54 2006: **Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e** to 00:0b:85:33:84:a0 on port '1' Thu May 25 06:53:54 2006: **Successful transmission of LWAPP Discovery-Response to AP** 00:15:63:e5:0c:7e on Port 1 Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e to ff:ff:ff:ff:ff:ff on port '1' Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP 00:15:63:e5:0c:7e on Port 1 Thu May 25 06:54:05 2006: **Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e** to 00:0b:85:33:84:a0 on port '1' Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e is 1500, remote debug mode is 0 Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e (index 51)Switch IP: 172.16.1.11, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679, next hop MAC: 00:15:63:e5:0c:7e Thu May 25 06:54:05 2006: **Successfully transmission of LWAPP Join-Reply to AP** 00:15:63:e5:0c:7e .....

```
.........................................
..................................... // the debug output continues for full
registration process.
```

2. Проверьте подсоединение по протоколу IP между сетью точек доступа и контроллером. Если контроллер и точка доступа расположены в одной и той же подсети, убедитесь, что они соединены правильно. Если они расположены в разных подсетях, убедитесь, что между ними используется маршрутизатор, который обеспечивает правильную маршрутизацию между двумя подсетями.
3. Проверьте, правильно ли настроен механизм обнаружения.Если для обнаружения контроллера беспроводной локальной сети используется система доменных имен (DNS), убедитесь, что сервер DNS правильно настроен и сопоставляет домен CISCO-LWAPP-CONTROLLER.local-domain с IP-адресом контроллера. Следовательно, если точка доступа может определить имя, с нее на определенный IP-адрес отправляется сообщение о подсоединении по протоколу LWAPP.Если в качестве параметра обнаружения используется Option 43, убедитесь, что он на сервере DHCP он настроен правильно.См. дополнительные сведения о процедуре и последовательности обнаружения в разделе Регистрация "облегченной" точки доступа на контроллере беспроводной локальной сети.См. ПАРАМЕТР DHCP 43 для Легковесного Примера конфигурации точек доступа Cisco Aironet для получения дополнительной информации о том, как настроить параметр DHCP 43.**Примечание:** Помните что при преобразовании статически обращенных AP, единственный механизм обнаружения Уровня 3, который работы являются DNS, потому что статический адрес сохранен во время обновления.**На точке доступа можно ввести команду debug lwapp client events и команду debug ip udp для получения сведений, достаточных для определения того, что происходит.** Следует просмотреть последовательность пакетов протокола датаграмм пользователя (UDP), а именно:Переданную с IP-адреса точки доступа на IP-адрес интерфейса управления контроллером.Переданную с IP-адреса менеджера точки доступа контроллера на IP-адрес точки доступа.Набор пакетов, полученных с IP-адреса точки доступа на IP-адрес менеджера точки доступа.**Примечание:** В некоторых ситуациях может быть несколько контроллеров, и AP мог бы попытаться присоединиться к другому контроллеру на основе механизма состояний обнаружения LWAPP и алгоритмов. Такая ситуация может произойти из-за динамической балансировки нагрузки на точки доступа, которую контроллер выполняет по умолчанию. Эту ситуацию следует исследовать.**Примечание:** Это - пример выходных данных **команды debug ip udp**:

```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679),
dst=172.16.1.11(12222),
                     length=78
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223), length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679), length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=89
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
```

```
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=222
```

Разрешение

Выполните следующие действия:

1. Изучите руководство.
2. Исправьте ошибки инфраструктуры, чтобы она правильно поддерживала механизм обнаружения LWAPP.
3. Переместите точку доступа в ту же самую подсеть, в которой находится контроллер, чтобы он получил приоритет при установлении соединения.
4. *При необходимости введите в интерфейсе командной строки точки доступа команду lwapp ap controller ip address A.B.C.D, чтобы вручную задать IP контроллера:В этой команде A.B.C.D означает IP-адрес управляющего интерфейса контроллера беспроводной локальной сети.***Примечание:** Эта команда CLI может использоваться на AP, который никогда не регистрировался к контроллеру, или на AP, которому изменили его enable password по умолчанию, в то время как соединено с предыдущим контроллером. См. Сброс Конфигурации LWAPP на Легковесном AP (LAP) для получения дополнительной информации.

Причина 2

Время на контроллере находится вне пределов периода достоверности сертификата.

Устранение неполадок

Выполните следующие действия:

1. **Выполните команды debug lwapp errors enable и debug pm pki enable.Эти команды отладки отображают сведения о сообщениях о сертификации, которыми обмениваются точка доступа и контроллер беспроводной локальной сети.** Эти команды ясно выводят сообщение о том, что сертификат отклонен по причине того, что его дата не соответствует периоду достоверности.**Примечание:** Удостоверьтесь, что объяснили Согласованное текущее время (UTC) смещение.**Ниже приведены выходные данные команды debug pm pki enable на контроллере:**
```
Thu May 25 07:25:00 2006:
sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
.........................
.........................
.........................
.........................
```

```
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert validity
interval: make sure the controller time is set. Fri Apr 15 07:55:03 2005:
sshpmFreePublicKeyHandle: called with (nil)
```

В этих выходных данных обратите внимание на выделенные сведения. **Эти данные отчетливо свидетельствуют о том, что время на контроллере находится вне пределов периода достоверности сертификата точки доступа.** Следовательно, точка доступа не может быть зарегистрирована на контроллере. Сертификаты, установленные на точке доступа, имеют заданный период достоверности. Необходимо установить время на контроллере таким образом, чтобы оно соответствовало периоду достоверности сертификата точки доступа.

2. **Введите в интерфейсе командной строки точки доступа команду show crypto ca certificates, чтобы проверить, какой период действия сертификата установлен на точке доступа.**Ниже представлен пример:

```
AP0015.63e5.0c7e#show crypto ca certificates
..........................................  ..........................................
..........................................
..........................................  Certificate Status: Available Certificate
Serial Number: 4BC6DAB80000000517AF Certificate Usage: General Purpose Issuer: cn=Cisco
Manufacturing CA o=Cisco Systems Subject: Name: C1200-001563e50c7e ea=support@cisco.com
cn=C1200-001563e50c7e o=Cisco Systems l=San Jose st=California c=US CRL Distribution Point:
http://www.cisco.com/security/pki/crl/cmca.crl Validity Date: start date: 17:22:04 UTC Nov
30 2005 end date: 17:32:04 UTC Nov 30 2015 renew date: 00:00:00 UTC Jan 1 1970 Associated
Trustpoints: Cisco_IOS_MIC_cert ..................................
..................................  ..................................
```

Выходные данные приведены не полностью, поскольку в выходных данных этой команды могут присутствовать несколько сроков действия. **Необходимо обратить внимание только на срок действия, указанный как Associated Trustpoint: Cisco_IOS_MIC_cert и имеющий соответствующее имя точки доступа в поле имени (здесь, Name: C1200-001563e50c7e), как выделено в данном примере. Это и есть период действия сертификата, который необходимо принять во внимание.**

3. **Введите в интерфейсе командной строки контроллера команду show time, чтобы убедиться, что дата и время, установленные на контроллере, соответствуют этому сроку действия.**Если время на контроллере находится все периода достоверности сертификата, измените время на контроллере, чтобы оно попадало в этот период.

Разрешение

Выполните следующее действие:

Выберите в режиме графического пользовательского интерфейса контроллера Commands > Set Time или введите в интерфейсе командной строки контроллера команду config time, чтобы задать время на контроллере.

Причина 3

При использовании точек доступа с сертификатом SSC, политика точек доступа SSC отключена.

Устранение неполадок

В таких случаях на контроллере выводится сообщение об ошибке:

```
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                          :spamDecodeJoinReq failed
Wed Aug  9 17:20:21 2006  [ERROR] spam_crypto.c 1509: Unable to free public key for
                          AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                          valid certificate in CERTIFICATE_PAYLOAD from
                          AP 00:12:44:b3:e5:60.
Wed Aug 9 17:20:21 2006 [CRITICAL] sshpmPkiApi.c 1493: Not configured to accept Self-signed AP
cert
```

Выполните следующие действия:

Выполните одно из следующих двух действий:

- **Введите в интерфейсе командной строки команду show auth-list, чтобы убедиться, что контроллер настроен таким образом, чтобы обслуживать точки доступа с протоколами SSC.Ниже приведен пример выходных данных команды show auth-list:**`#show auth-list Authorize APs against AAA ..... disabled Allow APs with Self-signed Certificate (SSC) .... enabled Mac Addr Cert Type Key Hash ---------- --------- ---------- 00:09:12:2a:2b:2c SSC 12345678901234567890123456789012345678901234567890`
- **Выберите в графическом пользовательском интерфейсе Security (Безопасность) > AP Policies (Политики точек доступа).**

1. **Убедитесь, что установлен флажок Accept Self Signed Certificate (Принимать самоподписанные сертификаты).** Если флажок снят, установите его.
2. **Выберите в качестве типа сертификата SSC.**
3. **Добавьте точку доступа, ее mac-адрес и хеш-ключ к списку авторизации.Этот хеш-ключ выводится в данных команды debug pm pki enable .** [См. сведения о получении хеш-ключа в разделе Причина 4.]

Причина 4

Неверный открытый хеш-ключ SSC, или он отсутствует.

Устранение неполадок

Выполните следующие действия:

1. **Введите команду debug lwapp events enable.**Убедитесь, что точка доступа делает попытки подсоединиться.
2. **Введите команду show auth-list.**Эта команда отображает открытый хеш-ключ, хранящийся в контроллере.
3. **Введите команду debug pm pki enable.**Эта команда отображает реальный открытый хеш-ключ. Реальный открытый хеш-ключ должен соответствовать открытому хеш-ключу, хранящемуся в контроллере. При их расхождении возникает проблема. Ниже приведен пример вывода этого сообщения отладки:`(Cisco Controller) > debug pm pki enable Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon May 22`

```
06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Mon May
22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Mon May
22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122 300d0609 2a864886 f70d0101 Mon May
22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f00 3082010a 02820101 Mon
May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0 cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7 ad425fa7
face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b876251
43b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e 56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data
f81fa6ce cd1f400b b5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key
Data dde0648e c4d63259 774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
Key Data 0f463f9e c77b79ea 65d8639b d63aa0e3 Mon May 22 06:34:10 2006:
sshpmGetIssuerHandles: Key Data 7dd485db 251e2e07 9cd31041 b0734a55 Mon May 22 06:34:14
2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502d c54e75f2 6d28fc6b Mon May 22
06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e31 02d37140 7c9c865a Mon May
22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f 7a9bac00 d13ff85f Mon
May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb 88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bc bc1acc13
0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df
2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f
de2a6fe3 23311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data
1bfae1a8 eb076940 280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key
Data f7020301 0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This is the actual SSC key-hash value. Mon
May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote
debug mode is 0 Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization
failure for 00:0e:84:32:04:f0
```

Разрешение

Выполните следующие действия:

1. **Скопируйте открытый хеш-ключ из выходных данных команды debug pm pki enable и замените им открытый хеш-ключ в списке авторизации.**
2. *Введите команду config auth-list add ssc MAC-адрес_точки_доступа ключ_точки_доступа для добавления MAC-адреса и хеш-ключа точки доступа к списку аутентификации.*Ниже приведен пример выходных данных этой команды:`(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

Причина 5

На точке доступа поврежден сертификат или открытый ключ.

Устранение неполадок

Выполните следующее действие:

Выполните команды debug lwapp errors enable и debug pm pki enable.

Отображаются сообщения о повреждении сертификатов или ключей.

Разрешение

Для устранения этой проблемы выберите один из двух вариантов действия:

- Точка доступа MIC — затребуйте разрешение на гарантийный возврат (RMA).
- Точка доступа SSC—Понизьте версию программного обеспечения Cisco IOS до выпуска 12.3(7)JA.Выполните следующие шаги для понижения версии:

1. Используйте кнопку сброса.
2. Очистите настройки контроллера.
3. Повторно выполните обновление.

Причина 6

Возможно, контроллер работает в режиме уровня 2.

Устранение неполадок

Выполните следующее действие:

Проверьте режим работы контроллера.

Преобразованные точки доступа поддерживают только механизмы обнаружения уровня 3.
Преобразованные точки доступа не поддерживают механизмы обнаружения уровня 2.

Разрешение

Выполните следующие действия:

1. Установите на контроллере беспроводной локальной сети режим уровня 3.
2. Выполните перезагрузку и присвойте интерфейсу менеджера точки доступа IP-адрес в той же подсети, где расположен управляющий интерфейс.При наличии сервисного порта (например, сервисного порта в модели 4402 или 4404) необходимо использовать его в суперсети, отличной от той, где расположен менеджер точки доступа и управляющие интерфейсы.

Причина 7

Во время процесса обновления отображается следующее сообщение:

```
FAILED   Unable to Load  the LWAPP Recovery Image on to the AP
```

Устранение неполадок

Для устранения этой ошибки выполните следующие действия:

1. Убедитесь, что сервер TFTP настроен правильно.При использовании средства обновления, встроенного в сервер TFTP, обычно причиной ошибки является персональный брандмауэр, блокирующий входящий TFTP.
2. Убедитесь, что для обновления используется правильный образ.Обновление до облегченного режима требует использовать специальный образ и не выполняется с

обычными образами обновления.

Причина 8

После преобразования на точке доступа отображается следующее сообщение об ошибке:

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_
                     certs no certs in the SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
                     Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

Точка доступа перезагружается через 30 секунд, и процесс начинается сначала.

Разрешение

Выполните следующее действие:

Используется точка доступа SSC. После преобразования в точку доступа LWAPP добавьте SSC и его MAC-адрес в список аутентификации точки доступа на контроллере.

Советы устранения неполадок

Когда вы обновляете от автономного до режима LWAPP, эти советы могут использоваться:

- Если NVRAM не очищен, когда контроллер пытается записать в него после того, как преобразование, вызваны проблемы. Cisco рекомендует очистить конфигурацию перед преобразованием AP в LWAPP. Для очистки конфигурации:От GUI IOS — Переходят **к Системному программному обеспечению> Конфигурация системы> Сброс к Настройкам по умолчанию** или **Сброс к Настройкам по умолчанию Кроме IP**.От CLI — Проблема **write erase** и команды **повторной загрузки** в CLI и не позволяют конфигурации быть сохраненной, когда предложено.Это также делает текстовый файл AP, которые будут преобразованы Инструментом обновления, более простым создать, поскольку записи становятся <ip address>, Cisco, Cisco, Cisco.
- Cisco рекомендует использовать tftp32. Можно загрузить последний сервер TFTPD в http://tftpd32.jounin.net/.
- Если межсетевой экран или список контроля доступа включены во время процесса обновления, инструмент обновления может стать неспособным скопировать файл, который содержит переменные окружения от рабочей станции до AP.Если межсетевой экран или список контроля доступа блокируют операцию копирования, и вы выбираете опцию Use Upgrade Tool TFTP Server, вы не можете продолжить обновление, потому что программное средство не может обновить переменные окружения и загрузку изображения к сбоям AP.
- Проверьте дважды образ, к которому вы пытаетесь обновить. Обновление от IOS до образов LWAPP отличается от обычных Образов IOS.В соответствии с Моими Документами/Моим компьютером-> Программные средства-> Параметры папки, удостоверьтесь, что вы сняли флажок **со Скрыть расширениями файла для известного**

флажка **типов файла**.
- Всегда удостоверяйтесь, что использовали последний доступный Образ для восстановления Инструмента обновления и Обновления. Последние версии доступны в Разделе Wireless Software Center.
- AP не может загрузить графический файл **.tar**. Это - архив, подобный файлам архива zip. Необходимо разъединить файл **.tar** во флэш-память AP с **командой archive download** или иначе вытащить образ загрузки из файла TAR, сначала тогда помещает образ загрузки во флэш-память AP.

Дополнительные сведения

- Модернизация автономных точек доступа Cisco Aironet до упрощенного режима
- Сброс конфигурации LWAPP на Lightweight AP (LAP)
- Пример конфигурации DHCP OPTION 43 для облегченных точек доступа Cisco
- Как восстановиться, хэш выключают точку доступа и импортируют его на контроллер
- Может Автономная точка доступа Cisco Aironet быть преобразованной в Протокол LWAPP с помощью CLI
- Cisco Systems – техническая поддержка и документация