Устранение неполадки: облегченная точка доступа не соединяется с контроллером беспроводной LAN

Содержание

Введение

В настоящем документе представлен краткий обзор процесса обнаружения и присоединения для контроллера беспроводной локальной сети (WLC). В документе также рассмотрены некоторые из проблем, препятствующих присоединению упрощенной точки доступа (LAP) к WLC, и описан порядок их диагностики.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основные сведения о конфигурации точек LAPи контроллеров Cisco WLC
- Общие сведения о протоколе упрощенных точек доступа (LWAPP)

Условные обозначения

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

Обзор процесса обнаружения и присоединения контроллера беспроводной локальной сети (WLC)

В унифицированной беспроводной сети Cisco упрощенные точки доступа (LAP) должны вначале обнаружить контроллер WLC и присоединиться к нему, прежде чем они смогут обслуживать беспроводные клиентские устройства.

Изначально контроллеры работают только в режиме 2-го уровня. В режиме 2-го уровня упрощенные точки доступа должны находиться в одной подсети с интерфейсом управления, а интерфейс диспетчера точек доступа 3-го уровня на контроллере отсутствует. Точки доступа обмениваются данными с контроллером, используя только инкапсуляцию 2-го уровня (инкапсуляцию сети Ethernet), не реализуют протокол динамической конфигурации узла (DHCP) и не имеют IP-адреса.

В результате разработки режима 3-го уровня для контроллера появился и новый интерфейс 3-го уровня, получивший название диспетчера точек доступа. В режиме 3-го уровня упрощенные точки доступа вначале получают IP-адрес по протоколу DHCP, а затем посылают запрос открытия интерфейсу управления, используя IP-адрес (на 3-м уровне). Это позволяет располагать упрощенные точки доступа в другой подсети, отдельно от интерфейса управления контроллером. Сегодня режим 3-го уровня является самым распространенным. Некоторые контроллеры и упрощенные точки доступа способны работать только в режиме 3-го уровня.

Однако это породило новую проблему: как упрощенным точкам доступа определить IP-адрес интерфейса управления контроллера, находящегося в другой подсети?

В режиме 2-го уровня им требовалось находиться в одной и той же подсети. В режиме 3-го уровня фактически происходит «игра в прятки» между контроллером и точкой доступа. Если местоположение контроллера не сообщено точке доступа посредством параметра DHCP 43, путем разрешения адреса «cisco-lwapp-controller@локальный_домен» посредством DNS либо путем его статической настройки, то упрощенная точка доступа не будет владеть информацией о местонахождении интерфейса управления контроллера в сети.

В дополнение к этим методам упрощенная точка доступа автоматически производит поиск в локальной подсети контроллеров с локальными широковещательными адресами 255.255.255.255. Кроме того, точка доступа запоминает IP-адрес интерфейса управления любого контроллера, к которому она подключена, и сохраняет эту информацию при перезагрузке. Поэтому если упрощенная точка сначала будет помещена в локальную подсеть интерфейса управления, то она сможет найти интерфейс управления контроллера и запомнит его адрес. Это называется активацией (priming). Этот шаг не поможет найти контроллер в том случае, если позднее точка доступа будет заменена. Поэтому компания Cisco рекомендует использовать параметр DHCP 43 или методы на основе DNS.

Когда упрощенные точки доступа обнаруживают контроллер, они не владеют информацией о том, находится ли контроллер в режиме 2-го уровня или 3-го уровня. Поэтому упрощенные точки доступа перед запросом обнаружения всегда соединяются с адресом интерфейса управления контроллера. Затем контроллер в отклике обнаружения сообщает точке доступа, в каком режиме он находится. Если контроллер функционирует в режиме 3-го уровня, то в отклике обнаружения будет содержаться IP-адрес диспетчера точек доступа, таким образом, упрощенная точка доступа впоследствии сможет отправить запрос присоединения интерфейсу диспетчера точек доступа.

Примечание: По умолчанию и управление и интерфейсы менеджера точки доступа оставляют без меток на их VLAN во время конфигурации. В случае использования меток убедитесь в том, что метки относятся к одной и той же сети VLAN, чтобы надлежащим образом происходило получение откликов обнаружения и присоединения от контроллера WLC.

Точки доступа LWAPP при запуске в режиме 3-го уровня проходят следующий процесс:

1. Упрощенная точка доступа загружается и выполняет запрос IP-адреса по DHCP, если ей не был предварительно назначен статический IP-адрес.
2. Точка доступа направляет контроллерам запросы обнаружения посредством различных алгоритмов и выстраивает список контроллеров. Фактически точка доступа LAP пытается запомнить как можно больше адресов интерфейсов управления для списка контроллеров, прибегая к следующим способам:Параметр 43 DHCP (больше

подходит для глобальных компаний, в которых офисы и контроллеры разнесены по разным континентам)Запись DNS для `cisco-capwap-controller` (хороший для локальных компаний - может также использоваться для обнаружения, где совершенно новые AP присоединяются),**Примечание:** При использовании CAPWAP удостоверьтесь, что существует Запись DNS для `cisco-capwap-controller`.IP-адреса управления контроллеров LAP, запомненные ранееШироковещательная рассылка 3-го уровня в подсетиЭфирная инициализацияСтатически настроенные сведенияИз этого списка наилегчайший метод для использования для развертываний должен иметь LAP в той же подсети как интерфейс управления контроллера и позволить ЛАПА s широковещание Уровня 3 находить контроллер. Этот метод следует применять компаниям, располагающим небольшой сетью и не имеющим локального сервера DNS.Следующий по простоте метод развертывания состоит в использовании записи DNS с DHCP. Можно иметь несколько записей одного и того же имени DNS. Это позволяет упрощенной точке доступа обнаруживать несколько контроллеров. Этот метод следует использовать тем компаниям, в которых все контроллеры собраны вместе и имеют локальный сервер DNS. Он также пригоден в тех случаях, когда компания имеет несколько суффиксов DNS, а контроллеры разделены по суффиксам.Параметр DHCP 43 используется крупными компаниями для локализации сведений DHCP. Этот метод используется крупными предприятиями, имеющими единственный суффикс DNS. Например, компания Cisco владеет зданиями в Европе, Австралии и США. Предполагая разрешить только локальное присоединение упрощенных точек к контроллерам, компания Cisco не может использовать запись DNS. IP-адрес управления локального контроллера сообщается точкам посредством параметра 43 DHCP.Наконец, статичная конфигурация используется для сети, которая не имеет сервера DHCP. Можно статически настроить информацию, необходимую для присоединения к контроллеру через консольный порт и APA s CLI. Статическая настройка сведений о контроллере с использованием интерфейса командной строки точки доступа описана в разделе Ручная настройка информации о контроллере с использованием интерфейса командной строки точки доступа.Более подробное пояснение различных алгоритмов обнаружения, используемых упрощенными точками доступа для поиска контроллеров, см. в документе Регистрация упрощенных точек доступа на WLC.Описание настройки параметра DHCP 43 на сервере DHCP см. в документе Пример настройки параметра DHCP 43 для упрощенных точек доступа Cisco Aironet.

3. Каждому контроллеру в списке отправляется запрос обнаружения с ожиданием отклика обнаружения контроллера, в котором должны содержаться: имя системы, IP-адреса диспетчера точек доступа, число точек доступа, уже подключенных к каждому интерфейсу диспетчера, а также общий избыточный объем ресурсов контроллера.
4. Проверяется список контроллеров, и контроллерам отправляется запрос присоединения в следующем порядке (только если точка доступа получила от них отклик обнаружения):Имя системы первичного контроллера (предварительно настроенное на упрощенной точке доступа)Имя системы вторичного контроллера (предварительно настроенное на упрощенной точке доступа)Имя системы третичного контроллера (предварительно настроенное на упрощенной точке доступа)Главный контроллер (если на точке доступа не были предварительно настроены имена первичного, вторичного и третичного контроллеров). Позволяет задать заранее известный контроллер, к которому будут присоединяться новые точки доступаВ отсутствие вышеперечисленных вариантов – равномерное распределение между

контроллерами с использованием значения объема избыточных ресурсов из отклика обнаружения.Если два контроллера имеют одинаковый объем избыточных ресурсов, то запрос обнаружения вначале отправляется первому контроллеру, который отвечает на запрос откликом обнаружения. Если у одного контроллера имеется несколько диспетчеров точек доступа на разных интерфейсах, выбирается интерфейс диспетчера точки доступа с наименьшим числом точек доступа.Контроллер отвечает на все запросы обнаружения, не проверяя сертификатов или реквизитов точки доступа. Тем не менее запросы присоединения должны иметь действительный сертификат для получения отклика присоединения от контроллера. Если упрощенная точка доступа не получит отклик присоединения от выбранного контроллера, то она предпримет попытку обратиться к следующему контроллеру в списке, если этот контроллер не входит в список настроенных (как первичный/вторичный/третичный).

5. Получив отклик присоединения, точка доступа проверяет, совпадает ли загруженный в нее образ с образом контроллера. Если нет, точка доступа загружает образ с контроллера и перезагружается для запуска нового образа, после чего процесс повторяется заново с шага 1.
6. Если же образы программного обеспечения совпадают, точка доступа спрашивает конфигурацию у контроллера и переходит в зарегистрированное состояние на контроллере.После загрузки конфигурации пользователем точка доступа может снова перезагрузиться для вступления новой конфигурации в силу. По этой причине дополнительная перезагрузка является обычным явлением.

Отладочная информация контроллера

В контроллере предусмотрено несколько команд debug, которые позволяют пронаблюдать за ходом всего процесса из командной строки.

- **события debug lwapp enableâ** Показывают пакеты соединения и пакеты обнаружения.
- **пакет debug lwapp enableâ** Показывает информацию о пакетном уровне пакетов соединения и обнаружения.
- **pki debug pm enableâ** Показывает процесс проверки достоверности сертификата.
- **отладка отключает-allâ** , Выключает отладки.

Используя приложение эмуляции терминала, позволяющее протоколировать вывод команд в файл журнала, подключитесь к консоли или порту защищенной командной оболочки (SSH) / Telnet контроллера и введите следующие команды:

```
    config session timeout 120 config serial timeout 120 show run-config (and spacebar thru to collect all) debug mac addr <ap-mac-address> (in xx:xx:xx:xx:xx format) debug client <ap-mac-address> debug lwapp events enable debug lwapp errors enable debug pm pki enable
```

По завершении протоколирования отладочных сообщений отключить вывод всех отладочных данных командой debug disable-all.

В следующих разделах показан вывод этих команд debug, в которых упрощенная точка доступа регистрируется на контроллере.

debug lwapp events enable

Эта команда предоставляет информацию о событиях и ошибках LWAPP, имеющих место в

процессе обнаружения и присоединения LWAPP.

Это вывод команды debug lwapp events enable для упрощенной точки доступа, образ в которой совпадает с образом на WLC:

Примечание: Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
debug lwapp events enable Wed Oct 24 16:59:35 2007: 00:0b:85:5b: fb:d0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:5b: fb:d0 to 00:0b:85:33:52:80 on port '2' !--- LWAPP discovery request
sent to the WLC by the LAP. Wed Oct 24 16:59:35 2007: 00:0b:85:5b:fb:d0 Successful transmission
of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2 !--- WLC responds to the discovery
request from the LAP. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2' !--- LAP sends a join request to the
WLC. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 AP ap:5b:fb:d0: txNonce 00:0B:85:33:52:80
rxNonce 00:0B:85:5B:FB:D0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 LWAPP Join-Request MTU
path from AP 00:0b:85:5b:fb:d0 is 1500, remote debug mode is 0 Wed Oct 24 16:59:46 2007:
00:0b:85:5b:fb:d0 Successfully added NPU Entry for AP 00:0b:85:5b:fb:d0 (index 55) Switch IP:
10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0 AP IP: 10.77.244.219, AP Port: 49085,
next hop MAC: 00:0b:85:5b:fb:d0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully
transmission of LWAPP Join-Reply to AP 00:0b:85:5b:fb:d0 !--- WLC responds with a join reply to
the LAP. Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Register LWAPP event for AP
00:0b:85:5b:fb:d0 slot 0 -- LAP registers with the WLC Wed Oct 24 16:59:48 2007:
00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:5b:fb:d0 to
00:0b:85:33:52:81 !--- LAP requests for the configuration information from the WLC. Wed Oct 24
16:59:48 2007: 00:0b:85:5b:fb:d0 Updating IP info for AP 00:0b:85:5b:fb:d0 -- static 1,
10.77.244.219/255.255.255.224, gtw 10.77.244.220 Wed Oct 24 16:59:48 2007: spamVerifyRegDomain
RegDomain set for slot 0 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007:
spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -AB Wed Oct 24
16:59:48 2007: Send AP Timesync of 1193245188 source MANUAL Wed Oct 24 16:59:48 2007:
spamEncodeDomainSecretPayload:Send domain secret
TSWEBRET<0d,59,aa,b3,7a,fb,dd,b4,e2,bd,b5,e7,d0,b2,52,4d,ad,21,1a,12> to AP 00:0b:85:5b:fb:d0
Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:5b:fb:d0 !--- WLC responds by providing all the necessary configuration information
to the LAP. Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'eap fast' Wed
Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48
2007: Running spamEncodeCreateVapPayload for SSID 'webauth' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'eap fast' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48 2007: Running
spamEncodeCreateVapPayload for SSID 'webauth' . . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0
Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5b:fb:d0 . . Wed
Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP Up event for AP 00:0b:85:5b:fb:d0 slot 0!
!--- LAP is up and ready to service wireless clients. Wed Oct 24 16:59:48 2007:
00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5b:fb:d0 . . . Wed Oct
24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP RRM_CONTROL_RES from AP 00:0b:85:5b:fb:d0 !--
- WLC sends all the RRM and other configuration parameters to the LAP.
```

Как упомянуто в предыдущем разделе, при регистрации на WLC упрощенная точка доступа проверяет, совпадает ли загруженный в нее образ с образом контроллера. Если образы на точке доступа и WLC различаются, то вначале точка доступа загружает с WLC новую версию образа. Если образ в упрощенной точке доступа совпадает с образом в контроллере, то точка доступа продолжает загружать конфигурацию и другие параметры с WLC.

Если в процессе регистрации точка доступа загрузит с контроллера образ, то в выводе команды debug lwapp events enable будут присутствовать следующие сообщения:

```
Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from AP
00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from
```

```
AP 00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES
from AP 00:0b:85:5b:fb:d0
```

По завершении загрузки образа точка доступа перезагружается и заново отрабатывает алгоритм обнаружения и присоединения.

debug pm pki enable

В рамках процесса присоединения WLC выполняет аутентификацию каждой точки доступа, проверяя действительность ее сертификата.

Когда точка доступа отправляет запрос присоединения LWAPP контроллеру, она вставляет в сообщение LWAPP свой сертификат X.509. Кроме того, она генерирует случайный идентификатор сеанса, который также включается в запрос присоединения LWAPP. Когда WLC получает запрос присоединения LWAPP, он проверяет подпись сертификата X.509 с помощью открытого ключа AP и удостоверяется в том, что сертификат был выдан доверенным центром сертификации.

Это также посмотрело на срок начала работы и время для интервала законности сертификата AP и сравнивает эту дату и время к его собственной дате и времи (следовательно, controllerâ s часы должен быть установлен в близко к текущей дате и времени). Если сертификат X.509 действителен, WLC генерирует случайный ключ шифрования AES. WLC интегрирует ключ AES в свое криптоядро, получая возможность зашифровывать и расшифровывать последующие сообщения управления LWAPP при двустороннем обмене ими с точкой доступа. Следует учесть, что пакеты данных в туннеле LWAPP между упрощенной точкой доступа и контроллером передаются в незашифрованном виде.

Команда debug pm pki enable отображает ход процесса проверки сертификата на этапе присоединения к контроллеру. Команда debug pm pki enable также отображает хэш-ключ точки доступа в процессе присоединения, если у точки доступа имеется самоподписанный сертификат (SSC), созданный программой преобразования LWAPP. Если у точки доступа имеется искусственный установленный сертификат (сертификат MIC), то хэш-ключ отображаться не будет.

Примечание: Все AP, произведенные после июня 2006, имеют MIC.

Ниже приведен вывод команды debug pm pki enable в случае присоединения к контроллеру упрощенной точки доступа с MIC:

Примечание: Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: locking ca cert table
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b8591c3c0, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <issuer>  C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:91:c3:c0
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
```

Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 2d812f0c
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 20f00bf3
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: **user cert verfied using >bsnOldDefaultCaCert<** Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: **ValidityString (current): 2007/10/25/13:52:59** Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: **AP version is 0x400d900, sending Cisco ID cert...**
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <cscoDefaultIdCert> Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59
2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 2, ID cert >bsnSslWebadminCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 3, ID cert >bsnSslWebauthCert< Thu Oct 25 13:52:59 2007:
sshpmGetIssuerHandles: **Airespace ID cert ok; sending it...** Thu Oct 25 13:52:59 2007:
sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing
to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row
4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 5,
CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCID: comparing to row 0, ID
cert >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromHandle: calling
sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: called
to get cert for CID 156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 0,
certname >bsnOldDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
1, certname >bsnDefaultRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 2, certname >bsnDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 3, certname >bsnDefaultBuildCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing
to row 4, certname >cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID:
comparing to row 5, certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007:
sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03
2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: called to get cert for CID 156af135 Thu Oct 25 13:53:03
2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 3, certname >bsnDefaultBuildCert< Thu
Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 4, certname
>cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 5,
certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: called to
encrypt 16 bytes Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: successfully encrypted, out is
192 bytes Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for CID 156af135 Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: match in row 0
Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 172 bytes Thu
Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25

```
13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 24 bytes Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25 13:53:03
2007: sshpmPrivateKeyEncrypt: encrypted bytes: 384 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: called with 0xae0c358 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: freeing public key
```

Для упрощенной точки доступа с SSC вывод команды debug pm pki enable будет выглядеть следующим образом. Обратите внимание, что в выводе также присутствует хэш SSC.

Примечание: Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
(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
300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003
82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd
7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0
39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3
9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce
cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e
c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e
c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db
251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc
1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490
881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b
d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693
f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f
76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3
b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f
de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8
eb076940280cbed1 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
```

Отладочная информация упрощенной точки доступа

Если в отладочных сообщениях контроллера не указан запрос присоединения, то можно выполнить отладку процесса на упрощенной точке доступа при условии наличия у нее консольного порта. Следующие команды позволяют просмотреть процесс загрузки точки доступа, однако перед этим необходимо вначале войти в разрешенный режим (пароль по умолчанию – «Cisco»):

- **debug dhcp detailâ** Показывает параметру DHCP 43 информации.
- **отладьте ip udpâ** , Показывает соединение/пакеты обнаружения контроллеру, а также DHCP, и запросы DNS (все они являются пакетами UDP. Порт 12223 является controllerâ s исходный порт).
- **клиент debug lwapp eventâ** Показывает События lwapp для AP.

- **не отладьте allâ** , Отключает отладки на AP.

Ниже приведен пример выходных данных команды debug ip udp. Этот фрагмент вывода даёт представление о пакетах, которые посылаются точкой LAP во время процесса загрузки для присоединения к контроллеру.

```
UDP: sent src=10.77.244.199(20679), dst=10.77.244.208(12223)
!--- LWAPP Discovery Request sent to a controller to which !--- the AP was previously registered
to. UDP: sent src=10.77.244.199(20679), dst=172.16.1.50(12223) !--- LWAPP Discovery Request
using the statically configured controller information. UDP: sent src=10.77.244.199(20679),
dst=255.255.255.255(12223) !--- LWAPP Discovery Request sent using subnet broadcast. UDP: sent
src=10.77.244.199(20679), dst=172.16.1.51(12223) !--- LWAPP Join Request sent to AP-Manager
interface on statically configured controller.
```

Предотвращение проблем, связанных с DHCP

Неверная настройка параметров, связанных с DHCP, может сделать невозможным получение IP-адреса по DHCP для упрощенных точек доступа, использующих этот протокол. В этом разделе поясняется работа DHCP с контроллерами беспроводных сетей (WLC) и приводятся рекомендации, позволяющие избежать связанных с DHCP проблем.

С точки зрения протокола DHCP контроллер ведет себя как маршрутизатор со вспомогательным IP-адресом. Другими словами, он заполняет IP-адрес шлюза и переадресует запрос посредством одноадресного пакета непосредственно на DHCP-сервер.

В возвращенном предложении DHCP контроллер заменяет IP-адрес DHCP-сервера своим виртуальным IP-адресом. Это необходимо по той причине, что при переключении между точками доступа операционная система Windows первым делом пытается обратиться к DHCP-серверу для обновления адреса.

С IP-адресом DHCP-сервера 1.1.1.1 (типичный виртуальный IP-адрес на контроллере) контроллер может перехватить пакет и оперативно ответить на запрос Windows.

Из-за этого, в частности, виртуальный IP-адрес на всех контроллерах совпадает. Если ноутбук с ОС Windows будет перемещен к точке доступа на другом контроллере, то он попробует обратиться к виртуальному интерфейсу контроллера. Благодаря возникновению события подвижности и передаче контекста новый контроллер, к которому перейдет клиент Windows, уже располагает всей необходимой информацией для повторного ответа на запрос Windows.

Если на контроллере требуется использовать внутренний DHCP-сервер, то достаточно поместить IP-адрес управления DHCP-сервера на динамический интерфейс, созданный для подсети. Затем этот интерфейс нужно назначить беспроводной локальной сети (WLAN).

Причина, по которой контроллеру нужен IP-адрес в каждой подсети, — это возможность заполнить адрес шлюза DHCP в запросе DHCP.

Ниже перечислены основные моменты, которые следует иметь в виду при настройке DHCP-серверов для беспроводной локальной сети:

1. IP-адрес DHCP-сервера не должен находиться в динамической подсети, принадлежащей контроллеру. Он будет заблокирован, однако это можно отменить следующей командой:
   config network mgmt-via-dynamic-interface on version 4.0 only (command not available in

version 3.2)

2. Контроллер будет пересылать DHCP-трафик в виде одноадресных пакетов со своего динамического интерфейса (в более поздних версиях программы), используя свой IP-адрес на этом интерфейсе. Следует убедиться в том, что имеющиеся межсетевые экраны пропускают трафик с этого адреса на DHCP-сервер.
3. Удостоверьтесь в том, что отклик DHCP-сервера достигает динамического адреса контроллера в этой сети VLAN через имеющиеся межсетевые экраны. Отправьте эхозапрос на динамический адрес интерфейса с DHCP-сервера. Отправьте эхозапрос на DHCP-сервер с исходным IP-адресом шлюза динамического интерфейса.
4. Убедитесь в том, что сеть VLAN точки доступа разрешена на коммутаторах и маршрутизаторах, а соответствующие порты настроены в качестве магистральных, позволяя пропускать через проводную сеть пакеты (в т.ч. пакеты DHCP), снабженные меткой этой сети VLAN.
5. Убедитесь, что сервер DHCP настроен для назначения IP-адреса сети VLAN точки доступа. Можно также настроить WLC в качестве DHCP-сервера. Подробное описание порядка настройки DHCP-сервера на WLC см. в разделе Настройка DHCP в графическом интерфейсеРуководства по настройке контроллеров беспроводных локальных сетей Cisco (выпуск 5.0).
6. Убедитесь в том, что IP-адрес контроллера на его динамическом интерфейсе находится в пределах одного из диапазонов DHCP на DHCP-сервере.
7. Наконец, убедитесь в том, что используемый вами сервер DHCP не относится к категории принципиально неспособных обрабатывать одноадресные DHCP-запросы, например PIX.

Если вам не удается решить проблему с DHCP, существуют 2 других решения:

- Попробуйте использовать внутренний сервер DHCP. В качестве адреса DHCP-сервера на динамическом интерфейсе настройте IP-адрес управления и затем выберите внутренний пул DHCP. Если диапазон DHCP включен, это решение должно работать.
- Проверьте отсутствие ответа на запрос DHCP, запротоколировав вывод в интерфейсе командной строки (консоли или SSH) от следующих команд:`0. debug mac addr <mac address>`
  `1. debug dhcp message enable`
  `2. debug dhcp packet enable` Это должно указывать на то, что пакет DHCP передан, но контроллер не получил ответ.

Наконец, в свете безопасности контроллера не рекомендуется помещать сеть VLAN или подсеть в состав контроллера, также содержащего упрощенные точки доступа, если последний не находится в подсети интерфейса управления.

Примечание: Сервер RADIUS или сервер DHCP не должны быть ни на одной из подсетей динамического интерфейса контроллера. Система безопасности блокирует возвращающиеся пакеты, которые пытаются обратиться к контроллеру.

Применение серверов SYSLOG для устранения неполадок, связанных с процессом присоединения LAP

В выпуске 5.2 программного обеспечения контроллера предусмотрена возможность настройки точек доступа для отправки всех ошибок, связанных с управлением и инициализацией беспроводных точек доступа (CAPWAP), на сервер SYSLOG. В

контроллере не нужно разрешать каких-либо команд отладки, поскольку все сообщения об ошибках CAPWAP можно просмотреть с сервера SYSLOG. Дополнительные сведения об этой функции и командах для ее активации см. в разделе Устранение неполадок, связанных с процессом присоединения точек доступа в Руководстве по настройке контроллеров беспроводных локальных сетей Cisco (выпуск 5.2).

Причины неприсоединения LAP к контроллеру?

Основные первоочередные проверки

- Возможен ли обмен данными между точкой доступа и WLC?
- Удостоверьтесь, что AP добирается, адрес от DHCP (проверьте арендные договоры сервера DHCP для APA s MAC-адрес).
- Попробуйте отправить эхозапрос точке доступа с контроллера.
- Проверьте, правильно ли настроена конфигурация остовного дерева (STP) на коммутаторе и не блокирует ли она пакеты для сетей VLAN.
- Если эхозапросы проходят успешно, убедитесь в том, что точка доступа может использовать по крайней мере один из возможных методов обнаружения. Подключитесь к контроллеру через консоль WLC или telnet/ssh для выполнения отладочных команд.
- Каждый раз перезагрузки точки доступа, это инициирует последовательность обнаружения WLC и пытается определить местоположение AP. Перезагрузите AP и проверку, если это присоединяется к WLC.

Ниже перечислены некоторые из наиболее распространенных проблем, препятствующие присоединению упрощенных точек доступа к WLC.

Проблема 1. Время на контроллере выходит за пределы срока действия сертификата

Для диагностики и устранения этой проблемы выполните приведенные ниже шаги:

1. **Выполните команды debug lwapp errors enable и debug pm pki enable.В выводе команды debug lwapp event enable отображаются сообщения о сертификации, которыми обмениваются точка доступа и контроллер беспроводной локальной сети.** Из этих данных четко ясно, что сертификат отклонен.**Примечание:** Удостоверьтесь, что объяснили Согласованное текущее время (UTC) смещение.**Команда debug lwapp events enable приводит к отображению следующих выходных данных:Примечание:** Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.`Thu Jan 1 00:09:46 1970: 00:0b:85:5b:fb:d0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '2' Thu Jan 1 00:09:46 1970: 00:0b:85:5b:fb:d0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2 Thu Jan 1 00:09:57 1970: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2' Thu Jan 1 00:09:57 1970: 00:0b:85:5b:fb:d0` **`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:5b:fb:d0.`** `Thu Jan 1 00:09:57 1970: 00:0b:85:5b:fb:d0` **`Unable to free public key for AP 00:0B:85:5B:FB:D0`** `Thu Jan 1 00:09:57 1970: spamProcessJoinRequest : spamDecodeJoinReq failed` **Ниже приведены выходные данные команды debug pm pki enable на контроллере.** Эти данные выводятся при выполнении процесса проверки сертификата.**Примечание:** Некоторые линии выходных

данных были перемещены во вторую линию из-за пространственных ограничений.
```
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)
```
Эти данные отчетливо свидетельствуют о том, что время на контроллере находится вне пределов периода достоверности сертификата упрощенной точки доступа. Следовательно, точка доступа не может быть зарегистрирована на контроллере. Сертификаты, установленные на точке доступа, имеют заданный срок действия. Время контроллера должно быть установлено таким способом, которым это в интервале Достоверности сертификата ЛАПА s сертификат.

2. **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 вне срока действия сертификата, измените время на контроллере, чтобы оно попадало в этот период.**Примечание:** Если время является "not set" правильно на контроллере, выберите **Commands> Set Time** в режиме графического интерфейса контроллера или выполните **команду config time** в CLI контроллера для установки времени контроллера.
3. **На упрощенных точках доступа с интерфейсом командной строки проверьте сертификаты командой show crypto ca certificates из интерфейса командной строки точки доступа.**Эта команда позволяет проверить срок действия сертификата, заданный 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. `Name: C1200-001563e50c7e.` Это и есть период действия сертификата, который необходимо принять во внимание.

Проблема 2. Рассогласование нормативного домена

Команда debug lwapp events enable приводит к отображению следующих выходных данных:

Примечание: Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.

```
Wed Oct 24 17:13:20 2007: 00:0b:85:91:c3:c0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:80 on port '2'
Wed Oct 24 17:13:20 2007: 00:0e:83:4e:67:00 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:91:c3:c0 on Port 2
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:81 on  port '2'
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 AP ap:91:c3:c0:
txNonce  00:0B:85:33:52:80 rxNonce  00:0B:85:91:C3:C0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 LWAPP Join-Request MTU path
from AP 00:0b:85:91:c3:c0 is 1500, remote debug mode is 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully added NPU Entry
for AP 00:0b:85:91:c3:c0 (index 48)
Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0
AP IP: 10.77.246.18, AP Port: 7228, next hop MAC: 00:17:94:06:62:88
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully transmission
of LWAPP Join-Reply to AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:91:c3:c0 to  00:0b:85:33:52:81
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP info for AP 00:0b:85:91:c3:c0 --
static 0, 10.77.246.18/255.255.255.224, gtw 10.77.246.1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP 10.77.246.18 ===> 10.77.246.18
for AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 0 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211a Regulatory Domain
(-N) does not match with country (US )  reg. domain -AB for the slot 0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 1 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211bg Regulatory Domain (-N)
does not match with country (US ) reg. domain -AB for the slot 1 Wed Oct 24 17:13:47 2007:
spamVerifyRegDomain AP RegDomain check for the country US failed Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: Regulatory Domain check Completely FAILED The AP will
not be allowed to join Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 apfSpamProcessStateChangeInSpamContext: Deregister
LWAPP event for AP 00:0b:85:91:c3:c0 slot 1 Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0 Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 1
```

Сообщение ясно говорит о наличии рассогласования нормативного домена между LAP и WLC. WLC поддерживает несколько нормативных доменов, но каждый нормативный домен необходимо выбрать, прежде чем из него сможет присоединиться упрощенная точка доступа. Например, если на WLC действует нормативный домен -A, этот контроллер можно использовать только с точками доступа, использующими нормативный домен -A (и т.д.). При приобретении точек доступа и WLC необходимо убедиться в том, что их нормативные домены совпадают. Только в этом случае упрощенные точки доступа могут зарегистрироваться на WLC.

Примечание: И 802.1b/g и 802.11a радио должен быть в том же управляющем домен для

одиночного LAP.

Проблема 3. Сообщение об ошибке: «AP cannot join because the maximum number of APs on interface 2 is reached» (Точка доступа не может быть добавлена, т.к. достигнуто максимальное количество точек доступа на интерфейсе 2)

Когда точка доступа пробует присоединиться к контроллеру, может возникнуть следующее сообщение об ошибке:

```
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 4498: AP cannot join because the maximum number of
APs on interface 2 is reached.
```

По умолчанию контроллеры серии 4400 поддерживают до 48 точек доступа на каждом порту. При подключении более чем 48 точек доступа к контроллеру появляется это сообщение об ошибке. Тем не менее контроллер серии 4400 можно настроить и так, чтобы он поддерживал большее число точек доступа на одном интерфейсе (в порту). Этого можно добиться несколькими способами:

- Агрегирование каналов (для контроллеров в режиме 3-го уровня)
- Организация нескольких интерфейсов диспетчера точек доступа (для контроллеров в режиме 3-го уровня)
- Подсоединение дополнительных портов (для контроллеров в режиме 2-го уровня)

За дополнительными сведениями обратитесь к разделу Настройка контроллеров серии 4400 для поддержки больше 48 точек доступа.

Примечание: Cisco представила WLC серии 5500 для корпоративных пользователей с дополнительными возможностями. Это не имеет никакого ограничения на количество AP на порт. См. Выбор Между Агрегированием каналов и Множественным разделом Интерфейсов менеджера точки доступа Выпуска 6.0 руководства по конфигурированию контроллера Cisco Wireless LAN для получения дополнительной информации.

Проблема 4. При использовании точек доступа с сертификатом SSC отключается политика точек доступа SSC

Если на контроллере отключена политика SSC, то команды debug lwapp events enable и debug pm pki enable на контроллере выдают следующие сведения:

```
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
```

Для диагностики и устранения этой проблемы выполните приведенные ниже шаги:

Выполните одно из следующих двух действий:

- **Введите в интерфейсе командной строки команду show auth-list, чтобы убедиться, что контроллер настроен для обслуживания точек доступа с протоколами SSC.**Ниже

показан пример выходных данных:`#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).Убедитесь, что установлен флажок Accept Self Signed Certificate (Принимать самоподписанные сертификаты).** Если флажок снят, установите его.**Выберите в качестве типа сертификата SSC.**Добавьте точку доступа, ее mac-адрес и хеш-ключ к списку авторизации.**Этот хеш-ключ выводится в данных команды debug pm pki enable .** См. порядок получения хеш-ключа в разделе Проблема 6.

Проблема 5. На контроллере включен список авторизации точек доступа, в котором отсутствует локальная точка доступа

В таких случаях по команде debug lwapp events enable контроллер будет выводить следующие сведения:

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:51:5a:e0
```

При использовании упрощенных точек доступа с консольным портом команда debug lwapp client error будет приводить к появлению следующего сообщения:

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: No more AP manager IP addresses remain.
```

Это снова свидетельствует о том, что упрощенная точка доступа не входит в список авторизации точек доступа на контроллере.

Состояние списка авторизации точек доступа можете просмотреть следующей командой:

```
(Cisco Controller) >show auth-list Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Для добавления упрощенной точки доступа в список авторизации точек доступа используйте команду config auth-list add mic <MAC-адрес точки доступа>. Более подробно настройка авторизации упрощенных точек доступа описана в документе Пример настройки авторизации упрощенных точек доступа (LAP) в унифицированной беспроводной сети Cisco.

Проблема 6. Открытый хеш-ключ SSC неверен или отсутствует

Для диагностики и устранения этой проблемы выполните приведенные ниже шаги:

1. **Введите команду debug lwapp events enable.**Она позволяет проверить, имела ли место попытка подсоединения со стороны точки доступа.
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:**Примечание:** Некоторые линии выходных данных были перемещены во вторую линию из-за пространственных ограничений.`(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 300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb 058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8 eb076940280cbed1 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**`

Чтобы устранить данную проблему, проделайте 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:**Примечание:** Эта команда была перемещена во вторую линию из-за пространственных ограничений.`(Cisco Controller)>**config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9**`

Проблема 7. На точке доступа поврежден сертификат или открытый ключ

Точка доступа не присоединяется к контроллеру из-за проблем с сертификатом.

Выполните команды debug lwapp errors enable и debug pm pki enable. Отображаются сообщения о повреждении сертификатов или ключей.

Примечание: Некоторые линии выходных данных были перемещены во вторые линии из-за пространственных ограничений.

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 LWAPP Join Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP
00:0f:24:a9:52:e0. Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Deleting and removing AP
00:0f:24:a9:52:e0 from fast path Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free
public key for AP
```

Для устранения этой проблемы выберите один из двух вариантов действия:

- APA MIC Запрос Return Materials Authorization (RMA).
- APA SSC понижает до Cisco IOS? Выпуск ПО 12.3 (7) JA.В случае точки доступа с SSC возвратите ее на программное обеспечение IOS кнопкой MODE. Затем при помощи инструмента обновления LWAPP снова выполните переход на LWAPP. В результате сертификат должен быть создан заново.

Выполните следующие шаги для понижения версии:

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

Подробное описание понижения функциональности ПО на упрощенной точке доступа см. в документе Обновление автономных точек доступа Cisco Aironet до упрощенного режима.

При наличии системы управления беспроводной сетью (WCS) можно форсировать SSC на новый контроллер WLC. Для получения дополнительной информации о настройке точек доступа с использованием WCS обратитесь к разделу Настройка точек доступаРуководства по настройке системы управления беспроводной сетью Cisco (выпуск 5.1).

Проблема 8. Возможно, контроллер работает в режиме 2-го уровня

Чтобы устранить данную проблему, проделайте следующую операцию:

Проверьте режим работы контроллера. Преобразованные точки доступа поддерживают только механизмы обнаружения уровня 3. Преобразованные точки доступа не поддерживают механизмы обнаружения уровня 2.

Чтобы устранить данную проблему, проделайте следующие действия:

1. Установите на контроллере беспроводной локальной сети режим уровня 3.
2. Перезагрузите и настройте интерфейс диспетчера точек доступа.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.

Проблема 9. После преобразования точки доступа в LWAPP на ней отображается следующее сообщение об ошибке

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.

Чтобы устранить данную проблему, выполните следующие действия:

1. Используется точка доступа SSC. Выполните возврат к автономному образу IOS.
2. **Очистите конфигурацию, выполнив команду write erase, затем выполните повторную загрузку.** Не сохраняйте конфигурацию при повторной загрузке.

Проблема 10. Неверно выбрана сеть VLAN, через которую контроллер получает сообщение об обнаружении точки доступа (можно видеть отладочное сообщение об обнаружении, но не ответ)

Команда debug lwapp events enable приводит к отображению следующих выходных данных:

```
Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!
```

Это сообщение означает, что контроллер получил запрос открытия через широковещательный IP-адрес, в котором исходный IP-адрес не лежит ни в одной из настроенных подсетей контроллера. Это также означает, что контроллер отбрасывает такой пакет.

Проблема состоит в том, что точка доступа не посылает запрос обнаружения на IP-адрес управления. Контроллер выдает широковещательный запрос обнаружения из сети VLAN, не настроенной на контроллере. Как правило, это происходит, когда заказчик настраивает разрешенные сети VLAN в магистральном режиме вместо того, чтобы ограничить их беспроводными сетями VLAN.

Чтобы устранить данную проблему, выполните следующие действия:

1. **Если контроллер находится в другой подсети, точки доступа должны быть активированы для IP-адреса контроллера либо точки доступа должны получить IP-адреса контроллеров посредством любого метода обнаружения.**
2. Настройки коммутатора позволяют использовать некоторые сети VLAN, отсутствующие на контроллере. Ограничьте состав разрешенных сетей VLAN на магистралях.

Проблема 11. Точка доступа 1250 не может присоединиться к WLC

В системе используется контроллер точки доступа 2106 с версией ПО 4.1.185.0. Точка доступа Cisco 1250 не может присоединиться к контроллеру.

В журнале на WLC присутствуют следующие сообщения:

```
Mon Jun 2 21:19:37 2008AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2
21:19:37 2008 AP Associated. Base Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:26 2008 AP
Disassociated. Base Radio MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:20 2008 AP with MAC
f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2 21:19:20 2008 AP Associated. Base
Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:09 2008 AP Disassociated. Base Radio
MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:03 2008 AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x)
is unknown.
```

Решение: Проблема вызвана тем, что упрощенная точка доступа Cisco 1250 не поддерживается в версии 4.1. Точки доступа Cisco Aironet серии 1250 поддерживаются начиная с версий контроллера 4.2.61. Для решения этой проблемы требуется обновить ПО контроллера до версии 4.2.61.0 или более поздней.

Проблема 12. Точка доступа не может присоединиться к WLC. Межсетевой экран блокирует необходимые порты

Если в корпоративной сети используется межсетевой экран, проследите за тем, чтобы на межсетевом экране были разрешены следующие порты, позволяющие упрощенной точке доступа присоединиться к контроллеру и взаимодействовать с ним.

Необходимо разрешить следующие порты:

- Включите данные порты UDP для трафика LWAPP:Данные – 12222Управляющий трафик – 12223
- Включите данные порты UDP для трафика Mobility:16666 - 1666616667 - 16667
- Включите порты UDP 5246 и 5247 для трафика CAPWAP.
- TCP 161 и 162 для SNMP (для системы управления беспроводной сетью – WCS)

Следующие порты открывать необязательно (зависит от ваших требований):

- UDP 69 для TFTP
- TCP 80 и/или 443 для HTTP или HTTPS для доступа GUI
- TCP 23 и/или 22 для доступа к интерфейсу командной строки посредством Telnet или защищенной командной оболочки (SSH)

Проблема 13. Дублирование IP-адреса в сети

Это еще одна распространенная проблема, возникающая при попытке присоединения точки доступа к WLC. Когда точка доступа пробует присоединиться к контроллеру, может возникнуть следующее сообщение об ошибке.

```
No more AP manager IP addresses remain
```

Одна из возможных причин появления этого сообщения об ошибке – наличие в сети дублирующегося IP-адреса, совпадающего с IP-адресом диспетчера точек доступа. В этом случае упрощенная точка доступа продолжает циклически включаться и отключаться и не может присоединиться к контроллеру.

В отладочных сообщениях будет показано, что WLC получает запросы обнаружения LWAPP от точек доступа и передает точкам доступа отклик обнаружения LWAPP. Однако контроллеры WLC не получают запросы присоединения LWAPP от точек доступа.

Чтобы расследовать эту проблему, отправьте эхозапрос диспетчеру точек доступа с проводного узла одной IP-подсети с диспетчером точек доступа. Затем проверьте кэш ARP.

При обнаружении дублирующегося IP-адреса удалите устройство с дублирующимся IP-адресом или смените IP-адрес на устройстве так, чтобы IP-адрес в сети был уникален.

После этого точка доступа получит возможность присоединения к WLC.

Проблема 14. Точки доступа LWAPP не присоединяются к WLC, если величина максимального блока передачи данных (MTU) для сети составляет менее 1500 байтов

Это связано с ошибкой Cisco с идентификатором CSCef50742. Могут возникнуть ошибки присоединения точек доступа LWAPP к WLC. Если длина запроса присоединения LWAPP превышает 1500 байт, то LWAPP будет фрагментировать запрос присоединения LWAPP. Логика для всех AP LWAPP заключается в том, что размер первого фрагмента составляет 1500 байтов (включая заголовки IP и UDP), а размер второго фрагмента составляет 54 байта (включая заголовки IP и UDP). Если на участке сети между точками доступа LWAPP и WLC размер MTU составляет менее 1500 байтов (это может иметь место при использовании протокола туннелирования, например VPN, IPsec, GRE, MPLS и т.п.), WLC не сможет обработать запрос присоединения LWAPP.

Вы столкнетесь с этой проблемой при следующих условиях:

- На WLC используется программное обеспечение версии 3.2 или более ранней
- Максимальный размер блока передачи данных (MTU) на участке сети между точкой доступа и WLC составляет менее 1500 байтов

Для устранения этой проблемы используйте одно из следующих решений:

- Обновите программное обеспечение WLC до версии 4.0, если платформа это поддерживает. В версии 4.0 WLC эта проблема исправлена: туннель LWAPP может собирать до 4 фрагментов.
- Увеличьте MTU на участке сети до 1500 байтов.
- Используйте 1030 REAP для участков, доступных по путям с низким MTU. Соединения REAP LWAPP с точками доступа 1030 изменены таким образом, чтобы решить эту проблему путем уменьшения размера MTU, используемого для режима REAP.

Проблема 15. Упрощенная точка доступа серии 1142 серии не присоединяется к WLC. Сообщение об ошибке на WLC: lwapp_image_proc: unable to open tar file (невозможно открыть TAR-файл)

В упрощенных точках доступа серии 1142 поддерживаются только выпуски WLC 5.2 и более поздние. При использовании версий WLC ниже 5.2 будет невозможно зарегистрировать упрощенную точку доступа на контроллере и появится сообщение об ошибке следующего вида:

```
*Mar 27 15:04:38.596: %LWAPP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.597: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.606: %LWAPP-3-CLIENTERRORLOG: not receive read response(3)
*Mar 27 15:04:38.609: lwapp_image_proc: unable to open tar fileMar 12 15:47:27.237
spam_lrad.c:8317 LWAPP-3-IMAGE_DOWNLOAD_ERR3:
Refusing image download request from AP 0X:2X:D0:FG:a7:XX - unable to open
image file /bsn/ap//c1140
```

Чтобы зарегистрировать упрощенные точки доступа серии 1140 на WLC, обновите

микропрограмму на WLC до версии 5.2 или выше.

Проблема 16. Упрощенные точки доступа серии 1000 не могут присоединиться к контроллеру беспроводной сети. На контроллере работает ПО версии 5.0

Эта проблема вызвана тем, что выпуск программного обеспечения WLC 5.0.148.0 и более поздние выпуски не совместимы с точками доступа Cisco Aironet серии 1000. Если у вас есть LAP серии Cisco 1000 в сети, которая выполняет версии WLC 5.0.48.0, LAP серии 1000 не присоединяется к контроллеру, и вы видите это сообщение прерывания на WLC.

```
"AP with MAC xx:xx:xx:xx:xx:xx is unkown"
```

Проблема 17: LAP с Сеткой отображают не способный присоединиться к WLC

Облегченная точка доступа не регистрируется в WLC. Журнал отображает это сообщение об ошибках

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
 Type: WLAN USER
```

Если Облегченная точка доступа была поставлена с образом сетки и находится в Мостовом режиме, это может произойти. Если бы LAP был упорядочен с программным обеспечением сетки на нем, то необходимо добавить LAP к списку авторизации AP. Выберите **Security> AP Policies** и добавьте **AP** к Списку авторизации. AP должен тогда присоединиться, загрузить образ от контроллера, затем зарегистрироваться в WLC в мостовом режиме. Затем необходимо изменить AP на автономный режим. LAP загружает образ, перезагрузки и регистрируется назад к контроллеру в автономном режиме.

Проблема 18: Сообщение об ошибках - Отбрасывание основного запроса на обнаружение от AP XX:AA:BB:XX:DD:DD - максимальные AP присоединилось к 6/6

Число упрощенных точек доступа, поддерживаемых контроллером беспроводной сети, ограничено. Каждый WLC поддерживает определенное число точек доступа, которое зависит от модели и платформы. Это сообщение об ошибке появляется на WLC при получении запроса обнаружения, когда максимальное число поддерживаемых точек доступа уже достигнуто.

Ниже указано число точек доступа, поддерживаемых различными платформами и моделями WLC:

- Контроллер серии 2100 поддерживает до 6, 12 или 25 упрощенных точек доступа. Это зависит от модели контроллера.
- Контроллер 4402 поддерживает 50 упрощенных точек доступа, а контроллер 4404 – до 100. Это делает его идеальным решением для крупных предприятий и приложений большой плотности.
- Модуль беспроводных служб Catalyst 6500 (WiSM) представляет собой интегрированный коммутатор Catalyst 6500 с двумя контроллерами Cisco 4404, который поддерживает до 300 упрощенных точек доступа.
- Маршрутизатор Cisco WiSM серии 7600 представляет собой интегрированный маршрутизатор Cisco 7600 с двумя контроллерами Cisco 4404, который поддерживает до 300 упрощенных точек доступа.

- Маршрутизатор с интеграцией сервисов Cisco серии 28/37/38xx представляет собой интегрированный маршрутизатор 28/37/38xx с сетевым модулем контроллера Cisco, который поддерживает до 6, 8, 12, или 25 упрощенных точек доступа в зависимости от версии сетевого модуля. Версии, поддерживающие 8, 12 или 25 точек доступа, а также версия NME-AIR-WLC6-K9 на 6 точек доступа, снабжены быстродействующим процессором и расширенным объемом встроенной памяти по сравнению с версией NM-AIR-WLC6-K9 на 6 точек доступа.
- Интегрированный коммутатор WLC Catalyst 3750G представляет собой интегрированный коммутатор Catalyst 3750 с контроллером серии Cisco 4400, который поддерживает до 25 или 50 упрощенных точек доступа.

Дополнительные сведения

- Авторизация облегченной точки доступа (LAP) в примере конфигурации единой беспроводной сети Cisco (UWN)
- Регистрация облегченных точек доступа у контроллеру беспроводных LAN (WLC)
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.1
- Cisco Systems – техническая поддержка и документация