Часто задаваемые вопросы по системным сообщениям и сообщениям об ошибках контроллера беспроводной LAN (WLC)

Содержание

Введение

Этот документ отвечает на большинство часто задаваемых вопросов, касающихся сообщений об ошибках и системных сообщений для контроллеров беспроводных локальных сетей (WLAN), выпускаемых Cisco (WLC).

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

Вопросы по сообщениям об ошибках

Вопрос. . Мы начали преобразование больше чем 200 точек доступа (AP) от программного обеспечения Cisco IOS до Протокола Lightweight AP Protocol (LWAPP) с WLC Cisco 4404. `48 AP WLC : "[ERROR] spam_lrad.c 4212: AP cannot join because the maximum number of APs on interface 1 is reached".` Почему возникает эта ошибка?

О. Необходимо создать дополнительные интерфейсы менеджера точки доступа для поддержки больше чем 48 AP. Иначе вы будете получать ошибку такого содержания:

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Настройте несколько интерфейсов управления AP и основной/резервный порты, которые другие интерфейсы управления AP не должны использовать. *Следует обязательно создать второй интерфейс управления AP, чтобы использовать дополнительные AP.* Но, удостоверьтесь, что не накладываются ваш главный порт и конфигурации резервного порта для каждого менеджера. Другими словами, если AP - диспетчер 1 порт 1 использования как основной и порт 2 как резервная копия, AP - диспетчер 2 должен использовать порт 3 в качестве основного и порта 4 как резервная копия.

Вопрос. . У меня есть Контроллер беспроводной локальной сети (WLC) 4402, и я использую 1240 облегченных точек доступа (LAP). Во время включения 128-

битного шифрования на WLC при выборе 128-битного WEP-шифрования возникает сообщение об ошибке, в котором говорится, что 128-битное шифрование не поддерживается на 1240 точках: `[ERROR] spam_lrad.c 12839: Not creating SSID mde on CISCO AP xx:xx:xx:xx:xx:xx because WEP128 bit is not supported.` Почему появляется это сообщение?

О. Длины ключа, показанные на WLC, являются фактически количеством битов, которые находятся в общем секретном ключе и не включают 24 бита Вектора инициализации (IV). Много продуктов, который включает Продукты Aironet, называют его 128-разрядным Ключом WEP. В реальности это 104-битный ключ с 24-битным IV. Размер ключа 104 бита как раз и надо включить на WLC для 128-битного WEP-шифрования.

При выборе 128-разрядного размера ключа на WLC это - фактически 152-разрядное (128 + 24 IV) шифрование Ключа WEP. Только облегченные точки доступа Cisco 1000 серии (AP1010, AP1020, AP1030) поддерживают использование значения Ключа WEP WLC 128 битов.

Вопрос. . Почему делают я добираюсь, `WEP 128 11xx, 12xx 13xx AP . Wlan` . сообщение об ошибках, когда я пытаюсь настроить WEP на WLC?

О. На Контроллере беспроводной локальной сети, когда вы выбираете Static WEP в качестве метода безопасности уровня 2, у вас есть эти опции или Размер КЛЮЧА WEP.

- не задано
- 40 бит
- 104 бита
- 128 битов

Эти значения размера ключа не включают 24-разрядный Вектор инициализации (IV), который связан с Ключом WEP. Так, для 64-разрядного WEP необходимо выбрать **40 битов** в качестве размера Ключа WEP. Контроллер добавляет 24-разрядный IV к этому для создания 64-разрядного Ключа WEP. Точно так же для Ключа WEP на 128 битов, выберите **104 бита**.

Контроллеры также поддерживают Ключи WEP на 152 бита (128 битов + IV на 24 бита). Эта конфигурация не поддерживается на 11xx, 12xx и 13xx AP модели. Таким образом, когда вы пытаетесь настроить WEP с 144 битами, контроллер дает сообщение, что эта конфигурация WEP не выдвинута к 11xx, 12xx и 13xx AP модели.

Вопрос. . Клиенты не в состоянии аутентифицироваться на WLAN, который настроен для WPA2, и контроллер отображает `apf_80211. c : 1923 APF-1-PROC_RSN_WARP_IE_FAILED: IE WARP RSN. , RSN (WPA2) WLAN, RSN.MobileStation:00:0c:f1:0c:51:22, SSID: <>` сообщение об ошибках. Почему появляется это сообщение?

О. Это главным образом происходит из-за несовместимости на клиентской стороне. Попробуйте эти шаги для устранения этой проблемы:

- Проверьте, является ли клиент Wi-Fi, сертифицируемым для WPA2, и проверьте конфигурацию клиента для WPA2.

- Проверьте таблицу данных, чтобы видеть, поддерживает ли служебная программа клиента WPA2. Установите любое исправление, освобожденное поставщиком для поддержки WPA2. При использовании Служебной программы Windows удостоверьтесь, что вы установили исправление WPA2 от Microsoft для поддержки WPA2.
- Обновите Драйвер и Микропрограммное обеспечение клиента.
- Выключите Расширения Aironet на WLAN.

Вопрос. . Как только я перезагружаю WLC, я получаю `MFP Anomaly Detected - 3023 Invalid MIC 15:23:28 2006 17 , , 00:XX:XX:XX:XX dot11 0 AP 00:XX:XX:XX:XX 300 ,` сообщения об ошибках . Почему эта ошибка происходит и как я избавляюсь от нее?

O. Когда кадры с неправильными значениями MIC обнаружены включенными LAP MFP, это сообщение об ошибках замечено. См. защиту кадров управления (MFP) Инфраструктуры с WLC и Примером конфигурации LAP для получения дополнительной информации о MFP. Выполните один из этих четырех шагов:

1. Проверьте и удалите любые посторонние или недопустимые AP или клиентов в вашей сети, которые генерируют недопустимые кадры.
2. Отключите Инфраструктуру MFP, если MFP не включен на других участниках Группы мобильности, поскольку LAP могут услышать кадры управления от LAP других WLC в группе, которые не имеют MFP включенным. См. часто задаваемые вопросы Групп мобильности Контроллера беспроводной локальной сети (WLC) для получения дополнительной информации о Группе мобильности.
3. Исправление для этого сообщения об ошибках доступно в версиях 4.2.112.0 и 5.0.148.2 WLC. Обновите WLC к любым из этих версий.
4. Как последний параметр, попытайтесь повторно загрузить LAP, который генерирует это сообщение об ошибках.

Вопрос. . Клиентский AIR-PI21AG-E-K9 успешно связывается с точкой доступа (AP) с помощью Гибкой аутентификации через защищенное туннелирование для расширяемого протокола аутентификации (EAP-FAST). Однако, когда связанный AP выключен, клиент не перемещается к другому AP. Это сообщение постоянно появляется в журнале сообщений контроллера: `"Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - perhaps the user is already logged onto the system? Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4"`. В чем причина?

O. То, когда клиентская карта должна сделать роуминг, она передает запрос аутентификации, но она правильно не обрабатывает ключи (не сообщает AP/контроллеру, не отвечают переаутентификации).

Эта проблема описана в идентификаторе ошибки Cisco CSCsd02837 (только для зарегистрированных пользователей) . Эта ошибка была исправлена с Cisco Aironet 802.11a/b/g Мастер Установки клиентских адаптеров 3.5.

В целом сообщение `Unable to delete username for mobile` также происходит из-за любой из этих причин:

- Определенное имя пользователя используется на нескольких устройствах клиента.
- Метод аутентификации, используемый для того WLAN, имеет внешнюю анонимную идентичность. Например, в PEAP-GTC или в EAP-FAST, возможно определить обобщенное имя пользователя как внешнюю (видимую) идентичность, и реальное имя пользователя скрыто в туннеле TLS между клиентом и сервером RADIUS, таким образом, контроллер не видит его и использует его. В таких случаях может появиться это сообщение. Эта проблема замечается более обычно с некоторой третьей стороной и некоторым клиентом старой микропрограммы.

Вопрос. . Когда я устанавливаю новый Модуль беспроводных сервисов (WiSM) блейд в этих 6509 коммутаторах и внедряю Защищенный расширяемый протокол аутентификации (PEAP) с сервером Microsoft IAS, я получаю эту ошибку: **`*1 0:00:23.526: %LWAPP-5-CHANGED: LWAPP *1 0:00:23.700: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT. Reload Reason: FAILED CRYPTO INIT. *1 0:00:23.700: %LWAPP-5-CHANGED: LWAPP *1 0:00:23.528: %LWAPP-5-CHANGED: LWAPP *1 0:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs certs SSC *1 0:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *1 0:00:23.557: lwapp_crypto_init: PKI_StartSession *1 0:00:23.706: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.`**. В чем причина?

O. RADIUS и отладки dot1x показывают, что WLC отправляет запрос доступа, но от сервера IAS нет никакого ответа. Чтобы устранить данную проблему, проделайте следующие действия:

1. Проверьте конфигурацию сервера IAS.
2. Проверьте файл журнала.
3. Установите ПО, такое как Ethereal, которое сообщит подробные данные об аутентификации.
4. Остановите и запустите сервис IAS.

Вопрос. . Облегченные точки доступа (LAP) не регистрируются в контроллере. Какова могла бы быть проблема? Я вижу эти сообщения об ошибках на контроллере: **`3 3:20:47 2028: LWAPP CERTIFICATE_PAYLOAD AP 00:0b:85:68:f4:f0. 3 3:20:47 2028: Unable to free public key for AP 00:0B:85:68:F4:F0.`**

O. Когда точка доступа (AP) передает Протокол LWAPP, Соединяют Запрос с WLC, это встраивает свой сертификат X.509 в сообщение LWAPP. Это также генерирует случайный идентификатор сеанса, который включен в Запрос на присоединение 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. Он также смотрит на дату и время начала периода действительности сертификата AP и сравнивает их с собственными показателями даты и времени.

Эта проблема может произойти из-за неправильного параметра времени на WLC. **Чтобы настроить часы на WLC, воспользуйтесь командами show time и config time.**

Вопрос. . AP Протокола LWAPP неспособен присоединиться к своему контроллеру. Журнал Контроллера беспроводной локальной сети (WLC) отображает сообщение, подобное этому: **`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01.`** В чем причина?

О. Если туннель LWAPP между AP и WLC пересекает сетевой путь с MTU менее чем 1500 байтов, можно получить это сообщение об ошибках. Это вызывает фрагментацию пакетов LWAPP. Это - известная ошибка в контроллере. См. идентификатор ошибки Cisco CSCsd39911 (только зарегистрированные клиенты).

Решением будет обновить микропрограмму контроллера до 4.0(155).

Вопрос. . Я пытаюсь установить гостевое туннелирование между своим внутренним контроллером и действительным якорным контроллером на De-Militarized Zone (DMZ). Однако когда пользователь пытается ассоциироваться с гостевым SSID, он не может получить IP-адрес из DMZ, что ожидалось. Таким образом, пользовательский трафик не туннелируется на контроллер на DMZ. Выходные данные команды debug mobile handoff содержат следующее сообщение: `WLAN <ID Wlan>. IP : <controller Ip address> Ignored.` В чем проблема?

О. Гостевое туннелирование предоставляет дополнительные меры безопасности для доступа гостя к корпоративной беспроводной сети. Это помогает убедиться в том, что гостевые пользователи не могут входить в корпоративную сеть без предварительного прохождения через корпоративный брандмауэр. Когда пользователь ассоциируется с WLAN, которая назначена как гостевая WLAN, пользовательский трафик туннелируется на контроллер WLAN, который находится на DMZ за пределами корпоративного брандмауэра.

С учетом этого сценария можно указать несколько причин неправильной работы гостевого туннелирования. **Как следует из выходных данных команды debug, проблема может заключаться в несоответствии какой-либо из политик безопасности, настроенных для этой конкретной WLAN, как во внутренних контроллерах, так и в контроллерах DMZ.** Проверьте, совпадают ли политики безопасности и другие настройки, такие как установки ожидания сеанса.

Другая распространенная причина этой проблемы - то, что контроллер DMZ не указан для себя якорным для этой конкретной WLAN. Для того чтобы гостевое туннелирование работало правильно, а DMZ администрировала IP-адрес пользователя (который относится к гостевой WLAN), важно, чтобы для конкретной WLAN был правильно указан якорь.

Вопрос. . Я вижу, что много " " сообщения на Контроллере беспроводной локальной сети (WLC) 2006 года, но не на этих 4400 WLC. В чем причина? Многоадресное вещание на контроллерах отключено. В чем разница между многоадресными пределами очереди на платформах WLC 2006 и 4400?

О. Поскольку переданный в многоадресном режиме отключен на контроллерах, сообщения, которые вызывают этот сигнал тревоги, могли бы быть сообщениями Протокола ARP. Разницы в глубине очереди (512 пакетов) между WLC 2000 и 4400 нет. Разница в том, что 4400 NPU фильтрует пакеты ARP, в то время как на 2006 все делается в программном обеспечении. Это объясняет, почему WLC 2006 видит сообщения, а 4400 - нет. WLC 44xx обрабатывает многоадресные пакеты аппаратно (через ЦП). WLC 2000 обрабатывает многоадресные пакеты программное. Обработка ЦПУ более эффективна, чем программное обеспечение. Поэтому очередь 4400 очищена быстрее, тогда как WLC 2006 года борется немного, когда это видит много этих сообщений.

Вопрос. . Я вижу" [] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] 1, AP, ". сообщение об ошибках в одном из моих контроллеров. Что означает эта ошибка и какие шаги я должен сделать для решения его?

О. Это сообщение замечено, когда контроллер получает запрос DHCP для MAC-адреса, для которого это не имеет механизма состояний. Его часто видно с моста или из системы, которая работает под управлением виртуальной машины типа VMWare. Контроллер слушает DHCP-запросы, поскольку он обрабатывает отслеживание DHCP и знает, какие адреса ассоциированы с клиентами, которые привязаны к его AP. Весь трафик для беспроводных клиентов проходит через контроллер. Когда назначением пакета является беспроводной клиент, он идет на контроллер и затем проходит через туннель LWAPP на AP и с нее к клиенту. **Единственное, что можно сделать при появлении этого сообщения - с помощью ввода на коммутаторе команды switchport vlan allow разрешить VLAN, которые используются на контроллере, на транке, который идет на контроллер.**

Вопрос. . Почему делают я вижу это сообщение об ошибках на консоли: ' ' , = 0x0050b986 = 0xfffffffc?

О. Это может произойти из-за высокой загрузки ЦП. Когда ЦП контроллера в большой степени загружен такой как тогда, когда он делает архивные экземпляры или другие задачи, он не имеет времени для обработки всех ACK, которые NPU передает в ответ на сообщения настройки. Когда это происходит, ЦП генерирует сообщения об ошибке. Однако они не влияют на обслуживание или функциональность.

Это описано в разделе "Сильно загруженный ЦП контроллера" документа "Примечания к версии для контроллеров Cisco Wireless LAN и упрощенных точек доступа для версии 3.2.116.21".

Вопрос. . Я получаю эти сообщения об ошибках ключа Протокола WEP на своей беспроводной системе управления (WCS): WEP, , . Station MAC Address is 'xx:xx:xx:xx:xx:xx', AP base radio MAC is 'xx:xx:xx:xx:xx:xx' and Slot ID is '1'. Однако я не использую WEP в качестве параметра безопасности в моей сети. Я только использую Защищенный доступ по протоколу Wi-Fi (WAP). Почему я получаю эти сообщения об ошибках WEP?

О. Если все ваши связанные конфигурации безопасности совершенны, сообщения, которые вы получаете прямо сейчас, из-за дефектов. Существует несколько известных ошибок в контроллере. См. идентификаторы ошибки Cisco CSCse17260 (только для зарегистрированных клиентов) и CSCse11202 (только для зарегистрированных клиентов), под названием "Настроенный на станции WEP-ключ может быть несовместим с клиентами WPA и TKIP соответственно". **В принципе, CSCse17260 дублирует CSCse11202. Исправление для CSCse11202 уже доступно в релизе WLC 3.2.171.5.**

Примечание: Последние версии WLC имеют исправление для этих дефектов.

Вопрос. . Мы используем внешний сервер RADIUS для аутентификации беспроводных клиентов через контроллер. : "no radius servers are responding". ?

О. Когда запрос идет из WLC в сервер RADIUS, каждый пакет имеет порядковый номер, на

который WLC ожидает ответ. , "radius-server not responding".

Время по умолчанию ожидания WLC ответа от сервера RADIUS - 2 секунды. **Оно устанавливается из графического интерфейса WLC в разделе Security > authentication-server.** Максимальное значение - 30 секунд. Таким образом, для разрешения проблемы может быть полезно установить это ожидание на максимум.

Иногда серверы RADIUS производят 'silent discards' пакета запроса, который приходит от WLC. Сервер RADIUS может отклонять эти пакеты из-за несовпадения сертификатов и по некоторым другим причинам. Это правомочное действие со стороны сервера. Кроме того, в таких случаях контроллер будет помечать сервер RADIUS как "not responding".

Чтобы разрешить проблему silent discards, отключите функцию aggressive failover в WLC.

Если функция aggressive failover включена на WLC, он будет помечать сервер AAA как "not responding" слишком часто. Однако этого не стоит делать, поскольку сервер AAA может не отвечать только этому конкретному клиенту (методом silent discard). Он может отвечать другим действительным клиентам (с действительными сертификатами). Однако WLC может все же пометить сервер AAA как "not responding" и недействующий.

Чтобы избежать этого, отключите функцию aggressive failover. Выполните **команду config radius aggressive-failover disable** от CLI контроллера для выполнения этого. Если функция отключена, то контроллер будет просто переходить на следующий сервер AAA, если три клиента последовательно не смогут получить отклик от сервера RADIUS.

Вопрос. . Несколько клиентов неспособны связаться к LWAPP, и контроллер регистрирует `IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt` сообщение об ошибках. Почему это происходит?

О. Это главным образом происходит из-за проблемы с адаптерами Intel, которые поддерживают CCX v4, но то выполнение клиентская версия комплекта ранее, чем 10.5.1.0. При обновлении программного обеспечения к 10.5.1.0 или позже это исправляет эту проблему. См. идентификатор ошибки Cisco CSCsi91347 (только зарегистрированные клиенты) для получения дополнительной информации об этом сообщении об ошибках.

Вопрос. . Я вижу это сообщение об ошибках на Контроллере беспроводной локальной сети (WLC): `EAP Max (21) STA 00:05:4e:42:ad:c5`. В чем причина?

О. Это сообщение об ошибках происходит, когда пользователь пытается соединиться с EAP, защитил сеть WLAN и отказал предварительно сконфигурированное количество попыток EAP. Когда пользователь не в состоянии аутентифицироваться, контроллер исключает клиента, и клиент не может соединиться с сетью, пока таймер исключения не истекает или вручную отвергнут администратором.

Исключение опознает попытки аутентификации, сделанные отдельным устройством. Когда устройство превышает максимальное число отказов, этому MAC-адресу больше не разрешается ассоциироваться.

Исключение происходит:

- После 5 последовательных отказов аутентификации для общих аутентификаций (6-я

попытка исключается)
- После 5 последовательных отказов ассоциации для MAC-аутентификаций (6-я попытка исключается)
- После 3 последовательных отказов аутентификации EAP/802.1X (4-я попытка исключается)
- При любом отказе внешней политики сервера (NAC)
- При любых дублированных экземплярах IP-адресов
- После 3 последовательных отказов веб-аутентификации (4-я попытка исключается)

Можно настроить таймер срока исключения клиента, и исключение можно включать и отключать на контроллере или на уровне WLAN.

Вопрос. . Я вижу это сообщение об ошибках на Контроллере беспроводной локальной сети (WLC): `1 WLCSCH01/10.0.16.5, '10.0.16.5'. RADIUS server(s) are not responding to authentication requests.` В чем проблема?

О. Это мог бы быть из-за идентификатора ошибки Cisco CSCsc05495. Из-за нее контроллер периодически вставляет неправильные AV-Pair (атрибут 24, "state") в сообщения запроса аутентификации, что нарушает работу RADIUS RFP и вызывает проблемы для некоторых серверов аутентификации. Эта ошибка исправлена в версии 3.2.179.6.

Вопрос. . Я получаю Шумовое сообщение об ошибках Профиля под Монитором> 802.11b/g Радио. Почему возникает сообщение FAILED?

О. Шумовой Профиль ОТКАЗАЛ/ПЕРЕДАЛ, статус установлен после результата тестирования, сделанного WLC и по сравнению с текущим порогом набора. По умолчанию Шумовое значение установлено в-70. Неисправное состояние указывает, что было превышено пороговое значение для того конкретного параметра или точки доступа (AP). Вы можете скорректировать параметры в профиле, но рекомендуется изменять настройки после полного прояснения схемы сети и того, как эти изменения повлияют на ее производительность.

Пороговые значения статуса PASSED/FAILED управления радиоресурсами (RRM) можно установить для всех точек доступа одновременно на страницах 802.11a Global Parameters > Auto RF и 802.11b/g Global Parameters > Auto RF. Пороговые значения статуса PASSED/FAILED управления радиоресурсами (RRM) можно установить для каждой точки доступа отдельно на странице 802.11 AP Interfaces > Performance Profile.

Вопрос. . Я могу порт 2 "not set" как резервный порт для интерфейса менеджера точки доступа. `"Could not set port configuration".` Можно установить порт 2 в качестве резервного для интерфейса управления. Текущий активный порт для обоих интерфейсов - 1. Почему?

О. AP - диспетчер не имеет резервного порта. Он поддерживался в более ранних версиях. Начиная с версии 4.0 и в более поздних резервный порт для интерфейса AP-менеджера не поддерживается. Как правило, на каждом порте должен быть настоен один AP-менеджер (без резервов). При использовании LAG есть только один AP-менеджер.

Статический (или постоянный) интерфейс AP-менеджера должен быть назначен порту 1 системы распространения и иметь уникальный IP-адрес. Его нельзя сопоставить

резервному порту. Он обычно настраивается в той же VLAN или IP-подсети, что и интерфейс управления, но это не обязательное требование.

Вопрос. . Я вижу это сообщение об ошибках: **AP '00:0b:85:67:6b:b0' MIC WPA '1' '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds.** В чем причина?

O. Message Integrity Check (MIC), включенный в Защищенный доступ по протоколу Wi-Fi (WAP), включает счетчик кадра, который предотвращает атаку по перехвату и возможному изменению передаваемых данных. Эта ошибка означает, что кто-то в сети пытается повторить сообщение, которое было послано исходным клиентом, или это может означать, что клиент неисправен.

Если клиент неоднократно отказывает проверку MIC, контроллер отключает WLAN на интерфейсе AP, где ошибки обнаружены в течение 60 секунд. Первый сбой MIC зарегистрирован, и таймер инициируется для включения осуществления контрмер. Если последующий сбой MIC произойдет в течение 60 секунд после нового предыдущего сбоя, то STA, объект IEEE 802.1X которого действовал как Соискатель, должен быть deauthenticate сам или deauthenticate весь STAs с сопоставлением безопасности, если его объект IEEE 802.1X действовал как Средство проверки подлинности.

Кроме того, устройство не получает или передает любые кадры зашифрованных данных TKIP, и не получает или передает любые незашифрованные фреймы данных кроме сообщений IEEE 802.1X, к или от любого узла сроком на по крайней мере 60 секунд после того, как это обнаружит второе неудачное завершение. Если устройство является AP, оно запрещает новые ассоциации с TKIP в течение периода этих 60 секунд; в конце периода этих 60 секунд AP возобновляет нормальные работы и позволяет STAs (ре) партнер.

Это предотвращает возможную атаку на схему шифрования. Эти ошибки MIC не могут быть выключены в версиях WLC до 4.1. С версией 4.1 Контроллера беспроводной локальной сети и позже, существует команда для изменения времени просмотра для ошибок MIC. Команда является **config wlan безопасность tkip удержание <0-60 секунд> <wlan идентификатор>**. Используйте значение 0 для отключения обнаружения ошибок MIC для контрмер.

Вопрос. . Это сообщение об ошибках замечено в моих журналах контроллера: **[] dhcp_support.c 357: dhcp_bind (): servPort dhcpstate failed.** В чем причина?

O. Когда сервисному порту контроллера включили DHCP, но не получает IP-адрес от сервера DHCP, эти сообщения об ошибках главным образом замечены.

По умолчанию физический интерфейс порта служб имеет установленного клиента DHCP и ищет адрес через DHCP. WLC пытается запросить адрес DHCP для порта служб. Если DHCP-сервер недоступен, то запрос DHCP для порта служб получает отказ. Таким образом, генерируется сообщение об ошибке.

Обходной путь - настроить статический IP-адрес для порта служб (даже если этот порт отсоединен) или иметь сервер DHCP, который может назначить IP-адрес порту служб. Затем при необходимости перезагрузите контроллер.

Порт служб, в приципе, зарезервирован для внеполосного управления и восстановления системы, а также обслуживания в случае отказа сети. Это также единственный порт, который остается активным, когда контроллер находится в режиме перезагрузки. Порт

служб не поддерживает метки 802.1Q. Таким образом, он должен быть подключен к порту доступа на соседском коммутаторе. Использование порта служб необязательно.

Интерфейс порта служб управляет коммуникациями и статически сопоставляется системой порту служб. Он должен иметь IP-адрес в подсети, отличной от подсетей управления, AP-менеджера и любого динамического интерфейса. Кроме того, его нельзя сопоставить резервному порту. Порт служб может использовать DHCP, чтобы получить IP-адрес, или ему может быть назначен статический IP-адрес, но интерфейсу порта служб не может быть назначен шлюз по умолчанию. Статические маршруты для удаленного доступа сети к порту служб могут быть определены через контроллер.

Вопрос. . Мои беспроводные клиенты не в состоянии соединиться с сетью (WLAN) беспроводной локальной сети. WiSM, что точка доступа (AP) связана с отчётами это сообщение: **`Dos NAV AP MAC 00:0g:23:05:7d:d0, ID 0 MAC 00:00:00:00:00:00`**. Что это означает?

O. Как условие обратиться к среде, MAC - уровень проверяет значение своего сетевого вектора выделения (NAV). NAV является встречным резидентным объектом в каждой станции, которая представляет период времени, что предыдущий кадр должен передать свой кадр. NAV должен быть нулем, прежде чем станция сможет попытаться передать кадр. Перед передачей кадра станция вычисляет период времени, необходимый для передачи кадра на основе длины и скорости передачи данных кадра. Станция размещает значение, которое представляет на этот раз в поле продолжительности в заголовке кадра. Когда станции принимают кадр, они исследуют это значение поля продолжительности и используют его в качестве основания для установки их соответствующего NAVs. Этот процесс резервирует среду для посылающей станции.

Высокий NAV указывает на присутствие расширенного значения NAV (действительный механизм с обнаружением несущей для 802.11). Если MAC-адрес сообщил, 00:00:00:00:00:00, он, вероятно, имитируется (потенциально реальная атака), и необходимо подтвердить это с захватом пакета.

Вопрос. . После того, как мы настроим контроллер и перезагрузим его, мы не в состоянии обратиться к контроллеру в безопасной сети (https) режим. В то время как попытка обратиться к контроллеру защищает веб-режим, это сообщение об ошибках получено: **`: Web Authentication Certificate not found (error).`** Какова причина для этой проблемы?

O. Может быть несколько причин, привязанных к этой проблеме. Одна обычная причина может быть отнесена к конфигурации виртуального интерфейса контроллера. Для решения этой проблемы удалите виртуальный интерфейс и затем восстановите его с этой командой:

```
WLC>config interface address virtual 1.1.1.1
```

Затем перезагрузите контроллер. После того, как контроллер перезагружен, восстановите webauth сертификат локально на контроллере с этой командой:

```
WLC>config certificate generate webauth
```

В выходных данных этой команды необходимо видеть это сообщение: `Web Authentication certificate has been generated.`

Теперь, должна существовать возможность для доступа к безопасному веб-режиму

контроллера на перезагрузку.

Вопрос. . Контроллеры иногда сообщают об этом сигнальном сообщении атаки Подписи Лавинной рассылки Разъединения IDS против допустимых клиентов, в которых MAC-адрес атакующего является MAC-адресом точки доступа (AP), соединенной с тем контроллером: `.alert: IDS 'Disassoc ' , AP' < '802.11b/g'' name> AP 'x. x. x. x. ' ' 'x'. The attacker's mac address is 'hh:hh:hh:hh:hh:hh', channel number is 'x', and the number of detections is 'x'.` Почему это происходит?

O. Это вызвано тем, что идентификатора ошибки Cisco CSCsg81953 (только зарегистрированные клиенты).

О Лавинных атаках Разъединения IDS против допустимых клиентов иногда сообщают, где MAC-адрес атакующего является MAC-адресом AP, соединенного с тем контроллером.

Когда клиент будет привязан к AP, но прекратит связываться из-за извлечения карты, бродя из диапазона, и т.д. к AP, AP будет ждать до времени простоя. Как только время простоя достигнуто, AP передает тому клиенту разъединять кадр. Когда клиент не подтверждает разъединять кадр, AP повторно передает кадр многочисленные времена (приблизительно 60 кадров). Подсистема IDS контроллера слышит, что они повторно передают и предупреждают с этим сообщением.

Этот дефект решен в версии 4.0.217.0. Обновите свою версию Контроллера к этой версии для преодоления этого сигнального сообщения против допустимых клиентов и AP.

Вопрос. . Я получаю это сообщение об ошибках в системном журнале контроллера: `[] apf_80211.c 2408: <xx:xx:xx:xx:xx:xx> [] apf_utils.c 198: Missing Supported Rate.` В чем причина?

O. Фактически, сообщения указывают, что WLC настроен для определенных скоростей требуемых данных при беспроводных параметрах настройки, но плата NIC пропускает требуемую скорость.

Если вы имеете скорости передачи данных, такой как 1 и 2M, устанавливаете для требуемого на контроллере, но плата NIC не связывается на этих скоростях передачи данных, можно получить этот тип сообщения. Это - неверное поведение платы NIC. С другой стороны, если ваш контроллер является 802.11g, включен, и клиент 802.11b (только) карта, это - легитимное сообщение. Если эти сообщения не вызывают проблем, и карты могут все еще соединиться, эти сообщения могут быть проигнорированы. Если сообщения являются определенной картой, то удостоверьтесь, что драйвер для этой карты актуален.

Вопрос. . Этот системный журнал `AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: : WLAN <>`, сообщение об ошибках передано в нашей сети. Почему это происходит и как я останавливаю его?

O. Это сообщение передано LAP. Это замечено при настройке функции замены WLAN WLAN и что не объявлен определенный WLAN.

Настройте `config ap syslog host global 0.0.0.0` для остановки его, или можно поместить определенный IP-адрес, если у вас есть сервер системного журнала так, чтобы сообщение

было передано к одному только серверу.

Вопрос. . Я получаю это сообщение об ошибках на своем контроллере беспроводной локальной сети (WLC): `[] : apf_mm. c : : 581: Announce collision for mobile 00:90:7a:05:56:8a, deleting.` В чем причина?

О. Обычно это сообщение об ошибках указывает, что контроллер объявил о коллизиях для беспроводного клиента (т.е. отдельные AP объявляют, что у них есть клиент), и контроллер не получил handoff от одного AP до следующего. Нет никакого состояния сети для поддержания. Удалите беспроводного клиента и сделайте, чтобы клиент попробовал еще раз. Если эта проблема часто происходит, может быть проблема с конфигурацией мобильности. В противном случае это могла бы быть аномалия, которая отнесена определенному клиенту или условию.

Вопрос. . Мой контроллер повышает это аварийное сообщение: `'12'` . Какова эта ошибка и как она может быть решена?

О. Когда клиентское Отношение сигнала к шуму (SNR) падает ниже порогового значения SNR для определенного радио, это аварийное сообщение повышено. 12 пороговое значение SNR по умолчанию для обнаружения дыры покрытия.

Алгоритм обнаружения и исправления дыры покрытия определяет, существует ли дыра покрытия, когда Уровни отношения сигнал-шум клиентов проходят ниже данного порога SNR. Этот порог SNR варьируется на основе двух значений: мощность передачи AP и покрытие контроллера представляют значение.

Подробно, Клиентский порог SNR определен мощностью передачи каждого AP (представленный в ДБм) минус постоянное значение 17dBm, минус конфигурируемое пользователем значение профиля Покрытия (это значение принято значение по умолчанию к 12 дБ).

- **Клиентское Значение Сокращения SNR (|dB |) = [Мощность передачи AP (дБм) – Постоянный (17 дБм) – Профиль Покрытия (дБ)]**

К этому конфигурируемому пользователем значению профиля покрытия можно обратиться этот путь:

1. **В графическом интерфейсе контроллера перейдите к главному заголовку Wireless и выберите параметр Network в элементе выбора стандарта сети (802.11a или 802.11b/g) слева. Затем выберите Auto RF (Автоматический выбор радиочастоты) в верхнем правом углу окна.**
2. На Автоматической странице Глобальных параметров RF найдите Пороговый раздел Профиля. В этом разделе можно найти Покрытие (3 - 50 dbm) значением. Это значение является конфигурируемым пользователем значением профиля покрытия.
3. Это значение может быть отредактировано для влияния на Клиентское пороговое значение SNR. Другой способ влиять на этот порог SNR состоит в том, чтобы увеличить мощность передачи и компенсировать обнаружение дыры покрытия.

Вопрос. . Я использую ACS v 4.1 и 4402 Контроллера беспроводной локальной сети (WLC). Когда WLC пытается к MAC - аутентифицируют беспроводного

клиента на ACS 4.1, ACS не в состоянии отвечать ACS и сообщает об этом сообщении об ошибках: "*Внутренняя ошибка произошла*". У меня есть все свои корректные конфигурации. Почему происходит эта внутренняя ошибка?

O. Существует отнесенный идентификатор ошибки Cisco аутентификации CSCsh62641 (только зарегистрированные клиенты) в ACS 4.1, где ACS дает , сообщение об ошибках.

Этот дефект мог бы быть проблемой. Существует исправление, доступное для этого дефекта на Загрузках ACS 4.1 (только зарегистрированные клиенты) страница, которая должна решить проблему.

Вопрос. . Контроллер беспроводной локальной сети Cisco серии 4400 (WLC) не загрузится. Это сообщение об ошибках получено на контроллере: `** 0:4 fatload ** ( IRQ) dev 0 blk 0: 0x51 reg: 10 ** Can't read from device 0.` В чем причина?

O. Причина для этой ошибки могла бы быть проблемой аппаратных средств. Откройте кэйс TAC (Центра технической поддержки) для дальнейшего устренения этой проблемы. Для открытия кэйса TAC (Центра технической поддержки) у вас должен быть корректный контракт с Cisco. См. Техническую поддержку для контакта с Центром технической поддержки Cisco.

Вопрос. . Контроллер беспроводной локальной сети (WLC) сталкивается с проблемами буфера памяти. При заполнении буферов памяти происходит сбой контроллера и для продолжения работы необходима перезагрузка. В файле журнала можно увидеть следующие сообщения об ошибках: `Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537: Cannot allocate new Mbuf. Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet: no free Mbufs.` В чем причина?

O. Это происходит из-за идентификатора ошибки Cisco CSCsh93980 (только зарегистрированные клиенты). Этот дефект был решен в версии 4.1.185.0 WLC. Обновите свой Контроллер к этой версии программного обеспечения или позже для преодоления этого сообщения.

Вопрос. . Мы выполнили обновление наших 4400 Контроллера беспроводной локальной сети (WLC) к 4.1 кодам, и наш системный журнал был засыпан сообщениями, такими как это: `May 03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.233/TPA 192.168.1.233.` Что означают эти сообщения?

O. Когда WLAN отмечен как требуемый DHCP, это может произойти. В таких случаях только станциям, которые получают IP-адрес через DHCP, позволяют связаться. Статическим клиентам не разрешают связаться к этому WLAN. WLC действует как агент ретрансляции DHCP и IP-адрес записей всех станций. Это сообщение об ошибках генерируется, когда WLC получает запрос ARP от станции, прежде чем WLC получил пакеты DHCP от станции и сделал запись ее IP-адреса.

Вопрос. . При использовании Питания над Ethernet (PoE) на Контроллере беспроводной локальной сети Cisco 2106 радио AP не включены. `: AP is`

unable to verify sufficient in-line power. Radio slot disabled. Как устранить эту проблему?

О. Это сообщение об ошибках происходит, когда коммутатор, который включает точку доступа, является предстандартным коммутатором, но AP не поддерживает Предварительный стандартный режим мощности на входе.

Коммутатор предварительного стандарта Cisco не поддерживает интеллектуальное управление электропитанием (IPM), но имеет достаточную мощность для питания стандартной точки доступа.

Необходимо включить режим питания Pre-Standard (Предварительный стандарт) для точки доступа, указанной в сообщении об ошибке. Это может быть сделано из интерфейса командной строки контроллера, с помощью команды config ap power pre-standard {enable | disable} {all | Cisco_AP}.

При обновлении программного обеспечения до версии 4.1 данная команда должна быть введена заранее, при необходимости. Однако, возможно, что вам придется использовать эту команду при новой установке программного обеспечения или после сброса настроек точки доступа на заводские.

Доступны следующие 15-ваттные коммутаторы предварительного стандарта Cisco:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

Вопрос. . Контроллер генерирует **dtl_arp. c : 2003 dtl-3-npuarp_add_failed: ARP xx:xx.-xxx.x . .** сообщение системного журнала, подобное этому. Что означает это сообщение системного журнала?

О. В то время как некоторый беспроводной клиент передает ответ ARP, Модуль сетевого процессора (NPU) должен знать тот ответ. Поэтому ответ ARP отправляется сетевому процессору NPU, но программному обеспечению контроллера WLC не следует выполнять попытку добавления этой записи в сетевой процессор. Если это происходит, то выводятся данные сообщения. Эта ситуация не влияет на функциональность контроллера WLC, но WLC приходится генерировать это сообщение для системного журнала.

Вопрос. . Я установил и настроил новый WLC Cisco 2106. WLC указывает, что отказал температурный датчик. Когда вы входите в веб-интерфейс в соответствии со "сводкой контроллера", это говорит ", " следующий за внутренней температурой. Все остальное, кажется, обычно функционирует.

О. Отказ датчика внутренней температуры является косметическим и может быть решен с

обновлением к версии 4.2.61.0 WLC.

WLC 2106 и **основанный** WLC 526 **или после 01.07.2007** могут использовать микросхему температурного датчика от другого поставщика. Этот новый датчик хорошо работает, но не совместим с программным обеспечением позже, чем эти 4.2 выпуска. Следовательно, более старое программное обеспечение не в состоянии считать температуру и показывает эту ошибку. На всю другую функциональность контроллера не влияет этот дефект.

Существует известный идентификатор ошибки Cisco CSCsk97299 (только зарегистрированные клиенты), отнесенные к этой проблеме. Этот дефект упомянут в Комментариях к выпуску версии 4.2 WLC.

Вопрос. . Я получаю `radius_db. c : 1823 AAA-5-RADSERVER_NOT_FOUND: RADIUS WLAN < WLAN> - "` сообщением для ALL SSIDs. Это сообщение появляется даже для SSIDs, которые не используют AAA-серверы.

O. Это сообщение об ошибках означает, что контроллер не смог связаться с сервером радиуса по умолчанию или что каждый не был определен.

Одна возможная причина для этого поведения является идентификатором ошибки Cisco CSCsk08181 (только зарегистрированные клиенты), который был решен в версии 4.2. Обновите свой контроллер к версии 4.2.

Вопрос. `. : 10 17:55:00.725 sim. c : 1061 SIM-3-MACADDR_GET_FAIL: 1 MAC- .` сообщение об ошибках появляется на Контроллере беспроводной локальной сети (WLC). Что это означает?

O. Это означает, что контроллер имел ошибку, в то время как он передал полученный пакет ЦП.

Вопрос. . Эти сообщения об ошибках появляются на Контроллере беспроводной локальной сети (WLC):

- `Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'cliWebInitParms.cfg'`
- `Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'rfidInitParms.cfg'`
- `Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'dhcpParms.cfg'`
- `Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: Failed to read configuration file 'bcastInitParms.cfg'`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file : sshpmInitParms.cfg. file removal failed. -Process: Name:fp_main_task, Id:11ca7618`
- `Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file : bcastInitParms.cfg. file removal failed. -Process: Name:fp_main_task, Id:11ca7618`

На что они сообщение об ошибках указывают?

O. Эти сообщения являются информационными сообщениями и являются частью обычной процедуры загрузки. Эти сообщения, кажется, из-за сбоя читают или удаляют несколько других файлов конфигурации. Когда файлы определенной конфигурации не найдены или если файл конфигурации не может быть считан, последовательность config для каждого процесса отсылает это сообщение, например, никакой config сервера DHCP, никакие метки (ID RF) config, и т.д. Это сообщения низкой степени серьезности, которые могут безопасно

быть проигнорированы. Эти сообщения не прерывают использование контроллера.

Вопрос. . `HE6-WLC01, local0, , 2008-07-25,12:48:18, apf_rogue. c : 740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN: 00:14:XX:02:XX:XX - AP .` сообщение об ошибках появляется. Что это означает?

O. Это означает, что AP, который выполнил постороннюю функцию включения, больше не доступен, и контроллер не может найти, что любой подходящий AP выполняет постороннее включение.

Вопрос. . `DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1), SPA 192.168.1.152/TPA 192.168.0.206` системных сообщения, появляется на Контроллере беспроводной локальной сети. Что подразумевает это сообщение?

O. Возможно, что система обнаружила спуфинг ARP или отравление. Но, это сообщение не обязательно подразумевает, что произошел любой злонамеренный спуфинг ARP. Когда эти условия истинны, сообщение появляется:

- WLAN настроен с Требуемым DHCP, и устройство клиента, после соединения на том WLAN, передает сообщение ARP без первого DHCP завершения. Это может быть нормальным поведением; это может произойти, например, когда клиент статически обращен, или когда клиент держит допустимую аренду DHCP от предшествующей ассоциации. Сообщение об ошибках может быть похожим на данный пример:`DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206`Эффект этого условия состоит в том, что клиент неспособен передать или получить любой трафик данных до него DHCPs через WLC.См. DTL передает раздел Руководства по системным сообщениям контроллера беспроводной локальной сети Cisco для получения дополнительной информации.

Вопрос. . LAP не используют Питание над Ethernet (POE) для включений. Я вижу вход в систему Контроллера беспроводной локальной сети: `AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power` В чем проблема?

O. Если параметры настройки Питания над Ethernet (POE) не настроены правильно, это может произойти. Когда точка доступа, которая была преобразована в облегченный режим, например, AP1131 или AP1242 или точку доступа серии 1250, приведена в действие инжектором питания, который связан с Cisco предынтеллектуальное Управление питанием (предIPM) коммутатор, необходимо настроить Питание над Ethernet (PoE), также известное как встроенное питание.

См. Питание Настройки над Ethernet для получения дополнительной информации о том, как настроить Питание над Ethernet (POE).

Вопрос. . Вы видите это сообщение на Контроллере беспроводной локальной сети (WLC): `*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6` Что это означает?

О. Облегченные точки доступа придерживаются определенного алгоритма для обнаружения контроллера. Процесс обнаружения и соединения объяснен подробно в регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC)

Это сообщение об ошибке появляется на WLC при получении запроса обнаружения, когда максимальное число поддерживаемых точек доступа уже достигнуто.

Если главный контроллер для LAP не настроен или если это - новое из LAP коробки, это отсылает запросы обнаружения LWAPP во все достижимые контроллеры. Если запросы на обнаружение достигают контроллера, который выполняется в его полной емкости AP, WLC получает запросы и понимает, что это в его максимальной емкости AP, и не отвечает на запрос и дает эту ошибку.

Вопрос. . Где я могу найти дополнительные сведения о системных сообщениях LWAPP?

О. См. Руководство по системным сообщениям контроллера беспроводной локальной сети Cisco, 4.2 для получения дополнительной информации о Системных сообщениях LWAPP.

Вопрос. . `webauth` сообщения об ошибках появляется на Контроллере беспроводной локальной сети (WLC). Что это означает?

О. WLC не в состоянии загружать Пользовательскую Web-аутентификацию / Транзитная связка (bundle), если кто-либо из связанных файлов имеет больше, чем 30 символов в имени файла, которое включает расширение файла. Специализированная веб-подлинная связка (bundle) имеет предел до 30 символов для имен файлов. Гарантируйте, что никакие имена файлов в связке (bundle) не больше, чем 30 символов.

Вопрос. . Контроллеры беспроводной локальной сети (WLC), выполняя 5.2 или 6.0 кодов с большим числом групп точек доступа, веб-GUI может не отобразить все настроенные группы точек доступа. В чем проблема?

О. Недостающие группы точек доступа могут быть замечены при использовании **команды show wlan ap-groups** CLI.

Попытайтесь добавить одну дополнительную группу точек доступа к списку. Например, 51 группа точек доступа развернулась, и 51-е отсутствует (Страница 3). Добавьте 52-ю группу, и Страница 3 должна появиться в веб-GUI.

Для решения этого вопроса обновите к версии 7.0.220.0 WLC.

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Вопросы и ответы по устранению неполадок WiSM
- Wireless LAN Controller (WLC) Troubleshoot FAQ
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация