Вопросы и ответы по ошибкам и системным сообщениям контроллера беспроводной LAN

Вопросы

Введение
Вопросы и ответы по сообщениям об ошибках
Дополнительные сведения

Введение

Данный документ содержит вопросы и ответы по ошибкам и системным сообщениям контроллеров Cisco Wireless LAN (WLC).

Дополнительную информацию о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

Вопросы и ответы по сообщениям об ошибках

Вопрос. Мы начали перевод более чем 200 точек доступа с ПО Cisco IOS® на облегченный протокол точек доступа (LWAPP) с Cisco 4404 WLC. Мы завершили перевод 48 точек доступа, после чего получили следующее сообщение на WLC: `[ERROR] spam_lrad.c 4212: AP cannot join because the maximum number of APs on interface 1 is reached` Точка доступа не может быть добавлена, т.к. достигнуто максимальное количество точек доступа на интерфейсе 1. Почему возникает эта ошибка?

Ответ. Следует создать дополнительные интерфейсы менеджера точки доступа, чтобы поддерживать более 48 точек доступа. Иначе будет выводиться сообщение об ошибке следующего 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 менеджера точки доступа, а также основной и резервный порты, которые другие интерфейсы менеджера точки доступа не должны использовать. Следует *обязательно* создавать второй интерфейс менеджера точки доступа, чтобы использовать дополнительные точки доступа. Однако, убедитесь в том, что конфигурации основного и резервного портов для каждого менеджера не перекрываются. Другими словами, если менеджер точки доступа №1 использует порт 1 как основной и порт 2 как резервный, менеджер точки доступа №2 должен использовать порт 3 как основной и порт 4 как резервный.

Вопрос. Я использую контроллер Wireless LAN Controller (WLC) 4402 и точки доступа с облегченным

протоколом 1240 (LAPs). Я пробую включить 128-битное шифрование на WLC. При выборе 128-битного WEP-шифрования появляется сообщение об ошибке, в котором говорится, что 128-битное шифрование не поддерживается на точках 1240: `[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 я получаю это сообщение об ошибке?

Ответ. Длины ключей, отображающиеся на контроллерах WLC – это количество бит общего секретного ключа, они не включают в себя 24 бита вектора инициализации. Во многих продуктах, включая продукты Aironet, это называется 128-битным WEP-ключом. На самом деле, это 104-битный ключ с 24-битным вектором инициализации. Необходимо включить именно 104-битный размер ключа на WLC для 128-битного WEP-шифрования. При выборе WLC 128-битного размера ключа на самом деле выбирается 152-битное WEP-шифрование.

Вопрос. Клиент AIR-P121AG-E-K9 успешно подключается к точкам доступа при помощи протокола EAP-FAST. Однако, когда связанная точка доступа отключается, клиент не перенаправляется к следующей точке доступа. 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"`. Почему?

Ответ. Когда клиентскому адаптеру требуется выполнить роуминг, он отправляет запрос на аутентификацию, но ключи обрабатывает неправильно (не информирует точки доступа или контроллер, не отвечает на запросы повторной аутентификации).

Эта проблема описана в идентификаторе ошибок Cisco CSCsd02837 (только для зарегистрированных клиентов). Решением является переход с WPA2 на WPA1/TK1P.

Вопрос. При установке нового блейд-модуля Wireless Services Module (WiSM) на коммутатор 6509 и внедрении защищенного расширяемого протокола аутентификации PEAP на сервере Microsoft IAS, появляется следующее сообщение об ошибке: `*Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.Reload Reason: FAILED CRYPTO INIT. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPP changed state to DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY *Mar 1 00:00:230.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs no certs in the SSC Private File *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: *Mar 1 00:00:23.700: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.` Почему?

Ответ. Отладка RADIUS и dot1x показывает, что контроллер беспроводного доступа отправляет запрос на доступ, но отклик от сервера IAS не поступает. Чтобы устранить данную проблему, проделайте следующие действия:

1. Проверьте конфигурацию сервера IAS.
2. Проверьте файл журнала
3. Установите программное обеспечение, такое как Ethereal, которое может предоставить подробные сведения о процессе аутентификации.
4. Остановите и запустите службу IAS.

Вопрос. Облегченные точки доступа (LAP) не регистрируются контроллером. Что может являться причиной

проблемы? На контроллере отображается следующее сообщение об ошибке: `Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0. Thu Feb 3 03:20:47 2028: Unable to free public key for AP 00:0B:85:68:F4:F0.`

Ответ. Когда точка доступа отправляет по протоколу "облегченных" точек доступа (LWAPP) запрос на присоединение к WLC, в сообщение LWAPP она вкладывает сертификат X.509. Кроме того, она генерирует случайный идентификатор сеанса, который включается в запрос LWAPP на присоединение. Когда WLC получает LWAPP запрос на присоединение, он проверяет подпись сертификата X.509 с помощью открытого ключа точек доступа и удостоверяется в том, что сертификат был выдан доверенным центром сертификации. Он также проверяет дату и время начала действия сертификата точки доступа и сравнивает их с собственными значениями даты и времени.

Эта проблема может возникнуть из-за неправильных настроек времени на WLC. Чтобы настроить часы на WLC, воспользуйтесь командами **show time** и **config time**.

Вопрос. "Облегченная" точка доступа (LWAPP) не может присоединиться к своему контроллеру. В файле журнала контроллера беспроводной сети (WLC) отображается следующее сообщение: `LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01.` Почему?

Ответ. Данное сообщение об ошибке может быть получено в том случае, если туннель LWAPP между точкой доступа и контроллером WLC проходит через сетевой путь с MTU меньше 1500 байтов. Это вызывает фрагментацию пакетов LWAPP. Это известная ошибка в контроллере. Обратитесь к ошибке Cisco с идентификатором CSCsd39911 (только для зарегистрированных клиентов).

Решение проблемы – обновление микропрограммы контроллера до версии 4.0(155).

Вопрос. Я пытаюсь создать гостевой туннель между своим внутренним контроллером и виртуальным якорным контроллером в демилитаризованной зоне (DMZ). Однако, когда пользователь пытается ассоциироваться с гостевым SSID, он не может получить IP-адрес из DMZ. Вследствие этого пользовательский трафик не туннелируется на контроллер в DMZ. Выходные данные команды debug mobile handoff содержат следующее сообщение: `Security Policy Mismatch for WLAN <Wlan ID>. Anchor Export Request from Switch IP: <controller Ip address> Ignored.` В чем проблема?

Ответ. Гостевое туннелирование обеспечивает дополнительную безопасность для доступа гостевых пользователей в корпоративную беспроводную сеть. Это помогает обеспечить то, что гостевые пользователи не могут входить в корпоративную сеть без предварительного прохождения через корпоративный брандмауэр. Когда пользователь ассоциируется с WLAN, которая назначена в качестве гостевой WLAN, пользовательский трафик туннелируется на контроллер WLAN, который находится на DMZ за пределами корпоративного брандмауэра.

Теперь, приняв во внимание этот сценарий, 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 время 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. На контроллере 2006 Wireless LAN Controller появляется много сообщений `"CPU Receive Multicast Queue is full on Controller"`, а на WLC 4400 их нет. Почему? На контроллерах отключена многоадресная рассылка. В чем разница между пределами многоадресных очередей на платформах WLC 2006 и 4400?

Ответ. Поскольку многоадресная рассылка на контроллерах отключена, сообщения, которые вызывают это уведомление, могут быть сообщениями протокола разрешения адресов (ARP). Разницы в глубине очереди (512 пакетов) между контроллерами WLC 2000 и контроллерами WLC 4400 нет. Разница заключается в том, что NPU 4400 фильтрует пакеты ARP, в то время как на 2006 все делается программно. Это служит объяснением того, почему контроллеры WLC 2006 видят сообщения, а контроллеры WLC 4400 - нет. WLC 44xx обрабатывает многоадресные пакеты аппаратно (с помощью центрального процессора). WLC 2000 обрабатывает многоадресные пакеты программно. Аппаратная обработка более эффективна, чем программная. Таким образом, очередь в 4400 очищается быстрее, в то время как WLC 2006 испытывает повышенную нагрузку при получении множества подобных сообщений.

Вопрос. Я получаю следующее сообщение об ошибке: `"[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port."` на одном из моих контроллеров. Что это означает и какие шаги я должен предпринять, чтобы устранить проблему?

Ответ. Это сообщение выдается, когда контроллер получает DHCP-запрос для MAC-адреса, для которого у него нет конечного автомата. Это часто можно увидеть из сетевого моста или из системы, которая работает под управлением виртуальной машины, подобной VMWare. Контроллер прослушивает DHCP-запросы, поскольку он выполняет отслеживание DHCP и знает, какие адреса ассоциированы с клиентами, которые привязаны к его точкам доступа (AP). Весь трафик для беспроводных клиентов проходит через контроллер. Когда пунктом назначения пакета является беспроводной клиент, пакет попадает на контроллер и затем проходит через туннель "облегченного" протокола точек доступа (LWAPP), оттуда на AP и с нее к клиенту. Единственное, что можно сделать для уменьшения количества подобных сообщений – ввести на коммутаторе команду **switchport vlan allow**, которая разрешит VLAN, используемым на контроллере, доступ к транку, который подходит к контроллеру.

Вопрос. Почему на консоль выдается следующее сообщение об ошибке: `Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc`?

Ответ. Это может быть вызвано высокой загрузкой центрального процессора. Когда центральный процессор контроллера сильно загружен (например, когда он копирует файлы или выполняет другие задачи), у него нет времени на обработку всех запросов ACK, которые NPU отправляет в ответ на сообщения конфигурации. Когда это происходит, центральный процессор генерирует сообщения об ошибке. Однако они не влияют на качество работы контроллера или его функциональность.

Это описано в разделе Высокая загрузка центрального процессора контроллера документа Примечания к версии для контроллеров Cisco Wireless LAN и "облегченных" точек доступа для версии 3.2.116.21.

Вопрос. Я получаю следующие сообщения об ошибке WEP-ключа от беспроводной системы управления (WCS): `The WEP Key configured at the station may be wrong. 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'`. Но я не использую WEP в качестве параметра безопасности моей сети. Я использую только защищенный доступ Wi-Fi (WPA). Почему я получаю эти сообщения об ошибках WEP?

Ответ. Если все ваши настройки безопасности идеальны, подобные сообщения возникают из-за ошибок в программном обеспечении. Существует несколько известных ошибок в программном обеспечении контроллера. 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** является копией **CSCse11202**. Исправление для **CSCse11202** уже доступно в выпуске WLC под номером 3.2.171.5.

Примечание: в последней версии WLC 4.0.206.0 эти ошибки устранены.

Вопрос. Мы используем внешний сервер RADIUS для аутентификации беспроводных клиентов через контроллер. Контроллер регулярно отправляет следующее сообщение об ошибке: `no radius servers are responding`. Почему мы получаем эти сообщения об ошибке?

Ответ. Когда запрос от контроллера WLC попадает на сервер RADIUS, каждый пакет имеет номер последовательности, для которой WLC ожидает ответа. Если отклика нет, появляется сообщение `radius-server not responding`.

Время ожидания WLC ответа от сервера RADIUS по умолчанию - 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 максимальное значение времени ожидания.

Иногда серверы RADIUS производят **'silent discard'** пакета запроса, который приходит от контроллера WLC. Сервер RADIUS может отклонять эти пакеты из-за несовпадения сертификатов, а также по некоторым другим причинам. Это правомочное действие со стороны сервера. Кроме того, в таких случаях контроллер будет помечать сервер RADIUS как "не отвечает".

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

Если функция **aggressive failover** включена на WLC, он будет слишком агрессивно помечать сервер AAA как не отвечающий. Однако, этого не следует делать, поскольку сервер AAA может посылать ответ только этому конкретному клиенту (с помощью silent discard). Он может отвечать другим действительным клиентам (с действительными сертификатами). Однако WLC может все же пометить сервер AAA как не отвечающий и бездействующий.

Чтобы преодолеть это затруднение, отключите функцию **aggressive failover**. Для этого введите команду **config radius aggressive-failover disable** из графического интерфейса контроллера. Если эта функция отключена, то контроллер будет просто переходить на следующий сервер AAA, если три клиента подряд не смогут получить отклик от сервера RADIUS.

Вопрос. Я получаю следующее сообщение на контроллере беспроводной локальной сети (WLC): `Reached Max EAP-Identity Request retries (21) for STA 00:05:4e:42:ad:c5`. Почему?

Ответ. Это сообщение об ошибке появляется, когда пользователь пытается подключиться к защищенной EAP сети WLAN и превышает предварительно установленное количество неудачных попыток подключения. Когда пользователь не может пройти аутентификацию, контроллер исключает клиента и клиент не может подключиться к сети до тех пор, пока не истечет срок исключения или он не будет вручную изменен администратором.

В процессе исключения опознаются попытки аутентификации, предпринимаемые отдельным устройством. Когда устройство превышает максимальное количество 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 внешнего сервера политик (NAC)
- При любых случаях повторения IP-адресов
- После 3 последовательных отказов веб-аутентификации (4-я попытка исключается)

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

Вопрос. Я получаю следующее сообщение на контроллере беспроводной локальной сети (WLC): `An Alert of Category Switch is generated with severity 1 by Switch WLCSCH01/10.0.16.5 The message of the alert is Controller '10.0.16.5'. RADIUS server(s) are not responding to authentication requests.` В чем проблема?

Ответ. Это может происходить из-за ошибки Cisco CSCsc05495. По причине этой ошибки контроллер периодически вставляет неправильные AV-Pair (атрибут 24, "state") в сообщения запроса аутентификации, что нарушает работу RADIUS RFP и вызывает проблемы у некоторых серверов аутентификации. Эта ошибка исправлена в версии 3.2.179.6.

Вопрос. В Monitor > 802.11b/g Radios появляется сообщение об отказе Noise Profile. Почему возникает сообщение FAILED?

Ответ. Статус FAILED/PASSED профиля Noise устанавливается после получения результатов проверки, выполненной контроллером WLC, и в соответствии с текущим установленным порогом. По умолчанию значение Noise установлено равным -70. Статус FAILED показывает, что пороговое значение для этого конкретного параметра или точки доступа было превышено. Скорректировать параметры можно в профиле, но рекомендуется изменять настройки только после достижения полного понимания 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. Не удается установить порт 2 в качестве резервного порта для интерфейса AP-менеджера. Возвращенное сообщение об ошибке имеет вид `Could not set port configuration`. Можно установить порт 2 в качестве резервного для интерфейса управления. Текущий активный порт для обоих интерфейсов – 1. Почему?

Ответ. У AP-менеджера нет 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 настроен один AP-менеджер (без резервов). При использовании агрегации каналов (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 требование не является обязательным.

Вопрос. Я вижу следующее сообщение об ошибке: `The AP '00:0b:85:67:6b:b0' received a WPA MIC`

error on protocol '1' from Station '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds. Почему?

Ответ. Функция проверки целостности сообщений (MIC), встроенная в реализацию защищенного доступа к Wi-Fi (WPA), включает в себя счетчик кадров, который предотвращает атаки класса "человек посередине". 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 не проходит проверку MIC несколько раз подряд, то контроллер отключает WLAN на 60 секунд, согласно требованиям протокола WPA. Это предотвращает возможную атаку на схему шифрования. Эти ошибки MIC нельзя отключить на контроллерах.

Вопрос. В файле журнала моего контроллера появляется следующее сообщение об ошибке: [ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed. Почему?

Ответ. Данные сообщения об ошибках появляются в том случае, когда DHCP включен на сервисном порту контроллера, но порт не получает IP-адрес от DHCP-сервера.

По умолчанию на физическом интерфейсе порта служб установлен клиент DHCP, и определение адреса происходит с помощью DHCP. WLC пытается запросить адрес DHCP для порта служб. Если DHCP-сервер недоступен, то запрос DHCP для порта служб получает отказ. Следовательно, 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. После этого перезагрузите контроллер, при необходимости.

Порт служб, в принципе, 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 загрузки. Порт служб не поддерживает метки 802.1Q. Поэтому он должен подключаться к порту доступа на соседнем коммутаторе. Использование порта служб необязательно.

Интерфейс порта служб управляет передачей данных с помощью порта служб, которому он статически сопоставлен системой. 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 для получения IP-адреса, или ему может быть назначен статический IP-адрес, но интерфейсу порта служб не может быть назначен шлюз по умолчанию. С помощью контроллера можно определить статические маршруты для удаленного доступа через сеть к порту служб.

Вопрос. Мои беспроводные клиенты не могут подключиться к беспроводной локальной сети (WLAN). WiSM, к которому подключена точка доступа, выдает следующее сообщение: Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00. Что это означает?

Ответ. Для доступа к среде передачи данный, подуровень контроля доступа к среде проверяет значение вектора NAV (Вектор сетевого размещения). Вектор NAV – это счетчик, присутствующий на каждой станции и отображающий количество времени, необходимое предыдущему кадру для отправки собственного кадра. Значение вектора NAV должно быть равным нулю перед тем, как станция произведет попытку отправки кадра. Перед передачей кадра, станция рассчитывает количество времени, необходимое для отправки кадра, учитывая длину кадра и скорость передачи данных. Станция размещает данное значение времени в поле длительности в заголовке кадра. При получении кадра станции проверяют значение поля длительности и используют его как основу для настройки собственных векторов сетевого размещения. Данный процесс резервирует среду передачи данных для отправляющей станции.

Высокий вектор сетевого размещения указывает на присутствие завышенного значения вектора (виртуальный механизм

контроля носителя для 802.11). Если сообщенный MAC-адрес равняется 00:00:00:00:00:00, то он, возможно, подвергается подмене адресов (вероятно, происходит реальная сетевая атака), и пользователю необходимо подтвердить это, воспользовавшись захватом пакетов.

Вопрос. После настройки и перезагрузки контроллера невозможно получить доступ к контроллеру в режиме безопасной сети (https). При попытке получения доступа к контроллеру в режиме безопасной сети выдается следующее сообщение об ошибке: `Secure Web: Web Authentication Certificate not found (error).` В чем причина данной проблемы?

Ответ. Данная проблема может заключаться в настройке виртуального интерфейса контроллера. Для решения проблемы удалите виртуальный интерфейс и восстановите его с помощью данной команды:

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

Затем перезагрузите контроллер. После перезагрузки заново сгенерируйте сертификат веб-аутентификации локально на контроллере, с помощью данной команды:

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

В выходных данных команды должно отобразиться следующее сообщение: `Web Authentication certificate has been generated`.

Теперь доступ к режиму безопасной сети контроллера должен быть открыт после перезагрузки.

Вопрос. Иногда контроллеры выдают сообщение об атаке IDS Disassociation Flood Signature для допустимых клиентов, у которых MAC-адрес одной из точек доступа (AP), закрепленных за контроллером, совпадает с MAC-адресом атакующего: `Alert: IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'. The Signature description is 'Disassociation flood', with precedence '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 так происходит?

Ответ. Это происходит по причине ошибки Cisco ID CSCsg81953 (только для зарегистрированных клиентов).

Иногда контроллеры выдают сообщение об атаке IDS Disassociation Flood Signature для допустимых клиентов, у которых MAC-адрес одной из точек доступа, закрепленных за контроллером, совпадает с MAC-адресом атакующего.

Если клиент ассоциирован с точкой доступа, но приостановил связь по причине вынимания платы, выхода из зоны действия и т. д., точка доступа будет ожидать до окончания определенного времени простоя. По завершении времени простоя точка доступа отправляет клиенту кадр разъединения. Если клиент не подтверждает прием кадра разъединения, точка доступа отправляет кадр несколько раз (около 60 кадров). Подсистема контроллера IDS распознает данные повторные передачи и выдает следующее предупреждающее сообщение.

Эта ошибка устранена в версии 4.0.217.0. Обновите контроллер до данной версии, чтобы устранить получение предупреждающего сообщения допустимыми клиентами и точками доступа.

Вопрос. Я получил следующее сообщение об ошибке в системном журнале контроллера: `[WARNING] apf_80211.c 2408: Received a message with an invalid supported rate from station <xx:xx:xx:xx:xx:xx> [ERROR] apf_utils.c 198: Missing Supported Rate.` Почему?

Ответ. Фактически, сообщения `Missing Supported Rate` (Отсутствует поддерживаемая частота) указывают на то, что контроллер настроен на некоторые необходимые частоты передачи данных , но плата сетевого интерфейса (NIC) не поддерживает требуемую частоту.

Если частоты передачи данных 1 и 2 настроены в качестве требуемых на контроллере, но плата сетевого интерфейса не функционирует на данных частотах, вы можете получить подобное сообщение. Это происходит в результате неправильного функционирования платы сетевого интерфейса (NIC). В другом случае, если ваш контроллер поддерживает 802.11g, а клиент поддерживает только 802.11b, это сообщение является допустимым. Если данные сообщения не вызывают каких-либо проблем и соединение между контроллером и клиентом функционирует, данные сообщения можно проигнорировать. Если сообщения имеют отношение к данной плате, убедитесь, что вы используете последнюю версию драйвера платы.

Вопрос. Я получил следующее сообщение об ошибке от моего контроллера беспроводной сети (WLC): `[ERROR] File: apf_mm.c : Line: 581 : Announce collision for mobile 00:90:7a:05:56:8a, deleting.` Почему?

Ответ. Как правило, данное сообщение об ошибке указывает на то, что контроллер конфликтует с беспроводным клиентом (т.е. разные точки доступа сообщают о наличии у них одного клиента) и контроллер не получил сообщение о передаче абонента от одной точки доступа к другой. Нет состояния сети для поддержания. Удалите беспроводного клиента и попросите клиента повторить попытку. Если проблема часто повторяется, это может означать ошибку в настройке мобильного доступа. Также это может означать ошибку, связанную со специфическим клиентом или состоянием.

Вопрос. Мой контроллер выдает предупредительное сообщение: `Coverage threshold of '12' violated.` Что это за ошибка и каким образом она может быть устранена?

Ответ. Данное предупредительное сообщение отображается, когда соотношение сигнал/шум (SNR) клиента опускается ниже порогового значения для данного радиоустройства. 12 – это предельное значение соотношения SNR для обнаружения пропусков в зоне покрытия.

Алгоритм обнаружения и корректировки пропусков в зоне покрытия определяет наличие пропуска при падении соотношения сигнал/шум (SNR) клиента ниже заданного предела. Изменение предела SNR происходит с учетом двух величин: значения мощности передачи точки доступа и профиля покрытия контроллера.

Пороговое значение SNR клиента определяется разницей между уровнем мощности передачи каждой точки доступа (представленной в дБм) и постоянным значением в 17 дБм, сложенным с пользовательским значением профиля охвата (значение по умолчанию — 12 дБ).

- **Критическая величина SNR клиента (|дБ|) = [Мощность передачи точки доступа (AP) (дБм) — Постоянная величина (17 дБм) — Профиль охвата (дБ)]**

Доступ к настраиваемому значению профиля покрытия можно получить следующим образом:

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 странице Auto RF Global parametrs (Основные параметры автоматического выбора частоты) найдите раздел Profile Thresholds (Пороговые значения профилей). В данном разделе указано значение Coverage (покрытие) (3 - 50 дБм). Данное значение может регулироваться пользователем.
3. Оно также может быть отредактировано для изменения порогового значения соотношения сигнал/шум (SNR) клиента. Другой способ изменения порогового значения SNR – это увеличение мощности передачи и компенсация обнаружения пропусков в зоне покрытия.

Вопрос. Я использую приложение ACS версии 4.1 и контроллер беспроводной сети 4402 (WLC). При попытке контроллера провести MAC-аутентификацию клиента для ACS 4.1, происходит сбой ACS и выводится следующее сообщение об ошибке: "*Internal error has occured* ". Все мои настройки сделаны правильно. Почему происходит эта внутренняя ошибка?

Ответ. Это ошибка аутентификации Cisco ID CSCsh62641 (только для зарегистрированных клиентов) в ACS 4.1, при которой выдается сообщение "**Internal error has occured**".

Это может быть вызвано данной программной ошибкой. Чтобы исправить данную программную ошибку, воспользуйтесь исправлением, доступным на стр. ACS 4.1 Downloads (только для зарегистрированных клиентов).

Вопрос. Не выполняется загрузка контроллера WLC беспроводной сети (LAN) Cisco серии 4400. Выводится следующее сообщение об ошибке: `** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0: status 0x51 Error reg: 10 ** Can't read from device 0.` Почему?

Ответ. Причина ошибки может заключаться в неисправностях оборудования. Воспользуйтесь службой технической поддержки для устранения неисправности. Чтобы воспользоваться службой технической поддержки, необходимо иметь действующий контракт с компанией Cisco. Обратитесь в службу поддержки для связи с центром TAC компании Cisco.

Вопрос. В ходе работы контроллера беспроводной сети (WLC) возникают проблемы с буфером 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.` Почему?

Ответ. Это ошибка Cisco ID CSCsh93980 (только для зарегистрированных клиентов). Единственный существующий на сегодня обходной путь – это перезагрузка контроллера для освобождения буферов памяти. Контроллер будет нормально функционировать до следующего сбоя.

Вопрос. Мы обновили микропрограммное обеспечение контроллера Wireless LAN Controller (WLC) 4400s до версии 4.1 и в файле системного журнала стали регулярно возникать следующие сообщения. `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?

Ответ. Это сообщение выводится в том случае, когда контроллер получает запрос протокола разрешения адресов (APR) от станции, от которой контроллер не получил новый IP-адрес в таблице станций.

Пример `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 against 0.0.0.0` показывает, что когда станция сгенерировала APR, контроллер не получил новый IP-адрес от станции в таблице станций.

Это может произойти, если сеть WLAN помечена как требующая DHCP. В подобных случаях контроллер ставит флаг на соединение и сообщает о получении запроса APR, в то время как он должен был получить запрос DHCP.

Вопрос. При использовании питания через Ethernet (PoE) на контроллере Cisco 2106 Wireless LAN Controller радиоточки доступа выключены. Выдается сообщение об ошибке: `AP is unable to verify sufficient in-line power. Radio slot disabled.` Как устранить эту проблему?

Ответ. Данное сообщение об ошибке появляется, когда коммутатор точки доступа является коммутатором предварительного стандарта, но точка доступа не поддерживает данный режим входной мощности.

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. Это `apf_foreignap.c:1246 APF-1-REGISTER_IPADD_ON_MSCB_FAILED: Could not Register IP Add on MSCB. MSCB still in init state. Address:xx:xx:xx:xx:xx:xx` сообщение об ошибке часто выдается контроллером. Что означает это сообщение об ошибке?

Ответ. Это сообщение об ошибке.

```
APF-1-REGISTER_IPADD_ON_MSCB_FAILED: Could not Register
 IP Add on MSCB. MSCB still in init state.
```

Блок управления мобильной станции (MSCB) представляет клиентов. Это сообщение об ошибке означает, что клиент выполняет попытку отправки трафика, несмотря на неготовность контроллера принять трафик клиента. Такие сообщения генерируются, когда контроллер получает запрос протокола разрешения адресов (ARP) от клиента, но при этом не добавляет IP-адрес клиента в список клиентов. Ошибка будет устранена после добавления IP-адреса в список клиентов.

В качестве обходного пути попробуйте перезагрузить контроллер. Это может помочь. Кроме того, убедитесь, что для плат беспроводного соединения клиента используются последние версии драйверов, так как известны случаи неполадок в соединении, связанные с более ранними версиями драйверов, особенно с платами беспроводных сетей от сторонних производителей.

Вопрос. Контроллер генерирует сообщение `tl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED: Unable to add an ARP entry for xx:xx.-xxx.x to the netwok processor. entry does not exist.` системного журнала, подобное этому. Что означает это сообщение системного журнала?

Ответ. Когда некоторые беспроводные клиенты отправляют ответ ARP, сетевому процессору NPU требуется знать этот 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.

Дополнительные сведения

- **Руководство по настройке контроллеров беспроводной локальной сети Cisco, выпуск 4,0**
- **WiSM Troubleshooting FAQ**
- **Вопросы и ответы по устранению неполадок в работе контроллера беспроводной LAN**
- **Страница поддержки беспроводных решений**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107648/wlc-error-system-faq.shtml