Пример конфигурации "Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller"

Содержание

Введение

В настоящем документе описаны общие принципы динамического назначения сетей VLAN. В документе поясняется процедура настройки контроллера беспроводной локальной сети (WLC) и сервера RADIUS для динамического назначения определенных беспроводных сетей VLAN клиентам беспроводной локальной сети (WLAN).

Предварительные условия

Требования

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

- Наличие общего представления о WLC и упрощенных точках доступа (LAP)
- Знакомство с практическими аспектами серверов AAA (аутентификации, авторизации и учета)
- Основательные знания беспроводных сетей и вопросов их безопасности
- Наличие общего представления о протоколе упрощенных точек доступа (LWAPP)

Используемые компоненты

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

- Cisco 4400 WLC с микропрограммой версии 5,2
- Упрощенные точки доступа Cisco серии 1130
- Беспроводной клиентский адаптер Cisco 802.11a/b/g с микропрограммой версии 4.4
- Служебная программа Cisco Aironet Desktop Utility (ADU) версии 4.4
- Сервер управления доступом CiscoSecure Access Control Server (ACS) версии 4.1
- Коммутатор Cisco серии 2950

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

Условные обозначения

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

Динамическое назначение сетей VLAN посредством сервера RADIUS

В большинстве систем с беспроводными локальными сетями (WLAN) каждая сеть WLAN имеет статическую политику, которая действует для всех клиентов, связанных с определенным идентификатором набора служб (SSID) или сетью WLAN – в терминологии контроллера. Будучи достаточно мощным, этот способ имеет ряд ограничений, поскольку он требует связывания клиентов с различным идентификаторами SSID для наследования разных политик QoS и безопасности.

В то же время решение Cisco для беспроводных локальных сетей поддерживает работу в сети на основе идентификационных данных. В этом случае сеть может объявлять только один идентификатор SSID, но позволять определенным пользователям наследовать различные политики QoS или безопасности исходя из полномочий пользователей.

Для этого, в частности, предназначена функция динамического назначения VLAN, которая назначает пользователю беспроводной сети определенную сеть VLAN исходя из предоставленных пользователем реквизитов учетной записи. Задача назначения определенной сети VLAN пользователям решается сервером аутентификации RADIUS, роль которого может играть система управления доступом CiscoSecure. Таким образом, например, можно сохранять одну и ту же сеть VLAN за мобильным беспроводным узлом, который переподключается к сети в разных точках комплекса зданий.

Когда клиент пытается связаться с упрощенной точкой доступа, зарегистрированной на контроллере, точка доступа передает реквизиты пользователя на сервер RADIUS для проверки. После прохождения аутентификации сервер RADIUS передает пользователю ряд атрибутов, предусмотренных спецификацией IETF (инженерной группы по развитию Интернета). Эти атрибуты RADIUS определяют идентификатор VLAN, назначаемый беспроводному клиенту. SSID (в терминах WLC – беспроводная локальная сеть) клиента не имеет значения, поскольку пользователю всегда назначается конкретный предопределенный идентификатор VLAN.

Атрибуты пользователя RADIUS, используемые для назначения идентификатора VLAN:

- IETF 64 (тип туннеля) – присваивается значение «VLAN».
- IETF 65 (тип передающей среды туннеля) – присваивается значение «802»
- IETF 81 (идентификатор частной группы туннеля) – присваивается значение идентификатора VLAN.

Идентификатор VLAN состоит из 12 двоичных разрядов и принимает значение от 1 до 4094 включительно. Поскольку идентификатор частной группы туннеля имеет строковый тип согласно стандарту RFC2868 в применении к сетям IEEE 802.1X, то целочисленное значение идентификатора VLAN кодируется как строка. При отправке этих атрибутов туннеля необходимо заполнить поле метки.

Согласно RFC2868 (разд. 3.1): **Поле метки имеет длину восемь двоичных разрядов и предназначено для группирования атрибутов в одном пакете, относящихся к одному и тому же туннелю.** Допустимые значения для этого поля – от 0x01 до 0x1F включительно. Неиспользуемые поля меток заполняются нулями (0x00). Дополнительные сведения обо всех атрибутах RADIUS см. в документе RFC 2868.

Настройка

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

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурация компонентов, представленных на этой схеме:

- IP-адрес сервера управления доступом (RADIUS) – 172.16.1.1.
- IP-адрес интерфейса управления WLC – 172.16.1.30.
- IP-адрес интерфейса диспетчера точек доступа – 172.16.1.31.
- Адрес сервера DHCP 172.16.1.1 используется для присвоения IP-адресов на LWAPP. **Для назначения IP-адресов беспроводным клиентам используется внутренний DHCP-сервер контроллера.**
- В этой конфигурации используются сети VLAN10 и VLAN11. Для пользователя user1 на сервере RADIUS настраивается вхождение в сеть VLAN10, а для пользователя user2 – в сеть VLAN11.**Примечание:** Этот документ только показывает все сведения о конфигурации, отнесенные user1. Для пользователя user2 следует выполнить процедуру, аналогичную описанной.
- В данном документе предполагается использование протокола 802.1x с механизмом

безопасности LEAP.**Примечание:** Cisco рекомендует использовать усовершенствованные методы аутентификации, такие как EAP-FAST и Проверка подлинности EAP-TLS, для обеспечения WLAN. В настоящем документе метод LEAP используется исключительно по соображениям простоты.

!--- конфигурацию

В данном документе предполагается, что упрощенная точка доступа перед настройкой уже зарегистрирована на контроллере WLC. Дополнительные сведения см. в документе Пример настройки контроллера беспроводной сети и упрощенных беспроводных точек доступа. Соответствующая процедура регистрации описана в документе Регистрация упрощенных точек доступа на контроллере беспроводной локальной сети (WLC).

Порядок действий для настройки

Эта настройка состоит из следующих частей:

1. Конфигурация сервера RADIUS
2. Настройка коммутатора для работы с несколькими сетями VLAN
3. Настройка WLC
4. Настройка клиентской служебной программы беспроводной сети

Конфигурация сервера RADIUS

В данной процедуре настройки необходимо выполнить следующие шаги:

- Настройте WLC как клиента AAA на сервере RADIUS
- Настройка пользователей и атрибутов RADIUS (IETF) для динамического назначения сетей VLAN на сервере RADIUS

Настройка клиента AAA для использования WLC на сервере RADIUS

Эта процедура поясняет порядок добавления WLC в качестве клиента AAA на сервере RADIUS, при котором WLC может передавать реквизиты учетной записи пользователя на сервер RADIUS.

Выполните следующие действия:

1. **В графическом интерфейсе ACS выберите Network Configuration (Конфигурация сети).**
2. **В разделе клиентов AAA выберите Add Entry (Добавить запись).**
3. Введите IP-адрес и ключ клиента AAA.В качестве IP-адреса указывается адрес интерфейса управления WLC.Убедитесь в том, что введенный ключ совпадает с ключом, настроенным в окне Security (Безопасность) WLC. Это секретный ключ, используемый для обмена данными между клиентом AAA (WLC) и сервером RADIUS.
4. **В поле Authenticate Using (Аутентификация посредством) выберите тип аутентификации RADIUS (Cisco Airespace).**

Настройка пользователей и атрибутов RADIUS (IETF) для динамического назначения сетей

VLAN на сервере RADIUS

Эта процедура поясняет порядок настройки пользователей на сервере RADIUS и состав атрибутов RADIUS (IETF), используемых для назначения идентификаторов VLAN этим пользователям.

Выполните следующие действия:

1. **В графическом интерфейсе ACS выберите User Setup (Настройка пользователей).**
2. **В окне User Setup введите имя пользователя в поле User (Пользователь) и нажмите Add/Edit (Добавить/изменить).**
3. На странице Edit (Редактирование) введите необходимые данные пользователя, как показано ниже:В отношении этой схемы обратите внимание на то, что пароль, указываемый в разделе настройки пользователей, должен совпадать с паролем, предоставляемым на стороне клиента во время аутентификации пользователя.
4. **Прокрутите вниз страницу редактирования до поля IETF RADIUS Attributes (Атрибуты IETF RADIUS).**
5. В поле IETF RADIUS Attributes (Атрибуты IETF RADIUS) отметьте флажки для трех атрибутов туннеля и настройте значения атрибутов, как указано ниже:**Примечание:** В начальной конфигурации сервера ACS не могли бы быть отображены атрибуты RADIUS IETF.**Для включения атрибутов IETF в окне настройки пользователя выберите Interface Configuration (Настройка интерфейсов) > RADIUS (IETF).Затем отметьте флажки атрибутов 64, 65 и 81 в столбцах User (Пользователь) и Group (Группа).Примечание:** Для сервера RADIUS для динамичного присвоения клиента на определенную VLAN **требуется, что VLAN-ID, настроенный под полем IETF 81 (Tunnel-Private-Group-ID) сервера RADIUS, существует на WLC.Для включения сервера RADIUS в конфигурации для отдельных пользователей отметьте флажок атрибута Per User TACACS+/RADIUS (TACACS+/RADIUS для отдельных пользователей) в разделе Interface Configuration (Настройка интерфейса) > Advanced Options (Расширенные параметры).**Кроме того, поскольку в качестве протокола аутентификации используется LEAP, убедитесь, что в окне System Configuration (Конфигурация системы) сервера RADIUS включен протокол LEAP, как показано ниже:

Настройка ACS с атрибутами Cisco Airespace VSA для динамического назначения сетей VLAN

В последних версиях ACS можно также настроить специализированные атрибуты поставщика (VSA) Cisco Airespace для назначения имени интерфейса VLAN (но не идентификатора VLAN) пользователю, прошедшему аутентификацию, согласно конфигурации пользователей в системе управления доступом. Для этого выполните действия, описанные в этом разделе.

Примечание: Этот раздел использует версию ACS 4.1 для настройки атрибута VSA Airespace Cisco.

Настройка группы ACS с параметром атрибута Cisco Airespace VSA

Выполните следующие действия:

1. В графическом интерфейсе ACS 4.1 выберите Interface Configuration (Настройка интерфейсов) в панели навигации. Затем на странице Interface Configuration (Настройка интерфейсов) выберите RADIUS (Cisco Airespace), чтобы настроить параметры атрибута Cisco Airespace.
2. В окне RADIUS (Cisco Airespace) отметьте флажок User (Пользователь), а также, при необходимости, флажок Group (Группа) рядом с полем Aire-Interface-Name, чтобы этот интерфейс стал доступен странице редактирования пользователей. Затем щелкните Submit (Отправить).
3. Перейдите на страницу редактирования пользователя user1.
4. Пролистайте страницу редактирования пользователя до раздела Cisco Airespace RADIUS Attributes (Атрибуты RADIUS Cisco Airespace). Отметьте флажок у атрибута Aire-Interface-Name и задайте имя динамического интерфейса, который будет назначен после прохождения пользователем аутентификации.В данном примере пользователю назначается сеть VLAN admin.
5. Нажмите кнопку Submit (Отправить).

Настройка коммутатора для работы с несколькими сетями VLAN

Для поддержки нескольких сетей VLAN на одном коммутаторе необходимо настроить порт коммутатора, соединенный с контроллером, при помощи следующих команд:

1. Switch(config-if)#switchport mode trunk
2. Switch(config-if)#switchport trunk encapsulation dot1q

Примечание: По умолчанию большинство коммутаторов позволяет все VLAN, созданные на том коммутаторе через магистральный порт.

Эти команды будут различными для разных коммутаторов с операционной системой Catalyst (CatOS).

Если к коммутатору подключена проводная сеть, то эта же конфигурация может применяться для порта коммутатора, соединенного с проводной сетью. Таким образом, возможно взаимодействие между одинаковыми сетями VLAN в проводном и беспроводном сегментах сети.

Примечание: Этот документ не обсуждает связь между сетями VLAN. Эта проблема не относится к тематике данного документа. Необходимо учесть, что для маршрутизации между разными сетями VLAN необходим коммутатор 3-го уровня или внешний маршрутизатор с надлежащей конфигурацией VLAN и группообразования. Настройка маршрутизации между разными сетями VLAN объясняется в нескольких документах.

Настройка WLC

В данной процедуре настройки необходимо выполнить следующие шаги:

- Настройка данных сервера аутентификации в WLC
- Настройка динамических интерфейсов (сетей VLAN)
- Настройка сетей WLAN (SSID)

Настройка данных сервера аутентификации в WLC

Необходимо настроить WLC для взаимодействия с сервером RADIUS при аутентификации клиентов, а также при любых других транзакциях.

Выполните следующие действия:

1. **В графическом интерфейсе контроллера выберите Security (Безопасность).**
2. Введите IP-адрес сервера RADIUS и общий секретный ключ, используемый сервером RADIUS и WLC.Этот общий секретный ключ должен совпадать с ключом, настроенным на сервере RADIUS в разделе Network Configuration (Настройка сети) > AAA Clients (Клиенты AAA) > Add Entry (Добавление записи). Ниже представлен пример окна, отображаемого WLC:

Настройка динамических интерфейсов (сетей VLAN)

Данная процедура поясняет порядок настройки динамических интерфейсов WLC. Как поясняется ранее в этом документе, идентификатор VLAN, определенный под атрибутом идентификатора частной группы туннеля (Tunnel-Private-Group ID) на сервере RADIUS, должен также существовать на контроллере WLC.

В данном примере пользователю user1 на сервере RADIUS назначается атрибут Tunnel-Private-Group ID, равный 10 (VLAN =10). См. раздел IETF RADIUS Attributes (Атрибуты IETF RADIUS) в окне настройки пользователя user1.

В этом примере можно видеть один и тот же самый динамический интерфейс (VLAN=10), настроенный на WLC. Динамический интерфейс настраивается в окне Controller (Контроллер) > Interfaces (Интерфейсы) графического интерфейса контроллера.

1. **В этом окне нажмите кнопку Apply (Применить).**Откроется окно редактирования этого динамического интерфейса (в данном случае – VLAN 10).
2. Введите IP-адрес и адрес шлюза по умолчанию для этого динамического интерфейса.**Примечание:** Поскольку этот документ использует внутренний сервер DHCP на контроллере, основном поле сервера DHCP этого окна точки к Интерфейсу управления самого WLC. Можно также использовать внешний DHCP-сервер, маршрутизатор или сам сервер RADIUS в качестве DHCP-сервера для беспроводных клиентов. В таких случаях в поле основного DHCP-сервера указывается IP-адрес устройства, выполняющего функции DHCP-сервера. За дополнительными сведениями обратитесь к документации используемого DHCP-сервера.
3. **Щелкните "Применить".**Теперь на WLC настроен динамический интерфейс. Аналогичным образом на WLC можно настроить несколько динамических интерфейсов. Однако следует помнить о том, что для назначения сети VLAN клиенту на сервере RADIUS должен существовать идентификатор VLAN.

Настройка сетей WLAN (SSID)

Данная процедура поясняет порядок настройки беспроводных локальных сетей (WLAN) на WLC.

Выполните следующие действия:

1. **Для создания новой сети WLAN В графическом интерфейсе контроллера выберите WLANs (Сети WLAN) > New (Создать).**Откроется окно создания сетей WLAN.
2. Введите идентификатор и параметры SSID для беспроводной локальной сети.В качестве SSID для беспроводной локальной сети можно ввести любое имя. В данном примере в качестве SSID используется «VLAN10».
3. **Для перехода в окно редактирования WLAN SSID10 щелкните Apply (Применить).**Как правило, в контроллере беспроводной локальной сети каждая беспроводная локальная сеть привязана к определенной сети VLAN (SSID) таким образом, чтобы конкретный пользователь, принадлежащий этой беспроводной локальной сети, входил в определенную привязанную сеть VLAN. Эта привязка обычно выполняется в поле Interface Name (Имя интерфейса) окна WLAN SSID.В данном примере функция назначения определенной сети VLAN беспроводному клиенту, прошедшему аутентификацию, возложена на сервер RADIUS. Беспроводные локальные сети не требуется привязывать к определенному динамическому интерфейсу на WLC. **Иначе даже при том, что привязка беспроводной локальной сети к динамическому интерфейсу выполняется на WLC, сервер RADIUS отменит эту привязку и назначит вошедшему в беспроводную локальную сеть пользователю ту сеть VLAN, которая указана в поле Tunnel-Group-Private-ID для этого пользователя на сервере RADIUS.**
4. **Чтобы разрешить серверу RADIUS отменять конфигурации WLC, отметьте флажок Allow AAA Override (Разрешать отмену параметров AAA).**
5. Флажок, разрешающий отмену параметров AAA, следует установить для каждой настроенной беспроводной локальной сети (SSID).Если разрешена отмена параметров AAA и у клиента имеются параметры AAA, противоречащие параметрам аутентификации беспроводной локальной сети в контроллере, то аутентификация клиента выполняется сервером AAA (RADIUS). В процессе этой аутентификации операционная система перемещает клиенты в сеть VLAN, сообщаемую сервером AAA. Такой механизм предусмотрен изначальной конфигурацией интерфейсов контроллера.Например, если корпоративная беспроводная локальная сеть в основном использует интерфейс управления, назначенный сети VLAN 2, а в результате отмены параметров AAA происходит переброс в сеть VLAN 100, то операционная система переадресует весь клиентский трафик в сеть VLAN 100, даже если имеется физический порт, которому назначена сеть VLAN 100. Если отмена параметров AAA отключена, то аутентификация всех клиентов по умолчанию осуществляется в соответствии с настройками параметров аутентификации на контроллере, а сервер AAA выполняет аутентификацию только в том случае, если беспроводная локальная сеть контроллера не содержит никаких определенных для клиента параметров аутентификации.

Настройка клиентской служебной программы беспроводной сети

В этом документе в качестве клиентской служебной программы для настройки профилей пользователей применяется программа ADU. Эта конфигурация также использует LEAP в качестве протокола аутентификации. Настройте ADU в соответствии с примером, приведенным в этом разделе.

Для создания нового профиля в строке меню ADU выберите Profile Management (Управление профилями) > New (Создать).

В примере клиент настраивается для работы в сети, имеющей идентификатор SSID VLAN10. На следующих иллюстрациях показана настройка профиля пользователя со стороны клиента:

Проверка

Активируйте профиль пользователя, настроенный в ADU. На основе конфигурации будет предложено ввести имя пользователя и пароль. Можно также указать программе ADU использовать для аутентификации имя пользователя и пароль Windows. Существует несколько способов получения аутентификации клиентом. Выбор этих способов происходит на вкладке Security (Безопасность) > Configure (Настройка) созданного профиля пользователя.

Обратите внимание на то, что в предыдущем примере пользователю user1 назначена сеть VLAN10, как определено на сервере RADIUS.

В этом примере имя пользователя и пароль с клиентской стороны используются для получения аутентификации и назначения сети VLAN сервером RADIUS:

- User Name (Имя пользователя) = user1
- Password (Пароль) = user1

В следующем примере показан запрос имени пользователя и пароля у SSID VLAN10. В этом примере вводятся имя пользователя и пароль:

После успешной аутентификации и получения соответствующего подтверждения появляется сообщение состояния о выполнении операции.

Затем необходимо проверить, назначена ли вашему клиенту соответствующая сеть VLAN согласно отправленным атрибутам RADIUS. Для этого выполните следующие действия:

1. **В графическом интерфейсе контроллера выберите Wireless (Беспроводная сеть) > AP (Точка доступа).**
2. **Щелкните Clients (Клиенты) в левом углу окна Access Points (Точки доступа).**Будет отображена статистика по клиентам.
3. **Для просмотра полных сведений о клиенте, включая IP-адрес, назначенную сеть VLAN и т. п., щелкните Details (Подробно).**В этом примере отображаются эти сведения о клиенте user1:В этом окне можно видеть, что данному клиенту назначена сеть VLAN10 в соответствии с атрибутами RADIUS, настроенными на сервере RADIUS.**Примечание:** Если динамическое назначение сетей VLAN будет основываться на значении **Атрибута VSA Airespace Cisco**, то **Имя интерфейса отобразит его как admin** согласно данному примеру на клиентской подробной странице.

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- **debug aaa events enable—при помощи этой команды можно проконтролировать передачу атрибутов RADIUS клиенту через контроллер.** Эта часть выходных данных отладки позволяет сделать вывод о том, что атрибуты RADIUS переданы успешно:`Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]: attribute 64, vendorId 0, valueLen 4 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]: attribute 65, vendorId 0, valueLen 4 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:`

```
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]: attribute 1, vendorId 9,
valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]: attribute 25,
vendorId 0, valueLen 28 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16 Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-
Type 16777229 should be 13 for STA 00:40:96:ac:e6:57 Fri Jan 20 02:25:08 2006:
00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222 should be 6 for STA 00:40:96:ac:e6:57 Fri Jan
20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57 setting dot1x reauth timeout =
1800
```

- Могут быть также полезны следующие команды:**debug dot1x aaa enabledebug aaa packets enable**

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Примечание: Динамическое назначение сетей VLAN не работает для web-аутентификации от WLC.

Дополнительные сведения

- Аутентификация EAP с помощью сервера RADIUS
- LEAP Cisco
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Cisco Systems – техническая поддержка и документация