Динамическое назначение сетей VLAN с NGWC и примером конфигурации ACS 5.2

Содержание

Введение

Этот документ описывает понятие динамического назначения сетей VLAN. Это также описывает, как настроить контроллер беспроводной локальной сети (WLC) и сервер RADIUS для присвоения беспроводной локальной сети (WLAN) клиенты к определенной VLAN динамично. В этом документе сервером RADIUS является Access Control Server (ACS), который выполняет Версию 5.2 системы управления доступом Cisco Secure Access Control System.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о WLC и Облегченных точках доступа (LAP)
- Функциональное знание аутентификации, авторизации и учета (AAA)
- Основательные знания беспроводных сетей и вопросов их безопасности

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco 5760 с Cisco IOS® XE Software Release 3.2.2 (Коммутационный шкаф следующего поколения или NGWC)
- Cisco Aironet облегченная точка доступа серии 3602
- Microsoft Windows XP с соискателем пронабора Intel
- Версия 5.2 системы управления доступом Cisco Secure Access Control System
- Коммутатор Cisco Catalyst серии 3560

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.

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. Это позволяет сети объявлять одиночный SSID, но позволяет определенным пользователям наследовать другое QoS, атрибуты VLAN и/или политику безопасности на основе учетных данных пользователя.

Для этого, в частности, предназначена функция динамического назначения VLAN, которая назначает пользователю беспроводной сети определенную сеть VLAN исходя из предоставленных пользователем реквизитов учетной записи. Эта задача пользовательского присвоения на определенную VLAN обрабатывается Сервером проверки подлинности RADIUS, таким как Cisco Secure ACS. Эта функция может быть использована, например, чтобы позволить хосту беспроводному сети оставаться на той же VLAN, как это перемещается в сети уровня кампуса.

В результате, когда клиент пытается связаться к LAP, зарегистрированному в контроллере, LAP передает учетные данные пользователя к серверу 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 клиента (WLAN, с точки зрения WLC) не имеет значения, потому что пользователя

всегда назначают на этот предопределенный ИДЕНТИФИКАТОР VLAN.

Атрибуты пользователя RADIUS, используемые для назначения идентификатора VLAN:

- (Тип туннеля) IETF 64 - Набор к VLAN.
- IETF 65 (туннельный тип среды) - набор к 802.
- IETF 81 (Tunnel-Private-Group-ID) - Набор к ИДЕНТИФИКАТОРУ VLAN.

Идентификатор VLAN состоит из 12 двоичных разрядов и принимает значение от 1 до 4094 включительно. Поскольку Tunnel-Private-Group-ID имеет введите строку, как определено в RFC 2868, атрибутах RADIUS для Поддержки протокола туннеля для использования с IEEE 802.1X, целое значение ИДЕНТИФИКАТОРА VLAN закодировано 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 Поля метки являются 0x01 через 0x1F, включительно. Неиспользуемые поля меток заполняются нулями (0x00). Дополнительные сведения обо всех атрибутах RADIUS см. в документе RFC 2868.

Настройка

Конфигурация динамического назначения сетей VLAN состоит из двух следующих действий:

1. Настройте WLC с интерфейсом командной строки (CLI) или с GUI.
2. Настройка RADIUS-сервера.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Этот документ использует 802.1X с Защищенным расширяемым протоколом аутентификации (PEAP) как механизм обеспечения безопасности.

Предположения

- Коммутаторы настроены для всего Уровня 3 (L3) VLAN.
- Серверу DHCP назначают область DHCP.
- Подключение L3 существует между всеми устройствами в сети.
- LAP уже соединен с WLC.
- Каждая VLAN имеет/24 маску.
- ACS 5.2 установили подписанный сертификат.

Настройте WLC с CLI

Настройте WLAN

Это - пример того, как настроить WLAN с SSID DVA:

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
 security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

Настройте сервер RADIUS на WLC

Это - пример конфигурации сервера RADIUS на WLC:

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-control
```

Настройте ПУЛ DHCP для клиентской VLAN

Это - пример конфигурации пула DHCP для клиентского VLAN 30 и VLAN 40:

```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
 network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

Настройте WLC с GUI

Настройте WLAN

Эта процедура описывает, как настроить WLAN.

1. Перейдите к вкладке **Configuration> Wireless> WLAN> NEW**.

2. Нажмите **Вкладку Общие**, чтобы видеть, что WLAN настроен для 802.1X WPA2, и сопоставьте Interface/Interfrace Group (G) с VLAN 20 **(VLAN0020)**.

3. Нажмите **Вкладку Дополнительно** и проверьте флажок **Allow AAA Override**. Замена должна быть позволена для этой функции работать.

4. Нажмите **Вкладку Безопасность** и вкладку **Layer2**, проверьте флажок **WPA2 Encryption AES** и выберите **802.1x** от Подлинного Ключевого выпадающего списка Mgmt.

Настройте сервер RADIUS на WLC

Эта процедура описывает, как настроить сервер RADIUS на WLC.

1. Перейдите к вкладке**> Security Конфигурации**.

2. Перейдите к **AAA> Группы серверов> Радиус** для создания Radius Server Groups. В данном примере Radius Server Group называют ACS.

3. Отредактируйте запись сервера RADIUS для добавления IP-адреса сервера и Общего секретного ключа. Этот Общий секретный ключ должен совпасть с Общим секретным ключом на WLC и сервере RADIUS.

   Это - пример завершенной конфигурации:

Настройте сервер RADIUS

Эта процедура описывает, как настроить сервер RADIUS.

1. На сервере RADIUS перейдите **Пользователям и Идентификационным Хранилищам> Внутренний Идентификационный> Users Хранилищ**.

2. Создайте соответствующую User Names and Identity Groups. В данном примере это - Студент и Весь Groups:Students, и Учитель и AllGroups:Teachers.

3. Перейдите к **Элементам Политики> Авторизация и Разрешения> Доступ к сети> Профили Авторизации**, и создайте Профили Авторизации для замены AAA.

4. Измените профиль авторизации для студента.

5. Установите ИДЕНТИФИКАТОР VLAN / Название как **Статичный** со Значением **30** (VLAN 30).

6. Измените профиль авторизации для учителя.

7. Установите ИДЕНТИФИКАТОР VLAN / Название как **Статичный** со Значением **40** (VLAN 40).

8. Перейдите к **Политике доступа> Службы доступа> Доступ к сети по умолчанию** и нажмите вкладку **Allowed Protocols**. Проверьте флажок **Allow PEAP**.

9. Перейдите к **Идентичности** и определите правила, чтобы позволить пользователям PEAP.

10. Перейдите к **Авторизации** и сопоставьте Студента и Учителя к Политике авторизации; в данном примере сопоставление должно быть Студентом для VLAN 30 и Учителем для VLAN 40.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно. Это процессы проверки:

- Контролируйте страницу на ACS, который показывает, какие клиенты аутентифицируются.

- Соединитесь с WLAN DVA с Student Group и рассмотрите клиентскую Утилиту Соединения WiFi.

- Соединитесь с WLAN DVA с Teacher Group и рассмотрите клиентскую Утилиту Соединения WiFi.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

> **Примечания:**
>
> Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).
>
> Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**
>
> Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Полезные отладки включают **MAC - адрес клиента отладки** *Mac*, а также эти команды трассировки NGWC:

- **отладка уровня беспроводного клиента группы set trace**
- **беспроводной клиент группы set trace фильтрует Mac** *xxxx.xxxx.xxxx*
- **show trace sys-filtered-traces**

Трассировка NGWC не включает dot1x/AAA, так используйте этот весь список объединенных трассировок для dot1x/AAA:

- **отладка уровня беспроводного клиента группы set trace**
- **отладка уровня события wcm-dot1x set trace**
- **отладка уровня aaa wcm-dot1x set trace**
- **отладка уровня событий wireless aaa set trace**
- **отладка уровня см ядра сеанса доступа set trace**
- **отладка уровня dot1x метода сеанса доступа set trace**

- беспроводной клиент группы set trace фильтрует Mac *xxxx.xxxx.xxxx*
- событие wcm-dot1x set trace фильтрует Mac *xxxx.xxxx.xxxx*
- aaa wcm-dot1x set trace фильтрует Mac *xxxx.xxxx.xxxx*
- события wireless aaa set trace фильтруют Mac *xxxx.xxxx.xxxx*
- см ядра сеанса доступа set trace фильтрует Mac *xxxx.xxxx.xxxx*
- dot1x метода сеанса доступа set trace фильтрует Mac *xxxx.xxxx.xxxx*
- show trace sys-filtered-traces

Когда динамическое назначение сетей VLAN работает правильно, необходимо видеть этот тип выходных данных от отладок:

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf: intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
 --More--        [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

 --More--        [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030'
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0
```

[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0) Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13) Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
 --More-- [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761 Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf: VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
**   vlanIfName: 'VLAN0040', aclName: ''**

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''
 --More--
[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID Cache entry (RSN 1)