Настройте для обеспечения порта коммутатора AP Flexconnect с Dot1x

Содержание

Введение

Этот документ описывает конфигурацию для обеспечения Switchports, где Точки доступа (AP) FlexConnect аутентифицируются с Dot1x, использующим device-traffic-class=switch VSA Радиуса для разрешения трафика от локально коммутируемых Беспроводных локальных сетей (WLAN).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- FlexConnect на контроллере беспроводной локальной сети (WLC)
- 802.1x на коммутаторах Cisco
- Топология аутентификации границы сети (NEAT)

Используемые компоненты

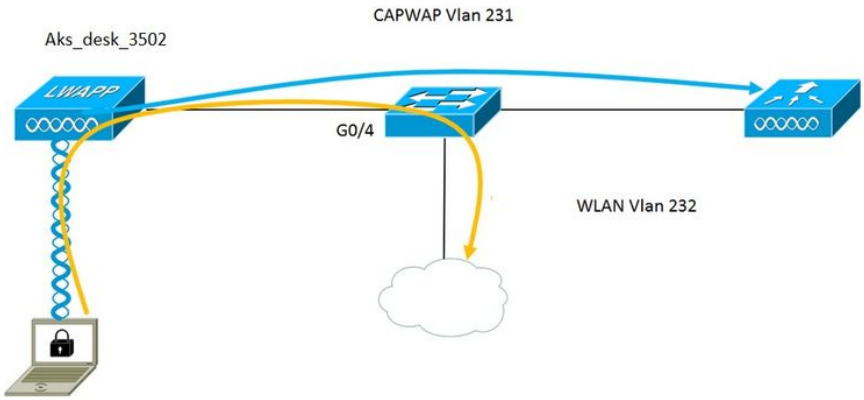
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WS-C3560CX-8PC-S, 15.2 (4) E1
- AIR-CT-2504-K9, 8.2.141.0
- Идентификационный механизм сервиса (ISE) 2.0

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.

Настройка

Схема сети



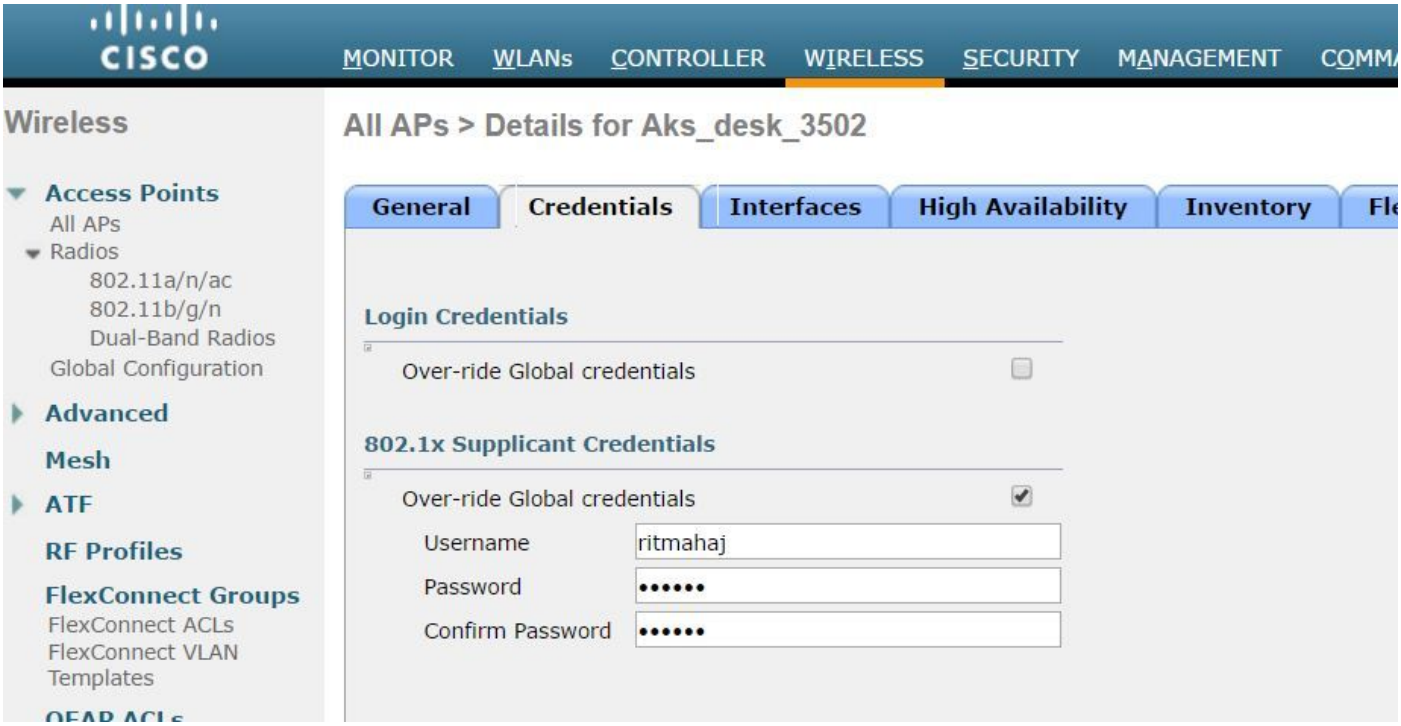
В этой настройке точка доступа действует как соискатель 802.1x и аутентифицируется коммутатором против ISE с помощью EAP-FAST. Как только порт настроен для аутентификации 802.1x, коммутатор не позволяет трафику кроме трафика 802.1x проходить через порт, пока устройство, связанное с портом, не аутентифицируется успешно.

Как только точка доступа аутентифицируется успешно против ISE, коммутатор получает Атрибут VSA Cisco "device-traffic-class=switch, и это автоматически перемещает порт для транкинга.

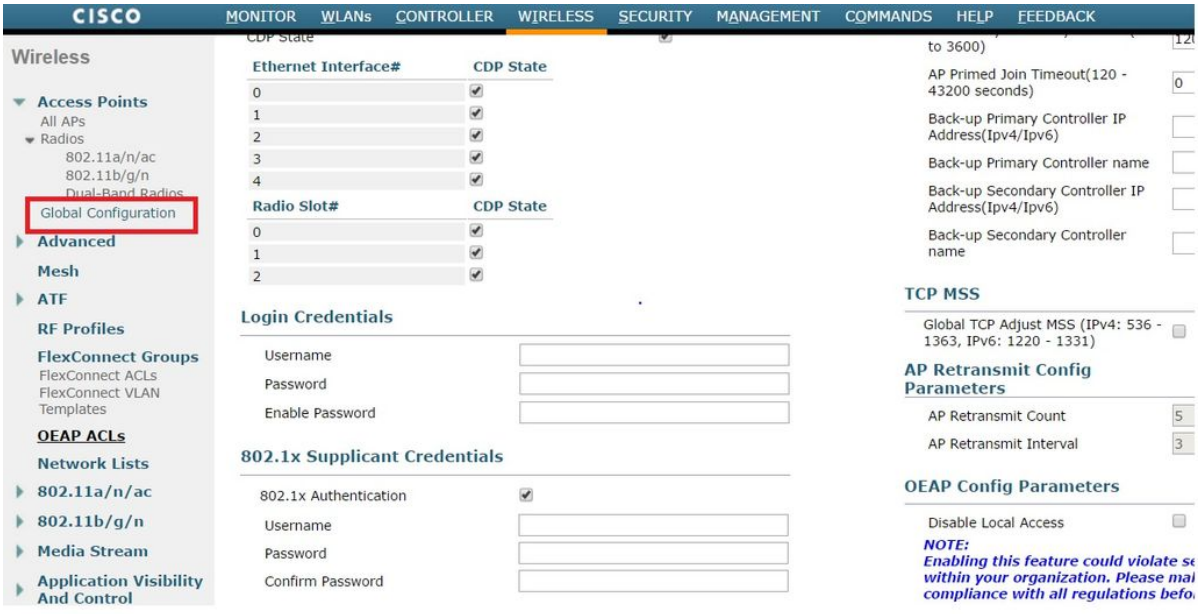
Это означает, если AP поддержит режим FlexConnect и локально коммутирует настроенный SSIDs, то это будет в состоянии передать помеченный трафик. Гарантируйте, что поддержка VLAN включена на AP, и корректная исходная виртуальная локальная сеть (VLAN) настроена.

Конфигурация точки доступа:-

1. Если AP уже соединен с WLC, пойдите вкладка Wireless и щелкните по точке доступа. Пойдите поле Credetials и nder заголовок Учетных данных Соискателя 802.1x, установите **Глобальный учетный** флажок **Замены** для установки имени пользователя и пароля 802.1x для этой точки доступа.



Можно также установить имя пользователя и пароль аферист для всех точек доступа, которые соединены с WLC с меню Global Configuration.



2. Если точка доступа еще не присоединилась к WLC, необходимо подключиться с консоли в LAP, чтобы установить учетные данные и использовать эту команду CLI:

LAP#debug capwap консольный cli
LAP#capwap <password> пароля <username> имени пользователя dot1x AP

Конфигурация коммутатора: -

1. Включите dot1x на коммутаторе глобально и добавьте сервер ISE для коммутации

aaa new-model

!
радиус aaa authentication dot1x default group

!
aaa authorization network default group radius

!

dot1x system-auth-control

!

ISE сервера RADIUS
address ipv4 10.48.39.161 acct-портов 1646 подлинного порта 1645
 ключевые 7 123A0C0411045D5679

2. Теперь настройте порт коммутатора AP

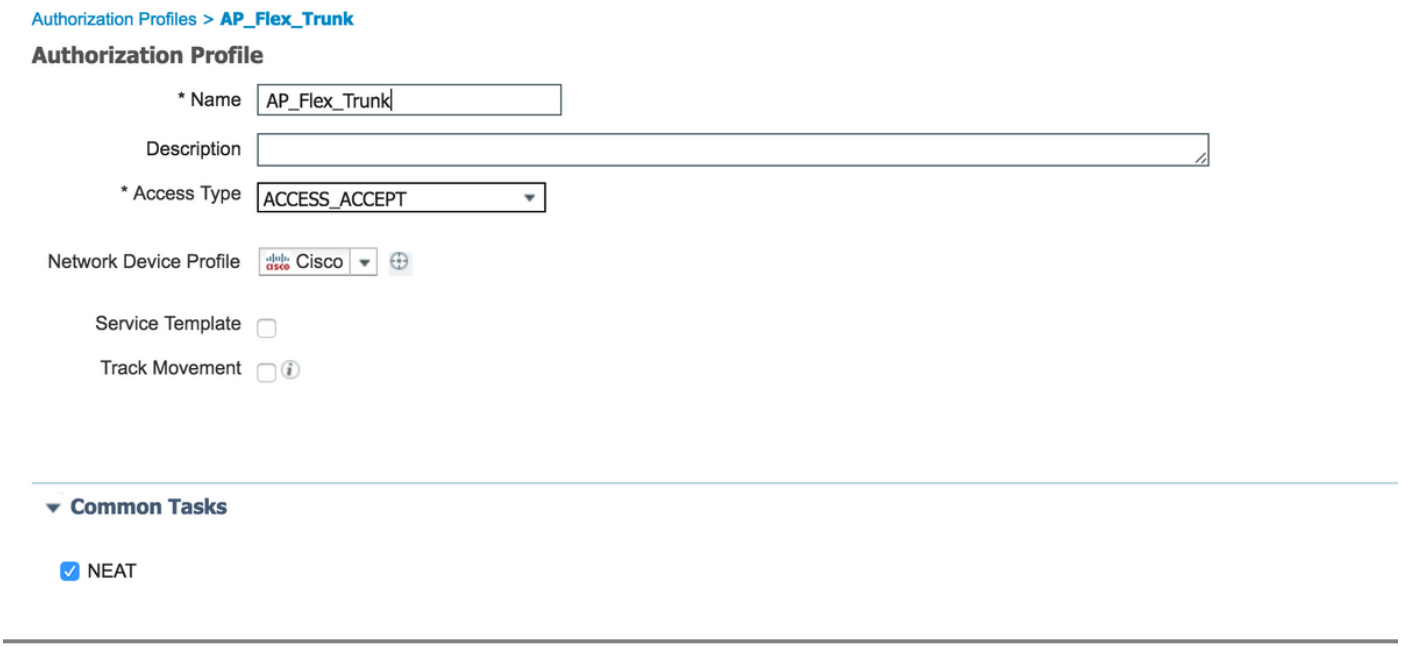
интерфейсный GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
отключение
мультихост authentication host-mode
dot1x authentication order
автоматический authentication port-control
средство проверки подлинности dot1x pae
край режима "portfast" связующего дерева

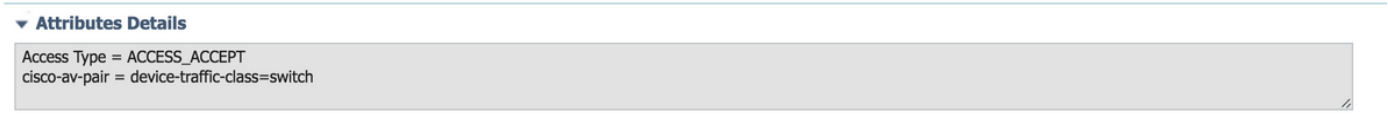
Если вы хотите настроить MAB вместо dot1x тогда, config порта похож на:-

интерфейсный GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
switchport mode access
отключение
мультихост authentication host-mode
mab authentication order
автоматический authentication port-control
mab
край режима "portfast" связующего дерева

Конфигурация ISE:-

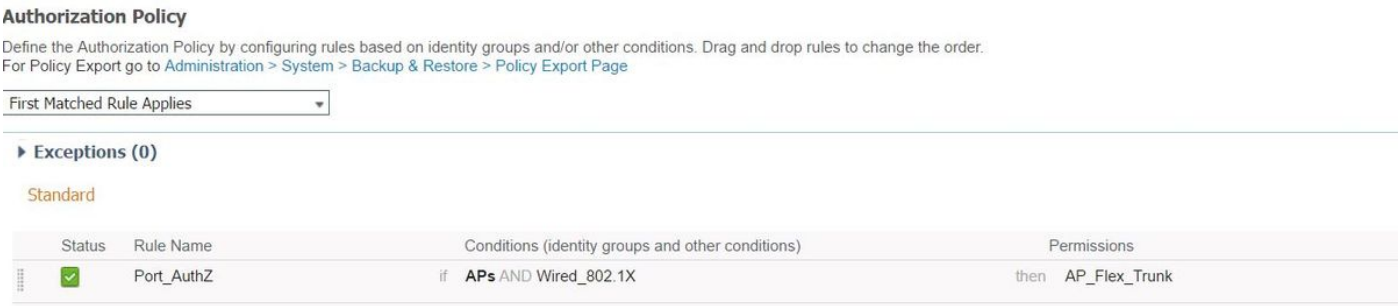
1. На ISE можно просто включить АККУРАТНЫЙ для профиля Авторизации AP для установки корректного атрибута, однако, на других серверах RADIUS, можно настроить вручную.





2. На ISE также нужно настроить Политику аутентификации и Политику авторизации. В этом случае мы поражаем правило проверки подлинности по умолчанию, которое соединено точка 1x проводом (соединенный проводом MAB в случае MAB), но можно настроить его согласно требованию.

Что касается Политики авторизации (Port_AuthZ), в этом случае мы добавили учетные данные AP к группе пользователей (AP) и выдвинули Профиль Авторизации (AP_Flex_Trunk) на основе этого.



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

1. На коммутаторе, однажды может использовать команду "автосfg функции debug authentication все", чтобы проверить, перемещается ли порт в магистральный порт или нет.

20 февраля 12:34:18.119: %LINK-3-UPDOWN: Интерфейсный GigabitEthernet0/4, измененное состояние к
20 февраля 12:34:19.122: %LINEPROTO-5-UPDOWN: Протокол линии связи на Интерфейсном GigabitEthernet0/4, измененном состоянии к
akshat_sw#

akshat_sw#
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: B dot1x AutoCfg start_fn, epm_handle: 3372220456
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] тип устройства = коммутатор
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] новый клиент
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Внутреннее Состояние приложения Макроса Автоcfg: 1
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Тип устройства: 2
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: НТП имеет port_config 0x85777D8
20 февраля 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: НТП port_config имеет bpdu guard_config 2
20 февраля 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Применение автоcfg на порту.
20 февраля 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231
20 февраля 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Применение dot1x_autocfg_supp макрос
20 февраля 12:38:11.116: команда Applying... 'никакой switchport access vlan 231' в Gi0/4
20 февраля 12:38:11.127: команда Applying... 'никакой switchport nonegotiate' в Gi0/4
20 февраля 12:38:11.127: команда Applying... 'switchport mode trunk' в Gi0/4
20 февраля 12:38:11.134: команда Applying... 'switchport trunk native vlan 231' в Gi0/4
20 февраля 12:38:11.134: команда Applying... 'spanning-tree portfast trunk' в Gi0/4
20 февраля 12:38:12.120: %LINEPROTO-5-UPDOWN: Протокол линии связи на Интерфейсном GigabitEthernet0/4, измененном состоянии к вниз
20 февраля 12:38:15.139: %LINEPROTO-5-UPDOWN: Протокол линии связи на Интерфейсном GigabitEthernet0/4, измененном состоянии к

2. Выходные данные "показывают, что выполненный интервал g0/4" покажет, что порт изменился на магистральный порт.

Текущая конфигурация: 295 байтов
!
интерфейсный GigabitEthernet0/4
switchport trunk allowed vlan 231,232,239
switchport trunk native vlan 231
!-- switchport mode trunk
мультихост authentication host-mode
dot1x authentication order
автоматический authentication port-control
средство проверки подлинности dot1x pae
граничный транк режима "portfast" связующего дерева
конец

3. На ISE при Операциях>> Радиус Livelogs каждый может мы аутентификация, являющаяся успешным и корректный выдвигаемый профиль Авторизации.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
	All								
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. Если мы подключим клиента после этого тогда, то его мак адрес будет изучен на порте коммутатора AP в клиентском vlan 232.

интервал таблицы MAC-адресов akshat_sw#sh g0/4
Таблица MAC-адресов

Vlan Mac Address Type Ports
---- ----------- -------- -----
231 588d.0997.061d СТАТИЧЕСКИЙ Gi0/4 - AP
232 c0ee.fbd7.8824 ДИНАМИЧЕСКИХ Gi0/4 - Клиент

На WLC в клиентской подробности можно заметить, что этот клиент принадлежит, vlan 232 и SSID локально коммутированы. Вот фрагмент.

(Cisco Controller)> show client detail c0:ee:fb:d7:88:24
MAC-адрес клиента..... c0:ee:fb:d7:88:24
Клиентское имя пользователя..... Н/Д
MAC-адрес AP..... b4:14:89:82:cb:90
Название AP..... Aks_desk_3502
Слот Id радио AP..... 1
Состояние клиента..... Связанный
Client User Group.....
Клиентский NAC Состояние OOB..... Доступ
Идентификатор беспроводной локальной сети..... 2
Название беспроводной локальной сети (SSID)..... Аутентификация порта
Имя профиля беспроводной локальной сети..... Аутентификация порта
Хот-спот (802.11u)..... Не поддерживается
BSSID..... b4:14:89:82:cb:9f
Связанный Для..... 42 secs
Канал..... 44
IP-адрес..... 192.168.232.90
Адрес шлюза..... 192.168.232.1
Маска подсети..... 255.255.255.0
Идентификатор ассоциации..... 1
Алгоритм аутентификации..... Open System
Код причины..... 1
Код статуса..... 0

Коммутация данных FlexConnect..... ЛОКАЛЬНЫЙ
Статус FlexConnect Dhcp..... ЛОКАЛЬНЫЙ
FlexConnect Vlan базирующаяся центральная коммутация..... Нет
Аутентификация FlexConnect..... Центральный
FlexConnect центральная ассоциация..... Нет
НАЗВАНИЕ FlexConnect VLAN..... vlan 232
Карантинная VLAN..... 0
VLAN доступа..... 232
Локальная VLAN мостового соединения..... 232

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Если аутентификация отказывает, используйте **команды debug dot1x, debug authentication**.
- Если порт не перемещен в транк, введите **автоcfg функции debug authentication вся** команда.
- Гарантируйте , что у вас есть режим мультихоста (мультихост authentication host-mode) настроенный. Мультихост должен быть включен для разрешения клиентских беспроводных MAC-адресов.
- команда "сети с проверкой подлинности AAA" должна быть настроена для коммутатора, чтобы принять и применить атрибуты, передаваемые ISE.