

Интеграция AxelNAC с контроллерами беспроводного доступа Huawei WLC

В данной статье рассматривается процесс интеграции AxelNAC с контроллером беспроводного доступа Huawei WLC.

Введение

Для корректной работы всего функционала контроллера беспроводного доступа (WLC) с AxelNAC необходимо обеспечить правильное сетевое взаимодействие на всем пути сетевого оборудования. На рисунке ниже представлена гибкая схема подключения сетевого оборудования, позволяющая реализовать весь функционал WLC:

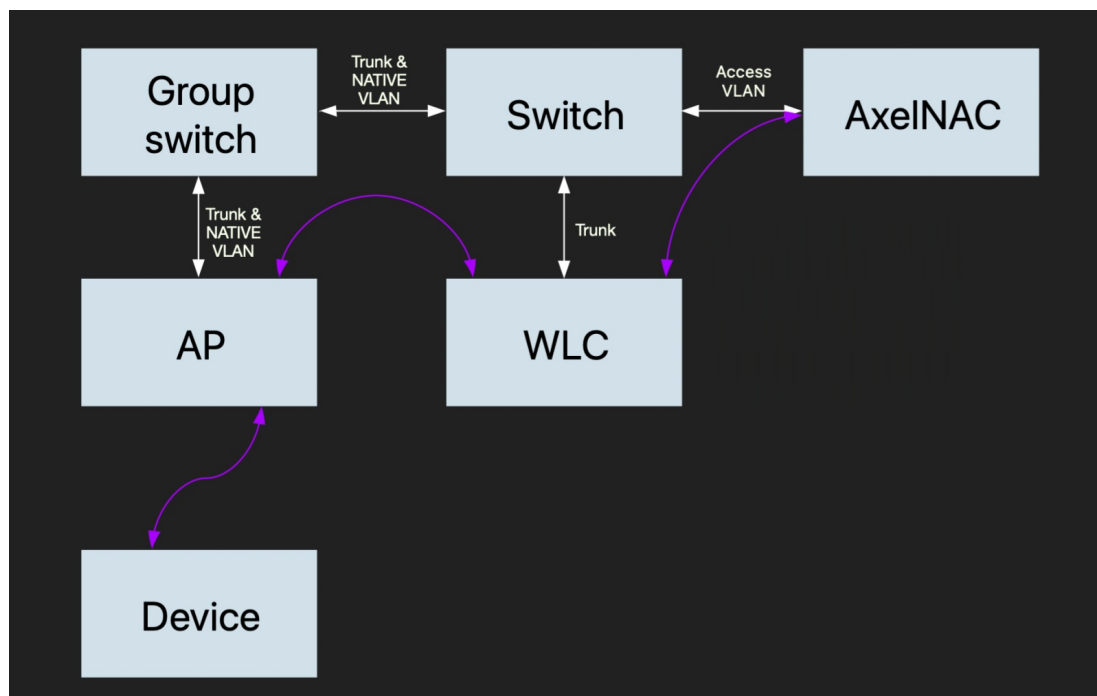


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

Белые стрелки отображают физическое соединение устройств. Фиолетовыми стрелочками показаны концептуальные соединения. Схема содержит следующие элементы:

- **AxelNAC** — виртуальный или физический сервер AxelNAC.
- **Switch** — физический коммутатор, на котором созданы все необходимые виртуальные локальные сети (VLAN);
- **Group switch** — физические коммутаторы, на которых созданы все необходимые VLAN;
- **WLC** — контроллер беспроводных сетей;
- **AP** — точка доступа;
- **Device** — конечное устройство, APM с беспроводным интерфейсом.

Настройка Huawei WLC

Первоначальная конфигурация VLAN

Для выполнения первоначальной конфигурации контроллера беспроводного доступа необходимо задать виртуальные локальные сети. В данном примере рассматриваются следующие идентификаторы:

- Сервисная VLAN — 100;
- Продуктивная VLAN — 101;
- Гостевая VLAN — 102.

Для этого необходимо подключиться к контроллеру доступа по протоколу **SSH** и назначить VLAN портам GE0/0/1 с помощью следующих команд:

```
<AC6605> system-view
[AC6605] sysname AC
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101 102
[AC-GigabitEthernet0/0/1] quit
```

Настройка RADIUS-сервера

Далее необходимо произвести настройку шаблона RADIUS-сервера, схемы аутентификации и аккаунтинга RADIUS. Для этого выполните следующие действия:

Шаг 1. Настройте шаблон RADIUS-сервера с помощью следующего набора команд:

```
[AC] radius-server authorization calling-station-id decode-mac-format ascii hyphen-sp lit common
[AC] radius-server template anac
[AC-radius-anac] radius-server authentication 10.10.10.1 1812
[AC-radius-anac] radius-server accounting 10.10.10.1 1813
[AC-radius-anac] radius-server shared-key cipher Huawei
[AC-radius-anac] quit
```

Шаг 2. Создайте схему аутентификации и настройте режим аутентификации RADIUS:

```
[AC-aaa] authentication-scheme anac
[AC-aaa-authen-anac] authentication-mode radius
[AC-aaa-authen-anac] quit
```

Шаг 3. Создайте схему аккаунтинга и настройте режим аккаунтинга RADIUS:

```
[AC-aaa] accounting-scheme anac
[AC-aaa-accounting-anac] accounting-mode radius
[AC-aaa-accounting-anac] accounting realtime 15
[AC-aaa-accounting-anac] quit
[AC-aaa] quit
```

Конфигурация portalной аутентификации

Для поддержки аутентификации через Captive-портал необходимо выполнить следующие действия:

Шаг 1. Настройте параметры перенаправления пользователей на Captive-портал с помощью следующих команд:

```
[AC] url-template name anac
[AC-url-template-anac] url http://<IP-адрес_AxeINAC>/Huawei::AC6605/
[AC-url-template-anac] url-parameter device-ip AC-IP device-mac AC-MAC redirect-url redirect-url ssid ssid user-ipaddress user-ipaddress user-mac user-mac
[AC-url-template-anac] url-parameter mac-address format delimiter : normal
[AC-url-template-anac] quit
```

Шаг 2. Настройте шаблон сервера Captive-портала:

```
[AC] web-auth-server anac
[AC-web-auth-server-anac] server-ip 10.10.10.1
[AC-web-auth-server-anac] shared-key cipher Huawei
[AC-web-auth-server-anac] port 50100 #вы можете использовать любой порт для подключения к Captive-порталу
[AC-web-auth-server-anac] url-template anac ciphered-parameter-name cpname iv-parameter-name iv-value key cipher Huawei
[AC-web-auth-server-anac] quit
```

Шаг 3. Настройте профиль доступа к Captive-порталу с именем **anac** и активируйте аутентификацию второго уровня:

```
[AC] portal-access-profile name anac
[AC-portal-access-profile-anac] web-auth-server anac direct
[AC-portal-access-profile-anac] quit
```

Шаг 4. Настройте профиль доступа к MAC для portalной аутентификации с приоритетом MAC-адреса:

```
[AC] mac-access-profile name anac
[AC-mac-access-profile-anac] quit
```

Конфигурация аутентификации 802.1x

Для реализации аутентификации с использованием стандарта 802.1x необходимо выполнить следующие действия:

Шаг 1. Создайте профиль доступа 802.1x с именем **anac**, используя следующую команду:

```
[AC] dot1x-access-profile name anac
```

Шаг 2. Установите метод аутентификации EAP на ретрансляторе:

```
[AC-dot1x-access-profile-anac] dot1x authentication-method eap
[AC-dot1x-access-profile-anac] quit
```

Шаг 3. Настройте профили аутентификации на контроллере. В нашем примере создается два профиля — **anac_prod** и **anac_guest**:

```
[AC] authentication-profile name anac_prod
[AC-authentication-profile-anac_prod] dot1x-access-profile anac
[AC-authentication-profile-anac_prod] authentication-scheme anac
[AC-authentication-profile-anac_prod] radius-server anac
[AC-authentication-profile-anac_prod] quit
[AC] authentication-profile name anac_anac_guest
[AC-authentication-profile-anac_anac_guest] portal-access-profile anac
[AC-authentication-profile-anac_anac_guest] mac-access-profile anac
[AC-authentication-profile-anac_anac_guest] free-rule-template default_free_rule
[AC-authentication-profile-anac_anac_guest] authentication-scheme anac
[AC-authentication-profile-anac_anac_guest] accounting-scheme anac
[AC-authentication-profile-anac_anac_guest] radius-server anac
[AC-authentication-profile-anac_anac_guest] quit
```

Конфигурация параметров службы WLAN

Для финальной настройки контроллера беспроводного доступа необходимо создать профили безопасности, SSID, VAP и связать их с группами точек доступа. Для этого выполните следующие действия:

Шаг 1. Создайте профили безопасности с именами **anac_prod** и **anac_guest**, и соответственно установите для них политики безопасности **WPA-WPA2+802.1X+AES** и **open**:

```
[AC] wlan
[AC-wlan-view] security-profile name anac_prod
[AC-wlan-sec-prof-anac_prod] security wpa-wpa2 dot1x aes
[AC-wlan-sec-prof-anac_prod] quit
[AC-wlan-view] security-profile name anac_guest
[AC-wlan-sec-prof-anac_guest] quit
```

Шаг 2. Создайте профили SSID с именами **anac_prod** и **anac_guest**, и соответственно установите для них имена SSID **anac_prod** и **anac_guest**:

```
[AC-wlan-view] ssid-profile name anac_prod
```

```
[AC-wlan-ssid-prof-anac_prod] ssid anac_prod
[AC-wlan-ssid-prof-anac_prod] security wpa2 dot1x aes
[AC-wlan-ssid-prof-anac_prod] quit
[AC-wlan-view] ssid-profile name anac_guest
[AC-wlan-ssid-prof-anac_guest] ssid anac_guest
```

Шаг 3. Создайте профили VAP с именами **anac_prod** и **anac_guest**, установите режим переадресации данных и сервисные VLAN и привяжите профили безопасности, SSID и аутентификации к профилям VAP:

```
[AC-wlan-view] vap-profile name anac_prod
[AC-wlan-vap-prof-anac_prod] forward-mode tunnel
[AC-wlan-vap-prof-anac_prod] service-vlan vlan-id 101
[AC-wlan-vap-prof-anac_prod] security-profile anac_prod
[AC-wlan-vap-prof-anac_prod] ssid-profile anac_prod
[AC-wlan-vap-prof-anac_prod] authentication-profile anac_prod
[AC-wlan-vap-prof-anac_prod] quit
[AC-wlan-view] vap-profile name anac_guest
[AC-wlan-vap-prof-anac_guest] forward-mode tunnel
[AC-wlan-vap-prof-anac_guest] service-vlan vlan-id 102
[AC-wlan-vap-prof-anac_guest] security-profile anac_guest
[AC-wlan-vap-prof-anac_guest] ssid-profile anac_guest
[AC-wlan-vap-prof-anac_guest] authentication-profile anac_guest
[AC-wlan-vap-prof-anac_guest] quit
```

Шаг 4. Свяжите профили VAP с группами AP и примените конфигурацию профилей VAP **anac_prod** и **anac_guest** к Radio 0 и Radio 1 точек доступа.

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile anac_prod wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile anac_prod wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] vap-profile anac_guest wlan 2 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile anac_guest wlan 2 radio 1
[AC-wlan-ap-group-ap-group1] quit
```

Интеграция WLC с AxelNAC

После того как Huawei WLC настроен, необходимо настроить его профиль для AxelNAC.

Шаг 1. Перейдите во вкладку **Конфигурация → Политики и контроль доступа → Сетевые устройства**, нажмите на кнопку **Новое сетевое устройство** и в выпадающем списке выберите к какой группе должно принадлежать устройство (по умолчанию создана группа **default**).

Новое сетевое устройство default

Определение

Роли

Режим Inline

RADIUS

SNMP

CLI

Веб-службы

Базовый режим ☐

IP-адрес/MAC-адрес/диапазон (CIDR)

10.13.234.15

Описание

Test_WLC

Тип

Huawei AC6605

Режим

Продуктивный

Группа сетевых устройств

default - (Switches Default Values)

Метод реаутентификации

1* Выберите опцию

Реаутентификация на предыдущем сетевом устройстве

☒ Да

Данный параметр позволяет выполнять реаутентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.

SSID гостевой сети

Axel_guest

SSID гостевых сетей для аутентификации через портал (разделенные знаком +)

Обеспечение работы внешнего портала

☒ Да

Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.

VoIP

☐ По умолчанию (Нет)

Обнаружение VoIP DHCP

☒ По умолчанию (Да)

Определить VoIP по отпечатку DHCP.

Примечание: Некоторые настройки, связанные с RADIUS, перенесены на новую вкладку RADIUS

Создать

Сбросить

Отмена

Шаг 2. Укажите IP-адрес контролера (вы можете указать IP-адрес/MAC-адрес/IP-netmask).

Шаг 3. Укажите тип устройства — в данном примере **Huawei AC6605**.

Шаг 4. В поле **Метод реаутентификации** из выпадающего списка выберите значение **RADIUS**.

Шаг 5. Активируйте переключатель **Обеспечение работы внешнего портала**.

Для корректной работы перенаправления, для гостевой сети необходимо задать явное имя.

Шаг 6. Переключитесь на вкладку **Роли**.

Шаг 7. Настройте VLAN который был создан и добавлен как VLAN для пользователей в WLAN WLC. В примере будет использоваться

роль **registration**.

Новое сетевое устройство default

Определение

Роли

Режим Inline

RADIUS

SNMP

CLI

Веб-службы

Базовый режим ☐

Назначение VLAN ID

Назначать VLAN ID ☒ По умолчанию (Да)

registration	1#	2
isolation	1#	3
macDetection		
inline	1#	6
Machine		
REJECT	1#	-1
User		

Теперь при подключении пользователя в роли **registration** через этот контроллер поместит его в VLAN 2 (registration).

Шаг 8. Активируйте переключатель **Сопоставление ролей по ACL** — данный функционал отвечает за отправку ACL или redirect-ACL.

Шаг 9. Укажите для роли **registration** созданный ранее на контроллере ACL. Теперь при подключении пользователя в роли **registration** через этот контроллер на него применится созданный ACL.

Шаг 10. Активируйте переключатель **Сопоставлять роль по URL веб-аутентификации**. Это необходимо для того, чтобы ACL применялся как redirect-ACL.

Шаг 11. Укажите для роли **registration** значение "http://<AxelNAC-ip-address>/Huawei::AC6605", уникальная ссылка будет генерироваться автоматически. Если вы хотите перенаправлять пользователей на HTTPS-портал, просто укажите значение "https://<AxelNAC-ip-address>/Huawei::AC6605".

Назначение URL веб-аутентификации

Назначать URL веб-аутентификации ☒ Да

registration	https://<AxelNAC-ip-address>/Huawei::AC6605
isolation	
macDetection	
inline	
Machine	
REJECT	
User	
default	
gaming	
guest	
voice	

Шаг 12. Перейдите на вкладку **RADIUS**.

Новое сетевое устройство

default

✕

Определение

Роли

Режим Inline

RADIUS

SNMP

CLI

Веб-службы

Базовый режим

Секретная фраза

••••••••

👁

Использовать CoA

По умолчанию (Да)

Использовать CoA, если он доступен, для реаутентификации пользователя. Если данный параметр отключен, вместо него будет использоваться RADIUS Disconnect, если он доступен.

Использовать коннектор для реаутентификации

По умолчанию (Да)

Использовать доступные коннекторы AxelNAC для выполнения реаутентификации RADIUS. По умолчанию на этом сервере размещен локальный коннектор.

IP-адрес контроллера

Данный IP-адрес будет использоваться для запросов на реаутентификацию. Обычно применяется только для Wi-Fi.

Disconnect-порт

Укажите порт для переадресации Disconnect-запроса.

CoA-порт

Укажите порт для переадресации CoA-запроса.

Валидация после MFA

По умолчанию (Нет)

Добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA.

Доступ к CLI/VPN разрешен

По умолчанию (Нет)

Разрешить данному сетевому оборудованию использовать AxelNAC в качестве RADIUS-сервера для доступа к CLI или VPN.

Создать

Сбросить

Отмена

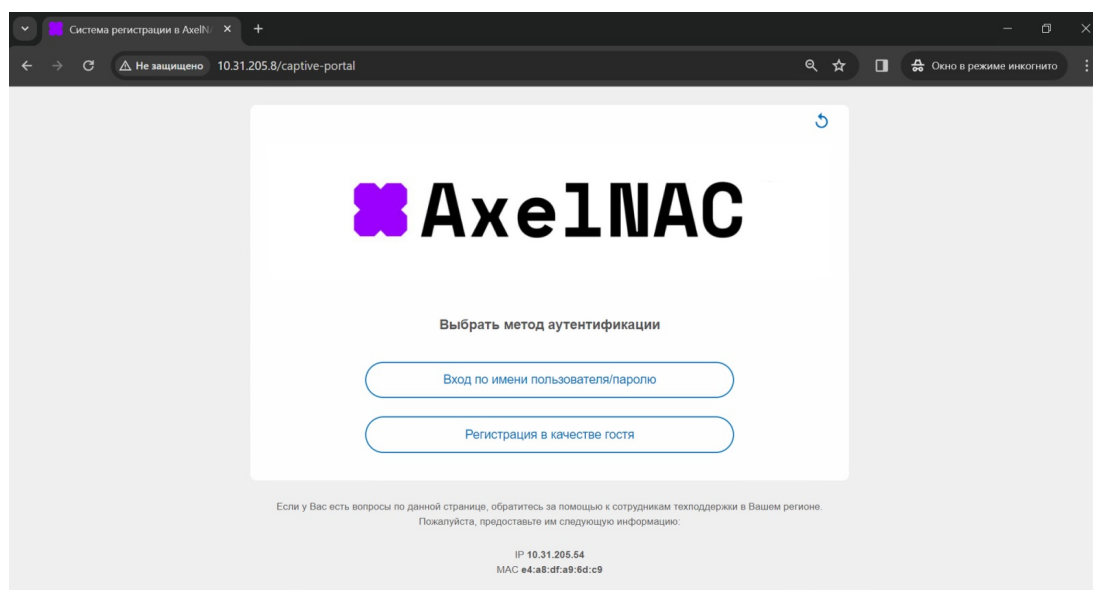
Шаг 13. Укажите секретную фразу, которую вы создали на контроллере.

Шаг 14. Установите переключатель **Использовать CoA** в положение **Да**.

Шаг 15. Активируйте переключатель **Использовать коннектор для реаутентификации** и нажмите **Создать** в левом нижнем углу окна.

После этого, профиль для сетевого оборудования считается настроенным. Теперь при подключении пользователя через контроллер, если он будет попадать в роль registration, пользователь будет попадать в VLAN 3143, ему будет отправлен redirect-ACL и ссылка на redirect.

Настройка Captive-портала в AxelNAC.



Для того, чтобы настроить работу Captive-портала в AxelNAC, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс на котором необходимо включить функционал Captive-портала.

Шаг 2. В строке **Дополнительный демон(ы) прослушивания** добавьте значение **portal** из выпадающего списка, затем нажмите **Сохранить**.

Шаг 3. Перейдите в раздел **Статус → Службы** и перезапустите следующие службы:

- haproxy-portal;
- httpd.portal;
- iptables.

ID статьи: 391

Последнее обновление: 27 мая, 2025

Обновлено от: Егоров В.

Ревизия: 5

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с контроллерами беспроводного доступа Huawei WLC

<https://docs.axel.pro/entry/391/>