Безопасность WLAN

HUAWEI

Предисловие

- Открытая среда передачи в беспроводной сети ставит вопросы обеспечения безопасности WLAN на первое место. С ростом скорости беспроводного доступа, обеспечиваемую новыми стандартами 802.11, все больше и больше пользователей начинают использовать WLAN. Пользователи наряду с предприятиями предъявляют высокие требования к безопасности доступа к WLAN и уделяют особое внимание безопасности передачи данных.
- В настоящем курсе приведена информация о принципах обеспечения безопасного доступа к WLAN, безопасности данных и настройки системы безопасности.

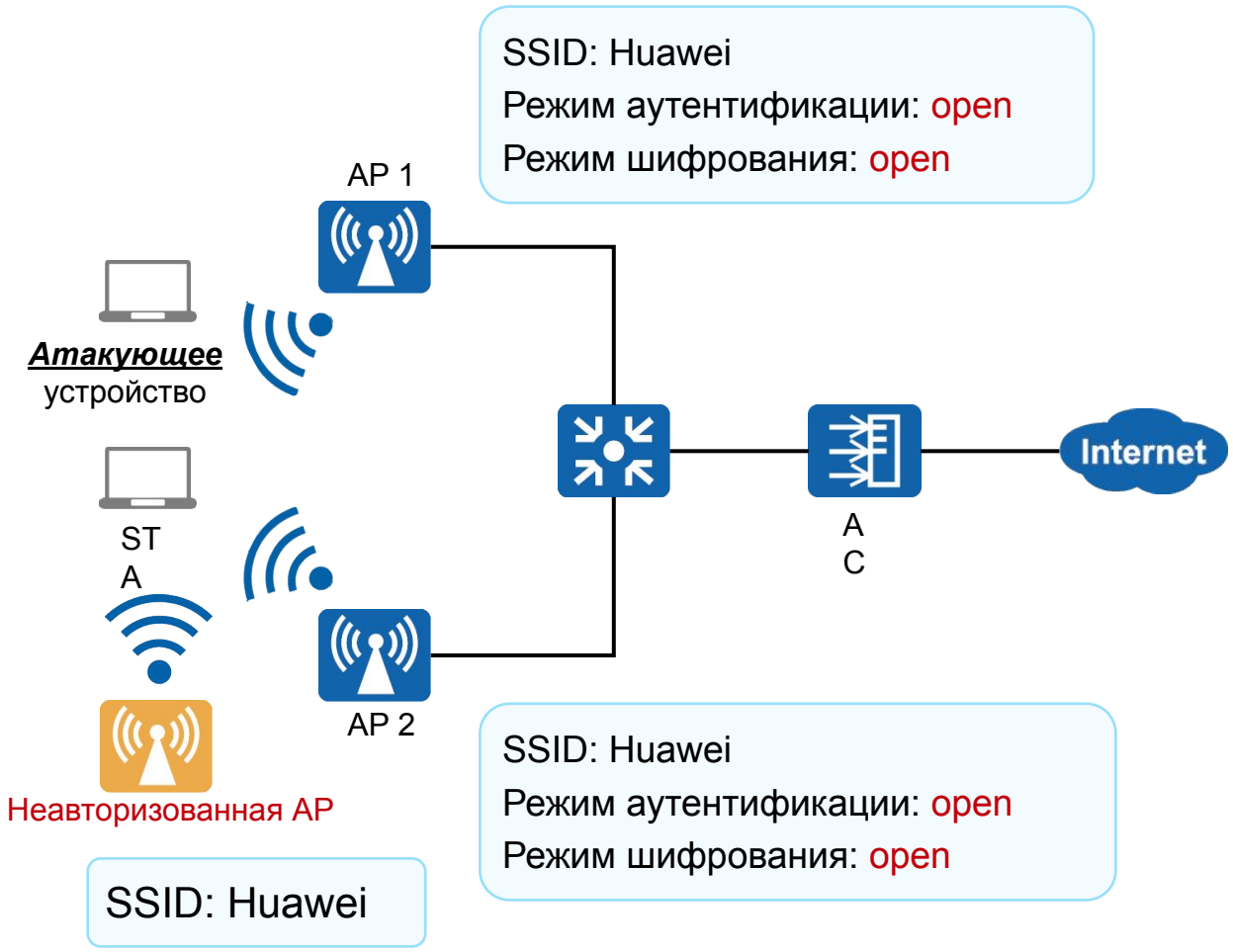
Цели

По окончании данного курса слушатели получат следующие знания:

- угрозы безопасности WLAN;
- механизмы обеспечения безопасности WLAN;
- стандартные режимы аутентификации доступа к WLAN.

Содержание

Распространенные угрозы безопасности WLAN



- **Без аутентификации (No authentication)**: злоумышленники могут случайным образом подключиться и незаконно проникнуть в сеть Wi-Fi.
- **Незашифрованные данные (Non-encrypted wireless data)**: злоумышленники могут перехватывать пакеты, передаваемые по радиоинтерфейсу, и подделывать служебные данные, передаваемые по каналам беспроводной связи.
- **Угроза по периметру (Perimeter threat)**: если несанкционированная точка доступа (AP) публикует тот же SSID, что и авторизованные AP, станция (STA) может подключиться к несанкционированной AP. В результате осуществляется перехват данных STA.

Обеспечение безопасности WLAN

- Аутентификация безопасности
  - Доступ и использование сети разрешен только авторизованным пользователям.
  - Доступна двусторонняя аутентификация: клиент и сервер могут проверить подлинность друг друга.
- Шифрование и целостность данных
  - Гарантируется конфиденциальность данных, передаваемых в среде передачи.
  - Хеширование, проверка целостности сообщения (MIC) и проверка циклическим избыточным кодом (CRC) гарантируют целостность данных.
- Безопасность периметра (в данном документе не описывается)
  - Беспроводная система обнаружения вторжений (WIDS) отслеживает рабочее состояние сетей и систем в соответствии с заданными политиками безопасности, анализирует действия пользователей и определяет тип событий вторжения для обнаружения неавторизованных сетей.
  - Беспроводная система предотвращения вторжений (WIPS) отслеживает беспроводные сети в режиме реального времени для обнаружения вторжений и обеспечивает активную защиту и предупреждения об атаках.

Содержание

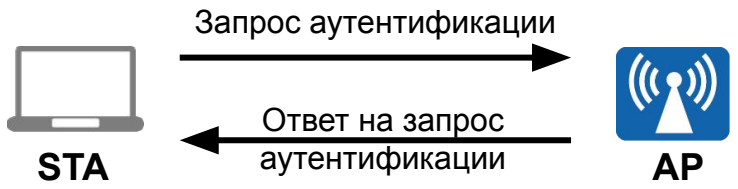
1. Угрозы безопасности WLAN и защита
2. **Безопасность доступа к WLAN**
3. Безопасность данных WLAN
4. Контроль доступа к сети WLAN
5. Настройки безопасности WLAN

Процедура подключения к WLAN

- Станция (STA) обнаруживает окружающие беспроводные сети в режиме активного/пассивного сканирования. После завершения аутентификации соединения, ассоциации и аутентификации доступа станция может подключиться к точке доступа и получить доступ к услугам беспроводной связи.

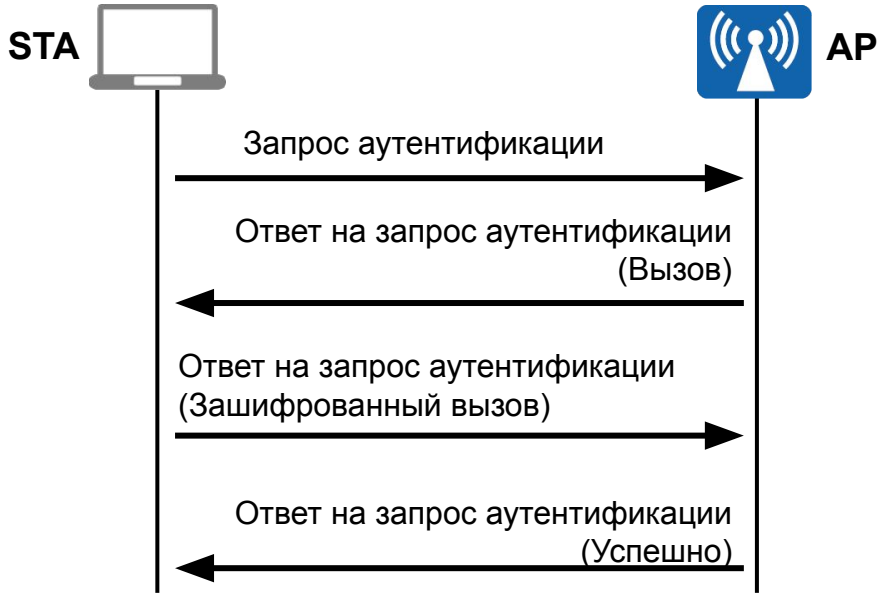
Аутентификация канала: аутентификация с помощью открытой системы

- Чтобы гарантировать безопасность беспроводного соединения, точка доступа должна аутентифицировать станции, которые пытаются подключиться к этой точке доступа. IEEE 802.11 определяет два режима аутентификации канала: аутентификация с помощью открытой системы и аутентификация с общим ключом.
- Аутентификация с помощью открытой системы не требует аутентификации. В этом режиме точка доступа отвечает на запрос аутентификации от любой станции сообщением, указывающим, что STA проходит аутентификацию.
- При подключении к SSID, который использует аутентификацию с помощью открытой системы, учетные данные для проверки подлинности не требуются, и система выводит сообщение об успешном присоединении к WLAN.



Аутентификация канала: аутентификация с общим ключом

- Аутентификация с общим ключом требует, чтобы станция и точка доступа имели один и тот же предварительно настроенный ключ. В этом режиме во время аутентификации канала точка доступа проверяет, совпадает ли ее ключ с ключом станции. Если ключ совпадает, значит аутентификация прошла успешно. В противном случае станция не проходит аутентификацию.

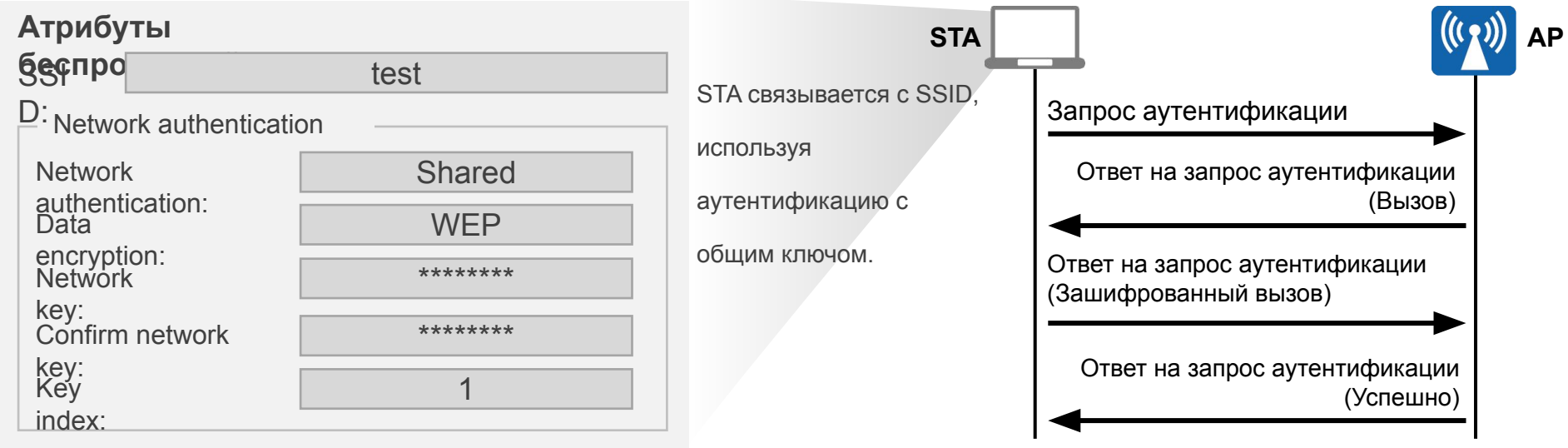


Общая информация о безопасности доступа пользователей

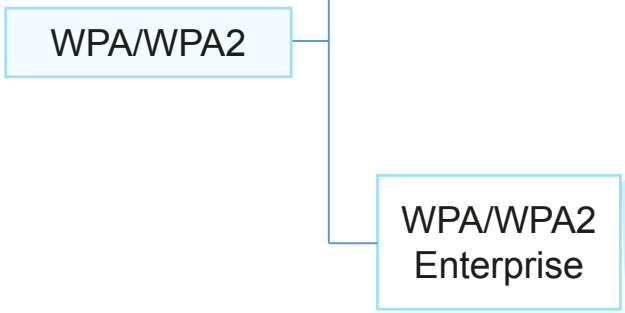
Чтобы обеспечить безопасный доступ пользователей беспроводной сети к WLAN, необходимо принять определенные меры безопасности, например, установить ассоциации безопасности (security associations) посредством аутентификации для подтверждения достоверности идентификаторов всех объектов связи.

Политика безопасности аутентификации доступа: WEP

- Wired Equivalent Privacy (WEP) — это механизм безопасности, определенный в IEEE 802.11 для предотвращения перехвата данных, передаваемых авторизованными пользователями в WLAN.
- WEP использует алгоритм Rivest Cipher 4 (RC4) и статический ключ для шифрования данных. Все станции, связанные с одним SSID, используют один ключ для присоединения к WLAN.
- Аутентификация с общим ключом поддерживается только WEP, при этом требуется, чтобы для станции и точки доступа, с которой связывается станция, был настроен один общий ключ.
- Использовать WEP не рекомендуется, так как обмен ключами WEP осуществляется в виде открытого текста.



Политика безопасности аутентификации доступа: WPA/WPA2



WPA/WPA2 Personal

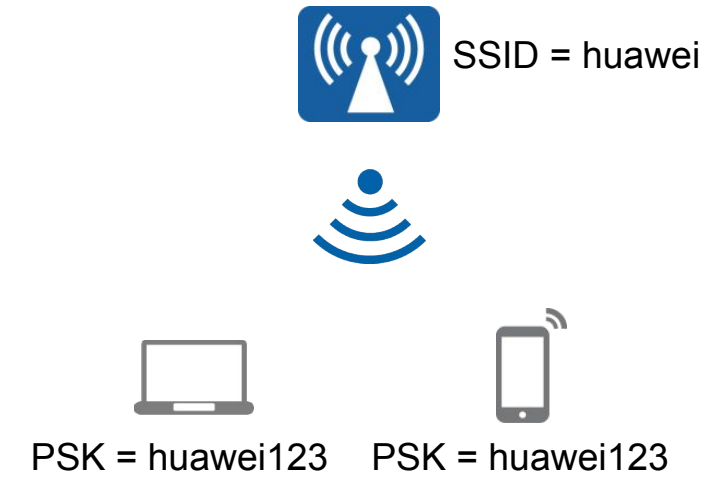
- Для малых или средних сетей WLAN развертывание специального сервера аутентификации является дорогостоящим мероприятием, при этом возникают сложность в обслуживании.
- WPA/WPA2-Personal использует предварительные общие (pre-shared key) ключи (WPA/WPA2-PSK) для простой реализации и управления.
- Специальный сервер аутентификации не требуется. На каждом узле WLAN (например, на сервере WLAN, беспроводном маршрутизаторе и сетевом адаптере) необходимо заранее ввести только предварительный общий ключ. Клиент WLAN может получить доступ к WLAN, если его предварительный общий ключ совпадает с ключом, настроенным на узле WLAN.
- Предварительный общий ключ используется только для аутентификации, не используется для шифрования; следовательно, не создает угроз безопасности, как аутентификация с общим ключом 802.11.

WPA/WPA2 Enterprise

- Используется режим аутентификации WPA/WPA2-802.1X.
- Для аутентификации используются сервер RADIUS и протокол Extensible Authentication Protocol (EAP).
- Пользователи предоставляют информацию, необходимую для аутентификации, включая имя пользователя и пароль, а сервер аутентификации (обычно сервер RADIUS) выполняет аутентификацию.
- Крупные корпоративные WLAN для аутентификации обычно используют WPA/WPA2-Enterprise.

Аутентификация PSK и PPSK

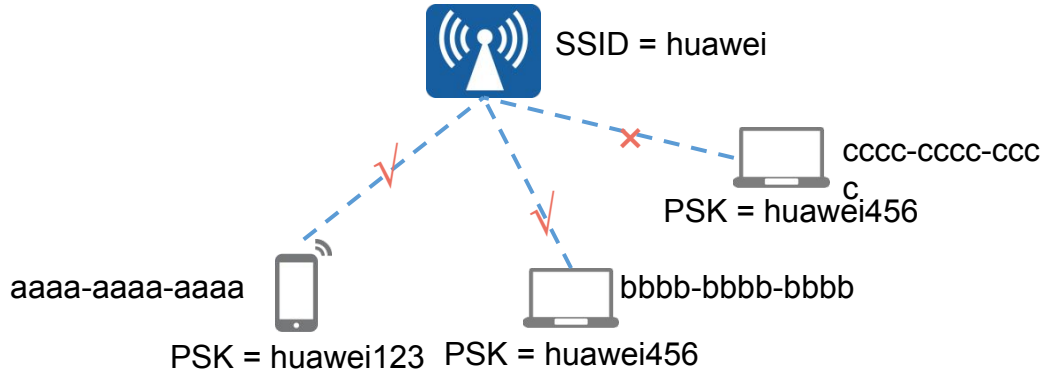
PSK



- Аутентификация WPA/WPA2-PSK требует, чтобы один и тот же предварительный общий ключ был настроен на беспроводном клиенте и беспроводном сервере (например, точке доступа).
- Все клиенты, подключенные к указанному SSID, используют один ключ, однако это представляет угрозу безопасности.

PPSK

MAC-адрес	Пароль
aaaa-aaaa-aaaa	huawei123
bbbb-bbbb-bbbb	huawei456



- Аутентификация WPA/WPA2-PPSK использует преимущества аутентификации WPA/WPA2-PSK и проста в развертывании. Кроме того, аутентификация WPA/WPA2-PPSK предоставляет разные предварительные общие ключи для разных клиентов, повышая безопасность сети.
- Пользователи, подключенные к одному SSID, могут иметь разные ключи.

Содержание

1. Угрозы безопасности WLAN и защита
2. Безопасность доступа к WLAN
3. **Безопасность данных WLAN**
4. Контроль доступа к сети WLAN
5. Настройки безопасности WLAN

Шифрование сети WLAN

- После аутентификации и авторизации пользователя для подключения к WLAN применяется механизм защиты данных пользователя от несанкционированного доступа и перехвата. Шифрование — это наиболее часто используемый механизм. Алгоритмы шифрования гарантируют, что только устройства с правильными ключами могут расшифровать полученные пакеты.
- Режимы шифрования WLAN:
  - Протокол целостности временного ключа (TKIP)
  - Протокол CBC-MAC режима счетчика (CCMP)
- WPA использует алгоритм шифрования TKIP для сброса ключа и увеличения допустимой длины ключа, устраняя недостатки ключа WEP.
- WPA2 использует механизм шифрования CCMP с алгоритмом шифрования Advanced Encryption Standard (AES). Этот алгоритм представляет собой технологию симметричного блочного шифрования, что сильно усложняет взлом ключа по сравнению с алгоритмом шифрования TKIP.
- Для лучшей совместимости и WPA, и WPA2 могут использовать алгоритм шифрования TKIP или AES. TKIP и AES обеспечивают практически одинаковый уровень безопасности.

Сравнение политик безопасности WLAN

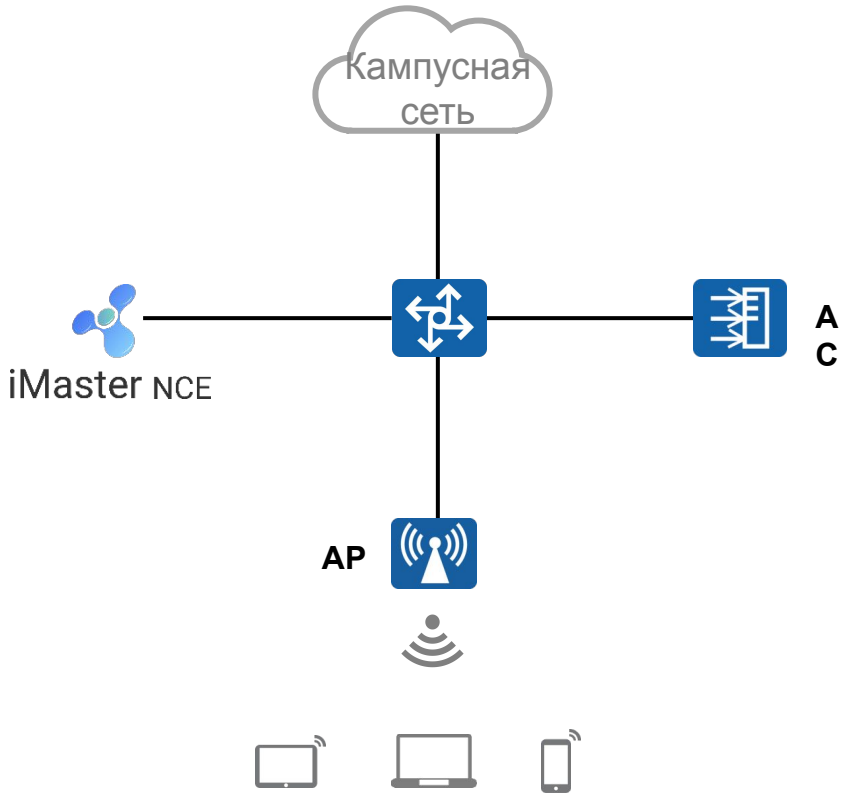
Политика безопасности	Аутентификация канала	Аутентификация доступа	Алгоритм шифрования	Рекомендуемый сценарий применения	Описание
Open	Аутентификация с помощью открытой системы	—	Без шифрования	Сети с низкими требованиями к безопасности	Беспроводные устройства могут подключаться к WLAN без аутентификации.
WEP-open	Аутентификация с помощью открытой системы	Аутентификация доступа не предусмотрена. Эта политика безопасности может использоваться вместе с аутентификацией Portal или MAC-адреса.	Без шифрования / RC4	Общественные места с большим количеством пользователей с высокой мобильностью (например, аэропорты, вокзалы, бизнес-центры и конференц-залы).	Определенные риски при независимом использовании, так как любые клиенты беспроводной сети могут получить доступ к WLAN без аутентификации. Рекомендуется настроить эту политику безопасности вместе с аутентификацией портала или MAC-адреса.
WEP-share-key	Аутентификация с общим ключом	—	RC4	Сети с низкими требованиями к безопасности	Эта политика безопасности не рекомендуется из-за ее низкой безопасности.
WPA/WPA2-PSK	Аутентификация с помощью открытой системы	Аутентификация PSK	TKIP/AES	Домашние пользователи или небольшие/средние корпоративные сети	Эта политика безопасности имеет более высокий уровень безопасности, чем аутентификация с общим ключом WEP. Сторонний сервер не требуется, невысокая стоимость.
WPA/WPA2-802.1X	Аутентификация с помощью открытой системы	Аутентификация 802.1X	TKIP/AES	Крупные корпоративные сети с высокими требованиями к безопасности	Эта политика безопасности обеспечивает высокий уровень безопасности и требует наличия стороннего сервера, что приводит к высоким затратам.

Содержание

1. Угрозы безопасности WLAN и защита
2. Безопасность доступа к WLAN
3. Безопасность данных WLAN
4. **Контроль доступа к сети WLAN**
5. Настройки безопасности WLAN

NAC

- Контроль доступа к сети (NAC) — это технология сквозной безопасности, которая позволяет аутентифицировать клиентов и пользователей доступа для обеспечения безопасности сети.



Для осуществления аутентификации доступа NAC работает вместе с сервером аутентификации, авторизации и учета (AAA).

- NAC:
  - Используется для взаимодействия между пользователями и устройствами доступа.
  - Управляет режимом доступа пользователя (802.1X, MAC или аутентификация Portal), а также параметрами и таймерами во время подключения пользователя.
  - Обеспечивает безопасные и стабильные соединения между авторизованными пользователями и устройствами доступа.
- AAA:
  - Используется для взаимодействия между устройствами доступа и сервером AAA.
  - Сервер AAA контролирует права доступа пользователей путем аутентификации, авторизации и учета.

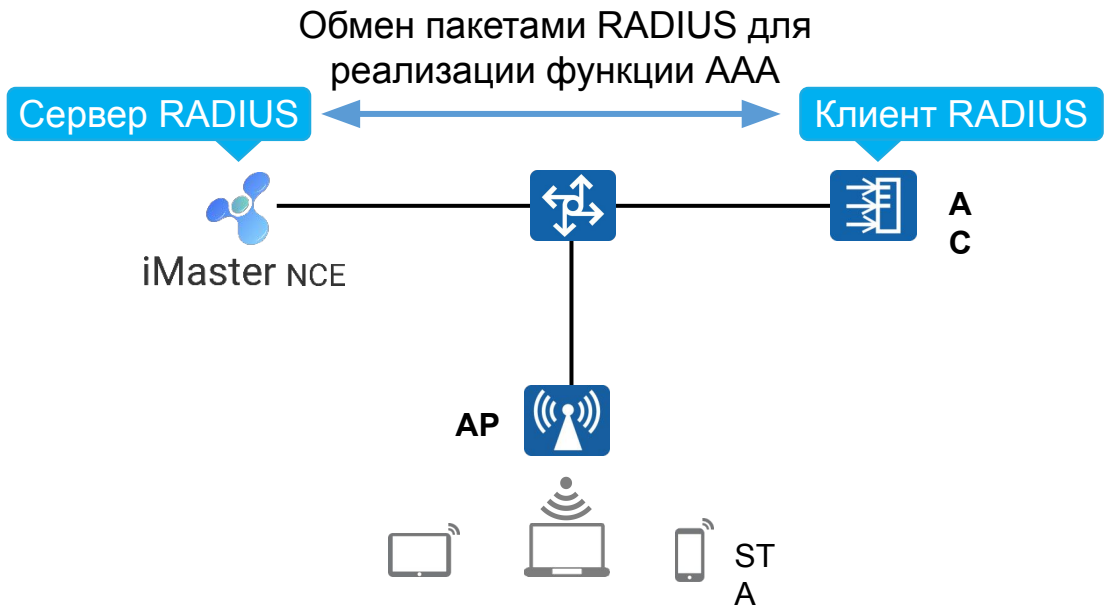
AAA

- Аутентификация, авторизация и учет (AAA) обеспечивают механизм управления сетевой безопасностью.
  - Аутентификация: проверяет, разрешен ли пользователям доступ к сети.
  - Авторизация: позволяет пользователям использовать определенные услуги.
  - Учет: записывает сетевые ресурсы, используемые пользователями.

Аутентификация	Авторизация	Учет
Для подключения к сети пользователь вводит имя пользователя и пароль для подтверждения подлинности.	Пользователь проходит аутентификацию. Сеть передает данные авторизации пользователя (пользователь принадлежит к VLAN 10 и может подключаться к Интернету).	Пользователь подключается к сети, после чего включается учет.

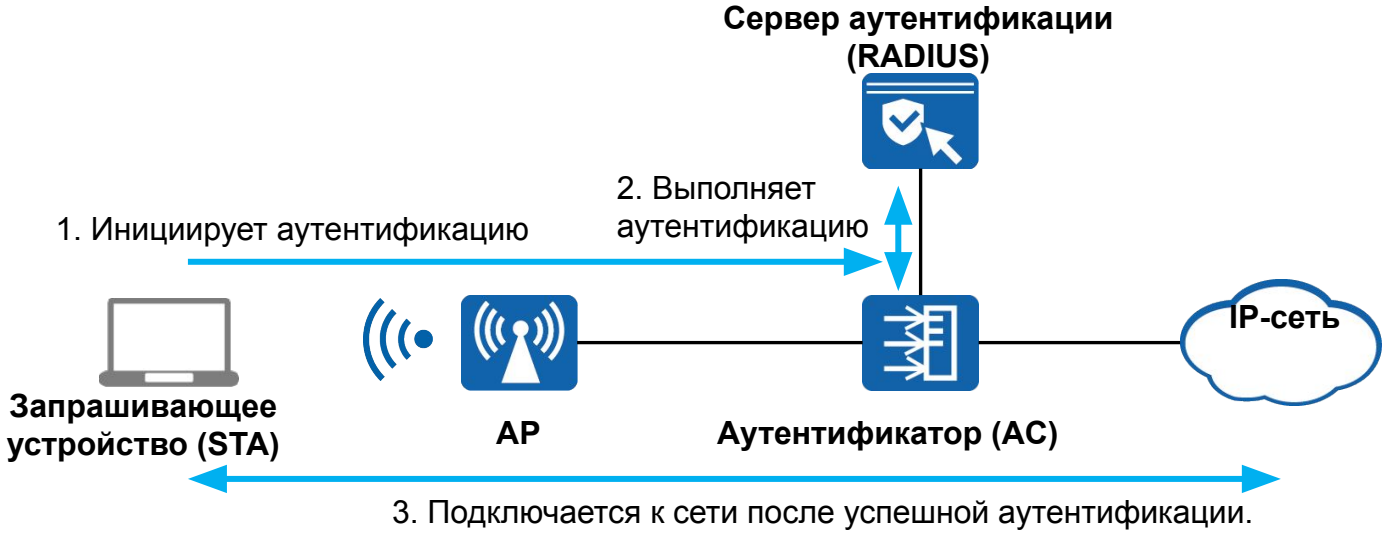
RADIUS

- AAA может быть реализован с использованием нескольких протоколов. RADIUS в основном используется в реальных сценариях.
- RADIUS — это протокол, который использует модель клиент/сервер в распределенном режиме и защищает сеть от несанкционированного доступа. Часто используется в сетевых средах, требующих высокой безопасности и разрешающих удаленный доступ пользователей.
- Определяет основанный на UDP формат пакета RADIUS и механизм передачи и определяет порты UDP 1812 и 1813 для аутентификации и учета соответственно.
- Характеристики RADIUS:
  - Модель клиент/сервер
  - Механизм безопасного обмена сообщениями
  - Отличная масштабируемость



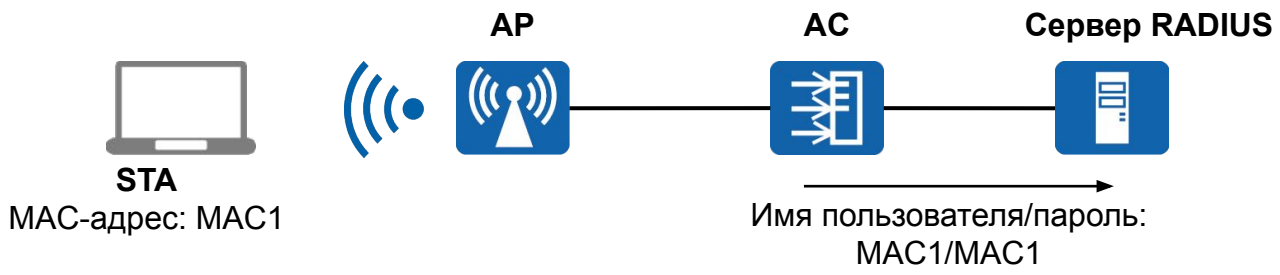
Аутентификация 802.1X

- IEEE 802.1X — это стандарт IEEE для управления доступом к сети на основе портов. В основном используется для аутентификации и безопасности в сети Ethernet.
- Аутентификация 802.1X использует модель клиент-сервер и состоит из трех объектов: запрашивающее устройство, аутентификатор и сервер аутентификации.
- Сервер аутентификации обычно представляет собой сервер RADIUS, который используется для выполнения аутентификации, авторизации и учета запрашивающих устройств.
- Аутентификация 802.1X рекомендуется для сотрудников средних и крупных предприятий.



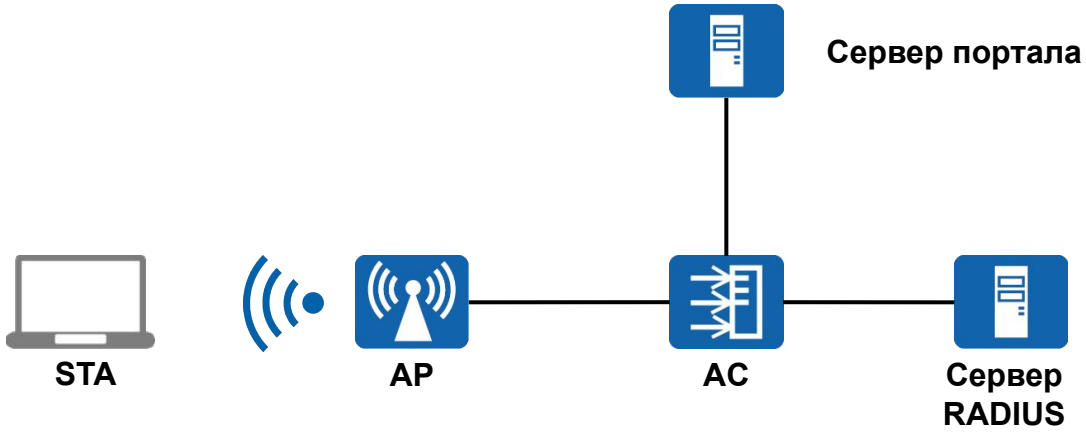
Аутентификация MAC-адреса

- Аутентификация MAC-адреса контролирует права доступа пользователя к сети на основе MAC-адреса пользователя. В этом режиме аутентификации пользователю не нужно устанавливать какое-либо клиентское программное обеспечение.
- Устройство доступа, в интерфейсе которого включена аутентификация MAC-адреса, начинает аутентификацию пользователя при обнаружении MAC-адреса пользователя в первый раз.
- В процессе аутентификации пользователю не нужно вводить имя пользователя или пароль.
- Аутентификация по MAC-адресу обычно используется при подключении «немых» терминалов (например, принтеров) к сети. Можно также использовать с сервером аутентификации для выполнения аутентификации Portal с приоритетом MAC-адреса: Пользователь впервые проходит аутентификацию, затем, в течение определенного периода времени, он сможет снова получить доступ к сети без аутентификации.



Аутентификация Portal

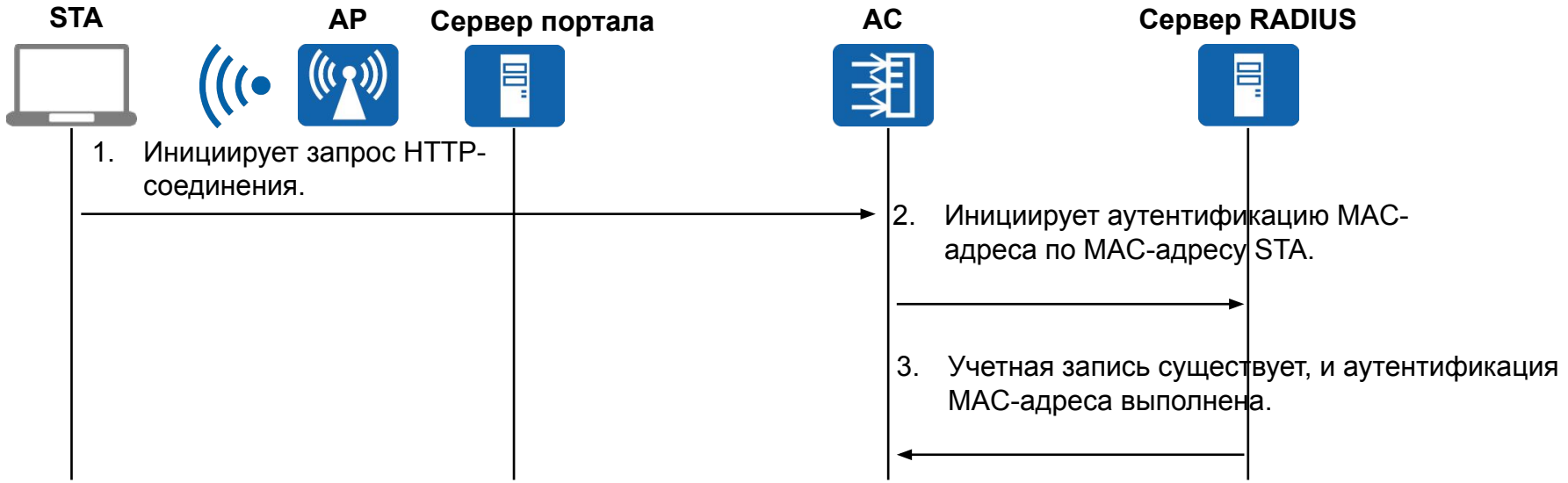
- Аутентификация Portal также называется веб-аутентификацией. В этом режиме аутентификации браузер используется в качестве клиента аутентификации, при этом устанавливать независимый клиент аутентификации не нужно. См. рис.
- Прежде чем пользователь сможет получить доступ к Интернету, он должен пройти аутентификацию на странице портала. Пользователь получает доступ к сетевым ресурсам только после прохождения аутентификации. На странице портала поставщик услуг может расширить свой бизнес, например, за счет показа рекламных объявлений.
- Аутентификация Portal рекомендуется для гостей, деловых выставок и общественных мест крупных и средних предприятий.
- Режимы аутентификации Portal:
  - Имя пользователя и пароль аутентификации: администратор регистрирует временную учетную запись для гостей. Гости используют эту временную учетную запись для аутентификации.
  - SMS-аутентификация: Гости проходят аутентификацию с использованием проверочных кодов.



Аутентификация Portal с приоритетом MAC-адреса

- Аутентификация Portal с приоритетом MAC-адреса позволяет отключенным пользователям, которые прошли аутентификацию Portal, снова получить доступ к сети в течение определенного периода времени без ввода имени пользователя и пароля, если они проходят аутентификацию по MAC-адресу.
- Пользователь проходит аутентификацию Portal и снова получает доступ к сети через аутентификацию MAC-адреса в течение срока действия MAC-адреса.
- Аутентификация Portal с приоритетом MAC-адреса экономит время пользователей на получение SMS-сообщений или выполнение инструкций для подключения через официальные учетные записи при каждой аутентификации.

Аутентификация MAC-адреса (После отключения от сети пользователь сможет снова подключиться к Интернету в течение срока действия MAC-адреса.)



Сравнение режимов аутентификации

- NAC предоставляет три режима аутентификации: аутентификация 802.1X, аутентификация MAC-адреса и аутентификация Portal Эти три режима аутентификации реализованы по-разному и применяются в разных сценариях. На практике можно использовать соответствующий режим аутентификации или несколько режимов аутентификации (смешанная аутентификация) в зависимости от сценария. Комбинация режимов аутентификации зависит от технических характеристик устройства.

Пункт	Аутентификация 802.1X	Аутентификация MAC-адреса	Аутентификация Portal
Сценарий применения	Новая сеть с высокой концентрацией пользователей и высокими требованиями к безопасности	Аутентификация «немых» терминалов (принтеры, факсы и т.п.)	Сценарий с рассредоточенными_или свободно перемещающимися пользователями
Клиент	Требуется	Не требуется	Не требуется
Преимущество	Высокая степень защиты	Клиент не требуется	Гибкое развертывание
Недостатки	Негибкое развертывание	Требуется регистрация MAC-адреса, что усложняет управление	Низкий уровень безопасности

Содержание

1. Угрозы безопасности WLAN и защита
2. Безопасность доступа к WLAN
3. Безопасность данных WLAN
4. Контроль доступа к сети WLAN
5. **Настройки безопасности WLAN**

Настройка открытой (open) аутентификации

- Создайте профиль безопасности.

```
[AC] wlan
[AC-wlan-view] security-profile name profile-name
```

  - Создайте профиль безопасности и войдите в режим профиля безопасности. По умолчанию создаются профили безопасности default, default-wds и default-mesh.

- Установите для политики безопасности значение open authentication.

```
[AC-wlan-sec-prof-wlan] security open
```

  - Установите для политики безопасности значение open authentication. По умолчанию для политики безопасности настроено значение open.

Настройка политики безопасности WEP

- Создайте профиль а безопасности.

```
[AC] wlan
[AC-wlan-view] security-profile name profile-name
```

- Установите для политики безопасности значение WEP.

```
[AC-wlan-sec-prof-wlan] security wep share-key
```

- Настройте общий ключ WEP.

```
[AC-wlan-sec-prof-wlan] wep key key-id { wep-40 | wep-104 | wep-128 } { pass-phrase | hex } key-value
```

  - Настройте общий ключ и индекс ключа для статического WEP.

Настройка аутентификации WPA/WPA2-PSK

- Создайте профиль безопасности.

```
[AC] wlan
[AC-wlan-view] security-profile name profile-name
```

- Установите для политики безопасности значение WEP/WPA2-PSK.

```
[AC-wlan-sec-prof-wlan] security { wpa | wpa2 | wpa-wpa2 } psk { pass-phrase | hex } key-value { aes | tkip | aes-tkip }
```

Настройка аутентификации WPA/WPA2-PPSK

- Создайте профиль безопасности.

```
[AC] wlan
[AC-wlan-view] security-profile name profile-name
```

- Установите для политики безопасности значение WEP/WPA2-PPSK.

```
[AC-wlan-sec-prof-wlan] security { wpa | wpa2 | wpa-wpa2 } ppsk { aes | tkip | aes-tkip }
[AC-wlan-sec-prof-wlan] quit
```

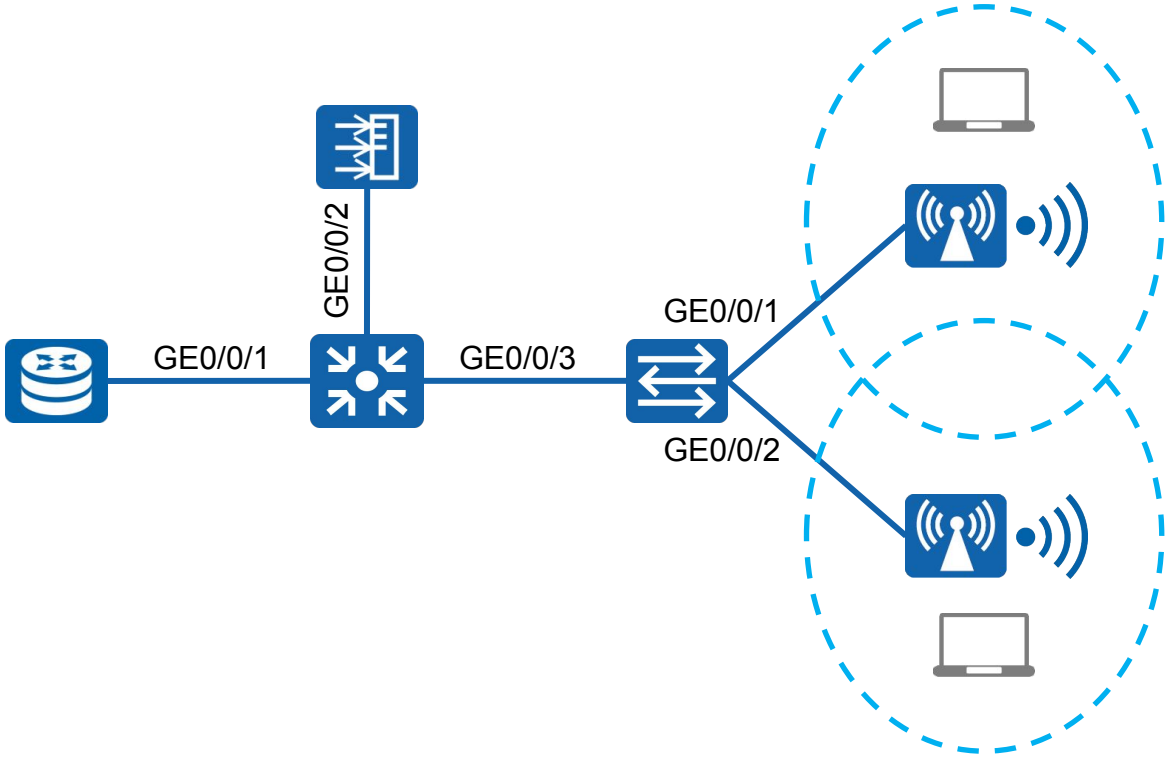
- Установите ключевые параметры PPSK.

```
[AC-wlan-view] ppsk-user psk { pass-phrase | hex } key-value [ user-name user-name | user-group user-group | vlan vlan-id | expire-date expire-date [ expire-hour expire-hour ] | max-device max-device-number | branch-group branch-group | mac-address mac-address ]* ssid ssid
```

  - Создайте пользователя PPSK и настройте пароль, имя пользователя, группу пользователей, авторизованную VLAN, время истечения срока действия, максимальное количество пользователей доступа, группу филиалов, MAC-адрес и SSID для пользователя PPSK.

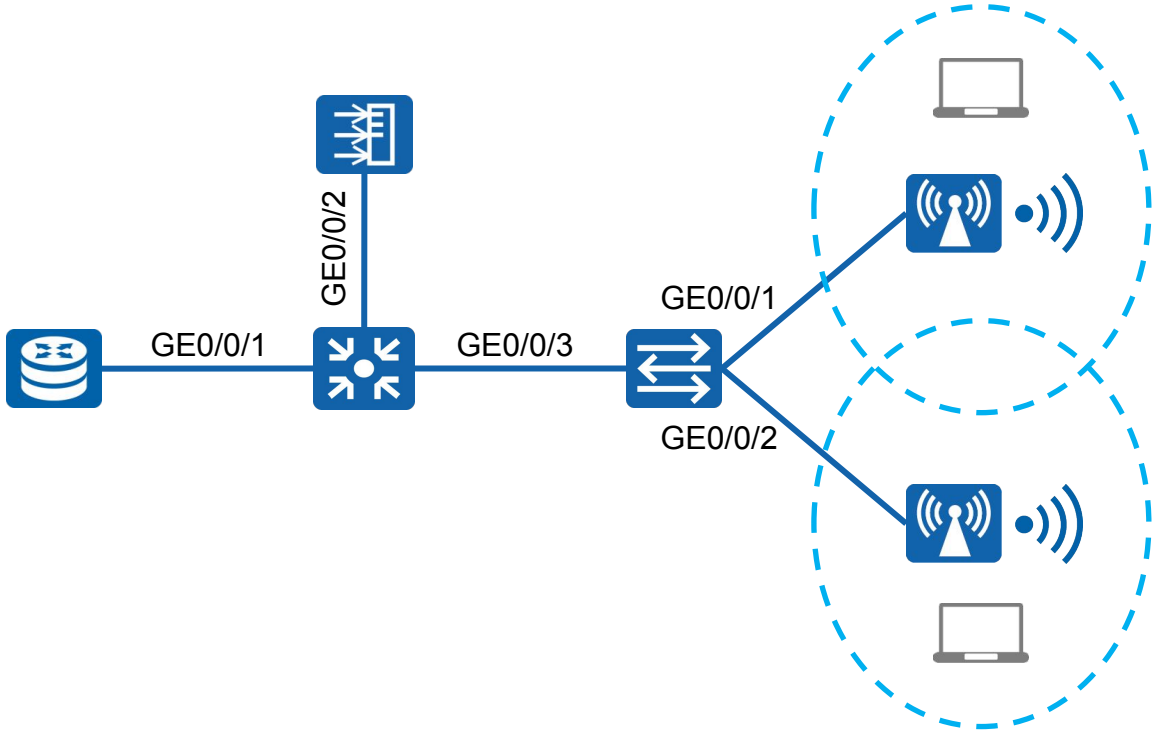
Пример: PSK и PPSK

- Как показано на рисунке, клиент требует, чтобы WLAN предоставляла услуги для отдела исследований и разработок и для финансового отдела. Для сотрудников финансового отдела необходим режим аутентификации по единому паролю с высокой защитой пароля. Для сотрудников отдела исследований и разработок каждому сотруднику требуется один пароль для аутентификации.



SSID1: Finance
Security policy: WPA2+PSK+AES
Password: Finance@123
SSID2: RD
Политика безопасности: WPA2+PPSK+AES
Password 1: Huawei@123
Password 2: Huawei12#$

Создание профилей безопасности



- Создайте профили безопасности **Finance** и **RD** и установите соответствующие политики безопасности.

[AC-wlan-view] **security-profile name *Finance***

[AC-wlan-sec-prof-Finance] **security wpa2 psk pass-phrase *Finance@123* aes**

[AC-wlan-sec-prof-Finance] **quit**

[AC-wlan-view] **security-profile name *Employee***

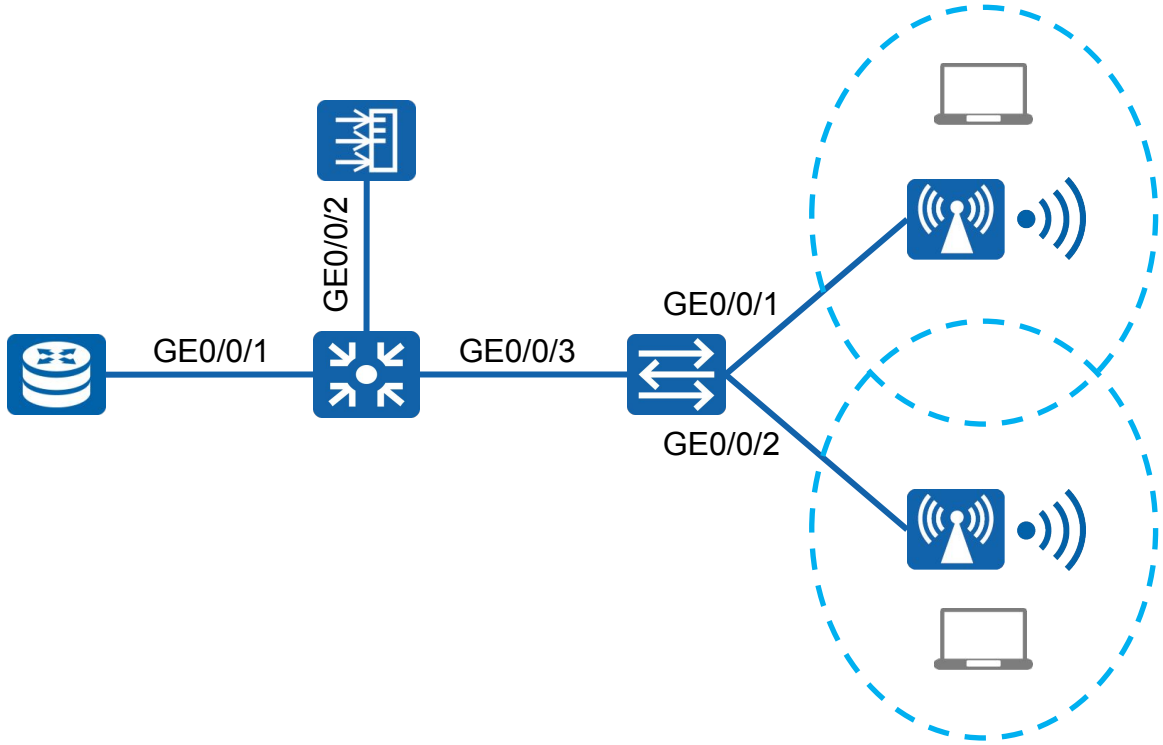
[AC-wlan-sec-prof-RD] **security wpa2 ppsk aes**

[AC-wlan-sec-prof-RD] **quit**

[AC-wlan-view] **ppsk-user psk pass-phrase *Huawei@123* max-device 1 ssid RD**

[AC-wlan-view] **ppsk-user psk pass-phrase *Huawei12#$* max-device 1 ssid RD**

Привязка профилей



- Привяжите два профиля безопасности к соответствующим профилям VAP.

```
[AC-wlan-view] vap-profile name Finance
[AC-wlan-vap-prof-Finance] security-profile Finance
[AC-wlan-vap-prof-Finance] quit
[AC-wlan-view] vap-profile name RD
[AC-wlan-vap-prof-RD] security-profile Guest
[AC-wlan-vap-prof-RD] quit
```

Просмотр информации о сигнале точки доступа

- Конфигурации услуг WLAN автоматически передаются в точки доступа. После завершения настроек выполните команду **display vap ssid RD**, чтобы порверить тип аутентификации (Auth type).

```
[AC-wlan-view]display vap ssid RD
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID         Status  Auth type  STA   SSID
--------------------------------------------------------------------------------
0     AP1     0    1    00E0-FC41-6340 ON      WPA/WPA2-PPSK   0     RD
0     AP1     1    1    00E0-FC41-6350 ON      WPA/WPA2-PPSK   0     RD
1     AP2     0    1    00E0-FCA2-5970 ON      WPA/WPA2-PPSK   0     RD
1     AP2     1    1    00E0-FCA2-5980 ON      WPA/WPA2-PPSK   0     RD
--------------------------------------------------------------------------------
```

Вопросы

1. (Несколько вариантов ответа) Что из перечисленного относится к аутентификации канала? ( )

   A. Аутентификация с помощью открытой системы

   B. Аутентификация с общим ключом

   C. WPA/WPA2 PSK

   D. WPA/WPA2 PPSK

Заключение

- Для передачи данных вместо сетевых кабелей WLAN использует радиоволны. По сравнению с проводной сетью развертывание WLAN намного проще. Однако из-за особенностей среды передачи проблемы безопасности WLAN выходят на первый план.
- В настоящем курсе описаны угрозы безопасности, с которыми сталкивается WLAN, и подробно описаны механизмы, позволяющие устранить такие угрозы.

Спасибо за внимание!

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Донесение цифровых данных до каждого человека, дома и организации для полностью взаимосвязанного интеллектуального мира

HUAWEI

История изменений

Не для печати

Код курса	Продукт	Версия продукта	Версия курса
H12-311	WLAN	V200R19C10	3.0

Составлено/ID сотрудника	Дата	Проверено/ID сотрудника	Новый/Обновление
У Ваньшэнь (Wu Wanshen)/WX343927	18.06.2020	Новая группа WLAN	Новый