

# Модели организации WLAN



# Предисловие

- Различные предприятия предъявляют различные требования к беспроводным локальным сетям (WLAN). Поскольку беспроводные локальные сети широко используются в корпоративных сетях, способ построения такой сети, удовлетворяющей потребности в обслуживании, становится основной проблемой для предприятий. Чтобы построить качественную сеть, необходимо разработать соответствующую архитектуру и выбрать подходящий режим организации сети.
- В этом курсе описывается структура WLAN-сети и типовые решения для организации сети.

# Цели

---

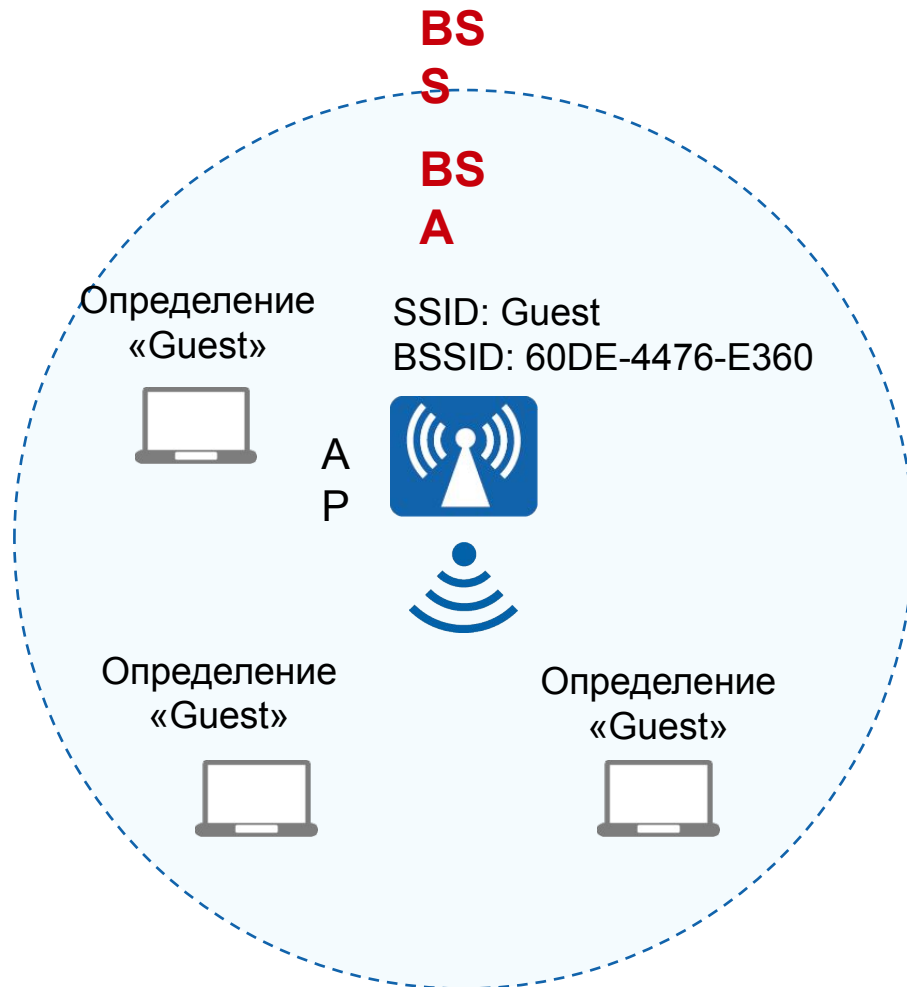
По завершении этого курса вы сможете:

- описать основные концепции WLAN;
- описать режимы организации сетей WLAN;
- проводить различия между моделями пересылки WLAN;
- оценивать типичные решения Huawei для организации сети WLAN.

# Содержание

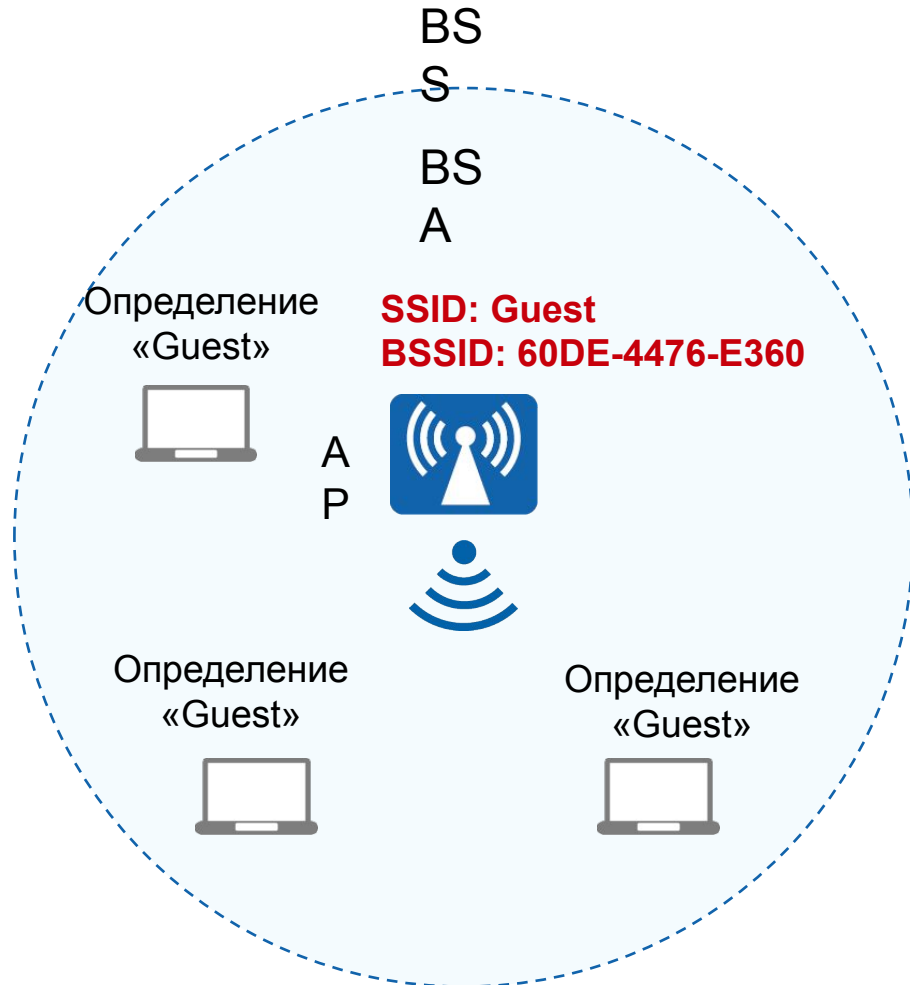
- 1. Основные понятия WLAN**
2. Архитектура сети WLAN
3. Типичные решения для организации сети WLAN

# BSS и BSA



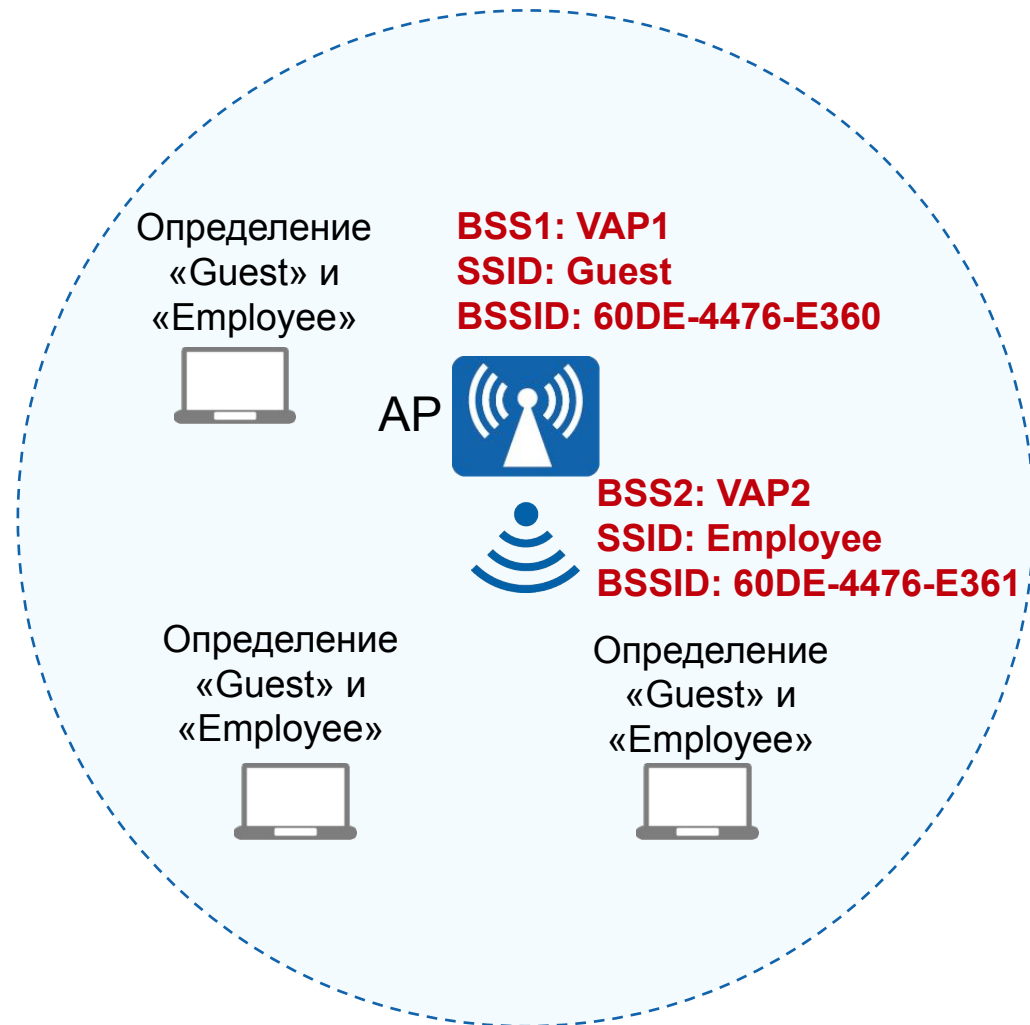
- Базовый набор услуг (BSS) является основным строительным блоком WLAN. Каждый BSS включает в себя одну фиксированную точку доступа (AP) и несколько станций (STA). Точка доступа используется как инфраструктура WLAN, предоставляющая услуги беспроводной связи для станции.
- Точка доступа находится в центре BSS и имеет относительно фиксированное местоположение. BSS находится там, где находится точка доступа. Станции в BSS распределены вокруг точки доступа, и их расположение относительно точки доступа не является фиксированным. Поэтому STA могут свободно перемещаться, рядом с точкой доступа или вдали от нее. Зона покрытия точки доступа называется базовой зоной обслуживания (BSA). Станции могут свободно входить или выходить из BSA, но только STA, входящие в BSA, могут связываться с соответствующей точкой доступа.

# SSID и BSSID



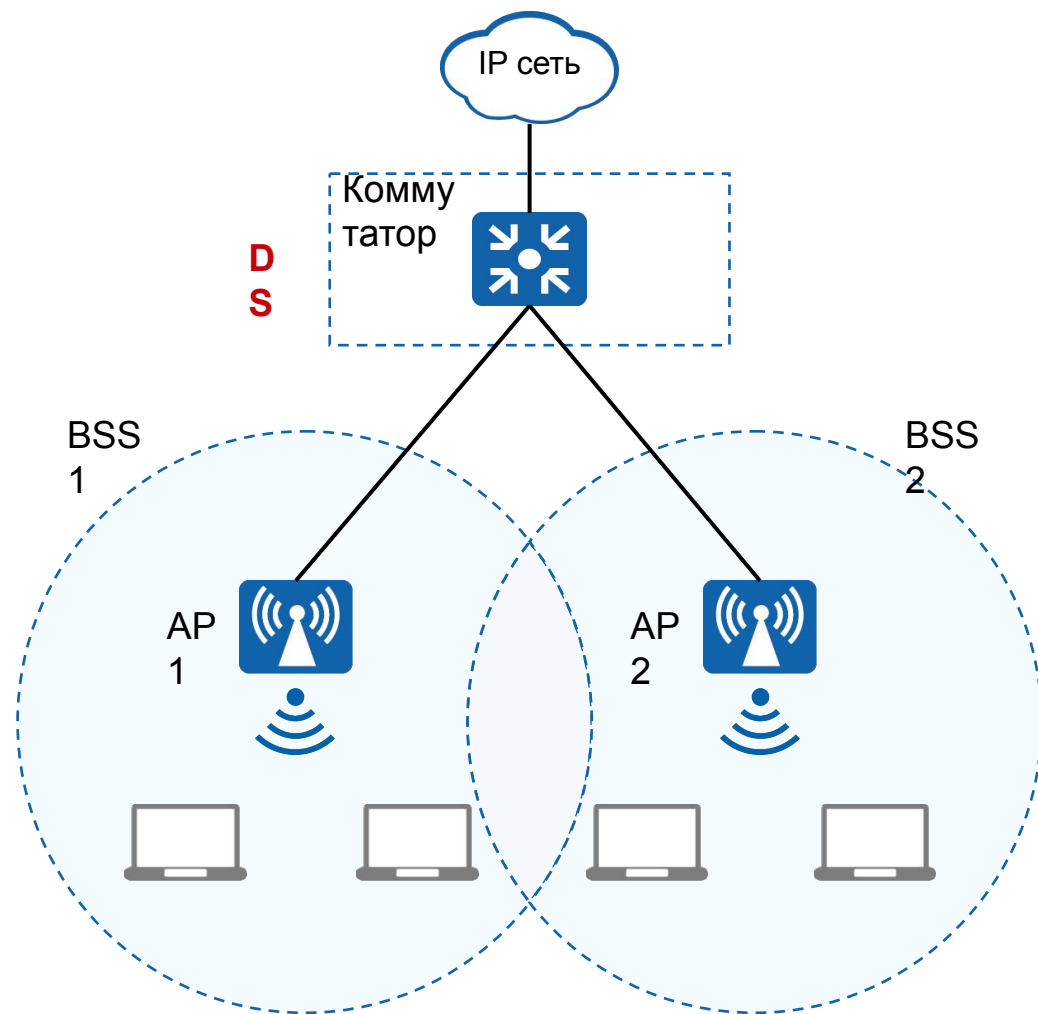
- Для того чтобы обнаружить точку доступа, STA необходимо, чтобы точка доступа предоставила информацию о своем идентификаторе, который называется идентификатором базового набора услуг (BSSID).
- Станция может видеть несколько BSSID в одной зоне радиосвязи с несколькими развернутыми BSS, при этом нужно выбрать только один необходимый BSSID. STA не выбирает BSSID автоматически. Необходимо выбрать один для нее. Поскольку BSSID обычно является MAC-адресом точки доступа в BSS, то если видны только строки символов MAC-адресов, можно и не понять, какой BSSID является нужным. Следовательно, для того, чтобы было проще идентифицировать точки доступа, для имени точки доступа можно задать строку символов. Такая строка символов называется идентификатором набора услуг (SSID).

# VAP



- Точку доступа можно настроить с несколькими виртуальными точками доступа (VAP), при этом каждая VAP будет соответствовать одному BSS. Поэтому для предоставления нескольких BSS, для которых можно установить разные идентификаторы SSID, необходимо развернуть только одну точку доступа. Таким образом, несколько WLAN могут сосуществовать в одной зоне радиосвязи, что также называется Multi-SSID.

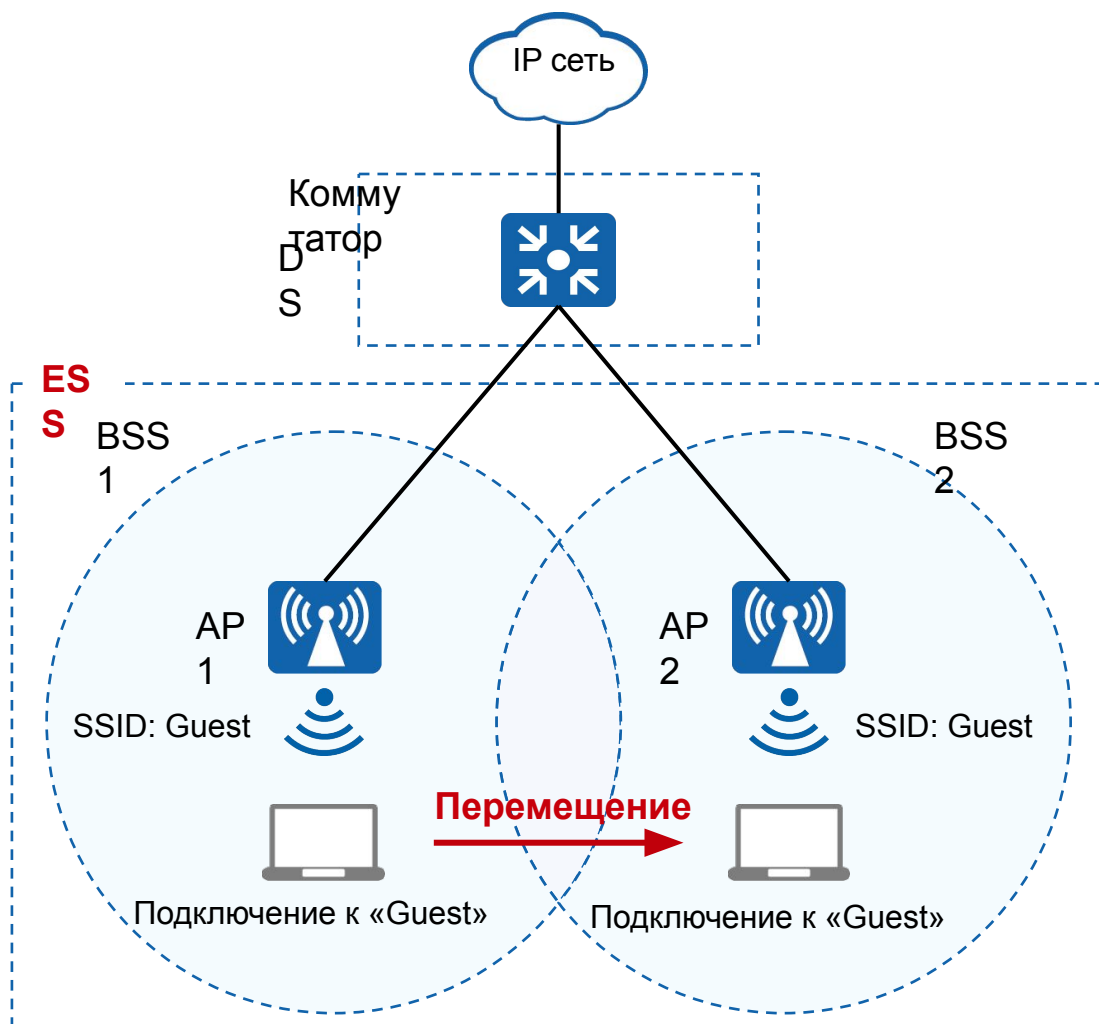
# DS



- BSS позволяет осуществлять беспроводную связь нескольких станций в одной области. Однако объекты, устанавливающие связь со станцией часто рассредоточены по разным областям, а иногда находятся на другом конце земли. В этом случае точке доступа необходимо подключиться к более крупной сети для подключения BSS в разных областях, чтобы станции могли обмениваться данными. Эта сеть является вышестоящей сетью, которая называется системой распределения (DS) BSS.



# ESS



- Как правило, эффективный радиус покрытия BSS составляет от 10 м до 15 м. Чтобы охватить большую площадь, можно использовать несколько BSS.
- Кроме того, чтобы пользователи не почувствовали изменение BSS, несколько BSS могут использовать один и тот же SSID. В результате создается ощущение, что используется одна и та же WLAN, независимо от того, куда перемещается пользователь.
- Это называется расширенным набором услуг (ESS), который расширяет диапазон BSS, позволяет гибко комбинировать BSS и делает развертывание WLAN простым и удобным.
- В этом случае SSID каждого BSS называется расширенным идентификатором набора услуг (ESSID), который используется для уведомления STA о непрерывной WLAN.

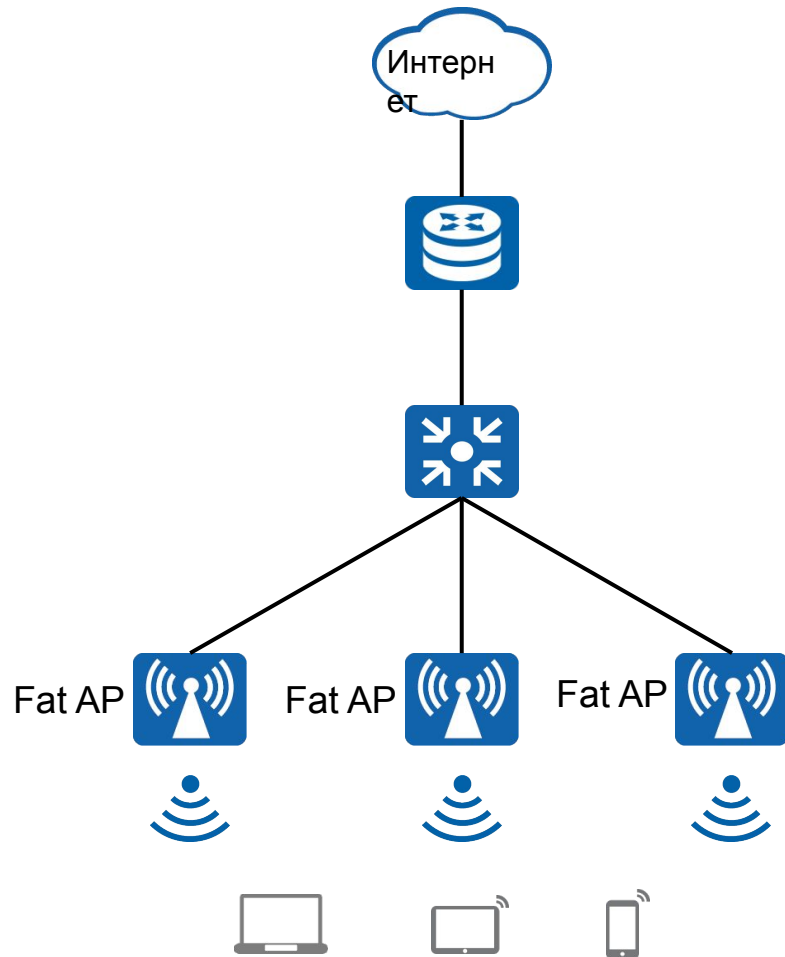
# Основные понятия WLAN

Понятие	Расшифровка	Описание
BSS	Basic Service Set — Базовый набор услуг	BSS является основным строительным блоком WLAN и состоит из одной точки доступа и нескольких станций, связанных с этой точкой доступа.
ESS	Extended Service Set — Расширенный набор услуг	ESS — набор из двух или более BSS, которые совместно используют один SSID, и который используется для расширения покрытия BSS.
SSID	Service Set Identifier — Идентификатор набора услуг	SSID идентифицирует беспроводную сеть.
ESSID	Extended Service Set Identifier — Идентификатор расширенного набора услуг	ESSID идентифицирует одну или группу беспроводных сетей.
BSSID	Basic Service Set Identifiers — Идентификатор базового набора услуг	Идентификаторы BSSID идентифицируют VAP на одной и той же физической AP на канальном уровне. Они также используются для идентификации BSS в ESS.
VAP	Virtual Access Point — Виртуальная точка доступа	VAP является логической сущностью, которая создается внутри физической точки доступа. Точка доступа может поддерживать несколько VAP для предоставления услуг беспроводного доступа разным группам пользователей.

# Содержание

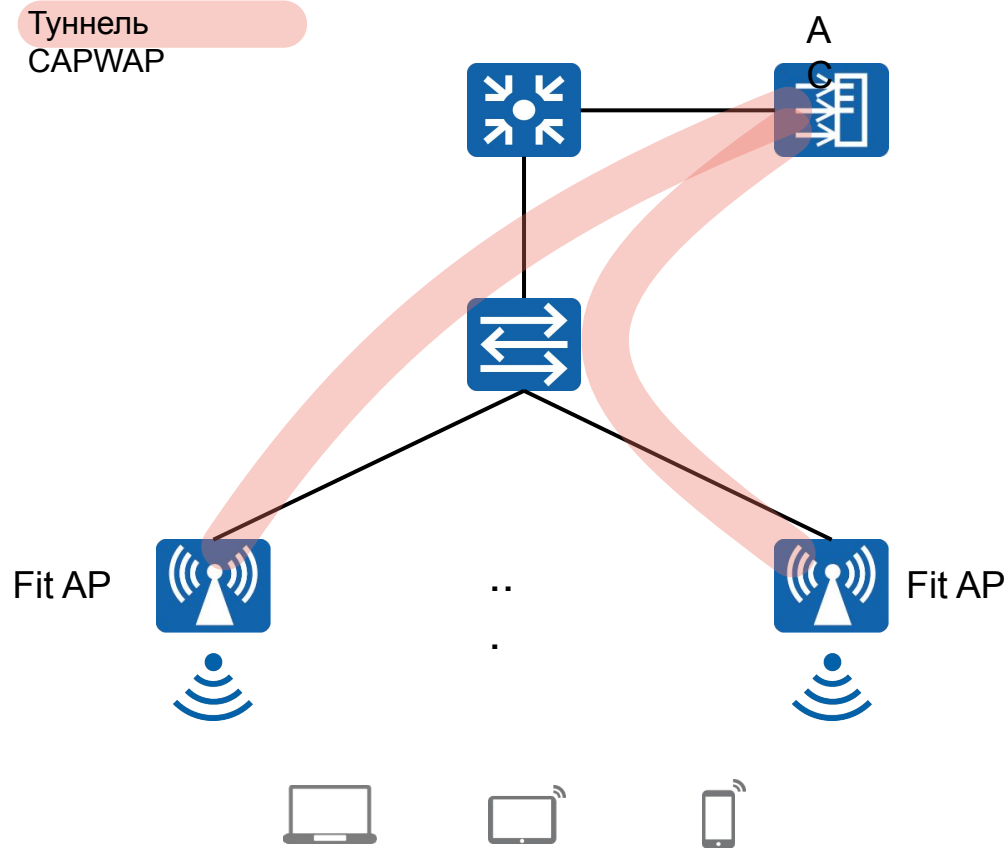
1. Основные понятия WLAN
- 2. Архитектура сети WLAN**
3. Типичные решения для организации сети WLAN

# Архитектура Fat AP



- Архитектура Fat AP также называется архитектурой автономной сети.
- Fat AP — это независимая архитектура, которая не требует дополнительного центрального управляющего устройства. Поэтому архитектура Fat AP проста в развертывании и экономична.
- Однако увеличение зоны покрытия WLAN и количества пользователей доступа на предприятиях требует применения все большего количества Fat AP. Для таких независимо работающих Fat AP не существует единого устройства управления, что затрудняет управление и обслуживание Fat AP.
- Следовательно, архитектура Fat AP не рекомендуется для развертывания на предприятиях. Для этого больше подходят архитектуры AC + Fit AP, облачное управление и Leader AP.

# Архитектура AC + Fit AP



- Контроллер доступа отвечает за контроль доступа к WLAN, пересылку данных и сбор статистики, настройку и мониторинг точек доступа, управление роумингом, мониторинг агентов управления сетью точек доступа и управление безопасностью.
- Fit AP осуществляет шифрование и расшифровку пакетов 802.11, предоставляет функции физического уровня 802.11, собирает статистику радиointерфейса. Управление Fit AP осуществляет контроллер доступа.
- Связь между контроллером доступа (AC) и Fit AP осуществляется с помощью протокола управления и предоставления беспроводных точек доступа (CAPWAP).
- По сравнению с архитектурой Fat AP, архитектура AC + Fit AP имеет следующие преимущества:
  - Более простая настройка и развертывание
  - Более высокий уровень безопасности

# Организация сети AC + Fit AP

## Режим организации сети

Сеть уровня 2 в сравнении с сетью уровня 3

Сеть In-Path в сравнении с сетью Off-Path

Режим пересылки данных

## Планирование

Планирование VLAN

Планирование IP-адресов

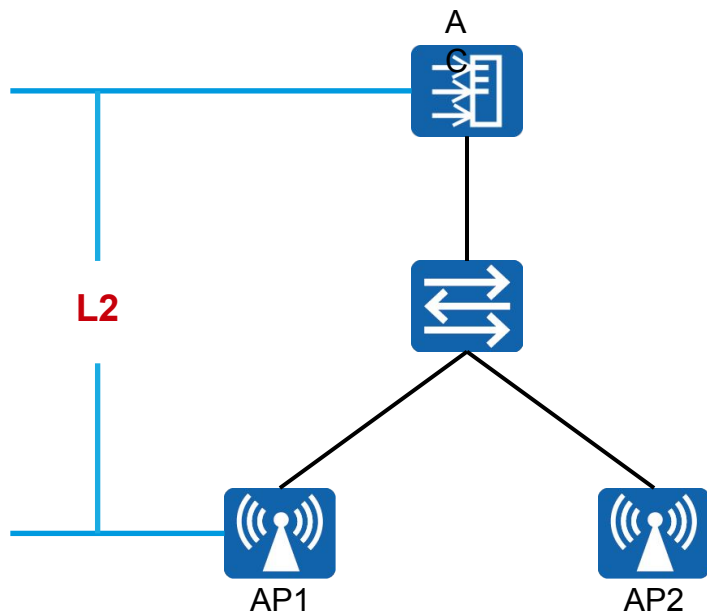
## Надежность

Надежность AC

Надежность услуг

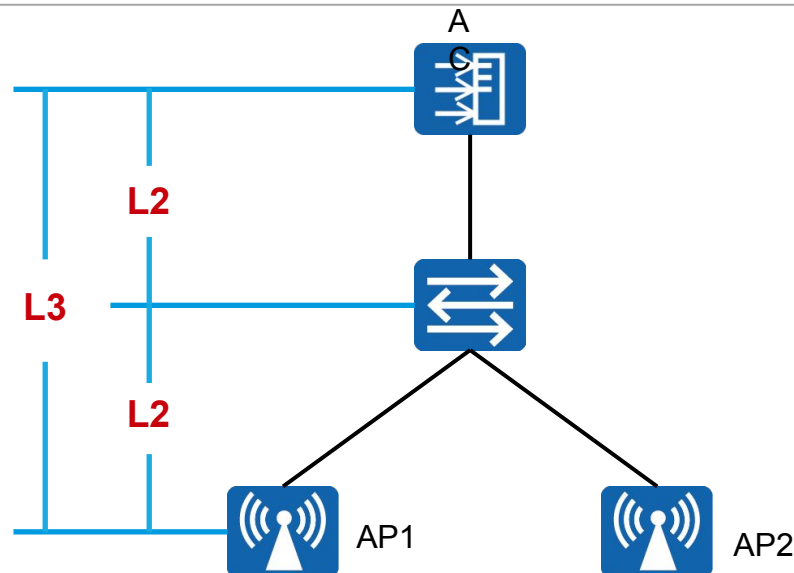
# Сеть уровня 2 в сравнении с сетью уровня 3

## Сеть уровня 2



- **Описание.** Контроллер доступа и Fit AP находятся в одном широковещательном домене. Fit AP обнаруживают контроллер доступа напрямую посредством трансляции в локальной сети. Сеть отличается простыми процедурами организации, настройки и управления сетью.
- **Область применения.** Способ организации сети уровня 2 применяется для небольших сетей, например, сетей малых предприятий. Данный способ не рекомендован для крупных предприятий, которые используют сложные сети WLAN и требуют детального управления.

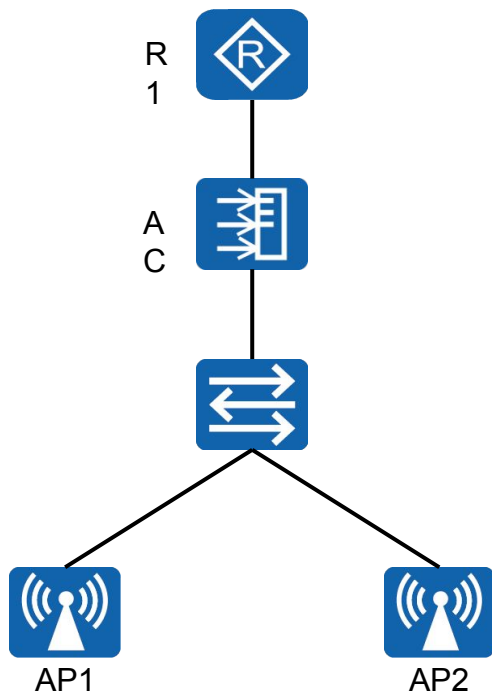
## Сеть уровня 3



- **Описание.** Контроллер доступа и Fit AP находятся в разных сегментах сети. Промежуточная сеть обеспечивает доступность Fit AP и контроллера доступа по отношению друг к другу. Для того чтобы Fit AP могли обнаруживать контроллер доступа требуются дополнительные настройки. Сеть отличается гибкостью и простотой расширения.
- **Область применения.** Способ организации сети уровня 3 подходит для средних и крупных сетей. Например, в крупномасштабной кампусной сети точки доступа развертываются в каждом здании для обеспечения беспроводного покрытия, а контроллеры доступа устанавливаются в основном аппаратном зале для унифицированного управления и контроля. В этом случае между Fit AP и контроллером доступа разворачивается сложная сеть уровня 3.

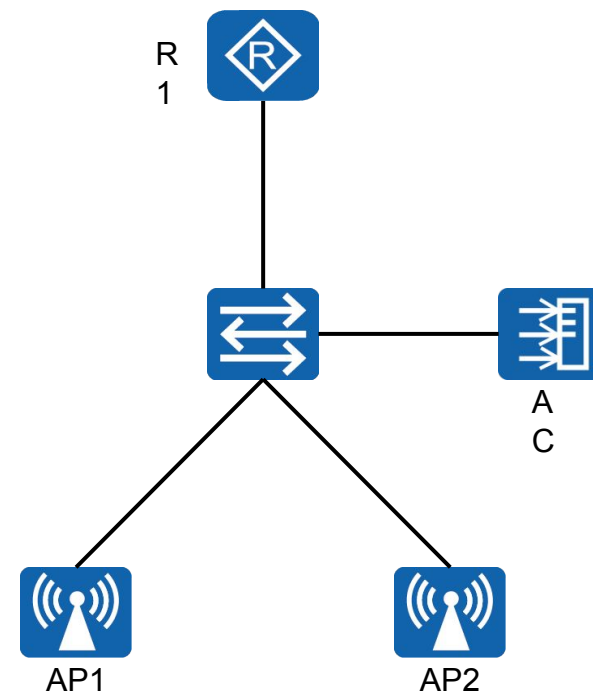
# Сеть In-Path в сравнении с сетью Off-Path

## Сеть In-Path



- **Описание.** Контроллер доступа выполняет функции и контроллера доступа и коммутатора агрегации для централизованной пересылки и обработки услуг передачи данных и управления.
- **Область применения.** Недавно развернутые малые и средние централизованные беспроводные сети WLAN.

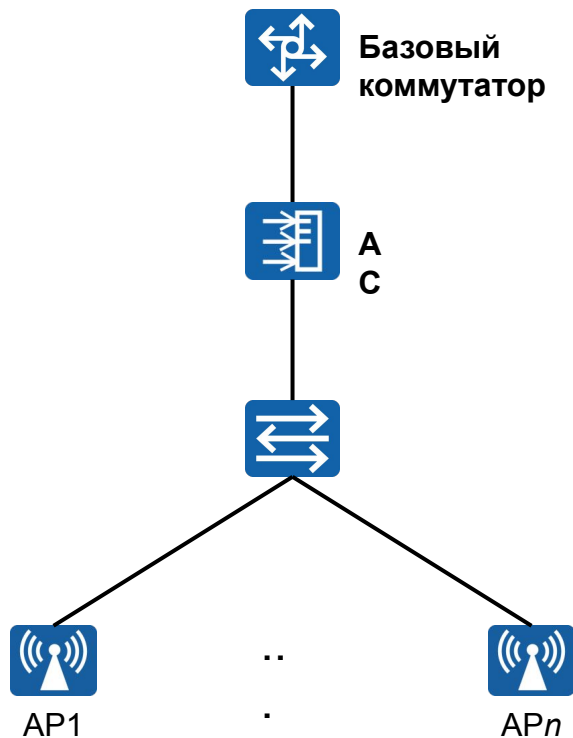
## Сеть Off-Path



- **Описание.** Контроллер доступа подключен к действующей сети в режиме off-path и обрабатывает только услуги управления точек доступа. Сервисные данные точек доступа поступают в вышестоящую сеть, не проходя через контроллер доступа.
- **Область применения.** Реконструкция сети или сооружение крупных и средних кампусных сетей.



# Сеть с включением AC в маршрут (сеть In-Path)



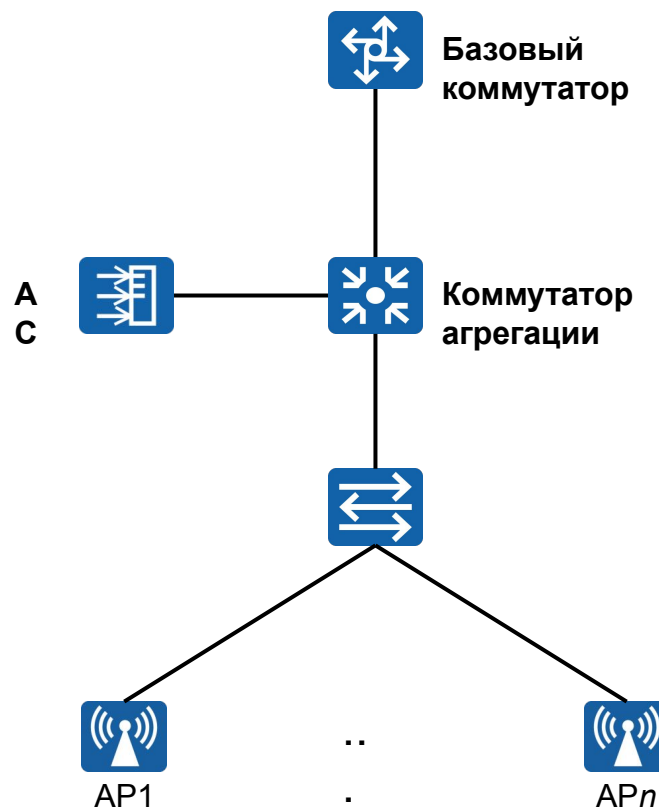
## Описание

- Точки доступа или коммутаторы доступа напрямую подключены к контроллеру доступа. Контроллер доступа также выполняет функции коммутатора агрегации для пересылки и обработки данных точек доступа и услуг управления.
- Контроллер доступа обеспечивает мощные возможности доступа, агрегирования и коммутации. Кроме того, он поддерживает источники питания PoE или PoE+. Поэтому точки доступа могут напрямую подключаться к контроллеру доступа.
- Поддерживаются туннельная и прямая пересылки. Поскольку контроллер включен в сеть (режим in-path), в большинстве случаев используется режим прямой пересылки.
- Трафик проходит через контроллер доступа. Неисправность контроллера доступа также затронет трафик, не являющийся трафиком беспроводной сети.

## Сценарий применения

Такой режим организации сети позволяет упростить сетевую архитектуру. Применим к малым и средним централизованным WLAN, недавно развернутым малым и средним кампусным сетям и сетям филиалов.

# Сеть с отдельным подключением АС (сеть Off-Path)



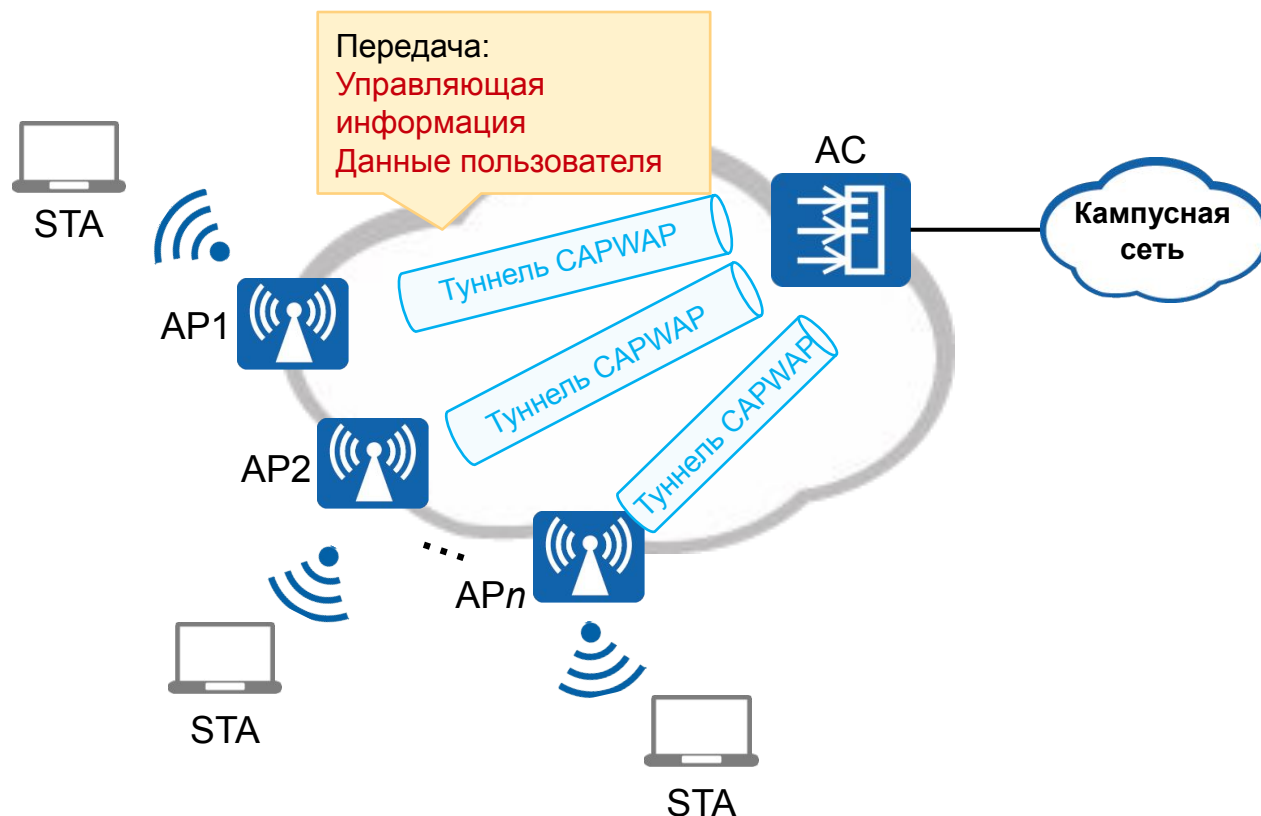
## Описание

- Контроллер доступа подключен к действующей сети в режиме off-path для управления сервисами WLAN точек доступа.
- Контроллер доступа отвечает за управление точками доступа. Потоки управления передаются по туннелям CAPWAP. Потоки данных передаются по туннелю CAPWAP и проходят через контроллер доступа, или коммутатором агрегации передает их в сеть верхнего уровня без прохождения через контроллер доступа.
- В режиме сети Off-path точки доступа, развернутые в пределах области управления коммутатора агрегации, управляются контроллером доступа, подключенным к коммутатору агрегации. Развёртывание контроллеров доступа выполняется централизованно. Следовательно, данная топология применяется в сценариях, в которых точки доступа подключены к интернету.
- Режим off-path редко изменяет структуру существующей сети и отличается возможностями быстрого развертывания.
- В зависимости от требований сети можно выбрать режим пересылки или туннельной пересылки.
- Для большинства корпоративных сетей рекомендуется режим туннельной пересылки.

## Область применения

- Этот режим применяется при реконструкции сети или при сооружении крупных и средних кампусных сетей.
- Исходная топология сети не изменяется.

# Обзор CAPWAP



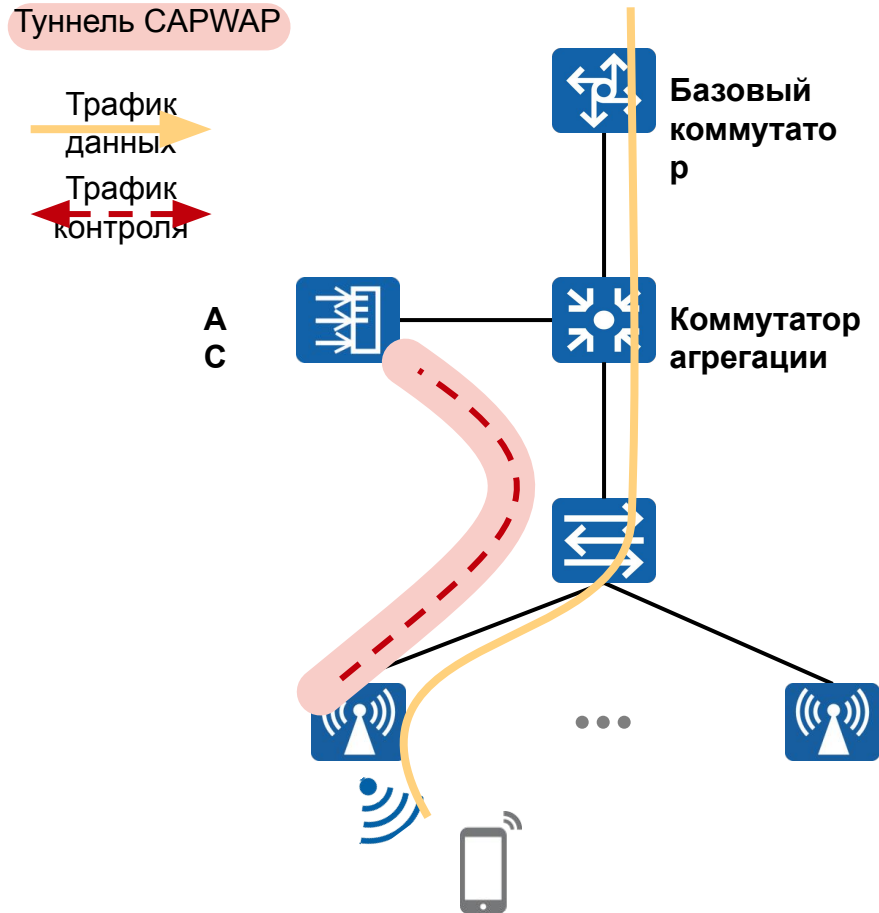
## Что представляет собой туннель CAPWAP?

- **CAPWAP**: протокол, который определяет способы управления и настройки точек доступа. Другими словами, контроллер доступа управляет и контролирует точки доступа централизованно через туннели CAPWAP.

## Функции туннеля CAPWAP

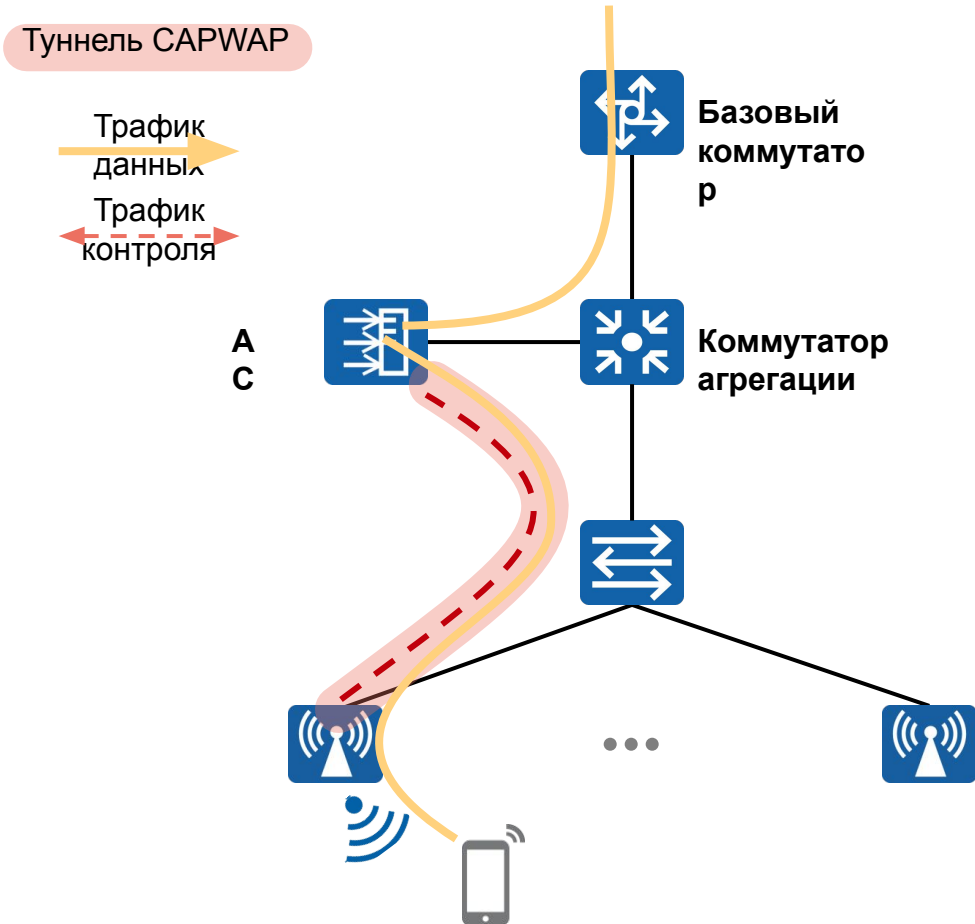
- Позволяет точкам доступа автоматически обнаруживать контроллер доступа.
- Поддерживает состояние подключения между контроллером и точками доступа.
- Позволяет контроллеру доступа управлять точками доступа и передавать конфигурации сервисов этим точкам доступа.
- Позволяет точкам доступа обмениваться данными, отправленными STA, с контроллером доступа через туннели CAPWAP в режиме туннельной пересылки.

# Прямая пересылка



- Прямая пересылка: точка доступа напрямую пересылает пакеты данных пользователя (без инкапсуляции) в сеть верхнего уровня через туннель CAPWAP. Контроллер доступа управляет только точками доступа. Все служебные данные пересылаются локально.
- Преимущества: трафик данных не проходит через контроллер доступа, поэтому нагрузка на контроллер доступа небольшая. Данный режим рекомендуется для кампусных сетей 10GE.

# Туннельная пересылка



- Туннельная пересылка: точки доступа инкапсулируют пакеты служебных данных, а затем передают на контроллер доступа для последующей пересылки. Контроллер доступа управляет точкой доступа и пересылает трафик точки доступа.
- Пакеты данных пользователя инкапсулируются в туннель CAPWAP, после чего контроллер доступа пересылает их в вышестоящую сеть.
- Преимущества: трафик служебных данных и трафик управления проходит через контроллер доступа, что упрощает реализацию политик управления безопасностью для пользователей беспроводной сети.

# Сравнение режимов организации сети AC + Fit AP

Режим организации сети	Характеристики
Режим In-path + сеть уровня 2 + прямая пересылка	Отсутствие обхода данных и высокая эффективность пересылки
Режим Off-path + сеть уровня 2 + прямая пересылка	Отсутствие обхода данных и высокая эффективность пересылки, простое развертывание WLAN в действующей сети и развертывание решения горячего резервирования (HSB)
Режим Off-path + сеть уровня 2 + туннельная пересылка	Простая конфигурация VLAN и туннели уровня 2, предоставляемые при туннельной пересылке для поддержки аутентификации 802.1X, простое развертывание WLAN в действующей сети и развертывание решения HSB.
Режим Off-path + сеть уровня 3 + туннельная пересылка	Простая конфигурация VLAN и туннели уровня 2, предоставляемые при туннельной пересылке для поддержки аутентификации 802.1X, простое развертывание WLAN в действующей сети и развертывание решения HSB.
Режим Off-path + сеть уровня 3 + прямая пересылка	Отсутствие обхода данных и высокая эффективность пересылки, простое развертывание WLAN в действующей сети и развертывание решения HSB

# Планирование архитектуры AC + Fit AP

## Режим организации сети

Сеть уровня 2 в сравнении  
с сетью уровня 3

Сеть In-Path в сравнении  
с сетью Off-Path

Режим пересылки данных

## Планирование

Планирование VLAN

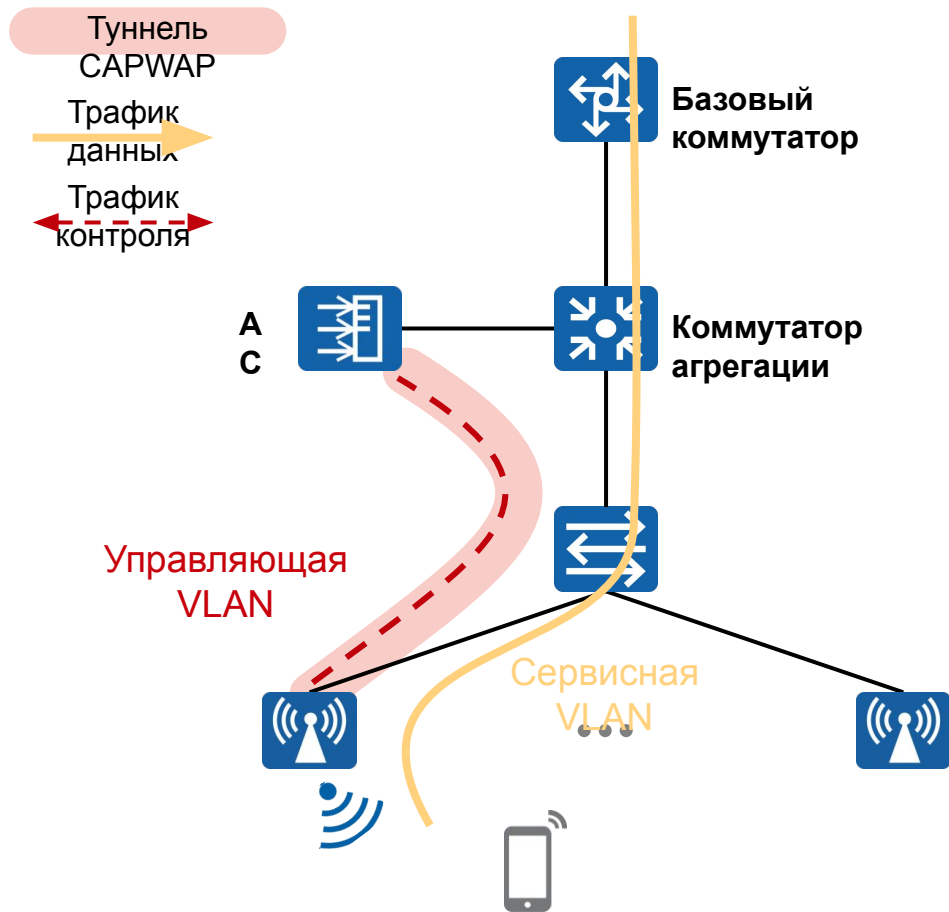
Планирование IP-адресов

## Надежность

Надежность AC

Надежность услуг

# Планирование VLAN

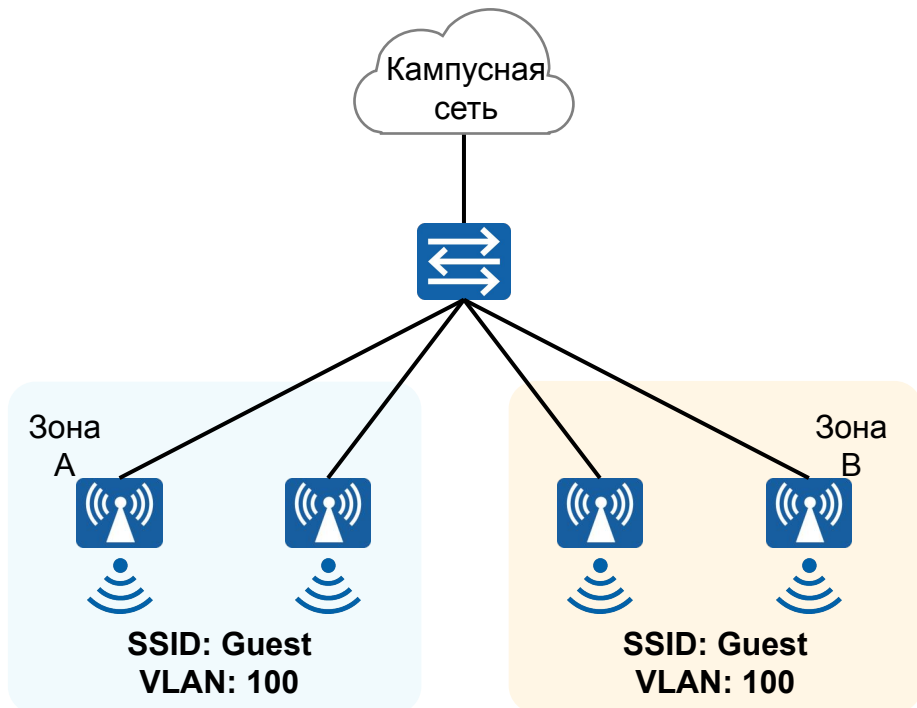


- Два типа VLAN в WLAN:
  - **Управляющая VLAN:** передает пакеты, пересылаемые через туннели CAPWAP, включая пакеты управления и пакеты служебных данных.
  - **Сервисная VLAN:** передает пакеты служебных данных.
- Обратите внимание на следующие принципы при планировании сетей VLAN:
  - Управляющая VLAN изолирована от сервисной VLAN.
  - Сервисные VLAN необходимо сопоставить с SSID в зависимости от требований к сервису.



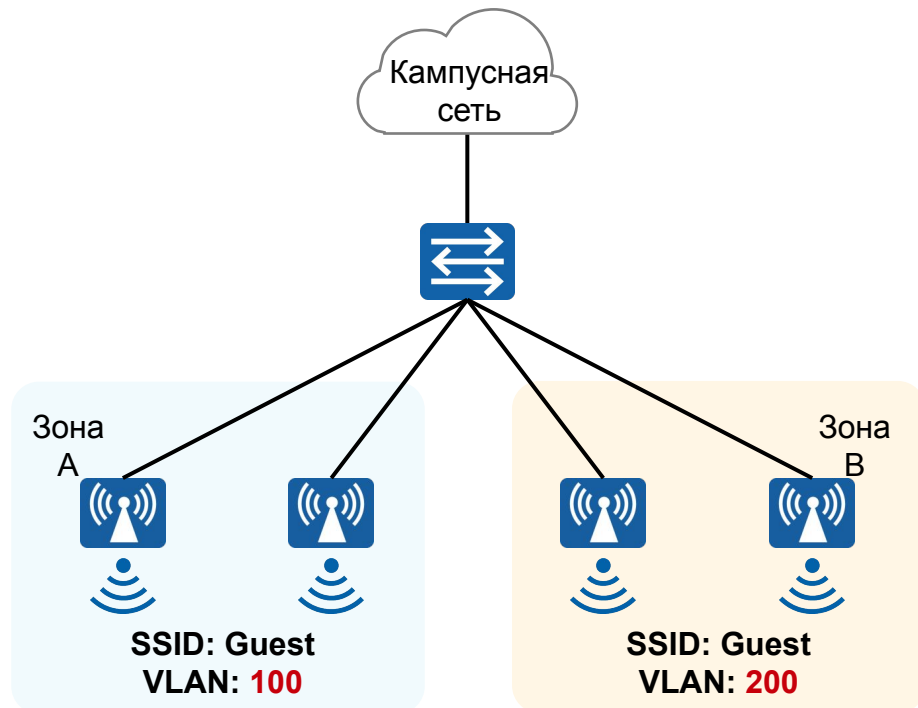
# Сопоставление между SSID и сервисными VLAN (1)

## SSID:VLAN = 1:1



- Предприятие должно обеспечить покрытие WLAN для зон А и В. Чтобы пользователи могли определить только один SSID и использовать одну и ту же политику управления пересылкой данных, необходимо запланировать только один SSID и одну VLAN, то есть SSID:VLAN = 1:1.

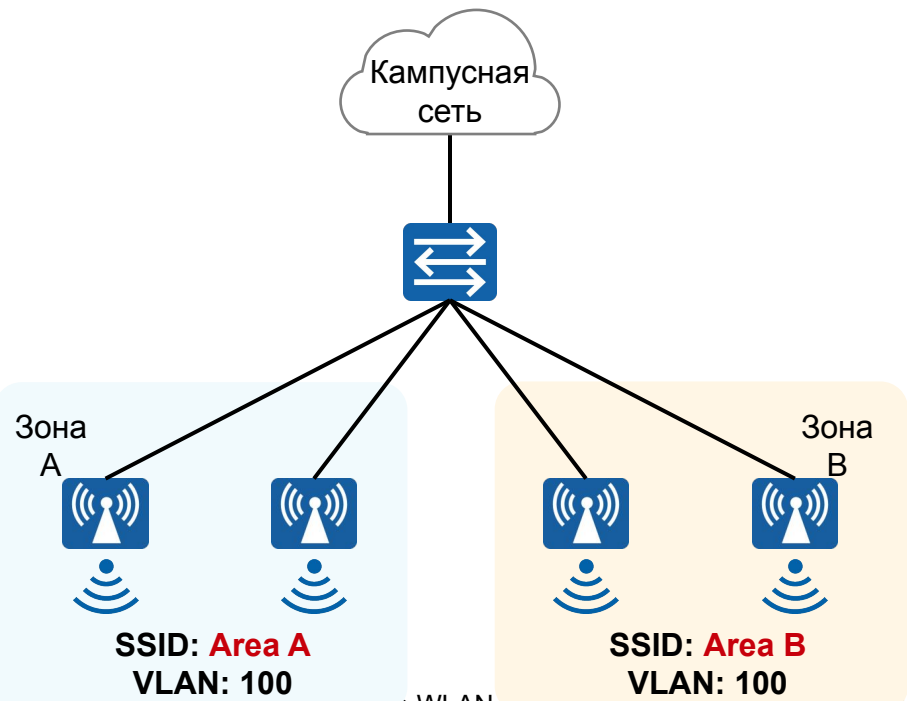
## SSID:VLAN = 1:N



- Предприятие должно обеспечить покрытие WLAN для зон А и В. Чтобы пользователи могли обнаружить только один SSID, но использовать разные политики управления пересылкой данных, необходимо запланировать один SSID и две VLAN для этих зон, то есть SSID:VLAN = 1:2.

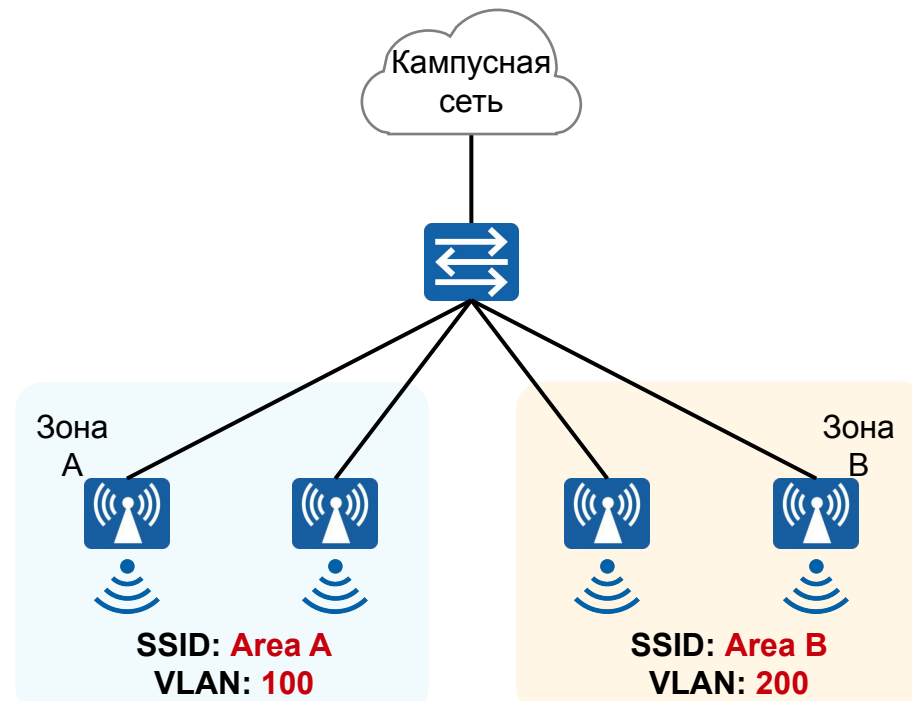
# Сопоставление между SSID и сервисными VLAN (2)

SSID:VLAN = N:1



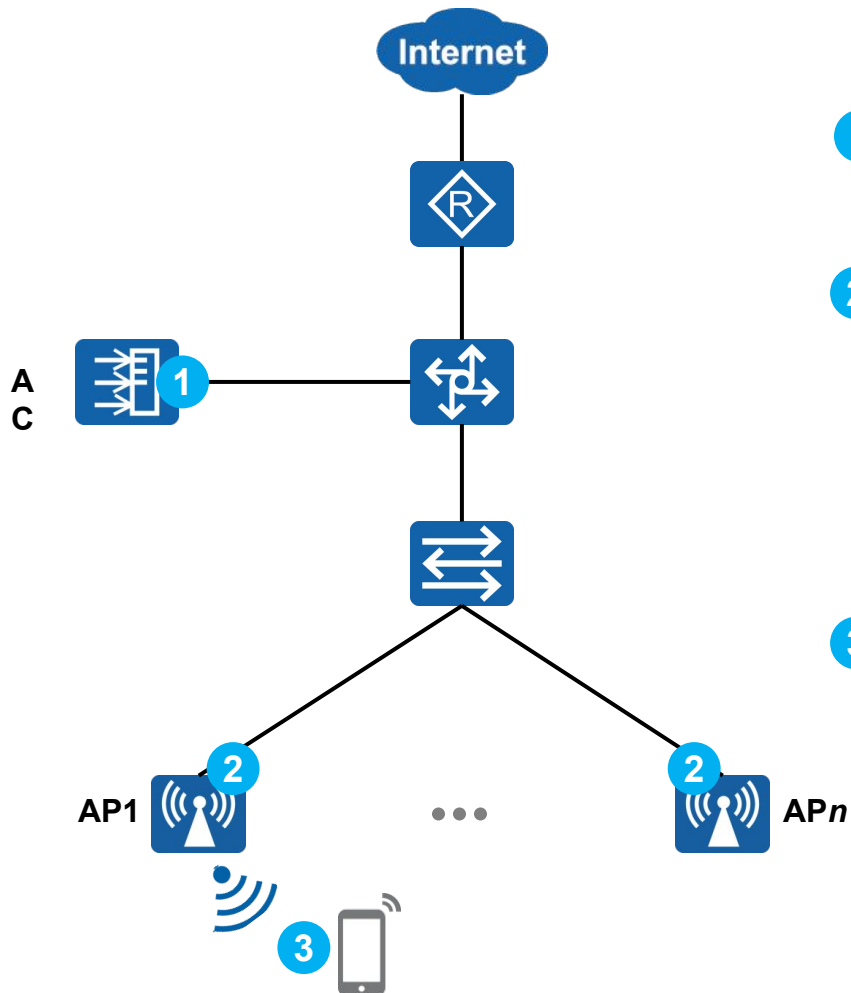
- Предприятие должно обеспечить покрытие WLAN для зон А и В. Чтобы пользователи могли получать информацию о зоне при обнаружении WLAN и использовать одну и ту же политику управления пересылкой данных, необходимо спланировать одну VLAN, но разные SSID для этих зон. В данном случае SSID:VLAN = 2:1.

SSID:VLAN = N:M



- Предприятие должно обеспечить покрытие WLAN для зон А и В. Чтобы пользователи могли получать информацию о зоне при обнаружении WLAN и использовать разные политики управления пересылкой данных, необходимо спланировать два SSID и два VLAN для этих зон. В данном случае SSID:VLAN = 2:2.

# Планирование IP-адресов



## 1 IP-адрес контроллера доступа:

- Статически настроен для управления точками доступа.

## 2 IP-адреса точек доступа:

- Используются для связи с контроллером доступа через CAPWAP. Поскольку существует большое количество точек доступа, DHCP-сервер обычно используется для динамического назначения IP-адресов этим точкам доступа.

## 3

## IP-адреса STA:

- Рекомендуется динамическое назначение IP-адреса через DHCP. Для фиксированных STA, например беспроводных принтеров, можно настроить статические IP-адреса. Контроллер доступа или независимый DHCP-сервер может функционировать как DHCP-сервер.

# Надежность архитектуры AC + Fit AP

## Режим организации сети

Сеть уровня 2 в сравнении с сетью уровня 3

Сеть In-Path в сравнении с сетью Off-Path

Режим пересылки данных

## Планирование

Планирование VLAN

Планирование IP-адресов

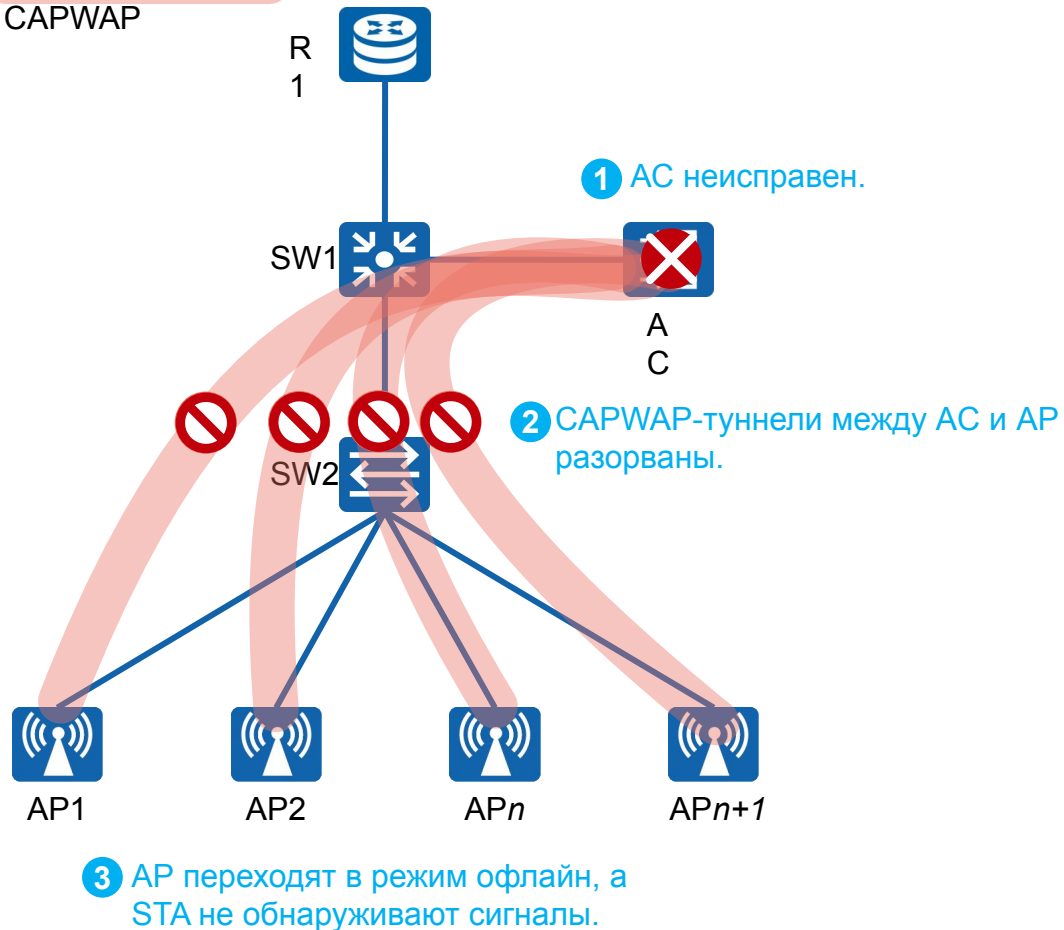
## Надежность

Надежность AC

Надежность услуг

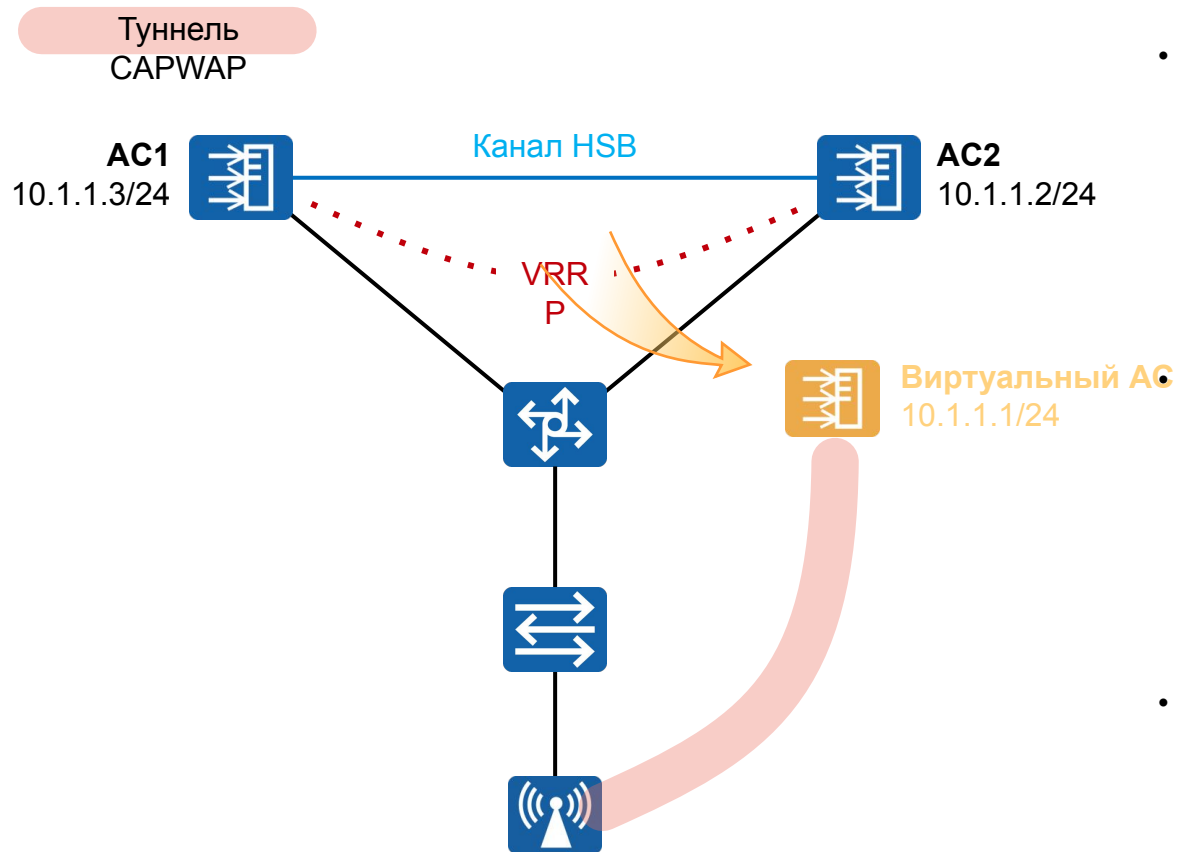
# Единичные отказы контроллера доступа

Туннель  
CAPWAP



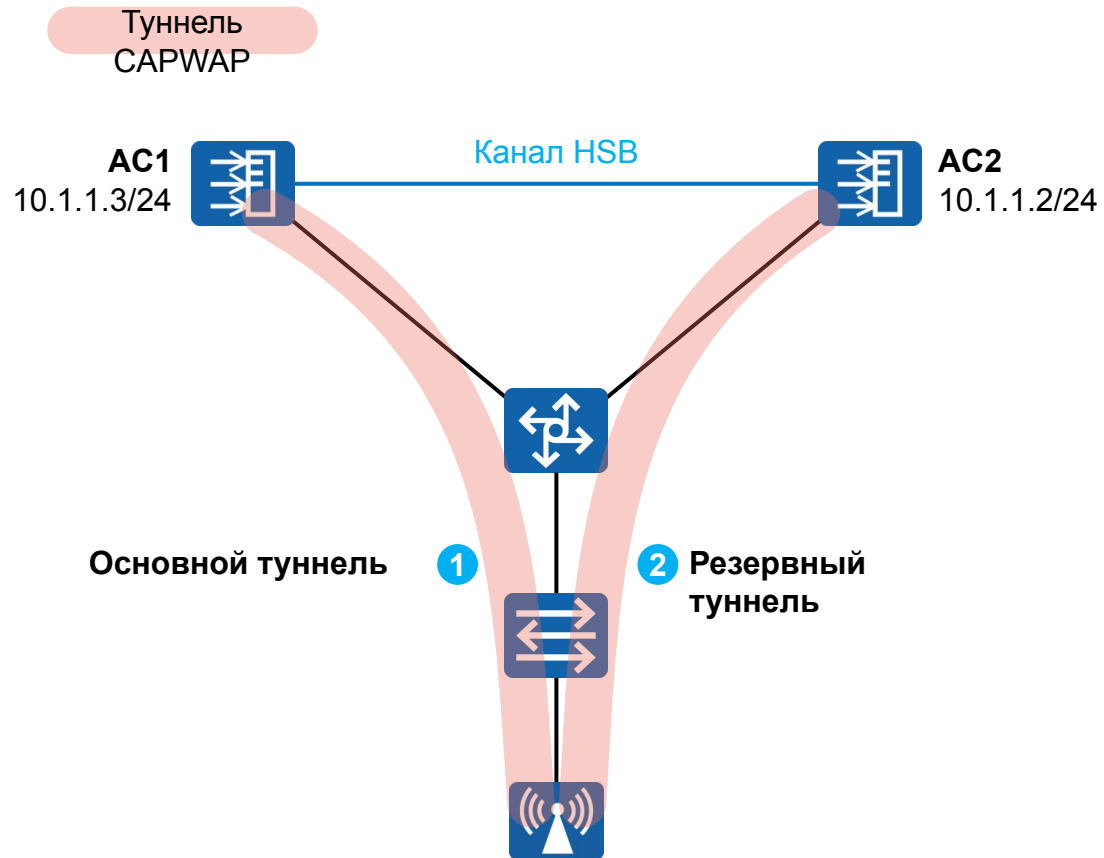
- В сети WLAN, использующей архитектуру AC + Fit AP, контроллер доступа осуществляет централизованное управление всеми точками доступа и передает им конфигурационные данные по туннелям CAPWAP.
- В случае неисправности контроллера доступа туннели CAPWAP между контроллером и точками доступа будут отключены. В результате точки доступа переходят в режим офлайн, а станции не могут обнаруживать сигналы WLAN. Пользователи WLAN в сети не могут подключиться к Интернету.

# Надежность AC: горячее резервирование с использованием протокола VRRP (VRRP HSB)



- В группу VRRP добавляются два контроллера доступа для совместного использования виртуального IP-адреса. Основной контроллер доступа синхронизирует служебную информацию с резервным контроллером доступа по каналу HSB.
- По умолчанию основной и резервный AC виртуализируются в один виртуальный контроллер доступа (AC). Если основной контроллер доступа выходит из строя, резервный начинает выполнять его функции. Все точки доступа устанавливают туннели CAPWAP с виртуальным контроллером.
- VRRP определяет переключение между контроллерами доступа. Для точек доступа имеется только один контроллер.
- Такой режим ограничивает места размещения двух контроллеров доступа, но поддерживает более высокую скорость переключения, чем другие резервные режимы.

# Надежность AC: горячий резерв (HSB) по двум каналам



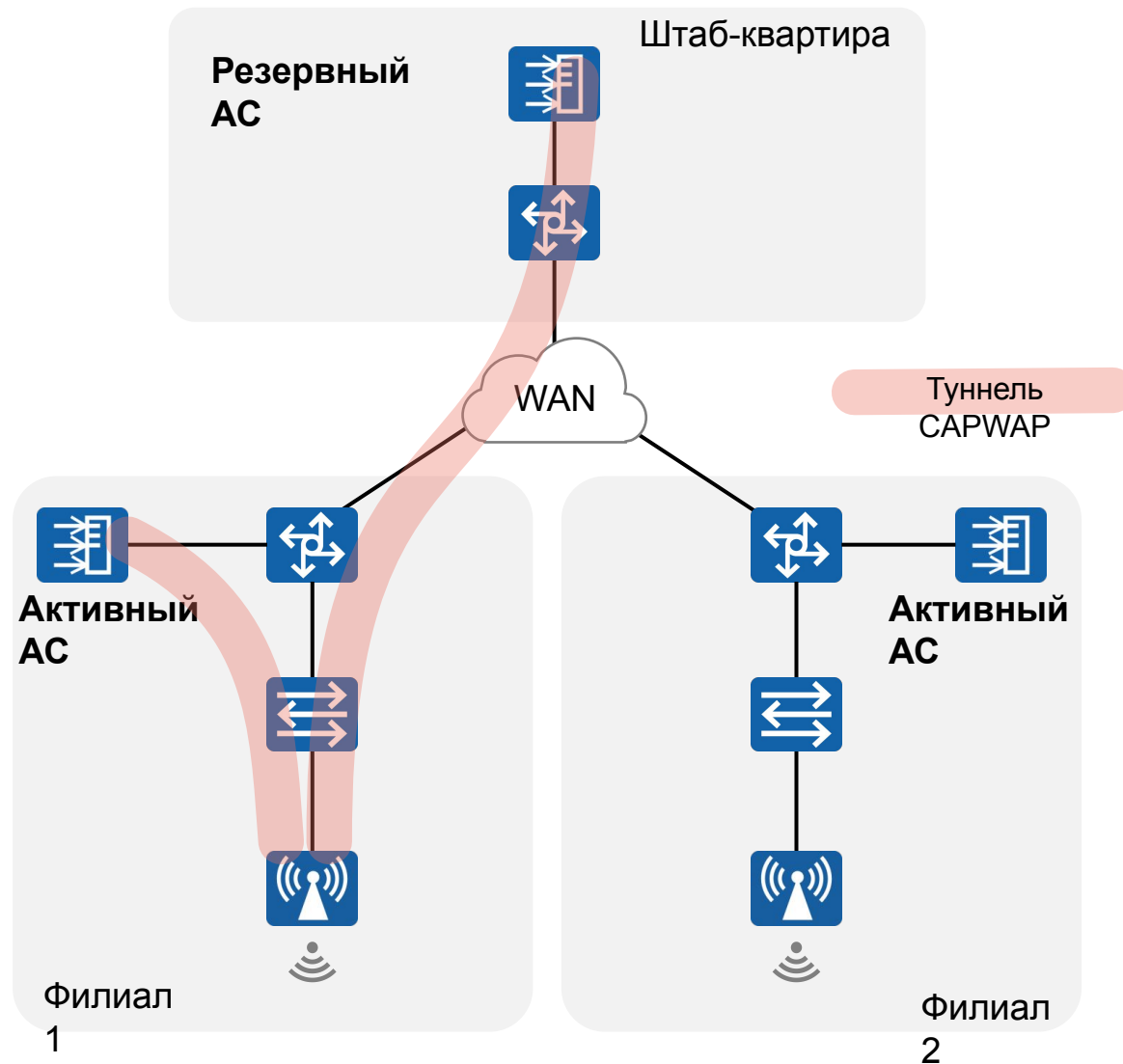
- Точка доступа устанавливает туннели CAPWAP как с активным, так и с резервным контроллерами доступа. Контроллеры доступа синхронизируют служебную информацию по каналу HSB.
- Когда туннель между точкой доступа и активным контроллером доступа выходит из строя, точка доступа дает команду резервному контроллеру о выполнении услуг активного контроллера доступа.
- Активный и резервный контроллеры определяются на основе приоритетов. Если контроллеры доступа имеют одинаковый приоритет, активный и резервный контроллеры определяются на основе нагрузки (количество подключенных точек доступа и станций).

# HSB

- HSB — это механизм горячего резервирования в режиме активный/резервный, разработанный компанией Huawei.
- Сервис HSB: устанавливает и поддерживает канал HSB, а также уведомляет активные и резервные сервисные модули о событиях подключения/отключения канала.
- Группа HSB: связана с сервисом HSB, обеспечивающим резервный канал данных для каждого из активных и резервных сервисных модулей. Группа HSB привязана к экземпляру VRRP, а активный и резервный экземпляры согласовываются с использованием механизма VRRP. Кроме того, группа HSB дает указание сервисным модулям обрабатывать такие события, как групповое резервирование, резервирование в реальном времени и переключение между активным и резервным режимами.



# Надежность AC: резервирование N+1



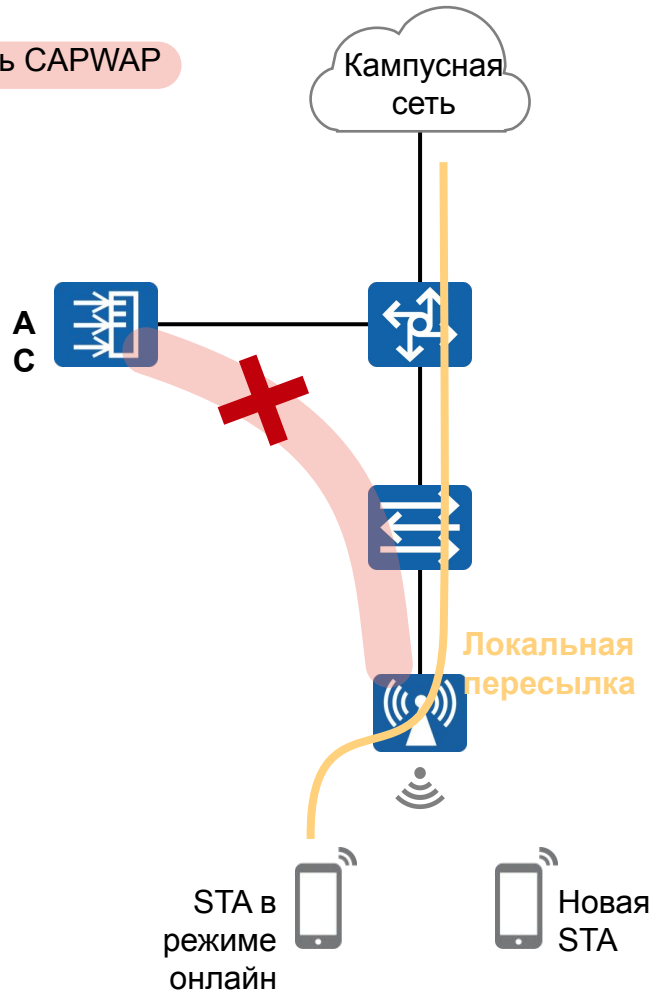
- В схеме резервирования N+1 используется один контроллер доступа для предоставления услуг резервного копирования для нескольких активных контроллеров доступа.
- Если сеть работает правильно, точка доступа устанавливает туннель CAPWAP только с активным контроллером, которому она принадлежит.
- Если активный контроллер доступа или туннель CAPWAP выходит из строя, резервный контроллер заменяет активный, управляет точками доступа и устанавливает туннель CAPWAP с точкой доступа для предоставления услуг.
- Поддерживаются переключение активный/резервный и обратное переключение.

# Надежность AC: резюме

Пункт сравнения	Горячее резервирование с использованием протокола VRRP (VRRP HSB)	Горячий резерв (HSB) по двум каналам	Резервирование N+1
Скорость переключения	Высокая скорость переключения, что практически не влияет на услуги. Конфигурация задержки внеочередного занятия линии VRRP реализует более быстрое переключение, чем другие режимы резервирования.	Переключение статуса точки доступа происходит медленно и только при обнаружении тайм-аута отключения соединения CAPWAP. После переключения статуса точки доступа STA не нужно снова переходить в режим офлайн, а затем снова в онлайн.	Переключение статуса точки доступа происходит медленно и только при обнаружении тайм-аута отключения соединения CAPWAP. Точка доступа и станция снова переходят в режим онлайн, и услуги прерываются на короткий период времени.
Развертывание активных и резервных контроллеров доступа в разных местах	VRRP является протоколом уровня 2 и не поддерживает развертывание активных и резервных AC в разных местах.	Поддерживается	Поддерживается
Область применения	Сценарии, требующие высокой надежности, без необходимости развертывания контроллера доступа в разных местах	Сценарии, требующие высокой надежности и развертывания контроллера доступа в разных местах	Сценарии с низкой надежностью, но высокими требованиями к контролю затрат

# Надежность сервиса: удержание сервиса при отключении канала CAPWAP в режиме локальной пересылки

Туннель CAPWAP



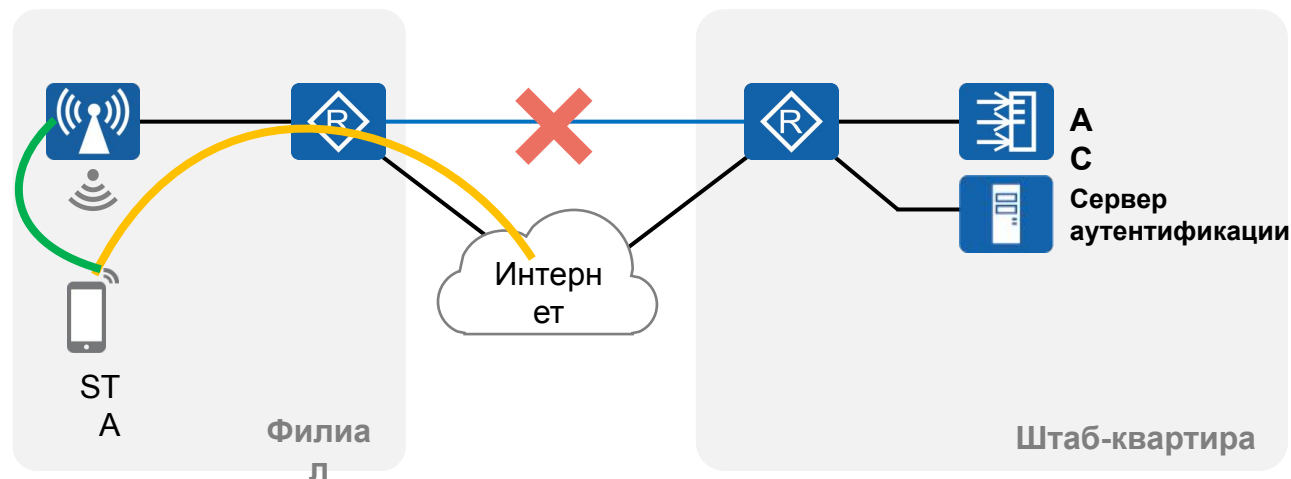
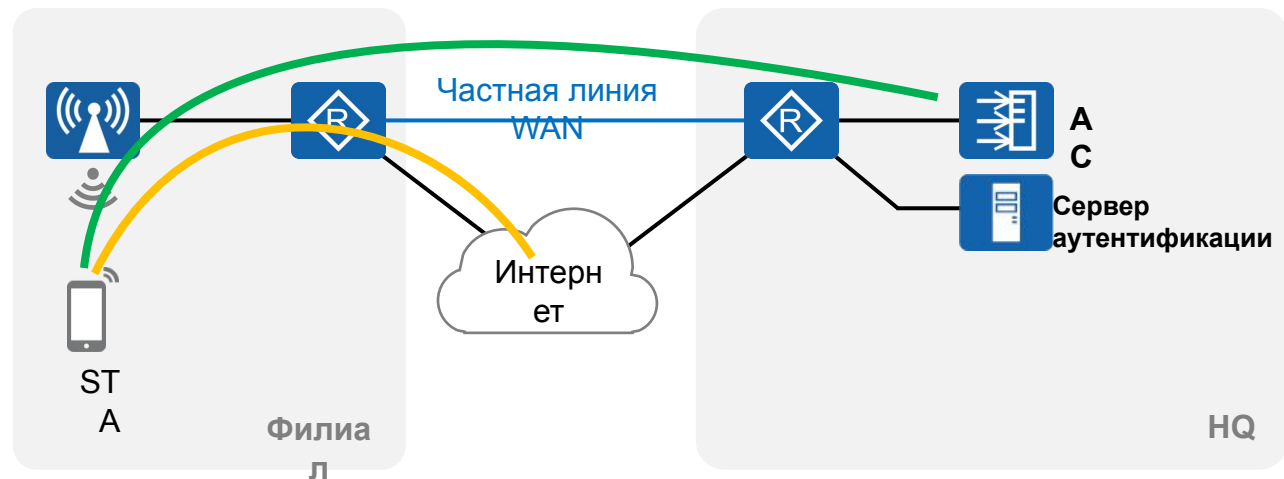
## Функция

- Если канал CAPWAP между точкой доступа и контроллером доступа отключен, сервисы онлайн-STA не прерываются, и данные пользователей пересылаются в обычном режиме.
- Данные пользователей пересылаются в режиме локальной пересылки.
- Если политикой безопасности на стороне беспроводной сети AP является открытая система, общий ключ (WEP) или WPA/WPA2-PSK, новые STA подключаются к сети.

## Сценарий применения

В малой WLAN без схемы резервирования контроллера доступа, при отключении точки доступа от контроллера, эта функция обеспечивает бесперебойную передачу пользовательских данных, повышая тем самым надежность обслуживания.

# Надежность сервиса: обход аутентификации WAN



→ Данные аутентификации

→ Служебные данные

## Функция

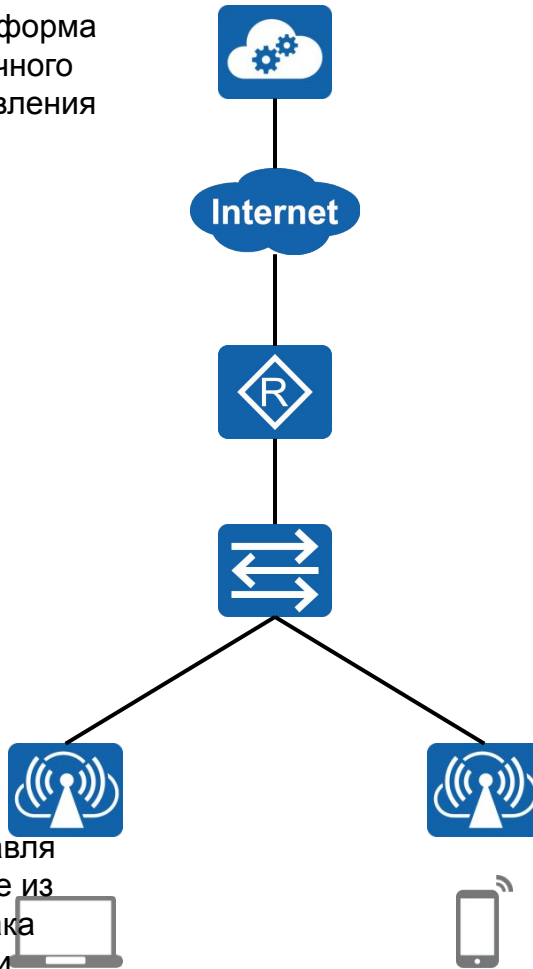
- Традиционно контроллер доступа выполняет аутентификацию пользователя. В случае прерывания связи между контроллером и точкой доступа новые пользователи не получают доступ к сети, поскольку не могут быть аутентифицированы.
- Обход аутентификации WAN: в случае отсоединения точки доступа от контроллера доступа точка доступа предоставляет функцию локальной аутентификации для подтверждения вновь подключенных пользователей, обеспечивая таким образом надежность обслуживания.

## Сценарий применения

Для связи между штаб-квартирой и филиалами используется глобальная сеть. Контроллер доступа развернут в штаб-квартире, а точки доступа — в филиалах. Если в штаб-квартире точки доступа филиала отключены от контроллера доступа, сервисы онлайн-STA будут работать правильно после настройки функции удержания обслуживания при отключении связи CAPWAP. Однако новые STA не могут подключиться к сети, что влияет на работу пользователей. чтобы новые STA могли подключаться к сети после отключения точек доступа филиала от контроллера доступа в штаб-квартире в кампусной сети можно развернуть решение для обхода аутентификации WAN.

# Архитектура облачного управления

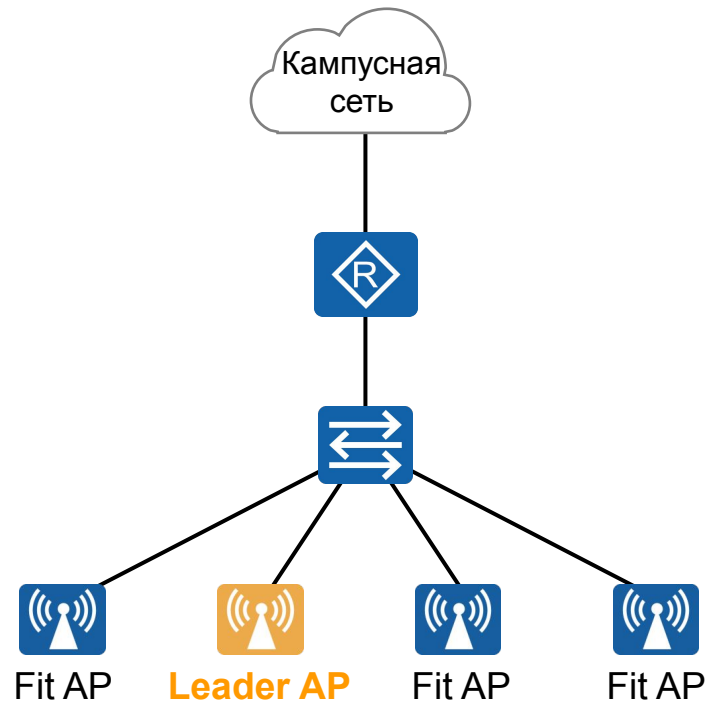
Платформа  
облачного  
управления



Управля  
емые из  
облака  
дочки  
доступа

- Платформа облачного управления управляет и настраивает облачные точки доступа и управляет доступом к STA унифицированным образом.
- По сравнению с традиционной архитектурой AC + Fit AP архитектура облачного управления имеет следующие преимущества:
  - Автоматическая настройка и запуск устройств и автоматическое развертывание сокращают затраты на развертывание сети.
  - Унифицированная система O&M: платформа облачного управления обеспечивает централизованный мониторинг и управление всеми сетевыми элементами из облака.
- Такая архитектура может применяться для WLAN малого и среднего размера и обеспечивает гибкое развертывание и низкие затраты на эксплуатацию и техническое обслуживание.

# Архитектура Leader AP

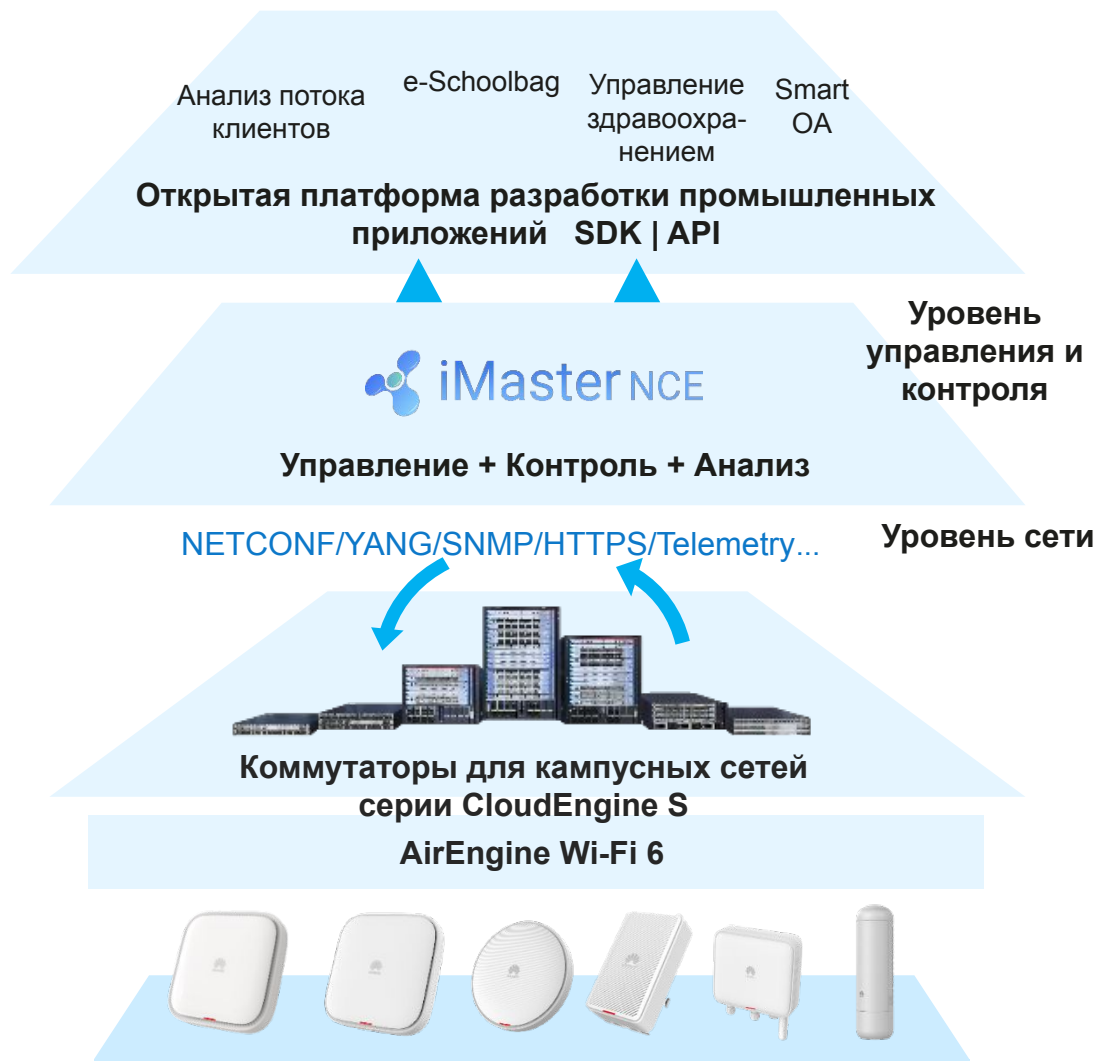


- Архитектура Leader AP включает только точки доступа. Одна точка доступа настраивается как ведущая (Leader), после этого другие точки доступа подключаются к сети в режиме Fit AP и связываются с ведущей точкой доступа на уровне 2.
- Ведущая точка доступа сообщает о своей роли по сети уровня 2. Другие точки доступа автоматически обнаруживают ведущую точку доступа и подключаются к ней.
- Подобно контроллеру доступа, ведущая точка доступа обеспечивает унифицированное управление доступом, настройку и эксплуатацию и обслуживание на базе CAPWAP-туннелей, обеспечивая централизованное управление беспроводными ресурсами и управление роумингом.
- Пользователям нужно только войти в систему ведущей точки доступа и настроить беспроводные услуги. После настройки все точки доступа предоставляют одни и те же беспроводные услуги, и STA могут перемещаться между разными точками доступа.

# Сравнение сетевых архитектур WLAN

Сетевая архитектура	Характеристики	Сценарий применения
Архитектура Fat AP	Fat AP («Толстые точки доступа») необходимо развертывать и настраивать независимо, что усложняет управление и обслуживание.	SOHO
Архитектура AC + Fit AP	Контроллер доступа осуществляет централизованное управление и настройку точек доступа, значительно упрощая процедуры настройки и развертывания.	WLAN большого и среднего размера
Архитектура облачного управления	Платформа облачного управления централизованно управляет и настраивает точки доступа, упрощая развертывание и эксплуатацию и техническое обслуживание.	WLAN малого и среднего размера
Архитектура Leader AP	Ведущая (Leader) точка доступа осуществляет централизованное управление и настройку точек доступа, значительно упрощая процедуры настройки и развертывания.	WLAN малого размера

# Архитектура сети следующего поколения: CloudCampus



- Решение Huawei CloudCampus для кампусных сетей малого и среднего размера использует технологию облачных вычислений для реализации автоматического и централизованного управления сетью и предоставляет возможности сбора и анализа данных, которые недоступны в традиционных сетях, для предоставления услуги NaaS (Network as a Service — сеть как услуга). Особенности:
  - Простые процедуры планирования и развертывания сети
  - Расширение сети и управления по требованию
  - Сетевые данные и открытость сетевой платформы



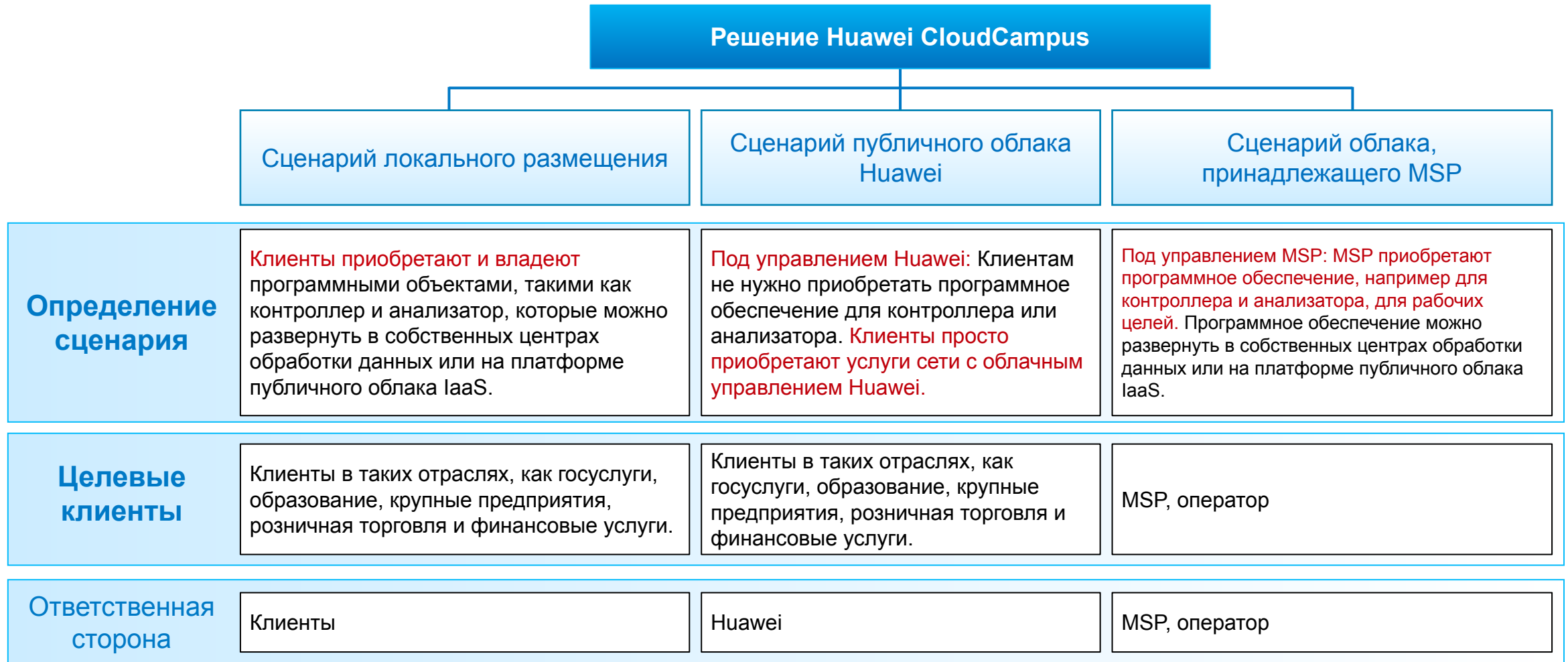
# Основные характеристики решения CloudCampus для кампусных сетей малого и среднего размера

- Решение Huawei CloudCampus для кампусных сетей малого и среднего размера использует технологию облачных вычислений для реализации автоматического и централизованного управления сетью и предоставляет возможности сбора и анализа данных, которые недоступны в традиционных сетях, чтобы предоставить услугу NaaS (Network as a Service — сеть как услуга).
  - Автоматическое развертывание: быстрое и простое развертывание устройств.
  - Планирование WLAN с управлением из облака и эксплуатация и обслуживание мобильных устройств: упрощенная конструкция WLAN и обслуживание устройств.
  - Широкая линейка продуктов: полная серия устройств (коммутаторы, межсетевые экраны, AR и AP) линейки продуктов корпоративной сети Huawei может использоваться для предоставления различных портфелей продуктов, отвечающих разнообразным сетевым требованиям клиентов.
  - Поддержка двух режимов работы и плавное развитие: все сетевые устройства, используемые в этом решении, могут работать как в режиме управления из облака, так и в традиционном режиме управления. После обновления устройств клиенты могут реализовать управление сетью из облака.
  - Дополнительные услуги: анализ поведения терминала —дополнительное приложение iMaster NCE. Данные анализа поведения терминала позволят разработать большее количество дополнительных услуг.

# iMaster NCE

- iMaster NCE — это контроллер, который объединяет функции управления, контроля и анализа. Поддерживает простые в эксплуатации кампусные сети, виртуальные кампусные сети и взаимосвязь между многофилиальными кампусными сетями и включает в себя следующие элементы:
  - iMaster NCE-Campus: обеспечивает функции управления и контроля, интегрирует функцию управления традиционными устройствами как услугу и обеспечивает перенаправление в один клик на iMaster NCE-CampusInsight на базе прокси-сервиса.
  - Компонент аутентификации iMaster NCE-Campus: может быть интегрирован в iMaster NCE-Campus как услуга или развернут независимо. Удаленно можно развернуть до 20 компонентов аутентификации, чтобы обеспечить локальную аутентификацию для удаленных филиалов. Компоненты аутентификации и iMaster NCE-Campus могут автоматически синхронизировать данные аутентификации пользователя и данные идентификации терминала по каналам TCP.
  - iMaster NCE-CampusInsight: платформа интеллектуального сетевого анализа Huawei. Основываясь на имеющихся данных эксплуатации и обслуживании (таких как индикаторы производительности устройств и журналы терминалов), iMaster NCE-CampusInsight использует большие данные, алгоритмы искусственного интеллекта и передовые технологии анализа для создания среды с цифровыми возможностями, помогая клиентам своевременно обнаруживать проблемы в сети и улучшить пользовательский опыт.

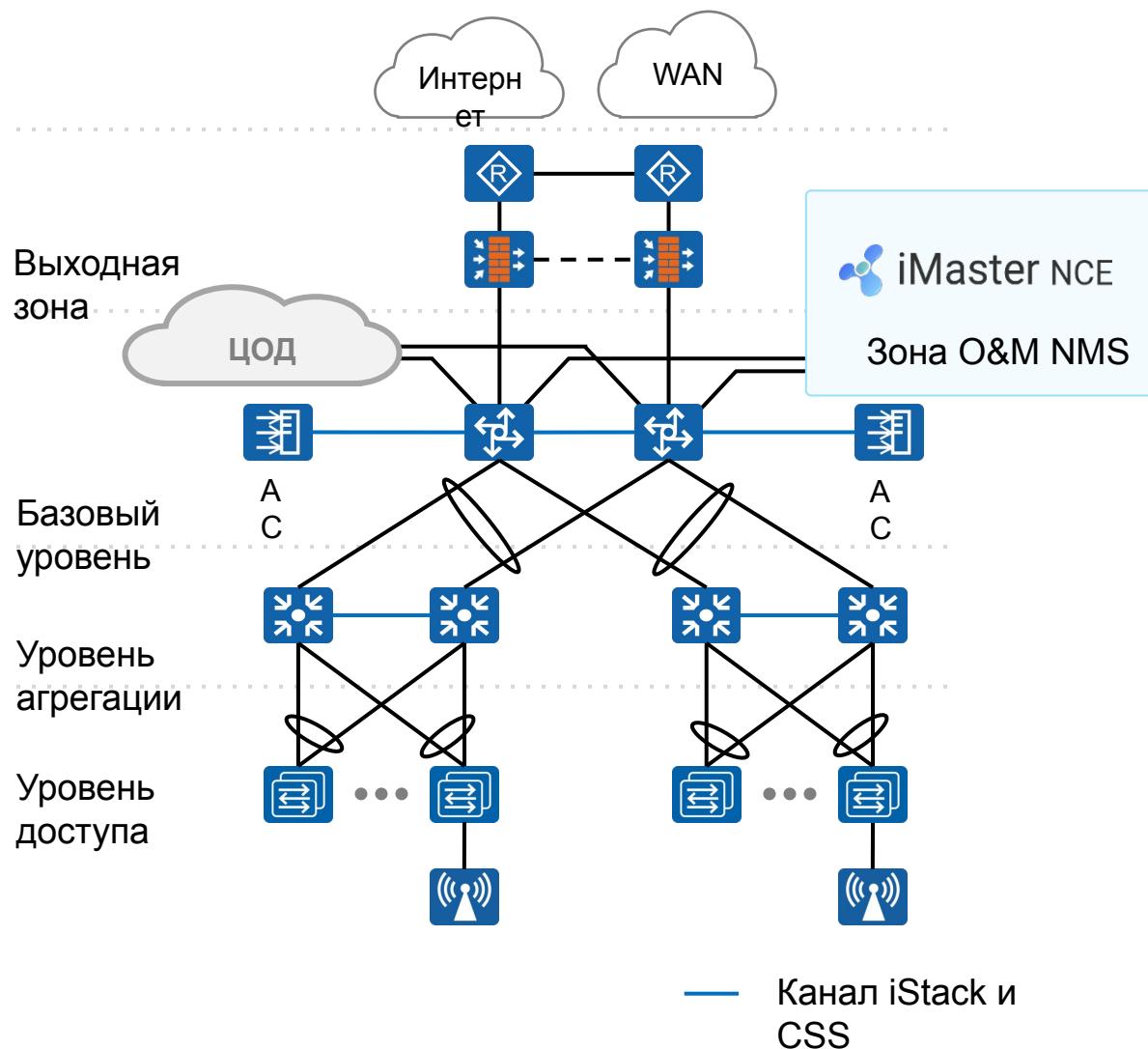
# Три режима развертывания решения Huawei CloudCampus



# Содержание

1. Основные понятия WLAN
2. Архитектура сети WLAN
- 3. Типичные решения для организации сети WLAN**

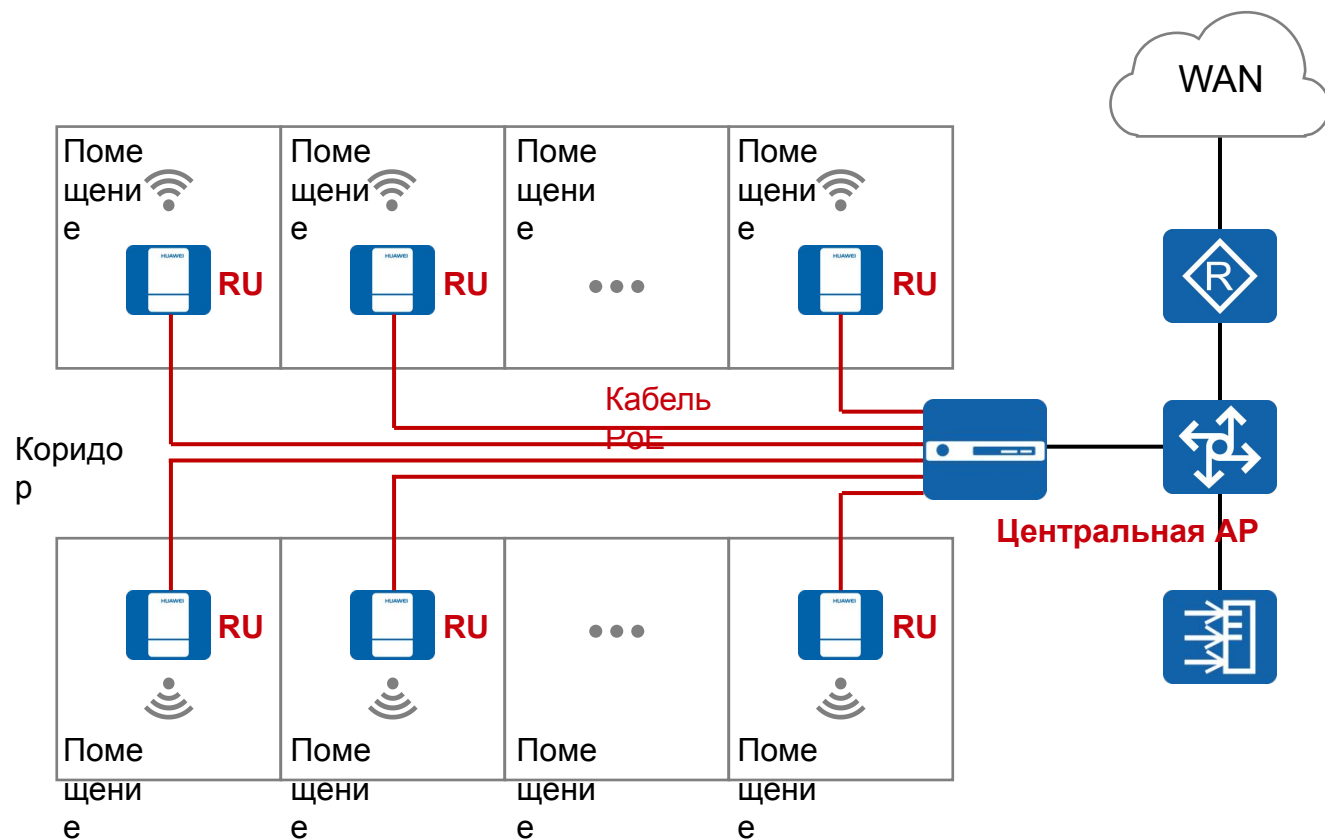
# Решение для крупной кампусной сети



## Описание решения

- Если развернута проводная кампусная сеть и требуется независимое развертывание беспроводной сети или если масштаб беспроводной сети слишком большой, рекомендуется развернуть независимые контроллеры доступа.
- В кампусной сети большого размера контроллер доступа обычно подключается к коммутатору агрегации или базовому коммутатору в режиме off-path.
- Чтобы уменьшить количество изменений в существующей проводной сети и упростить централизованное управление и контроль, рекомендуется использовать туннельную пересылку. В решении независимого контроллера доступа обычно используется VRRP HSB для повышения надежности контроллера доступа.

# Решение для гибкой распределенной сети Wi-Fi



## Описание решения

- В гибкой распределенной сетевой архитектуре традиционная точка доступа разделена на два независимых устройства: центральную точку доступа и выносной модуль (RU).
- Центральные точки доступа развертываются в аппаратных залах, слаботочных стояках или коридорах, а выносные модули устанавливаются в помещениях, при этом используются сетевые кабели, в результате в каждом помещении (комнате, номере, палате) предоставляются высококачественные эксклюзивные услуги беспроводного доступа.

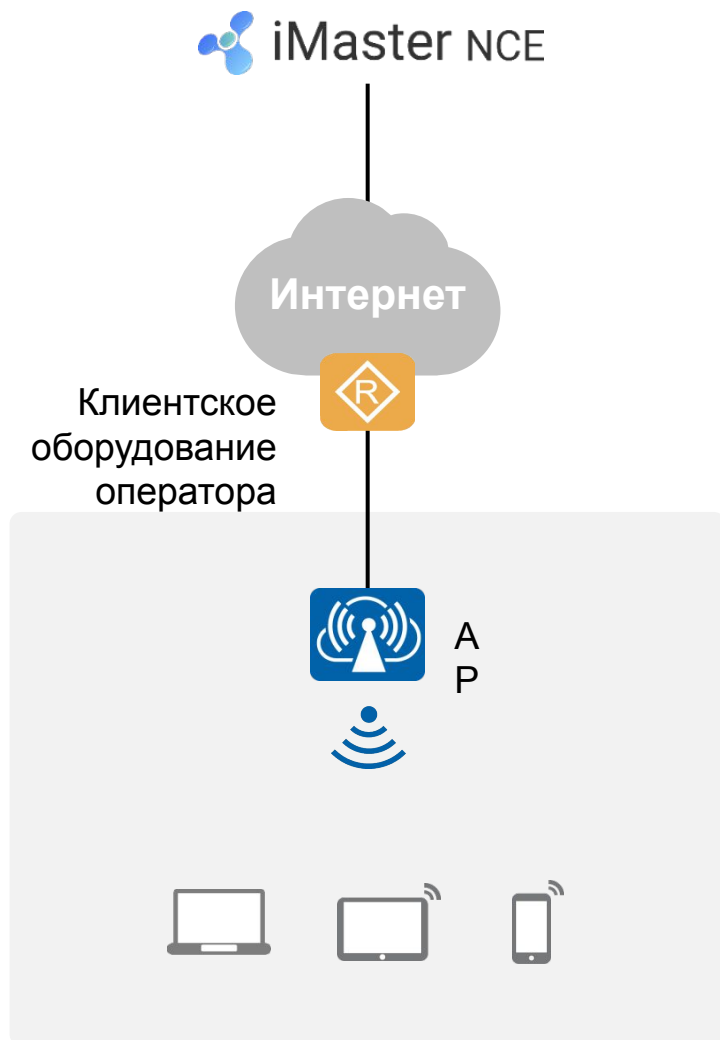
## Сценарий применения

Сценарии с плотно расположенными помещениями, например, гостиницы, общежития и больничные палаты.

## Преимущества

- Простое управление
- Гибкое развертывание и полное покрытие сигнала без «слепых зон» в покрытии.
- Покрытие на большие расстояния

# Решение для небольших и мини сетевых магазинов



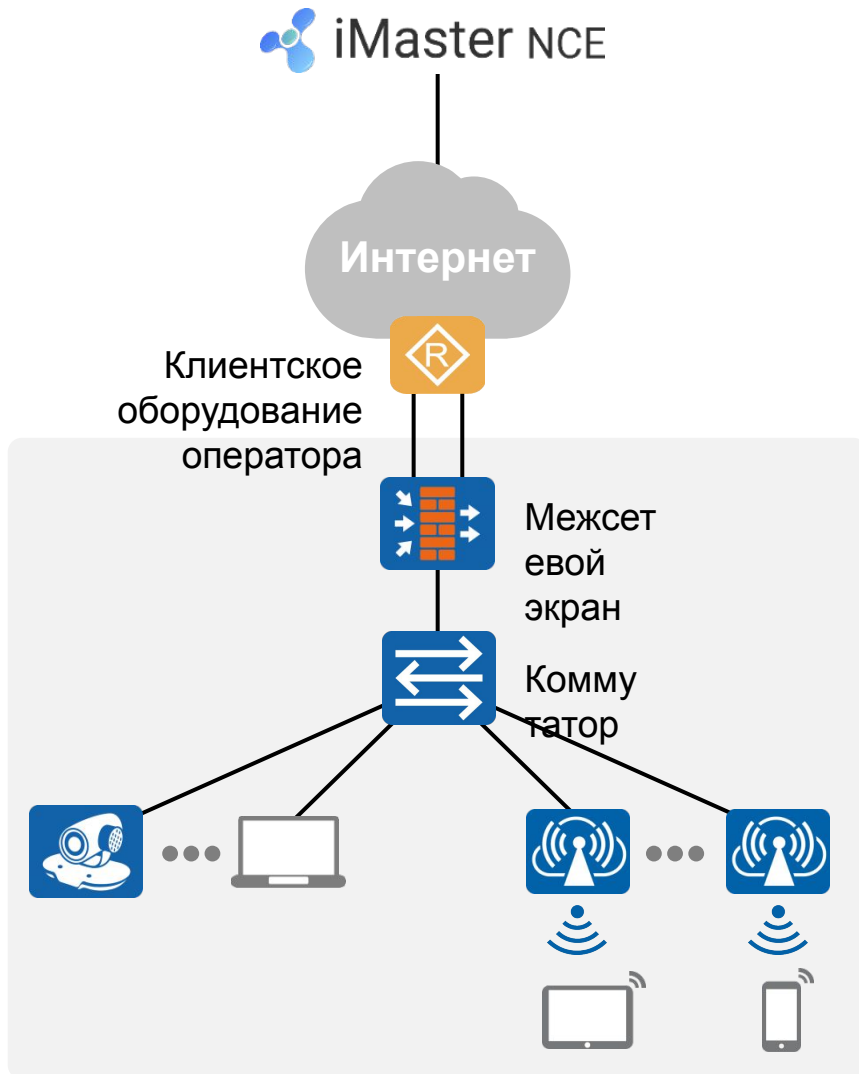
- **Описание решения**

- В сети с одной точкой доступа точка доступа выполняет функции шлюза для станций.

- **Сценарий применения**

- Небольшие магазины (например, агентские магазины и заправочные станции) площадью менее 50 м<sup>2</sup>
- Поддерживается не более 50 одновременных подключений станций к сети.
- Поддерживается только беспроводной доступ пользователей.
- Требуется только один проводной канал для выхода в Интернет.

# Решение для небольших и средних сетевых магазинов



- **Описание решения**

- Для обеспечения покрытия беспроводной сети несколько точек доступа подключаются к коммутатору через PoE. Межсетевой экран обеспечивает функции выхода, например, доступ к WAN, DHCP и NAT, а также функции пользовательского шлюза. Коммутатор обеспечивает расширенный доступ по PoE и функции доступа к проводному терминалу. Точки доступа предоставляют доступ для STA на объекте.

- **Сценарий применения**

- Малые и средние магазины, мелкие логистические и страховые компании площадью менее 3000 м<sup>2</sup> и менее 2000 одновременных онлайн-терминалов.
- Для обеспечения беспроводного доступа необходимо развернуть несколько точек доступа, необходимо выполнить высокие требования к безопасности (фильтрация URL-адресов/IPS/защита безопасности/антивирусные программы), а для доступа в Интернет требуется несколько восходящих каналов.



# Вопросы

---

1. (Единичный выбор) Предприятию необходимо реализовать резервирование устройств в WLAN для обеспечения стабильности сети. Требованиями предприятия являются: высокая надежность контроллера доступа, высокая скорость переключения при отказе канала, развертывание активного и резервного контроллеров доступа в штаб-квартире. Какое решение для обеспечения высокой надежности контроллера доступа может использовать предприятие в данном сценарии?
  - A. Горячее резервирование с использованием протокола VRRP (VRRP HSB)
  - B. Горячий резерв (HSB) по двум каналам
  - C. Холодный резерв по двум каналам
  - D. Резервирование N+1

# Заключение

---

- В настоящем курсе приведены основные понятия WLAN, описаны различные сетевые архитектуры WLAN, включая архитектуру Fat AP, архитектуру AC + Fit AP, архитектуру облачного управления, архитектуру Leader AP и архитектуру CloudCampus от Huawei. Данный курс позволит разобраться в режимах организации сети и моделях пересылки, используемых в архитектуре AC + Fit AP. После окончания курса вы сможете выполнять простые процедуры проектирования, включая проектирование VLAN, проектирование IP-адресов и проектирование систем высокой надежности.
- Этот курс также знакомит с несколькими типичными сетевыми решениями Huawei для WLAN.

# 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  
Авторские права © Huawei Technologies Co., Ltd. 2020.  
世界万物联接在一起的数字世界。

Информация, представленная в данном  
документе, может содержать  
прогностические высказывания,  
включая, в том числе, заявления о  
будущих результатах финансово-  
хозяйственной деятельности, будущих  
линейках продукции, новых  
технологиях и прочее. Существует ряд  
факторов, которые могут привести к  
тому, что фактические результаты и  
достижения будут отличаться от  
результатов, явно или косвенно  
описанных в указанных  
прогностических высказываниях.

 **HUAWEI** представленная  
информация не является офертой или  
акцептом. Компания Huawei может вносить  
изменения в представленную  
информацию в любое время без  
предварительного уведомления.

# История изменений

Не для печати

Код курса	Продукт	Версия продукта	Версия курса
H12-311	WLAN	V2R19	3.00

Составлено/ID сотрудника	Дата	Проверено/ID сотрудника	Новый/Обновление
У Ваньшэнь (Wu Wanshen)/WX343927	19.06.2020	Новая группа WLAN	Новый