Новая эра беспроводных сетей Cisco: WIFI6, WPA3, Catalyst 9100 и 9800

Платов Виктор, CCIE #24288, CWNE #283
Консультант по технологии WI-FI
13 ноября 2019

Беспроводная сеть Cisco следующего поколения

Cisco DNA Center

Трансляция бизнес требований в настройки оборудования и политики сети.
Интуитивная отладка и устранение неполадок.

Контроллеры серии
Cisco® Catalyst® 9800

Cisco DNA Spaces

Определение местоположения людей и предметов, аналитика

Точки доступа
Cisco Catalyst 9100

Надежно | **Безопасно** | **Интеллектуально**

Беспроводной доступ Cisco Catalyst следующего поколения

Интеграция и партнерство с Apple, Samsung, Intel и Microsoft

Контроллеры БЛВС Cisco Catalyst 9800

Управляются Cisco IOS® XE
Открытые и программируемые

Точки беспроводного доступа Cisco Catalyst 9100

Поддержка технологии Wi-Fi 6
Отличная радиочасть

Надежно

- Детерминированная емкость
- Большое время жизни батареи IoT устройств
- Обновления ПО с минимальными перерывами в работе

Лидерство в радиоподсистеме

Безопасно

- Обнаружение угроз в зашифрованном трафике Encrypted Traffic Analytics (ETA)
- Multi-lingual AP with RF snapshots
- WPA3, Trustworthy systems

Неотъемлемая часть intent-based сети Cisco

Интеллектуально

- Непревзойденная аналитика с Cisco DNA
- Контейнеры для IOT приложений
- Используйте в удобном для Вас виде

Инновации за пределами стандартов

Wi-Fi 6: Обзор 802.11ax

Что нам даст Wi-Fi 6 (802.11ax)

Стоит ли вообще обращать внимание?

Возросшие скорости

- 1024-QAM, до 9.6Гбит/с на радио, 1.2Гбит/с на одну антенну
- 8x8:8SS
- Позволяет использовать приложения нового поколения, основанные на 4K/8K и AR/VR видео

Увеличение емкости сети

- OFDMA увеличивает пропускную способность от 3х до 4х раз по сравнению с 802.11ac
- BSS coloring в сетях высокой плотности увеличивает емкость до 4-ех раз

Уменьшение задержек и увеличение надежности

- Scheduled uplink и downlink OFDMA дает предсказуемые “как в сотовых сетях” задержку, надежность и QoS
- Оптимизирован для сценариев подключения сотен IoT устройств к ТД

Экономия батареи устройств

- Увеличение времени жизни аккумулятора в 3 раза за счет Target Wake Time (TWT)
- Общая эффективность передачи и приема информации за счет отказа от борьбы за эфир

Более подробно здесь: https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html

Где может быть востребовано?

Широкополосный доступ

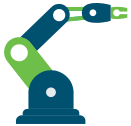
Больше полосы каждому клиенту

- 50бит/с или выше на клиента в сетях высокой плотности
- Видеоприложения (4K, 8K), AR/VR с эффектом погружения
- Учебные классы нового поколения, Стадионы, беспроводные офисы

Массовое внедрение IOT

Поддержка **высокой плотности IoT устройств**

- Отслеживание предметов, сервисы с учетом местоположения, электронные платежи
- Интеграция IOT и IT, автоматизация
- Гостиницы, магазины, Умные дома



Критически важные сервисы

Приложения, требующие высокой надежности и низкой задержки сети

- Автоматизация производственных процессов, автономные автомобили, аналитика реального времени
- Производство, телемедицина, склады

Надежно

Увеличенная детерминированная емкость

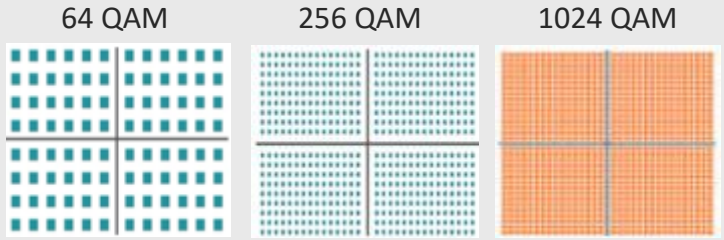
Путем увеличения эффективности передачи данных в эфире

802.11ax – это повышение эффективности беспроводной передачи

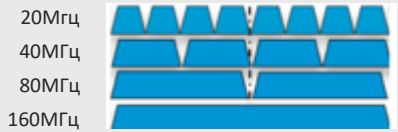
- .11ax High Efficiency Wireless (HEW) сфокусирован на оптимизации передачи данных в радиоэфире
- Четыре способа повысить эффективность

1. **Data rate (Modulation density)** или **QAM** - (число Битов на OFDM символ) 64 QAM более надежен, но 1024 QAM быстрее
2. **Число пространственных потоков и работа с доступным спектром** (появление OFDMA и Resource Units, а также UL/DL MU-MIMO
3. **Ширина канала** – сколько частот мы можем модулировать
4. **Накладные расходы** – Preamble/Ack/BA, Guard Interval “GI”, и т.д.

Типы QAM модуляций



Ширина Wi-Fi канала



Замечание: Channel Bonding уменьшает размер соты, т.к. каждые 20МГц спектра уменьшают SNR на 3 dB, что ведет к уменьшению типа QAM.

Безопасно

Безопасность

или что такое WPA3

Отодвиньте границу зоны безопасности вашей сети с ТД Cisco Catalyst 9100

Обнаружение Interference/Rogue

RF Snapshots

WPA3

Соответствие стандартам, улучшенная безопасность даже для open Wi-Fi

Обнаружение угроз в зашифрованном трафике (ETA)

Улучшенная классификация и сегментация клиентов

Безопасные и доверенные системы

Cisco Catalyst 9100 – самые защищенные точки доступа

Применение доверенных систем делает вашу инфраструктуру безопасной

- Plug and Play SUDI support: Two-way trust
- Image signing: Аутентичная ОС

- Secure boot: проверка последовательности
- Hardware authenticity: Аутентичная аппаратура

История защиты Wi-Fi сетей

(или WPA2) – хорошее, плохое, ужасное

История недавних попыток усилить безопасность Wi-Fi

- Если механизм безопасности является опциональным и не несет понятных преимуществ, он не будет внедрен.
- WPA preshared keys являются известной проблемой
  - Постоянное увеличение вычислительной мощности делает задачу их взлома все более легкой
  - Давно должны были быть отменены, потому что этот “пароль” небезопасен
- TKIP до сих пор широко используется
  - Статья 2013 года говорит, что 71% сетей с шифрованием использует его вместо нормальных алгоритмов http://people.cs.kuleuven.be/~mathy.vanhoef/papers/wpatkip.pdf
- ***Мало того, я знаю примеры использования WEP!***

WPA2 – хорошо, плохо, ужасно

- ***Хорошо***
  - WPA2 был создан, чтобы исправить проблемы WPA
    - TKIP был взломан
    - AES поддерживался в достаточном количестве чипсетов
    - 802.1x и RADIUS слишком сложны для домашнего использования, поэтому требовался более простой, основанный на пароле метод
  - Сейчас каждый (почти) может создать свою WPA2 домашнюю сеть!

WPA(2)-PSK: Плохо

- с WPA(2) – пароль или PSK используется и для “аутентификации” и шифрования
- Уязвим для некоторых атак: инструменты для взлома пароля можно легко скачать в Интернет
- Имея фреймы 4-way Handshake, злоумышленник, перебирая пароли из словаря, вычисляет MIC до тех пор, пока он не совпадет с содержащимся в message 3 или message 4
- Отсутствие ***прямой секретности*** – угадайте пароль и получите ключи шифрования для всех прошлых, текущих и будущих сеансов передачи данных
- Достаточно просто «подслушать» трафик, чтобы затем взломать пароль и подключиться к сети
- Brute force /Dictionary атаки: Amazon Cloud attack: осуществляет 2,400,000 проверок пароля в минуту при цене $0.23 в мин. – в наши дни размер словаря не имеет значения!

Что не так со старым добрым WPA2 PSK?

- При использовании WPA2 PSK, введенный пароль используется для генерации Pairwise Master Key (PMK)
- Как это работает:
  1. На обоих сторонах используется специальный псевдослучайный алгоритм (PBKDF2) для того, чтобы сделать введенную пользователем passphrase (“пароль”) немного более криптографически стойкой: PSK = функция от (Passphrase, SSID, SSIDlength) = 256-bit строка
  2. Этот процесс аналогичен как на стороне клиента, так и на стороне точки доступа. В результате они получают одинаковый PSK. Этот PSK используется как PMK.

PSK = PBKDF2 (PassPhrase, ssid, ssidLength, 4096, 256)

PSK = PBKDF2 (PassPhrase, ssid, ssidLength, 4096, 256)

WPA2 – Ужасно
Кто придумал transition mode для WPA/WPA2?

Вспомним – в то время не все ТД поддерживали Multiple BSS (несколько SSID)

- Transition mode был создан для сохранения совместимости с WPA и возможности подключения устаревших устройств.

- Что мы получили в transition mode:
  - ***В качестве группового шифра используется TKIP***
    - ***Наибольший общий знаменатель***
  - К тому же уязвимость для атак по словарю

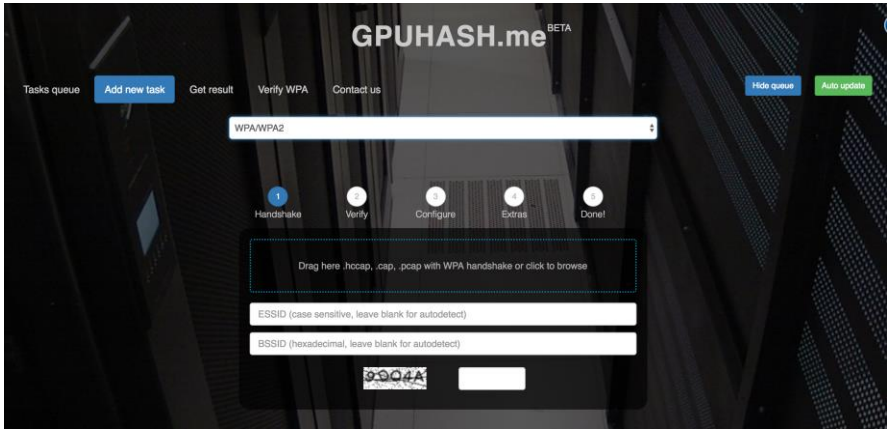
- Безопасность всегда страдает от простоты внедрения
  - *Мы никогда не читаем мелкий шрифт*

Замечание – с точки зрения безопасности: нет ничего хорошего в переходных режимах (никогда не было и никогда не будет)

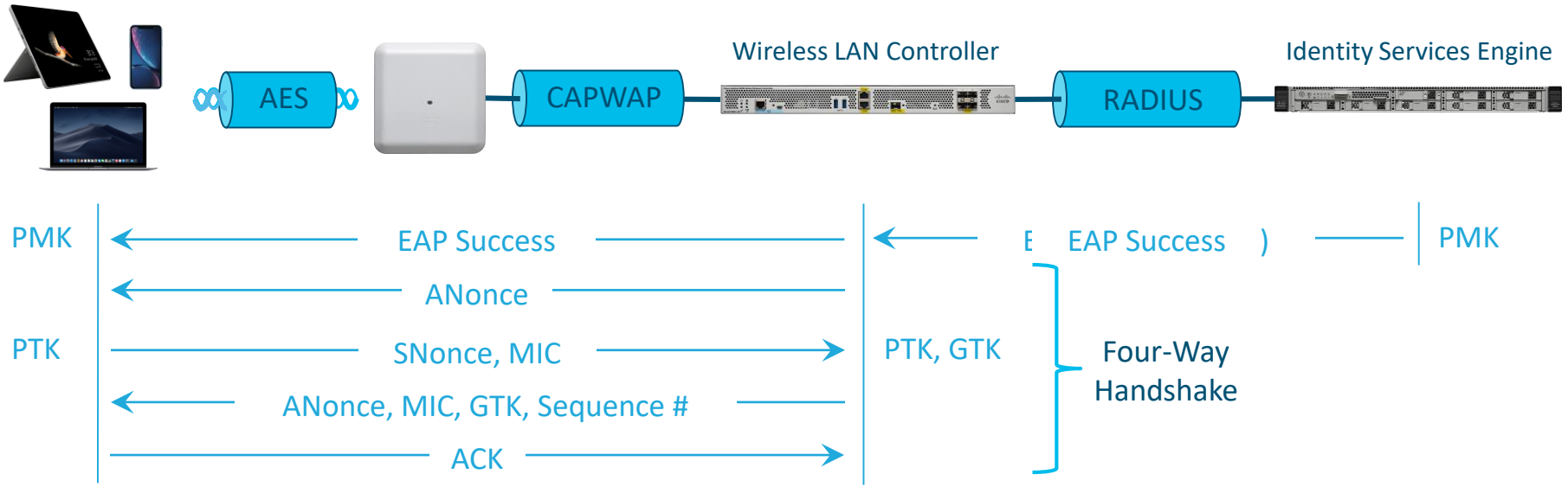
Почему легко взломать WPA2-Personal?

- Все, что требуется – это собрать фреймы 4-Way handshake
  - Как?– деаутентифицировать клиента
- Загрузить фреймы в виде pcap
- Заказчики/пользователи используют уязвимые пароли
- Как результат – простой доступ к проводной сети (мы даже не говорим про расшифровку пассивно собранных в эфире пакетов)
- Если моя цель получить доступ к проводной сети, то MAC based auth + PSK элементарно обходится

А теперь вспомним IoT, медицинские устройства, телевизоры и т.д.

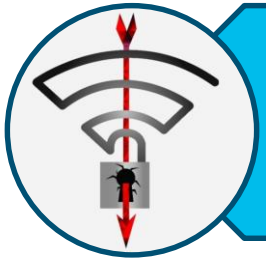


Что насчет WPA2-Enterprise



Внимание: вектор атаки меняется с уязвимого PSK на уязвимый пароль пользователя

«Выпускайте KRACKen-a!»
Key Reinstallation AttaCK (KRACK)

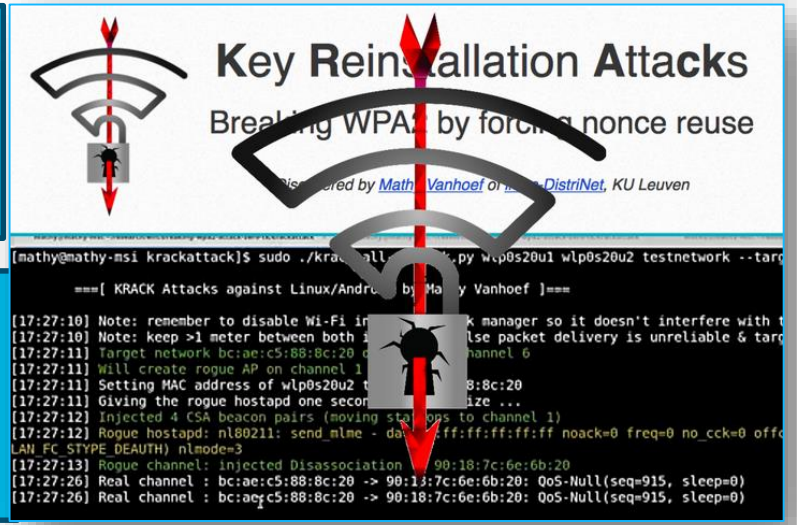


В октябре 2017 были опубликованы

10 возможных атак на WPA2

Все они касались нюансов методологии тестирования WPA2 :

- Ситуации, которые возможны в 802.11, но не тестировались
- Сейчас патчи доступны практически для всех платформ, но атака доказывает, что WPA2 стареет

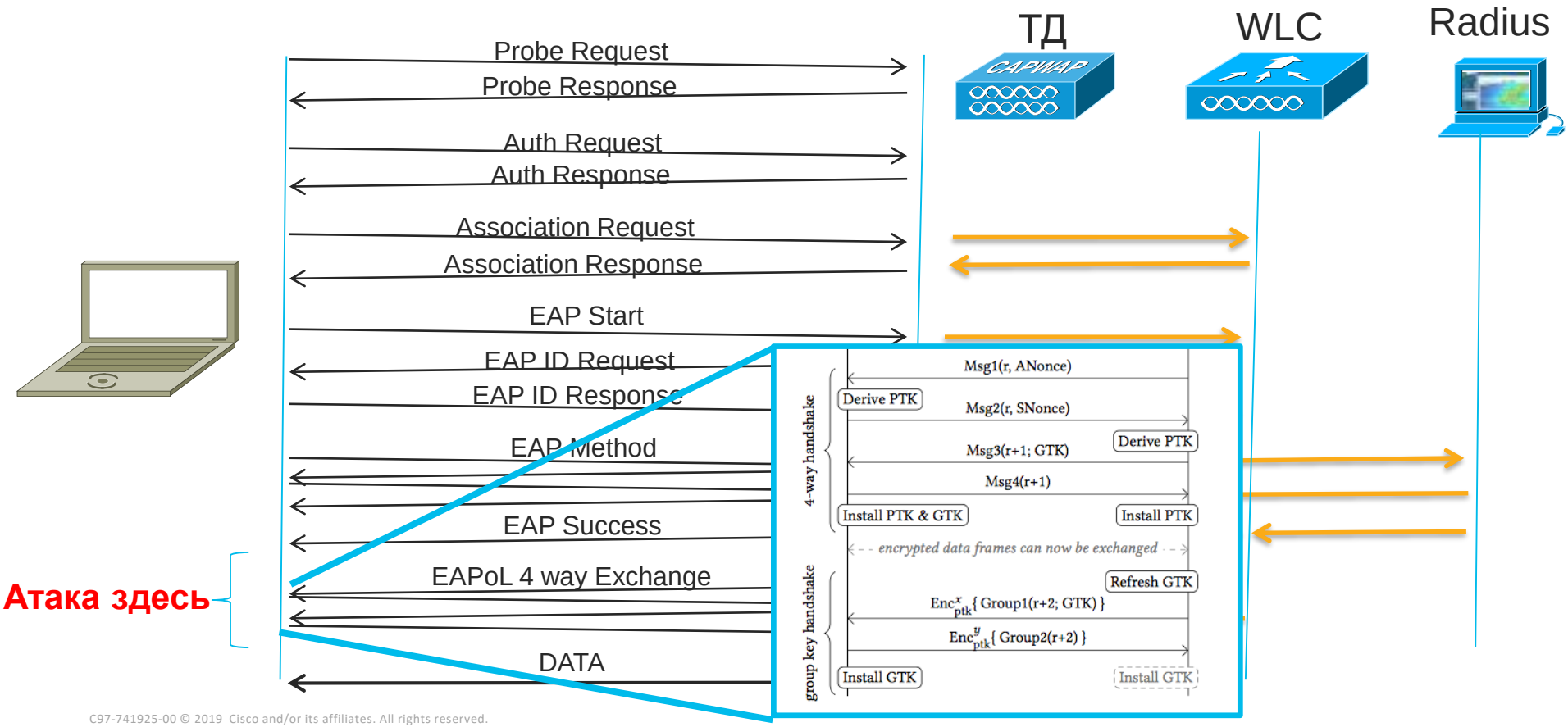


WPA2 выпущен в 2004 г.; пора его обновить!

Key Reinstallation AttaCK (KRACK) продолжение

- KRACK – это атака на 4-way handshake (в особенности на переиспользование nonce)
- Что делает 4-way handshake?
  - Взаимная аутентификация ТД и клиента
  - Генерация свежих Pairwise Transient ключей
- Где используется 4-way handshake?
  - WPA Personal и Enterprise
  - WPA2 Personal и Enterprise
  - 802.11r Fast BSS transition (FT)
  - 802.11ai Fast Initial Link Setup (FILS)

Аутентификация 802.1X



Сообщения 4-way handshake (упрощенно)

Сообщение 1:

- EAPoL frame содержит A-Nonce (nonce аутентификатора)
- Саппликант вычисляет PTK, т.к. теперь он знает A-Nonce, S-Nonce и PMK

Сообщение 2:

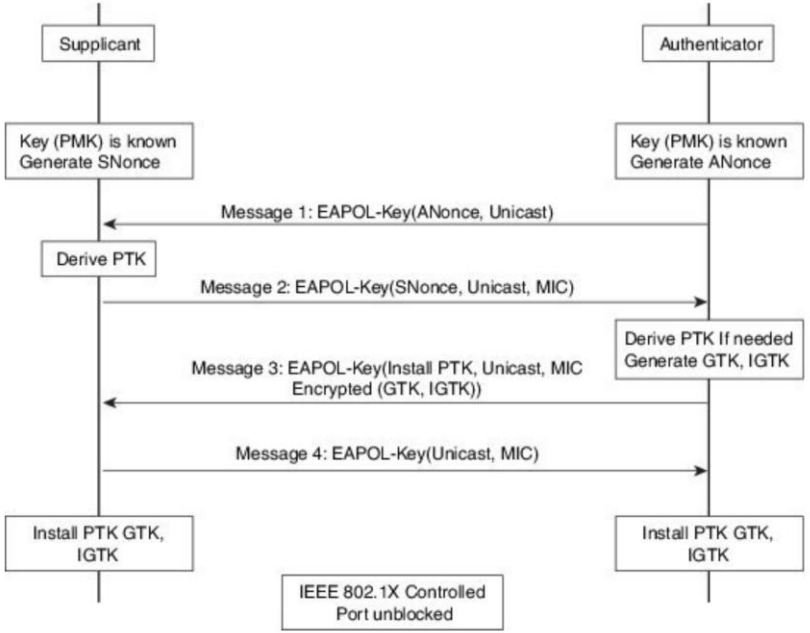
- Саппликант отправляет аутентификатору S-Nonce
- Аутентификатор вычисляет PTK, GTK и IGTK (для PMF)

Сообщение 3:

- GTK, IGTK доставляются саппликанту в зашифрованном с помощью PTK виде
- Саппликант устанавливает временные ключи шифрования

Сообщение 4:

- Саппликант сообщает аутентификатору, что временные ключи шифрования установлены



Key reinstallation осуществляется повторной отсылкой Сообщения 3

Opportunistic Wireless Encryption (OWE)

Открытые сети (без шифрования) получили обновление

Wi-Fi CERTIFIED Enhanced Open

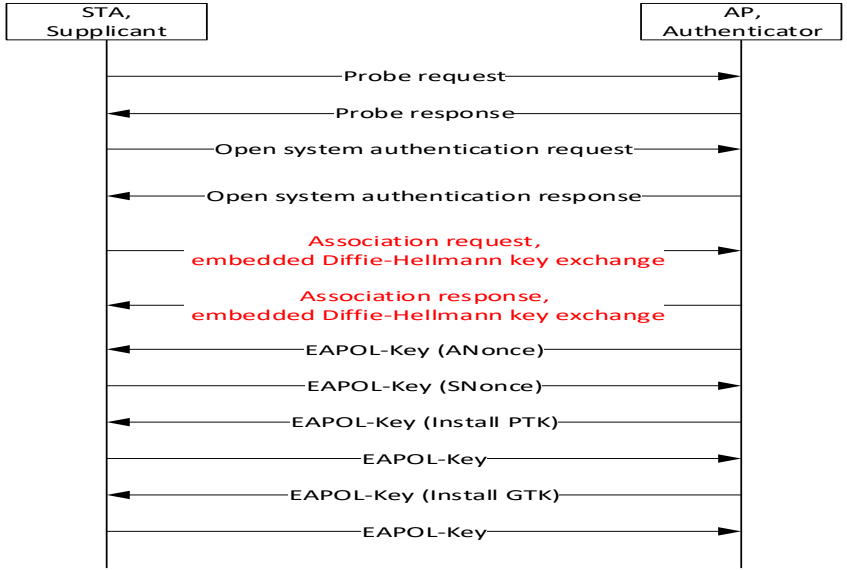
*не совсем WPA3 (по крайней мере пока)

Какую проблему мы пытаемся решить??

- Пассивное прослушивание – и все!!
- Немного лучше, чем Open Networks в плане приватности.
- Аналогичная открытым сетям процедура подключения (но теперь с шифрованием)
- Приватность – но не безопасность
- ***Никакой защиты от man-in-the-middle***

Wi-Fi CERTIFIED Enhanced Open

- Основана на Opportunistic Wireless Encryption (OWE)
  - Описана в RFC 8110– https://tools.ietf.org/html/rfc8110
- Дает конфиденциальность и проверку целостности, но аутентификация отсутствует
- Альтернатива открытым сетям, сфокусированная на приватности
- Не требует ни настройки, ни вмешательства пользователя – просто работает!
- Безопасность в OWE:
  - Считается невозможным для третьей стороны получить ключи шифрования
    - Diffie-Hellman group: 19, NIST p256 elliptic curve
      - Быстро и эффективно
      - Широко распространено
  - Подходит для 128-битного шифрования (CCMP или GCMP)
  - ***Требует PMF***
  - Уязвима к активным онлайн атакам, устойчива к пассивным офлайн атакам



Преимущества

- Enhanced Open в самом деле ***дает больше приватности,*** чем WPA2-PSK, использующий общеизвестный PSK в публичных зонах
- Если каждый знает PSK от WPA2-Personal сети, то никакого труда не составит расшифровать весь трафик (***прошлый и будущий***)…для хакера это все равно, что открытая сеть
- Enhanced Open – каждый клиент генерирует свои собственные ключи с использованием обмена ECDH

Enhanced Open Transition Mode

- Включение Enhanced Open SSID ведет к созданию отдельного скрытого BSS с аналогичными Open BSS свойствами
- Open BSS будет перенаправлять поддерживающих OWE клиентов на Enhanced Open BSS с помощью специального OWE Transition Mode Element
- Зачем так сложно???
  - Поведение устаревших клиентов – некоторые воспринимают Enhanced Open BSS как “Open, dot1x или PSK” что ведет к невозможности подключиться и плодит разгневанных пользователей

Замечание – если говорить про безопасность: ничего хорошего в transition modes нет (не было и не будет)

WPA3 как вершина эволюции механизмов безопасности Wi-Fi сетей

Причины появления WPA3

- “Комбинаторика механизмов безопасности” определяется количеством опций, доступных для подключения к беспроводным сетям
  - Анонсируемые IEs (2): WPA, WPA2
  - Наборы безопасности или AKM (18): PSK, SAE, 802.1x, Suite B, FT, FILS, и т.д. …
  - Шифры для юникаст трафика (6): WEP, TKIP, CCMP-128, CCMP-256, GCMP-128, GCMP-256
  - Шифры для широковещательного/мультикаст трафика (4): WEP, TKIP, CCMP, GCMP
  - Шифры проверки целостности (3): none, CMAC, GMAC
  - Алгоритмы хэширования (4): SHA-1, SHA-256, SHA384, SHA512
- Сюда также можно включить KDF для PMK и шифр TLS, используемый различными реализациями EAP аутентификации
- Не все из этих комбинаций «рабочие»:
  - Каждая возможная комбинация несет в себе вероятность ошибки, что приведет к невозможности устройства к сети и звонку в тех. поддержку
  - ТД/RADIUS сервер устанавливают политики безопасности, клиентское устройство выбирает из доступных вариантов

WPA3-Personal: Надежная аутентификация, основанная на «пароле»

- Устойчив к offline dictionary attacks; улучшенная защита пользователей от подбора «паролей»
- Защита даже при выборе пользователем слишком коротких и/или простых паролей
- Отсутствие изменений в процессе подключения (с точки зрения пользователя)
- Гарантирует «прямую секретность»; защищает трафик, даже если пароль будет позже взломан

WPA3-Enterprise: Безопасность корпоративного уровня для сетей с конфиденциальными данными

- 192-битная криптографическая стойкость для сетей, передающих конфиденциальную информацию
- 192-битный набор механизмов безопасности дает дополнительную защиту нуждающимся в ней сетям: например, правительственным или финансовым организациям
- Оптимальный выбор протоколов безопасности при подключении
- Лучшая надежность сети

Ключевые компоненты WPA3

- Замена WPA2-PSK новым алгоритмом WPA3-SAE (Simultaneous Authentication of Equals)
  - Защита от offline dictionary атак
- Suite B – просто, чем требование государства (США)
  - Добавление GCM и ECC для шифрования и SHA384 (более стойкий хэш)
  - Четкие правила касательно криптографической стойкости применяемых алгоритмов для минимизации ошибок в настройке
- Обязательна поддержка Protected Management Frames
- Прочие улучшения защищенности

Режимы WPA3

- WPA3-Personal
  - WPA3-SAE Mode
    - PMF Required
  - WPA3-SAE Transition Mode
    - Правила настройки: Если на ТД включен WPA2-PSK, режим WPA3-SAE Transition Mode должен быть включен по умолчанию. Тем не менее, администратор должен иметь возможность настроить WPA2-PSK Only Mode.
- WPA3-Enterprise Mode
  - PMF ***должен*** использоваться для соединений WPA3
- WPA3-Enterprise “192-bit” mode (CNSA)
  - Больше, чем соответствие требованиям правительства США
  - Проверенный набор криптографических стандартов для устранения ошибок в конфигурации
  - Добавление GCM & ECC для улучшения шифрования и хеширования (SHA384)
  - PMF Required

WPA3-Personal (aka WPA3-SAE)

You make customer experience **possible**

Требования к механизмам защиты, основанным на паролях

- **Устойчивость к Passive Attacks:** атакующий не должен иметь возможность получить любую информацию о самом пароле или результирующем shared secret путем пассивного прослушивания эфира.
- **Устойчивость к Active Attacks:** атакующий участвует в работе протокола, подменяя собой легитимного клиента.
- **Устойчивость к Dictionary attacks:** атакующий получает информацию путем прослушивания информационного обмена и пытается подобрать пароль путем перебора возможных вариантов из публикуемых сборников паролей.
- Взлом shared secret во время предыдущего запуска протокола не поможет атакующему во время следующего запуска протокола (атака Деннинга - Сакко).
- Взлом пароля не позволит атакующему получить shared secret во время более ранних запусков этого протокола (“прямая секретность”).

WPA3-Personal

Simultaneous Authentication of Equals (SAE)

- Основан на обмене ключами Dragonfly
- Balanced Password Authenticated Key Exchange (PAKE)
  - Общий пароль
  - Степень защиты SAE не связана со сложностью пароля
  - В результате SAE exchange генерируется 256-битный PMK
    - Защита от offline dictionary attacks
    - Прямая секретность гарантирует защиту трафика, даже если в будущем пароль будет взломан
- Требует Protected Management Frames
- WPA3-SAE Transition Mode поддерживает WPA2-PSK и WPA3-SAE на одном и том же SSID

SAE: комбинация OWE и «пароля»

g – функция пароля и MAC адресов.
Называется PWE (Password Element).

Параметры ECDH: **g**, p

Выбрать случайное **x**

Вычислить g^x

Отправить g^x

Отправить g^y

Выбрать случайное **y**

Вычислить g^y

Common Secret
s = $(g^y)^x = g^{xy}$

PMK = hash (**s**, lables)

«Невозможно»* вычислить s, зная g^x и g^y

Common Secret
s = $(g^x)^y = g^{xy}$

PMK = hash (**s**, lables)

Начало 4-Way handshake

* - на современном уровне развития компьютеров

Процесс подключения SAE

«Пароль» -> PWE ->P

Выбрать случайные r_A и m_A
$s_A = (r_A+m_A) \bmod q$
$E_A = -m_A*P$

Auth Commit [Group ID, s_A, E_A]
Auth Algo Number =3

Auth Commit [s_B, E_B]

Проверить s_B и E_B
$K = r_A*(s_B*P+E_B)$
$k = hash(K)$
$tr = (s_A, E_A, s_B, E_B)$
$c_A=HMAC(k, tr)$

Auth Confirm [c_A]

Auth Confirm [c_B]

Проверить c_B, если совпадает, то:
PMK=k

Assoc Request/Response [AKM 00-0F-AC:8]

EAPOL 4-way handshake

PTK = [KCK | KEK | TK]

CCMP с 128-битными ключами TK и GTK
BIP CMAC с 128-битным ключом IGTK
Остальные шифры опциональны

«Пароль» -> PWE
Выбрать случайные r_B и m_B
$s_B = (r_B+m_B) \bmod q$
$E_B = -m_B*P$

Обязательна поддержка Group 19

Проверить s_A и E_A
$K = r_B*(s_A*P+E_A)$
$k = hash(K)$
$tr = (s_B, E_B, s_A, E_A)$
$c_B=HMAC(k, tr)$

Проверить c_A, если совпадает, то:
PMK=k

PTK = [KCK | KEK | TK]

WPA3-Personal Transition Mode
Зачем вообще есть переходный режим для WPA2/WPA3?

Постойте – ТД, которая поддерживает WPA3, должна поддерживать Multiple BSS – на дворе 2019 год!

- Переходный режим был создан для сохранения совместимости с WPA2 и плавной миграции (с точки зрения пользователей сети).

- Что мы получим при использовании переходного режима:
  - ***Single BSS -Enabled by default when a WPA2-PSK BSS is enabled on a WPA3-Personal AP***
    - ***Одинаковый «пароль» для WPA2-PSK и WPA3-PSK***
    - ***WPA2-PSK уязвима к «классическим» атакам***

- Преимущества
  - Соединения WPA3-Personal безопасны – получив «пароль», атакующий может получить доступ к БЛВС, но не возможность расшифровывать трафик WPA3-PSK!

Замечание – если говорить про безопасность: ничего хорошего в transition modes нет (не было и не будет)

От KRACK к DragonBlood
Уязвимости WPA3-Personal (SAE)

- Тот же исследователь нашел 5 уязвимостей протокола SAE, используемого как часть WPA3-Personal (Simultaneous Authentication of Equals, определен в IEEE 802.11-2016)

- Данные уязвимости позволяют злоумышленнику провести:
  - Атаки на STA
    - Переключить клиентов с WPA3-Personal на WPA2-Personal в transition режиме BSS
    - Понизить Diffie-Hellman группы, используемые в SAE
    - ECC и MODP side-channel timing атаки
  - Атаки на ТД
    - DoS путем переполнения вычислительных возможностей ТД поддельными запросами на аутентификацию

WPA3-Enterprise

В чем разница?

- WPA2 vs WPA3 Enterprise
  - Все подключения WPA3 должны использовать PMF
- Это значит, что если WPA2 Client использует PMF, это подключение можно рассматривать как WPA3 Enterprise (MFPC)
- Однако, чтобы получить WPA3 Enterprise Only сеть, настройка Management Frame Protection должна быть установлена в Required (MFPR)

WPA3™-Enterprise

- Использование, как минимум, 192-битных алгоритмов защиты:
  - 802.1x TLS, 4-way handshake, pairwise/group/BIP шифры
- N-битовая защита означает, что для brute-force атаки потребуется перебрать 2^N значений

Размер ключа AES	Пространство ключей	Порядок величины
128 бит	2^{128}	Количество капель воды в мировом океане ~2^{85}
192 бита	2^{192}	Количество атомов в Солнце ~2^{188}
256 бит	2^{256}	Количество атомов в известной Вселенной ~2^{257}

- Для несимметричной криптографии длина приватного ключа должна быть 2 * N

Квантовые компьютеры….

Security

40

Let's harden Internet crypto so quantum computers can't crack it

Draft blends asymmetric public/private key encryption and one-time pad analogs

By Richard Chirgwin 18 Jul 2017 at 23:59 SHARE ▼

Security

The quantum clock is ticking on encryption – and your data is under threat

Quantum computers pose a major threat to the security of our data. So what can be done to keep it safe?

WHERE THERE'S A WILL

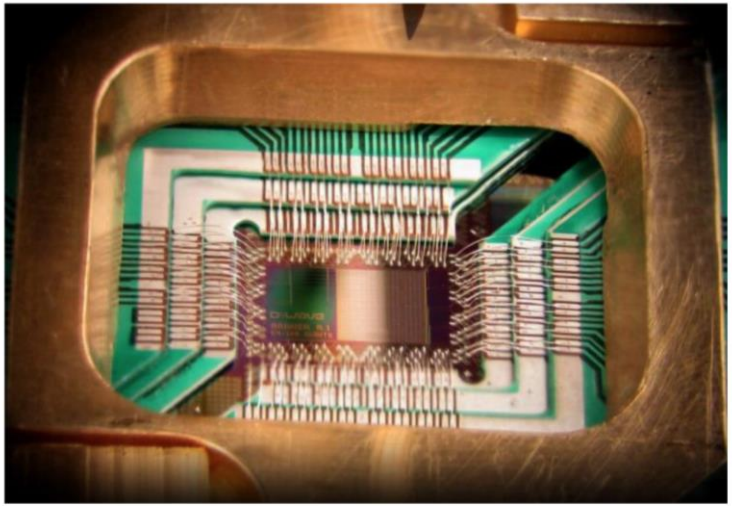
Quantum computing could make the encryption behind every internet transaction obsolete—someday

NSA preps quantum-resistant algorithms to head off crypto-apocalypse

Quantum computing threatens crypto as we know it. The NSA is taking notice.

by **Dan Goodin** - Aug 21, 2015 7:02am EDT

Share Tweet Email 90



Enlarge / A chip manufactured by D-Wave Systems that has some quantum properties.

D-Wave Systems

Почему это важно?

- Квантовые вычисления – новая парадигма:
  - Вместо битов – кубиты
  - Кубит может находится в состояниях «0» и «1» одновременно
  - Алгоритм Шора для разложения числа на множители => задача дискретного логарифмирования

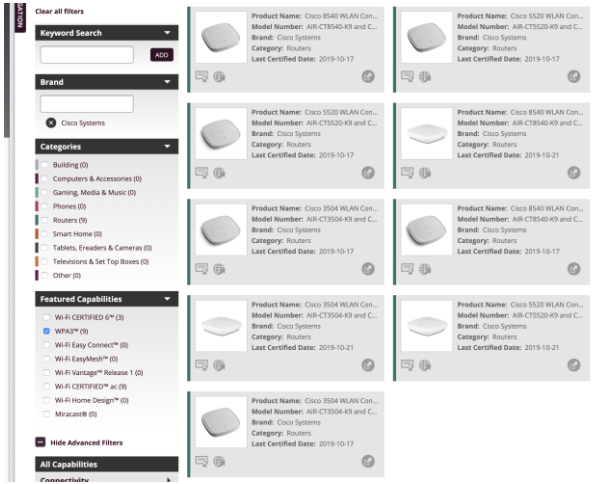
- Квантовые компьютеры способны быстро решать задачу дискретного логарифмирования = > Диффи-Хелман становится уязвимым. Т.е. WPA3-Enterprise уязвим для атак с применением квантовых компьютеров!

- Симметричные шифры (AES256, SHA384) останутся неуязвимыми (на горизонте 10-ти лет)

Взаимосвязь WPA3 и Wi-Fi 6 (11ax)

- Согласно текущим планам Wi-Fi Альянса WPA3 станет обязательным для всех Wi-Fi CERTIFIED устройств в течение двух лет после запуска программы
  - Программа запущена в апреле 2018 – станет обязательной в июне 2020
- Текущие планы по Wi-Fi 6
  - WPA3-Personal поддержка обязательна
  - WPA3-Enterprise поддержка опциональна
  - Enhanced Open поддержка опциональна
- Любое Wi-Fi устройство после июня 2020, независимо от поддерживаемого стандарта (11n/ac/ax) для получения сертификата должно будет поддерживать WPA3

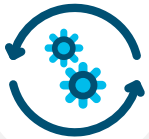
- Когда появятся Wi-Fi Certified WPA3 и Wi-Fi Certified Enhanced Open продукты?
- ***Они уже есть!!!!***



Надежно

Обновление ПО с минимальным влиянием на сеть

Управление ПО контроллера и точек доступа



Обновление контроллера

Новое ПО или исправления ошибок

SMU ★

PSIRT, Исправления ПО ТД

Обновление ПО ТД или исправление ошибок

AP Service pack ★

Поддержка новых моделей ТД

Установка патча «на лету»

AP Device pack ★

Без смены ветки ПО

Исправление ошибок или уязвимостей без необходимости тестировать новый релиз

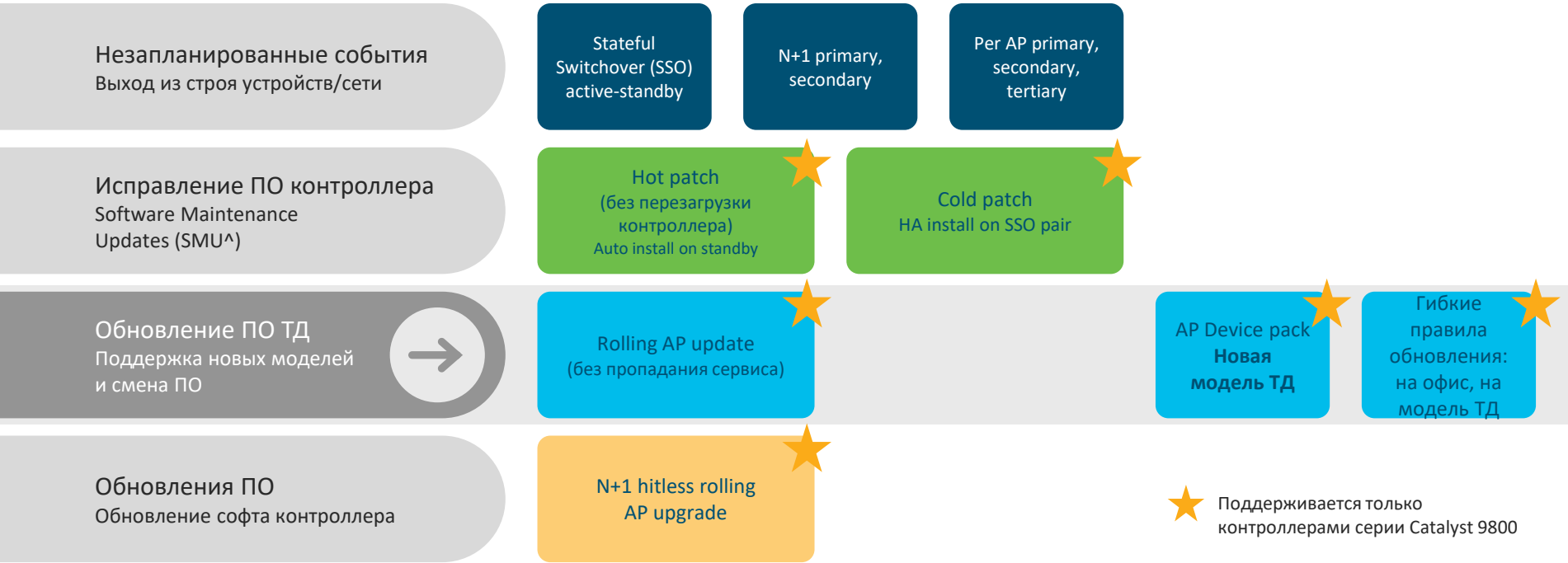
Быстрый выход из критических ситуаций

★ SMU только для MD релизов

Rolling AP update/upgrade infrastructure

High Availability (HA)

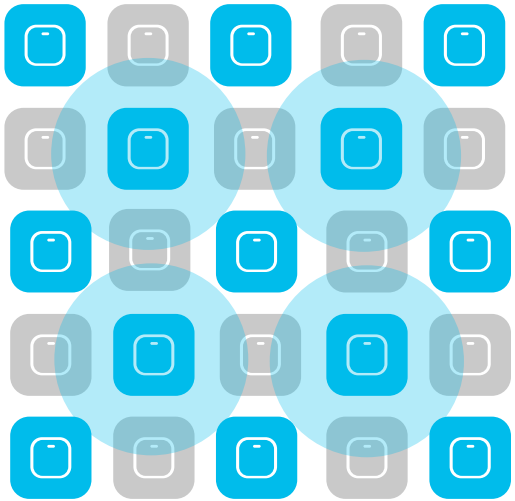
уменьшение времени простоя при авариях и обслуживании сети



★ Поддерживается только контроллерами серии Catalyst 9800

^ Только для MD Релизов

Rolling AP upgrade – использует RRM для поиска обновляемых за один шаг точек доступа



Пользователь выбирает долю ТД, которые будут обновлены за шаг алгоритма [5%, 15%, 25%]

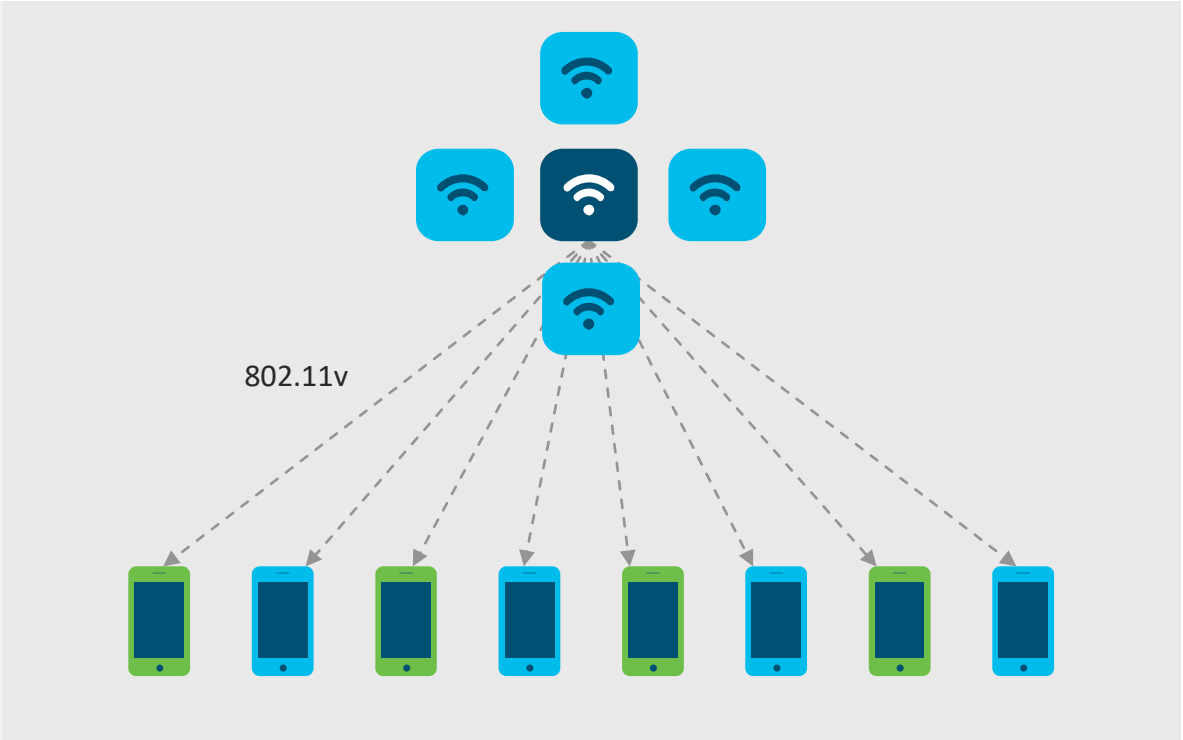
Для 25%, число «неприкасаемых» соседей = 6 [примерное число итераций~ 5]

Для 15%, число «неприкасаемых» соседей = 12 [примерное число итераций~ 12]

Для 5%, число «неприкасаемых» соседей = 24 [примерное число итераций~ 22]

Rolling AP upgrade – работа с клиентами

- Цель: перевести клиентские устройства с перегружаемой ТД на соседнюю
- 802.11v BSS transition request
- Disassociation Imminent
- Если клиенты «слов не понимают», перед перезагрузкой ТД их деаутентифицирует



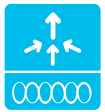
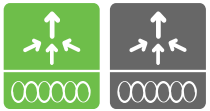
А теперь ISSU!

Обновление ПО БЛВС без простоя!

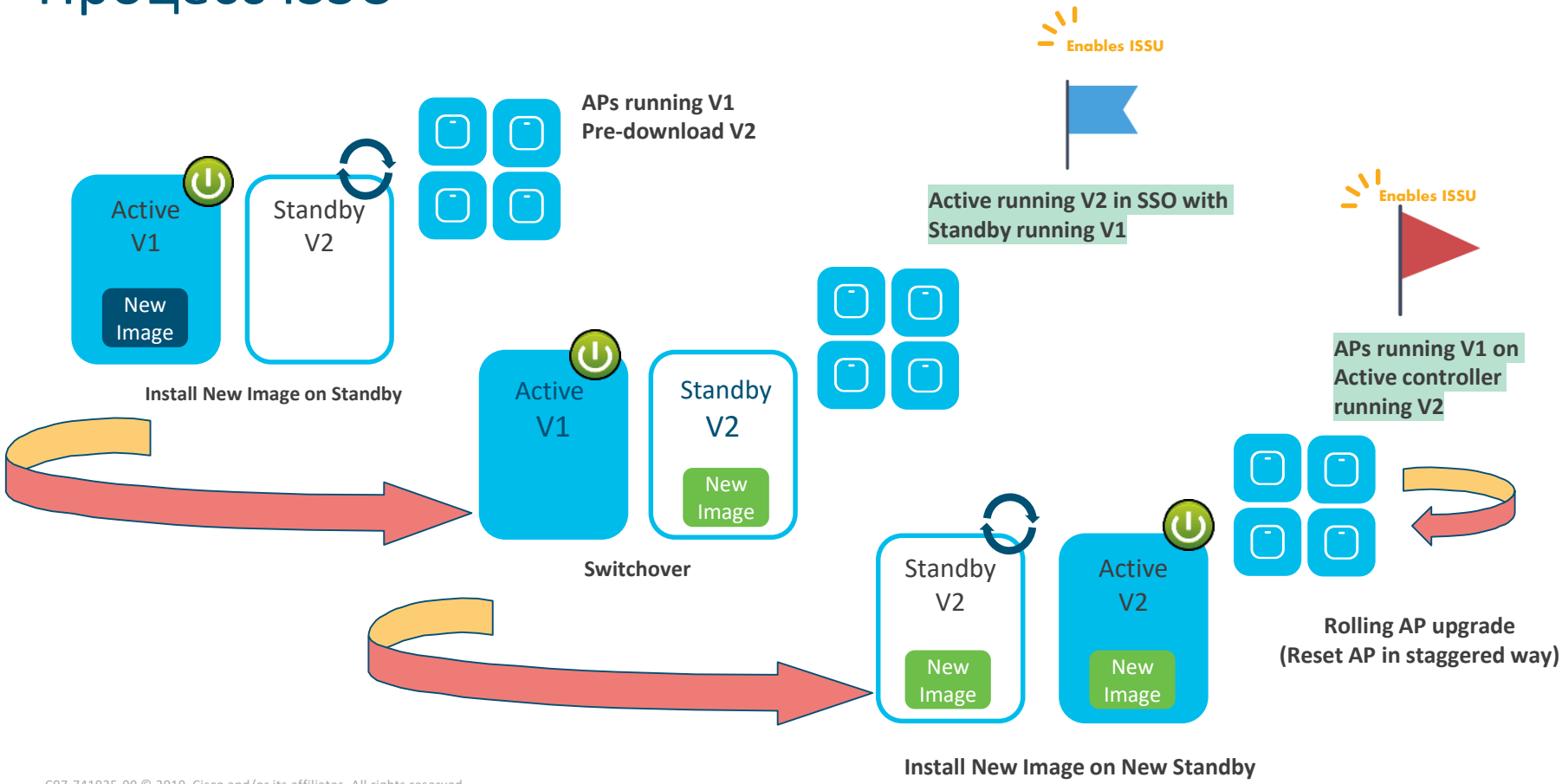
“те, кто этого так долго ждал”

Как долго моя сеть будет недоступна?

Отличительная особенность Catalyst 9800

	Controller Fault	Controller and AP s/w update	Image Upgrade
Standalone 	10s of minutes for AP and client recovery	Zero-downtime with SMU and APSP	Tens of minutes for AP and client recovery
N+1 HA 	Noticeable Outage to clients and APs	Zero-downtime with SMU and APSP	• No Outage to APs and Client • Automated Orchestration • from Cisco DNA Center
SSO Pair 	Sub-second AP and client recovery	Zero-downtime with SMU and APSP	• In Service Software Upgrade (ISSU)! • Automated from device and Cisco DNA Center (future)

Процесс ISSU



Семейство точек доступа

Новые модели серии Cisco Catalyst 9100

Новые ТД Cisco Catalyst 9100

Начальный уровень

9115AX

- 4x4 + 4x4
- MU-MIMO, OFDMA
- Spectrum Intelligence
- 1 x 2.5 mGig
- TWT

Критически важная сеть

На борту Cisco RF ASIC

9120AX

- 4x4 + 4x4
- Cisco RF ASIC
- Dual 5GHz, HDX
- RF signature capture
- IoT ready (Zigbee, Thread)
- Application Hosting
- 1 x 2.5 mGig
- TWT

Лучшая в своем классе

9130AX

- 8x8 + 4x4 или 4x4 + 4x4 + 4x4
- Три радио (Dual 5GHz + 2.4GHz), HDX
- Cisco RF ASIC
- RF Layer 1 detail, Application Hosting
- Decrypted data packet iCAP
- IoT ready (Zigbee, Thread)
- Первая на рынке 8x8 ТД с внешними антеннами
- 8-ми портовые Smart антенны
- 1 x 5 mGig

Cisco DNA Assurance с iCAP	Bluetooth 5	USB	Интегрированные или внешние антенны

Отличительные особенности радиоподсистемы Cisco

Точки доступа Cisco Catalyst 9120AX и 9130AX

Богатая история инноваций в БЛВС

1999 — Autonomous access

2011 — Cisco CleanAir®: Interference detection and mitigation

2014 — Application visibility and control

2016 — Flexible Radio Assignment (FRA) (dual 5 GHz)

2018 — Intelligent capture and real-time telemetry

2019 — Что теперь?

Cisco Next-Generation Wireless Stack

Controller and coordinated Access Points

Connected mobile experiences

Hyperlocation

Software-defined access

802.11b/g **802.11n**

Aironet® 3500 Series

Aironet 3600 Series

802.11ac Wave 1

Aironet 3700 Series

802.11ac Wave 2

Aironet 3800 Series

Aironet 4800

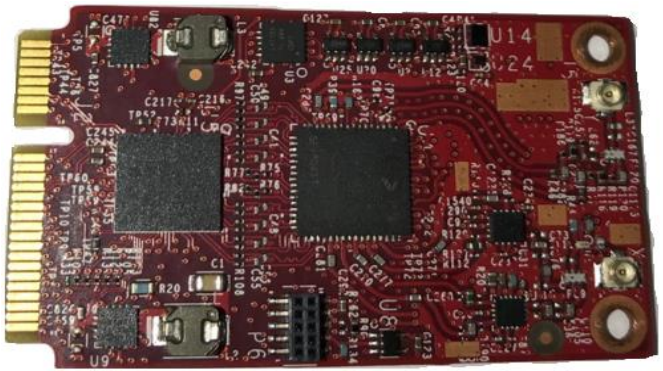
Почему Cisco RF ASIC?
Необходимость выйти за границы стандартного

Cisco RF ASIC

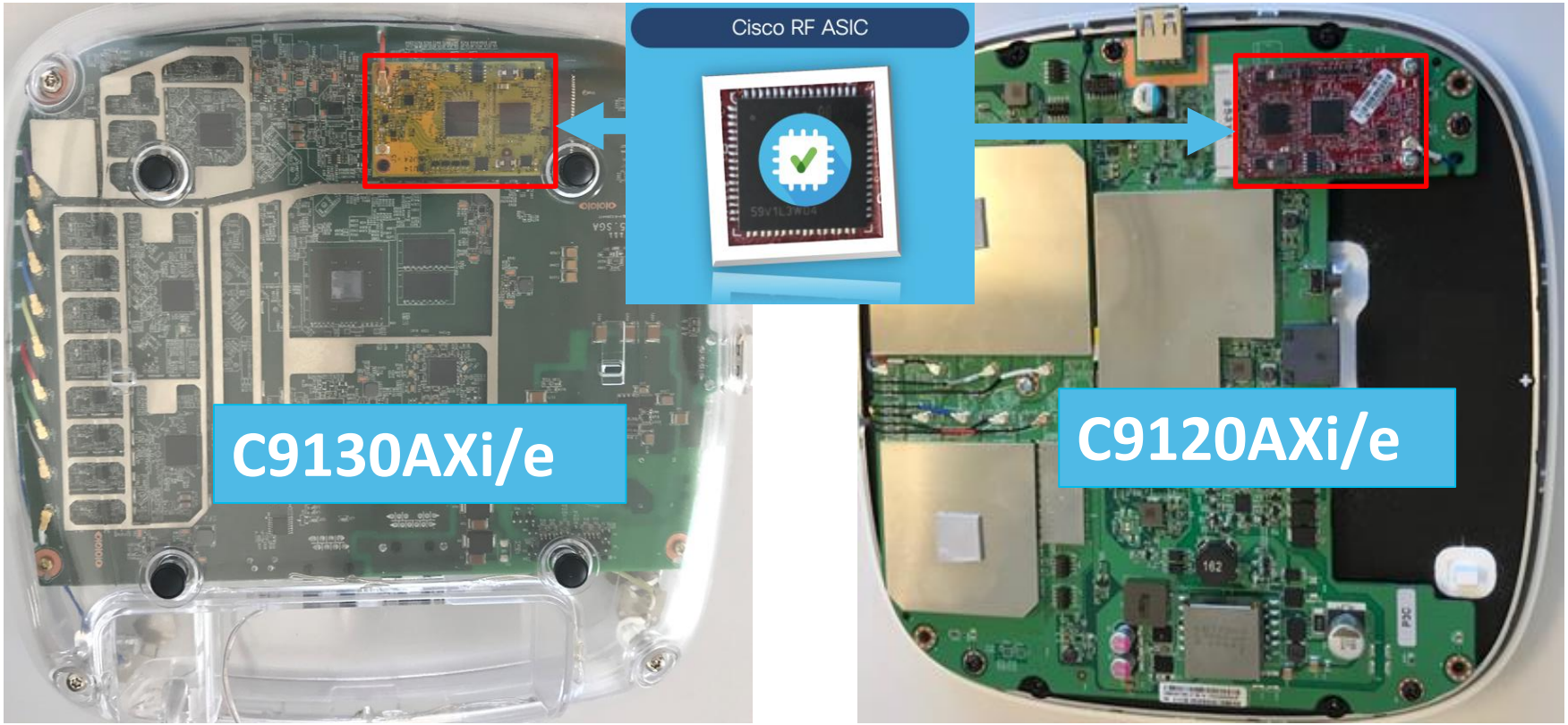
Cisco RF ASIC

- Cisco Custom RF ASIC
- 3 независимых RF подсистемы
  - 1x Dual Band 1x2 MIMO TRX
  - 1x Dual Band Observation Receiver RO1
  - 1x High Band Observation Receiver RO2
- Secret Sauce (SaGE) and a VSPA (Vector Signal Processing Accelerator)
- Custom AGC/Discreet Oscillators added for Cisco purposes (DFS/CleanAir) during design

cisco Technology

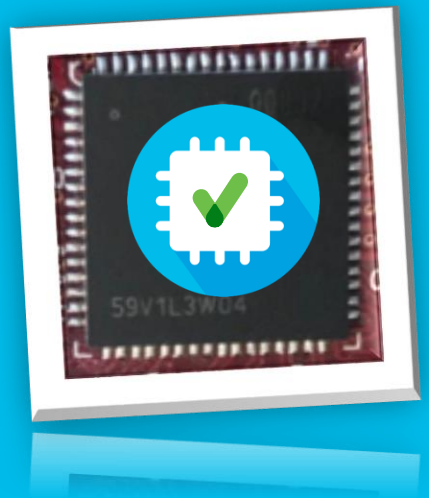


Разработанный Cisco чипсет
Анализ эфира в реальном масштабе времени



Точки доступа Catalyst 9120 и 9130 обладают встроенным Cisco RF ASIC

Cisco RF ASIC



- Offchannel RRM
- Clean Air
- Zero-Wait DFS* (NEW)
- Dual Filter DFS
- Fastlocate w/o performance impact
- WIDS/ Rogue Detection
- aWIPS*
- RF Layer1 details* (NEW)

*Roadmap

Контроллеры БЛВС серии Catalyst 9800

Новые контроллеры серии Cisco Catalyst 9800

Управляются IOS XE

Открытые и программируемые
Доверенные платформы
Модульная ОС

Всегда в работе

- Обновление ПО без перерывов в работе
- Последовательные обновления ТД
- Легкое добавление поддержки будущих моделей ТД

Безопасно

- Детектирование угроз в зашифрованном трафике ETA
- Автоматизированная макро/микро сегментация в режиме SDA
- Поддержка WPA3

Множество вариантов внедрения

- Отдельное устройство, виртуальный, встроенный в коммутатор, публичное облако
- Растет вместе с вами

Используйте так, как нужно вам!

Catalyst 9800-SW*
200 ТД, 4K клиентов

ENCS
KVM vmware ESXi

Catalyst 9800-CL+
1000 ТД, 10K клиентов

aws
KVM vmware ESXi

Catalyst 9800-CL
3000 ТД, 32K клиентов

KVM vmware ESXi

Catalyst 9800-CL
6000 ТД, 64K клиентов

250 ТД | 1000 ТД | 2000 ТД | 3000 ТД | 6000 ТД

Catalyst 9800-L
250 ТД, 5K клиентов, 5Гбит/с

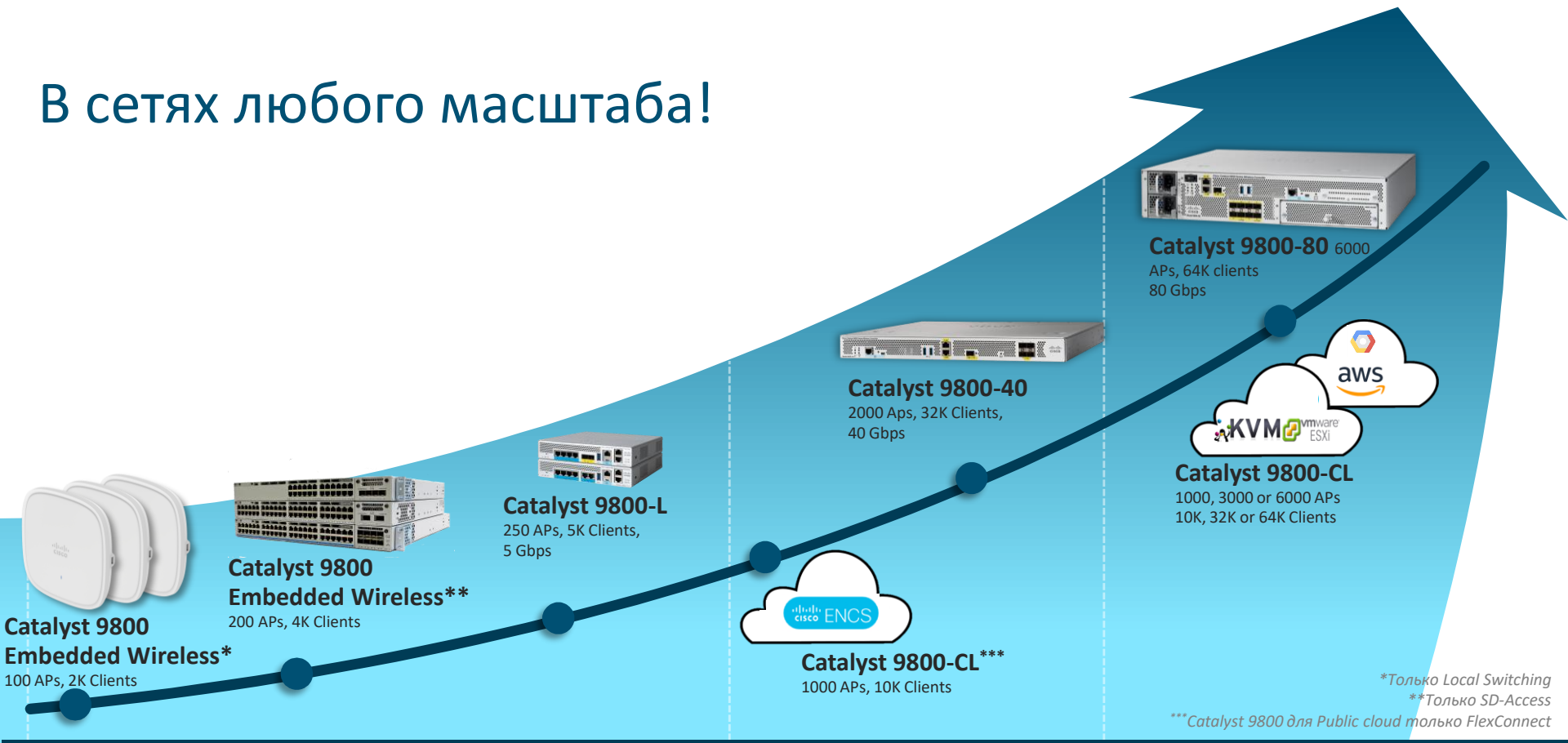
Catalyst 9800-40
2000 ТД, 32K клиентов, 40Гбит/с

Catalyst 9800-80
6000 ТД, 64K клиентов, 80Гбит/с

Аппаратный| Виртуальный (частный/публичный)| Встроен в коммутатор

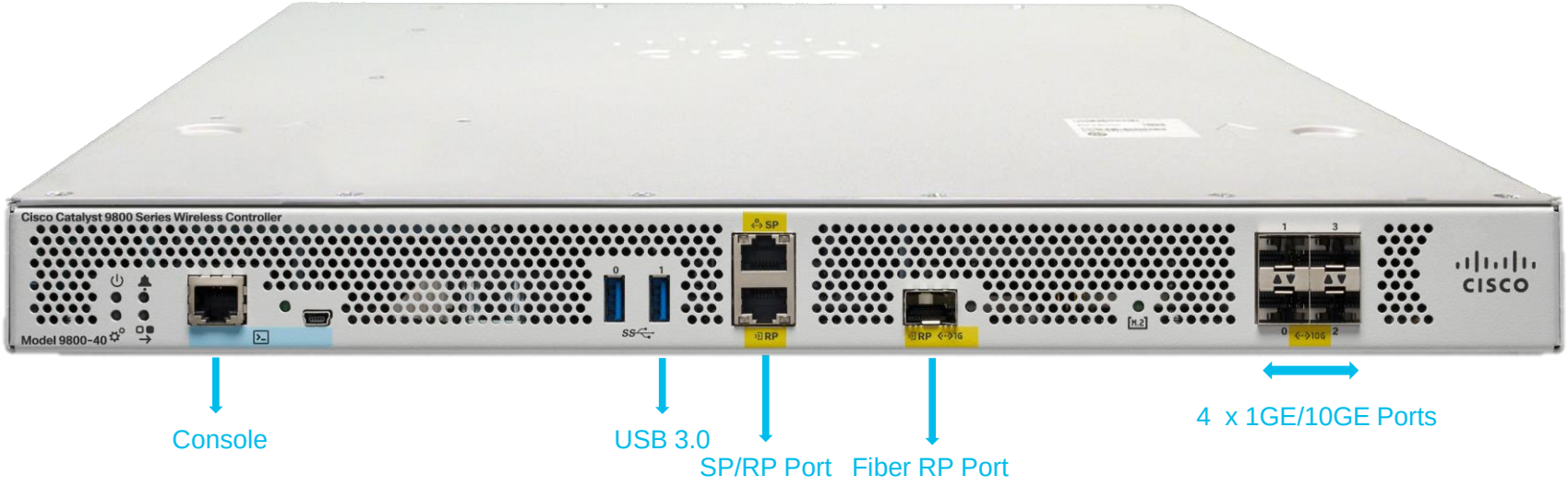
*SD-Access only

В сетях любого масштаба!



C9800-40: первый в индустрии фиксированный контроллер БЛВС с возможностью обновления без перерыва сервиса

До 2,000 ТД	До 32,000 клиентов	40Гбит/с



Программируемый многоядерный сетевой процессор

Поддержка Netflow, AVC и ETA

C9800-80: первый в индустрии модульный контроллер БЛВС с 100Гбит/с аплинком и возможностью обновления без перерыва сервиса

До 6,000 ТД	До 64,000 Клиентов	80 Гбит/с

Redundant Power Supply AC or DC	SP/RP Port Fiber RP Port	USB 3.0	8 X 10 GE Uplinks	Модульный аплинк - GE, 10GE, 40GE, 100GE

Программируемый многоядерный сетевой процессор	Поддержка Netflow, AVC и ETA

Виртуальный Catalyst 9800

Catalyst 9800 для частного облака

Масштабируется до 6,000 ТД и 64,000 клиентов

Centralize, FlexConnect, Fabric

Открытый и программируемый

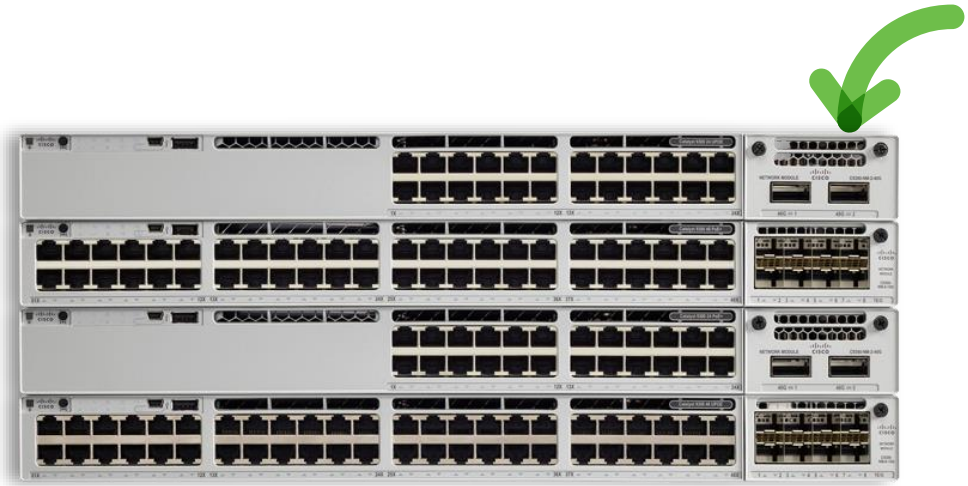
Catalyst 9800 для публичного облака

Масштабируется до 1,000 ТД и 10,000 клиентов

FlexConnect Local Switching

Открытый и программируемый

Встроенный контроллер Catalyst 9800 в коммутатор Cat 9k



Install Catalyst 9800 embedded wireless on your existing branch infrastructure

SD-Access

Оптимизирован для SDA with an always-on Fabric

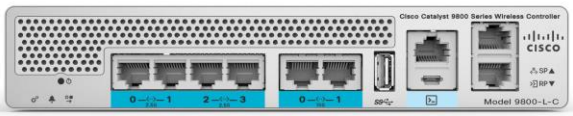
Catalyst 9300

Supported on Catalyst 9300 Series switches

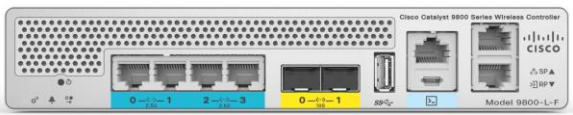
До 4,000 Клиентов

и 200 точек доступа

Cisco Catalyst 9800-L



COPPER



SFP

Размеры: 4см x 21.6см x 23см
Вес: 1.81 kg

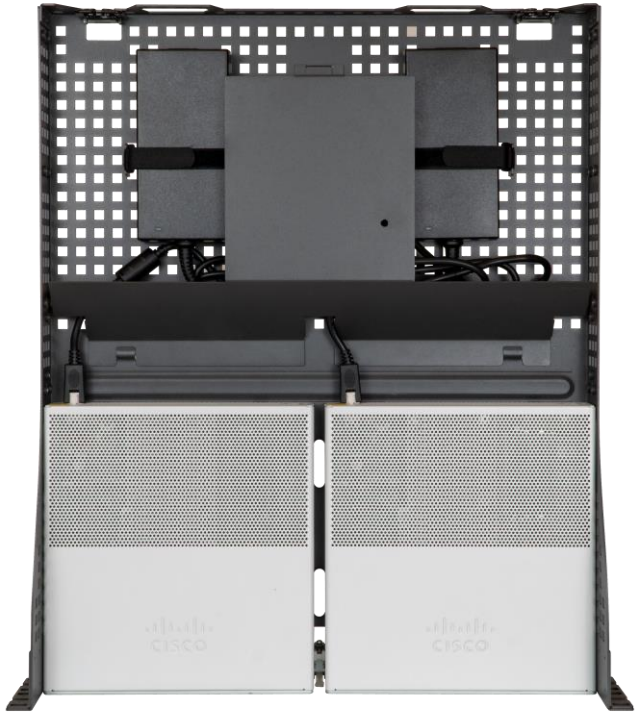
Высота	1RU
Пропускная способность	5Гбит/с
Число ТД	250
Число клиентов	5000
Порты	2x 10G/mGig Copper or 2x 10G/1G Fiber, 4x2.5G/1G Copper
Console port	RJ45+miniB USB Console port
USB port	Один USB3.0
Раб. температура	0-40˚C
Потребляемая мощность	79.3W
Шум	42.9dBA

Замечание: прямое подключение ТД не поддерживается

Компактный (1 RU) | mGig | Выделенные RP/SP порты | HA SSO | монтаж в стойку

Монтаж C9800-L в стойку

Позволяет смонтировать 2 контроллера в 1RU. Не требует инструментов (кроме как для крепления самого кронштейна в стойку)




CISCO

Бесплатно*

DNA Center Appliance при заказе $300K+ (GPL)

Любых подписок DNA **

+

два бесплатных

акселератора DNA

и две бесплатных

сессии Ask the Expert

Другие промо Cisco: cs.co/enpromotions

* Add “FREE-DNAC-OFFER” SKU to quote; Solution Support mandatory, see following instructions
** Excludes SD-WAN Cloud-based DNA Subscriptions
***Limit one free DNA Center Appliance per order.

Globally available and valid until end of 1H of FY2019
Questions? dna-offers-pm@cisco.com

GSX

Купите одну, получите вторую бесплатно

Точки доступа Cisco Aironet 1800

Преимущества

Не нужно выбирать между выгодной ценой и высокой производительностью. С промо-акцией 2=1 Вы получите и то и другое.

Точки доступа Cisco Aironet отличаются высокой надежностью, безопасностью, производительностью, простотой развертывания и управления, благодаря функционалу Mobility Express.

2=1

Две по цене одной

Стать обладателем лучшего Wi-Fi бизнес-класса стало проще. Купите одну точку доступа Cisco Aironet* с поддержкой стандарта 802.11ac Wave 2 и получите вторую бесплатно.

1815i **1852i/E**

*Акция применима только к точкам доступа, указанным в подробностях акции.

Подробности акции

- Модели точек доступа, участвующие в промо-акции: Cisco Aironet 1815i, 1852i/E
- Промо-акция распространяется только на текущие и будущие заказы.
- Правила и условия: пожалуйста, свяжитесь с партнером компании Cisco для получения дополнительной информации.
- **Данная акция является глобальной. Сроки акции и количество оборудования ограничены.**

C96-742867-00 09/19