Cisco Expo 2012

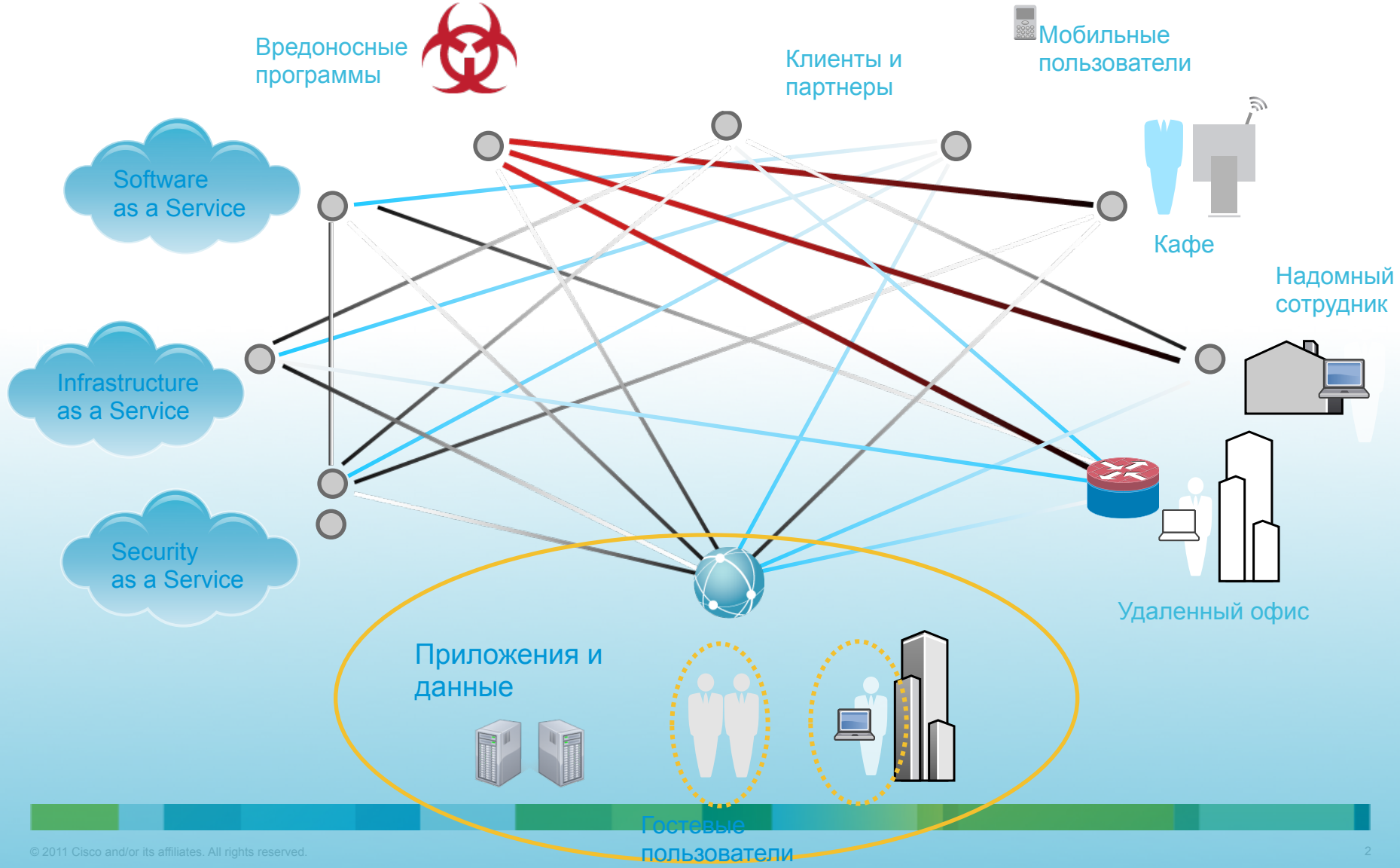
Архитектура беспроводных сетей Cisco и безопасность беспроводного эфира

Юрий Довгань
Системный инженер

ydovgan@cisco.com

© 2011 Cisco and/or its affiliates. All rights reserved.

Сети без границ
Мировые тенденции



© 2011 Cisco and/or its affiliates. All rights reserved.

Содержание

1 Централизированная архитектура Cisco Unified Wireless

2 Управление радиосредой и роуминг

3 Расширение беспроводной сети до удаленных офисов

4 Инновационные технологии – CleanAir, Client-link, VideoStream

5 Безопасность беспроводного эфира

Приз за знания

Принимайте активное участие в Cisco Expo и получите в подарок Linksys E900.

Как получить подарок:

- внимательно слушать лекции по технологиям Cisco
- посещать демонстрации, включенные в основную программу
- пройти тесты на проверку знаний

Тесты будут открыты:

с 15:00 25 октября по 16:30 26 октября

www.ceq.com.ua

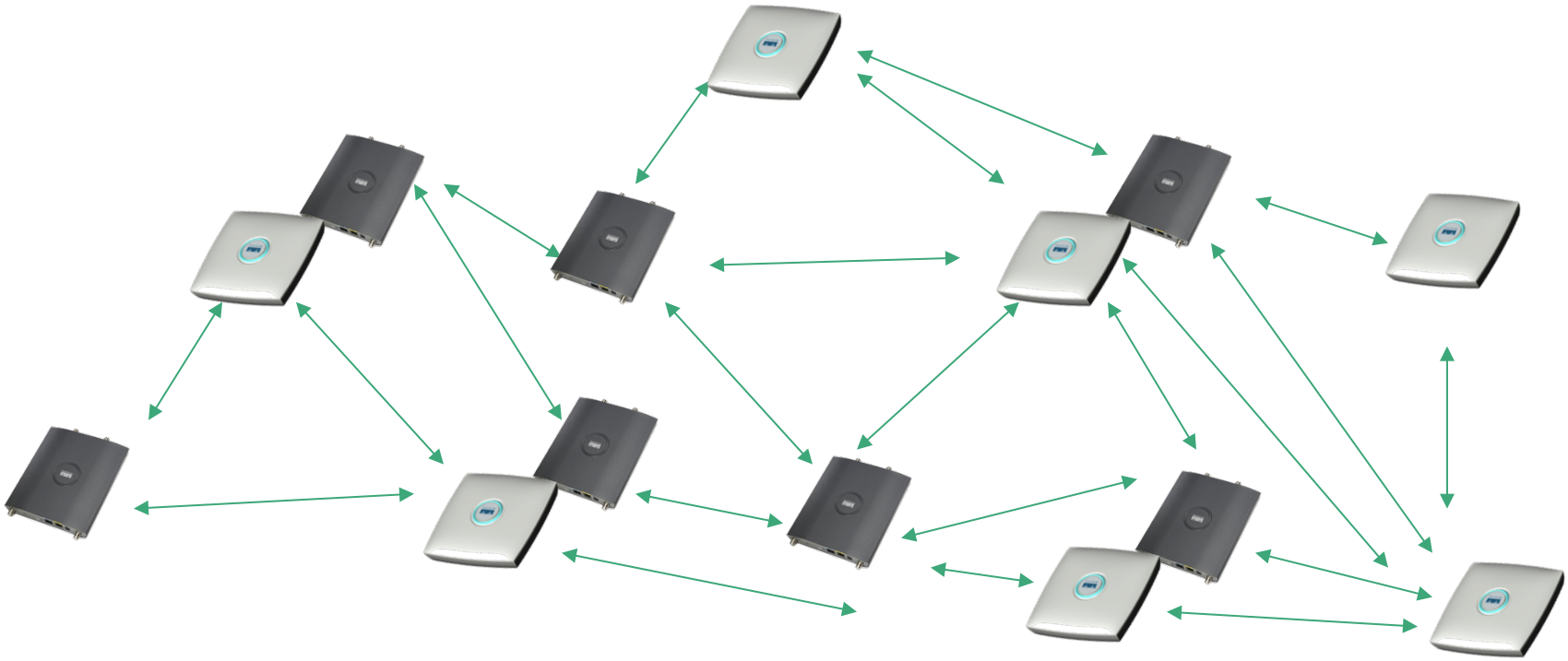
© 2011 Cisco and/or its affiliates. All rights reserved.

Архитектура Cisco Unified Wireless Network

© 2011 Cisco and/or its affiliates. All rights reserved.

Автономные внедрения - недостатки

- Каждая беспроводная точка доступа видит сеть по-своему
- Нет иерархического представления радиосреды
- Нет средств оптимизации радиопокрытия
- Настройка каждой беспроводной точки по отдельности



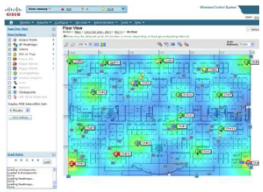
© 2011 Cisco and/or its affiliates. All rights reserved.

Архитектура Cisco Unified Wireless Network

© 2011 Cisco and/or its affiliates. All rights reserved.

Единый интегрированный беспроводной комплекс

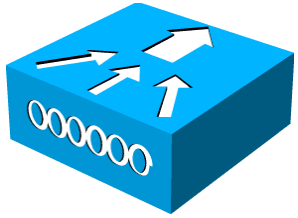
Capacity Management



RF Management

Security Management

Wireless Control System



Cisco WLC

Mobility Services:

- Context-Aware
- Wireless Security
- Secure Client Manager
- Mobile Intelligent Roaming

Сервис беспроводного доступа

Аутентификация пользователей

Шифрование данных

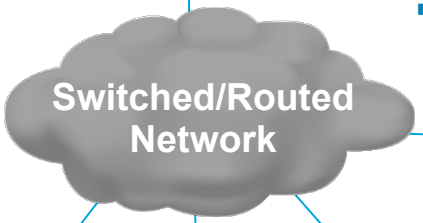
Управление плотностью подключений

Прозрачный роуминг

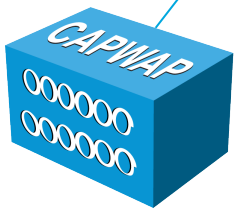
Управление радиосредой

Определение местоположения

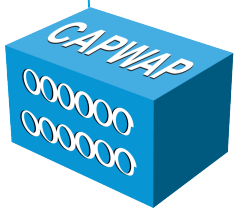
Централизированное управление



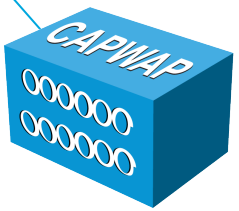
MSE



Sniffer Mode



Local AP Mode



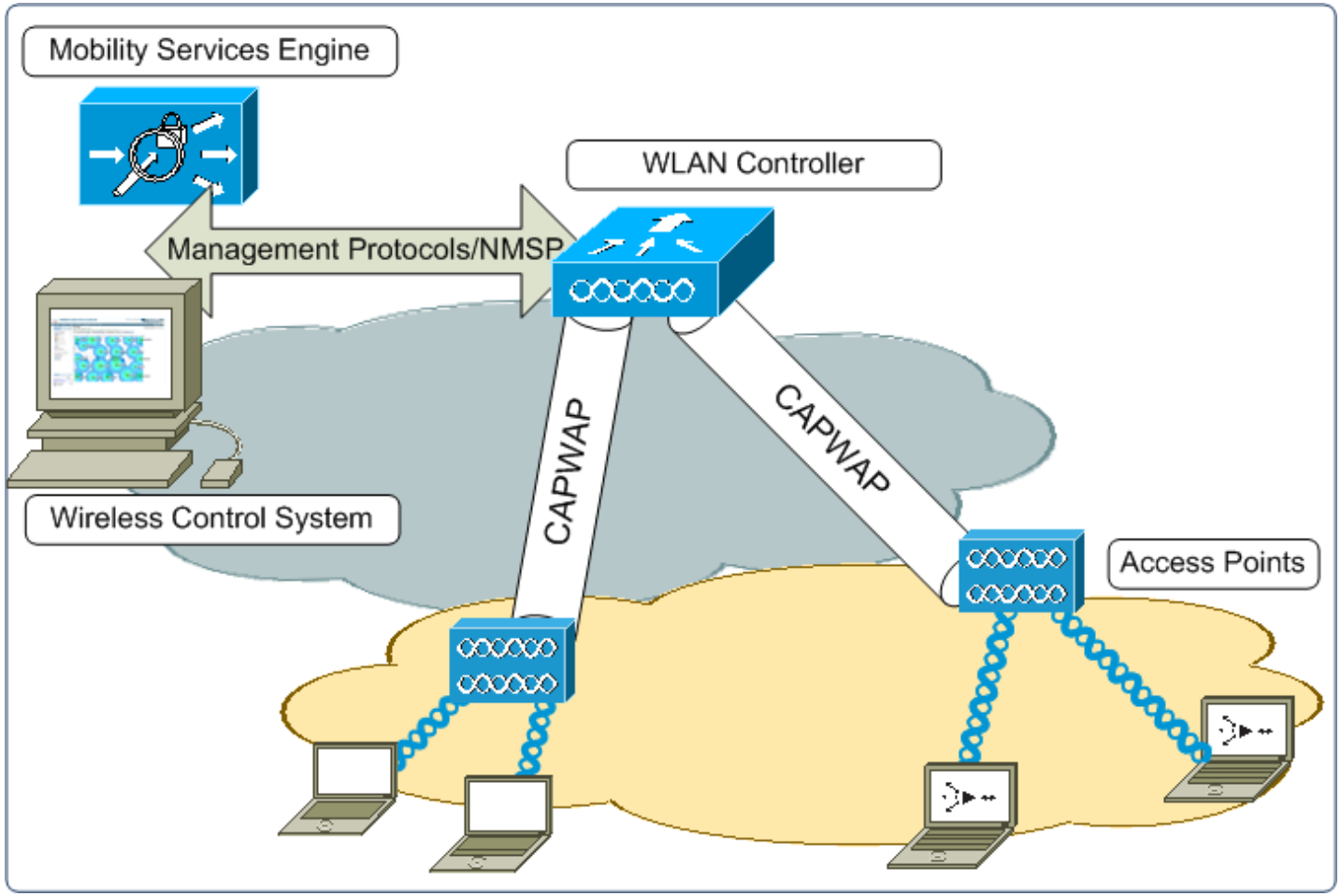
Rogue Detector

Cisco Wireless APs

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Unified Wireless Network

Архитектура



© 2011 Cisco and/or its affiliates. All rights reserved.

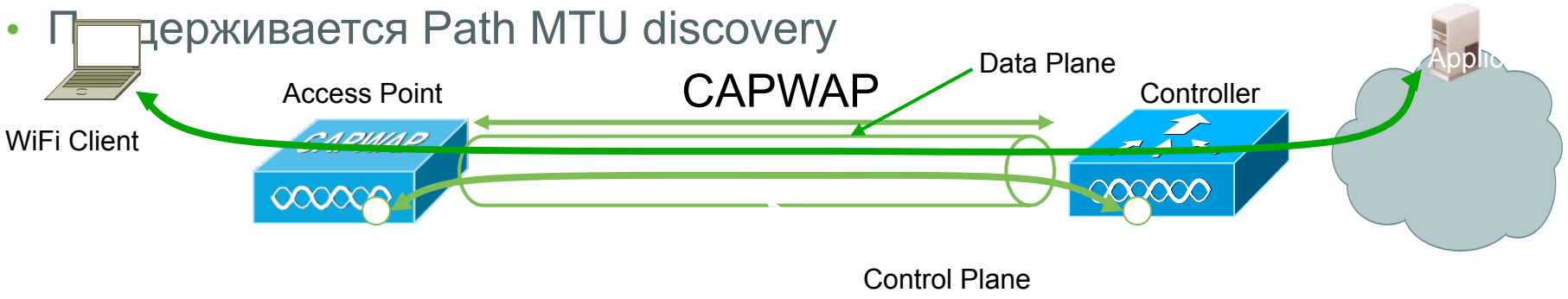
Преимущества централизированной архитектуры

- Централизированное управление беспроводными точками доступа и пользователями
- Динамическая балансировка между пользователями
- Динамическое управление радиопокрытием
- Сервисы определения местоположения
- Расширенный арсенал безопасности и QoS
- Прозрачный роуминг
- Возможность внедрения Voice over WLAN
- Унификация проводного и беспроводного доступа

© 2011 Cisco and/or its affiliates. All rights reserved.

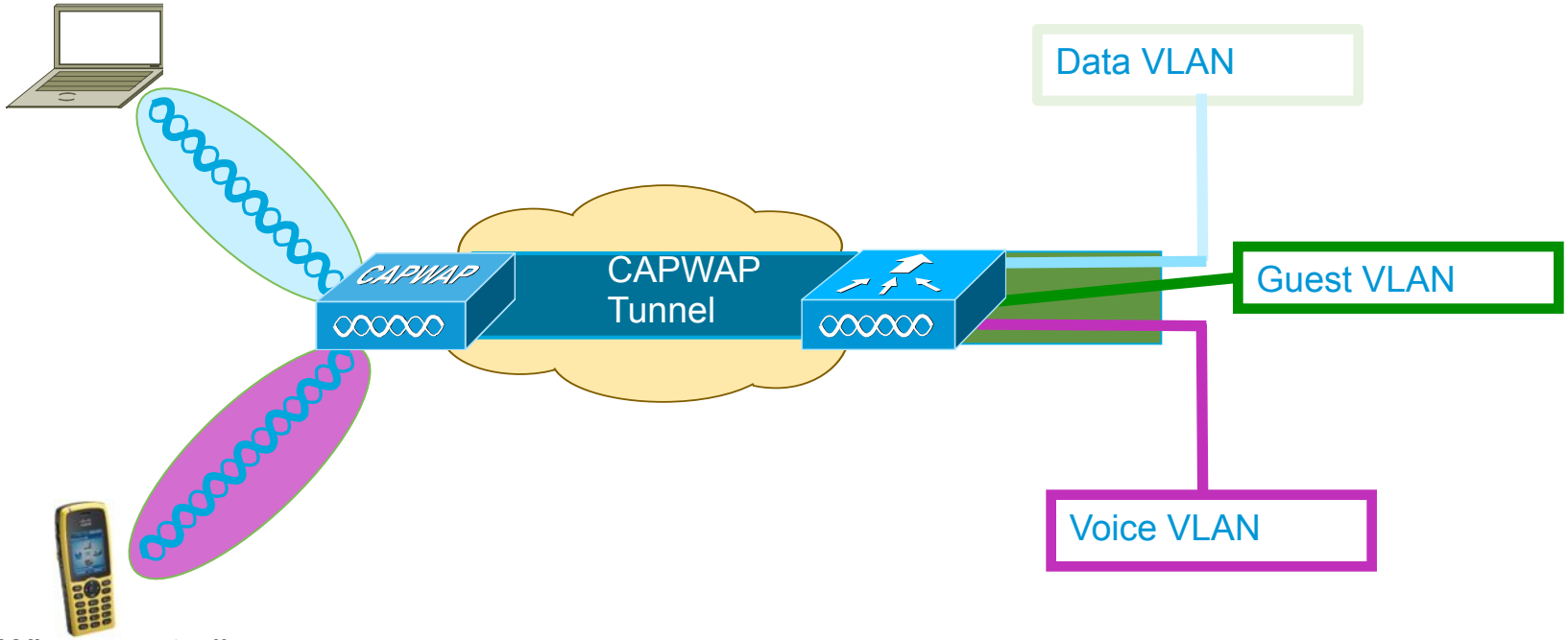
Централизированная архитектура WLAN
Что такое CAPWAP?

- CAPWAP - Control And Provisioning of Wireless Access Points, протокол, который используется между точками доступа и контроллером.
- CAPWAP передает контрольный трафик и трафик данных между ними двумя
  - Контрольный трафик шифруется с помощью DTLS
  - Трафик данных шифруется с помощью DTLS (Опционально)
- CAPWAP поддерживает только Layer-3 mode внедрения
- Поддерживается Path MTU discovery



© 2011 Cisco and/or its affiliates. All rights reserved.

Беспроводные контроллеры как сетевые устройства



- WLAN controller

  Для беспроводных клиентов контроллер является 802.1Q бриджем, который принимает трафик и помещает его в нужный VLAN

  Со стороны точки доступа, контроллер является концом LWAPP или CAPWAP туннеля с IP адресом

  С точки зрения сети, это layer-2 устройство, подключенное через один или несколько 802.1Q транковых интерфейсов

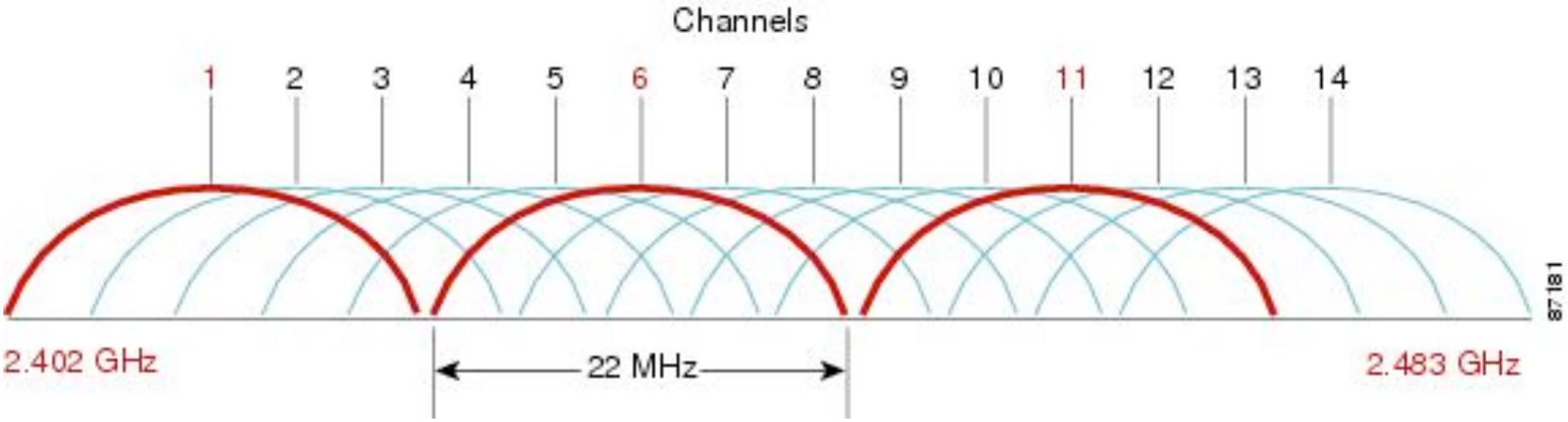
- Точка доступа подключается к порту – концепция VLAN'ов на точке доступа не рассматривается.

© 2011 Cisco and/or its affiliates. All rights reserved.

Управление радиосредой

© 2011 Cisco and/or its affiliates. All rights reserved.

802.11 DSS Распределение каналов



© 2011 Cisco and/or its affiliates. All rights reserved.

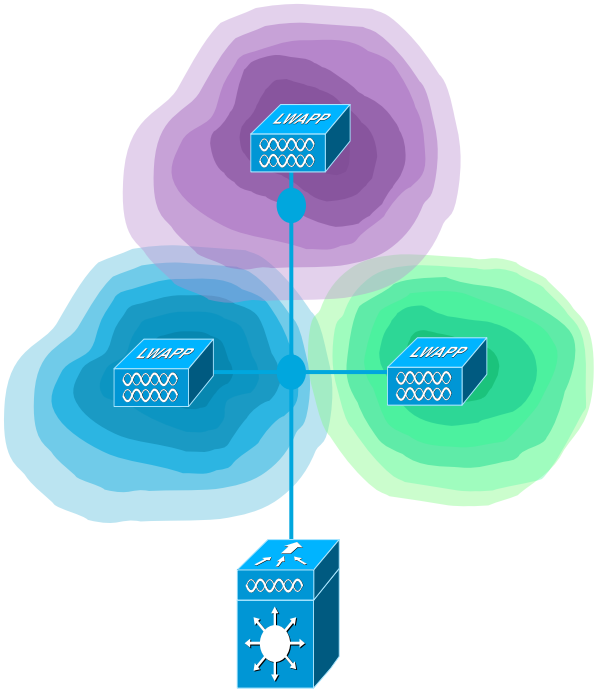
RRM—Radio Resource Management

- Какие цели RRM?
  - Динамически балансировать покрытие и избегать изменений
  - Мониторить и поддерживать покрытие для всех клиентов
  - Управлять эффективностью спектра так, чтобы предоставить оптимальную полосу пропускания при изменении условий
- Что не делает RRM
  - Не является заменой радиообследованию
  - Не исправляет неправильную архитектуру сети
  - Не производит спектр

© 2011 Cisco and/or its affiliates. All rights reserved.

Как RRM это делает?

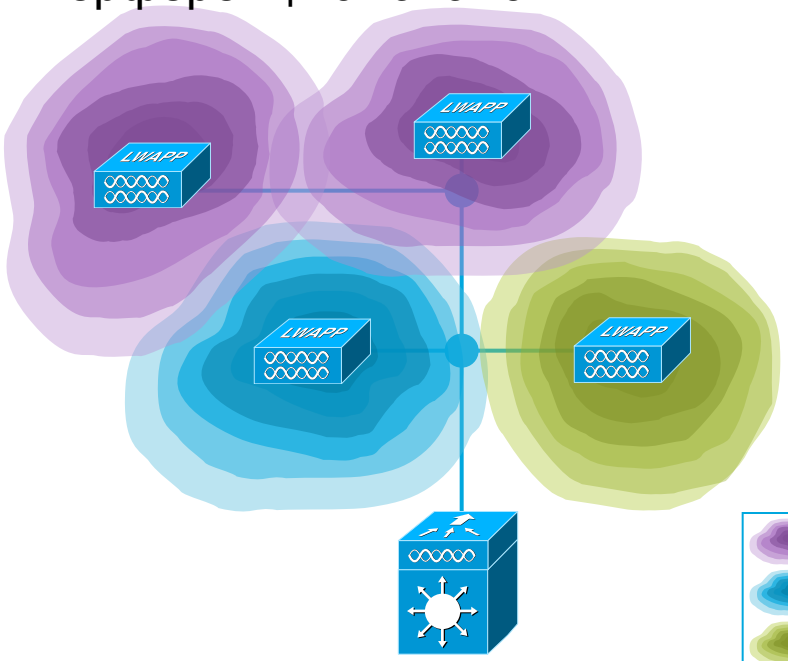
- **DCA**—Dynamic Channel Assignment
  - Каждая точка доступа получает канал для передачи данных
  - Изменения в радиосреде мониторятся, канал точки доступа изменяется при плохих условиях радосреды
- **TPC**—Transmit Power Control
  - Мощность передачи сигнала базируется на потерях между двумя радиоисточниками
  - TPC уменьшает мощность передачи на некоторых точках доступа, но может так же и увеличить ее при определенных условиях
- **CHDM**—Coverage Hole Detection and Mitigation
  - Обнаруживает клиентов в зонах без покрытия
  - Принимает решение увеличить мощность передачи на некоторых точках доступа, чтобы «дотянуться» до клиента



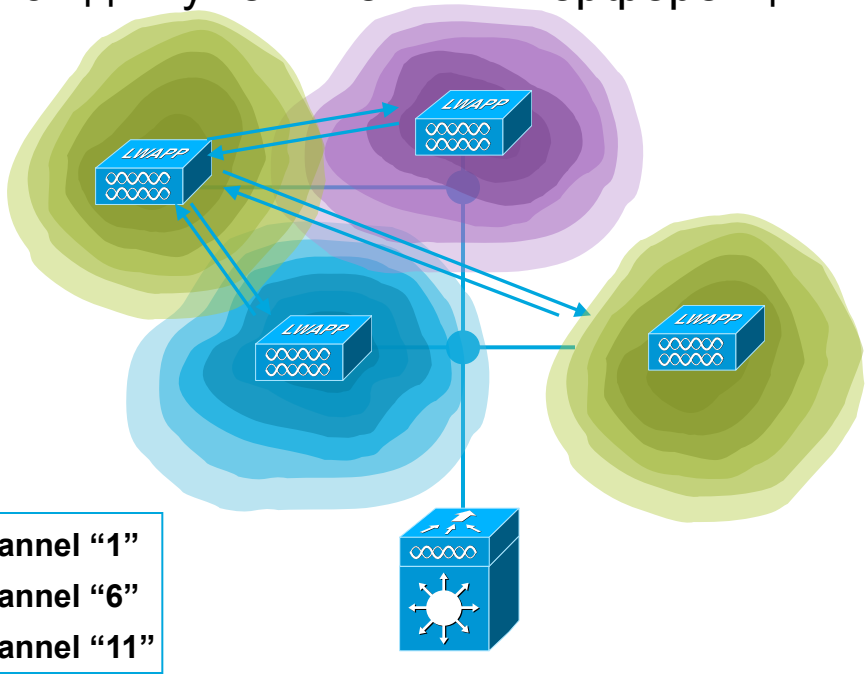
© 2011 Cisco and/or its affiliates. All rights reserved.

RRM DCA – Динамическое назначение каналов

Новая точка доступа создает интерференцию каналов



Система оптимизирует распределение каналов для уменьшения интерференции

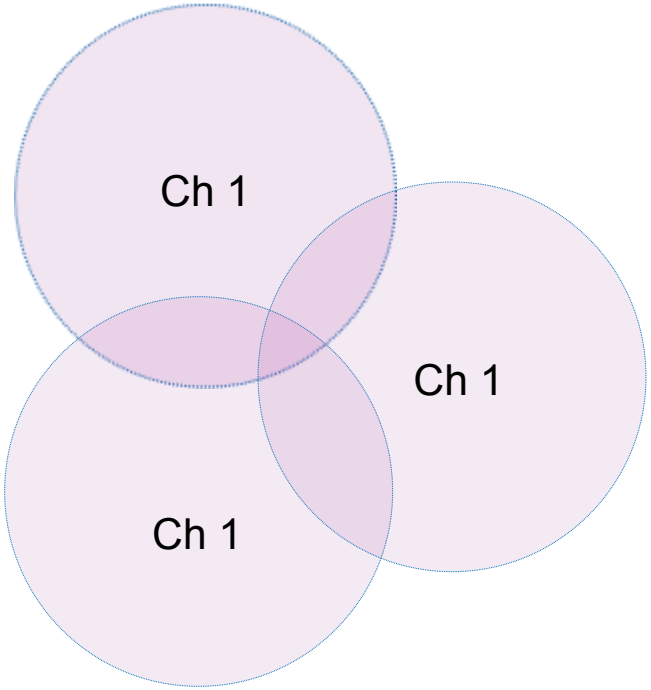


Как это делается

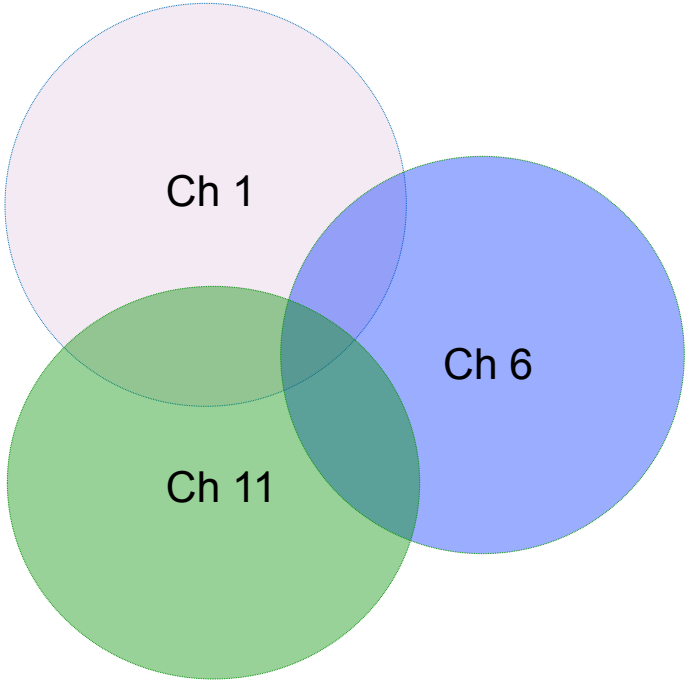
- Убеждается в том, что доступный радио спектр используется хорошо для всех частот/каналов
  - Лучшая полоса пропускания достигается без ущерба в работе точек доступа

© 2011 Cisco and/or its affiliates. All rights reserved.

Спектральная эффективность механизма Auto RF



Эффективность 33%

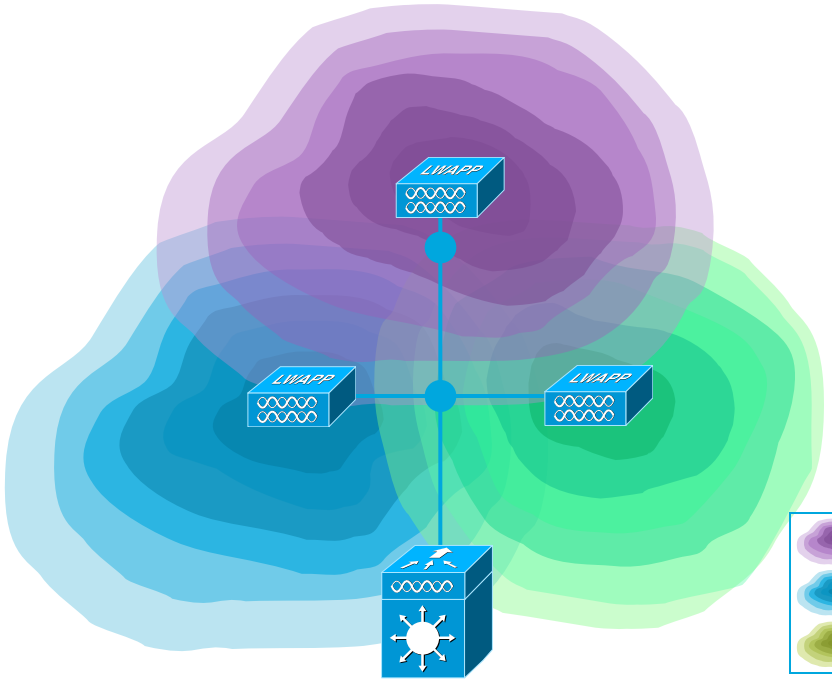


Эффективность 100%

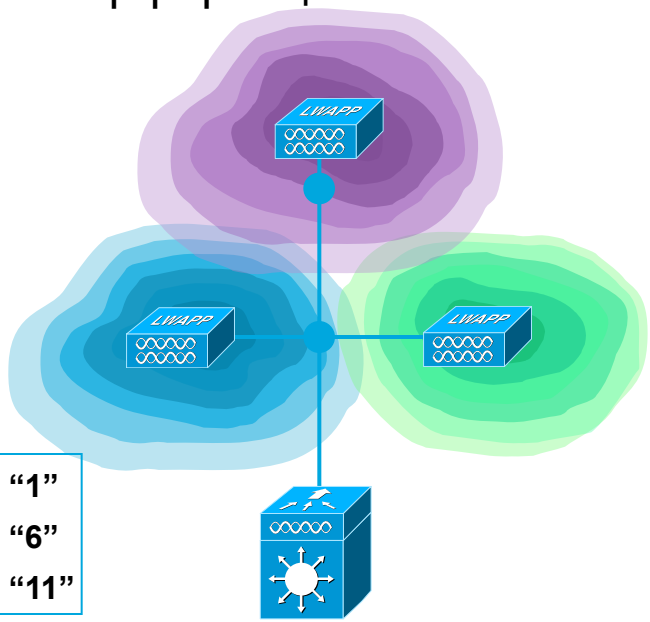
© 2011 Cisco and/or its affiliates. All rights reserved.

RRM – Управление мощностью передатчика

Мощность не оптимизирована — радиосигнал вызывает интерференцию



Уменьшает граничную мощность, тем самым минимизируя интерференцию



RF Channel “1”
RF Channel “6”
RF Channel “11”

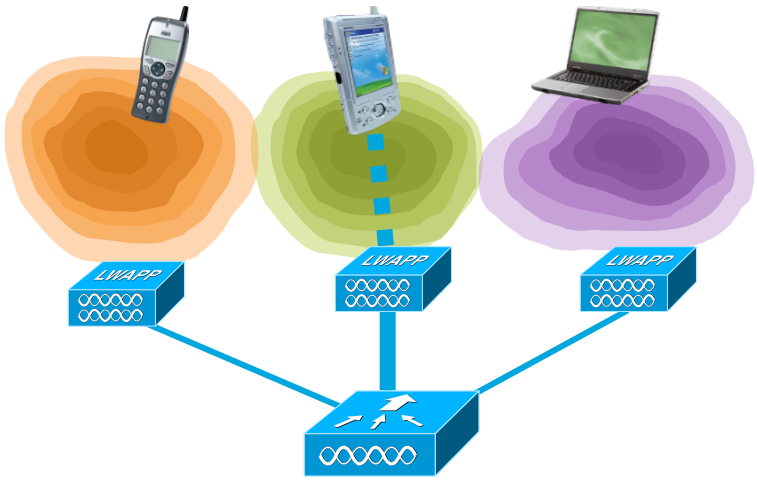
Как это делается

- Мощность передачи базируется на потерях между источниками сигнала
- TPC уменьшает мощность передачи на некоторых точках доступа, но так же может и увеличить ее при определенных условиях

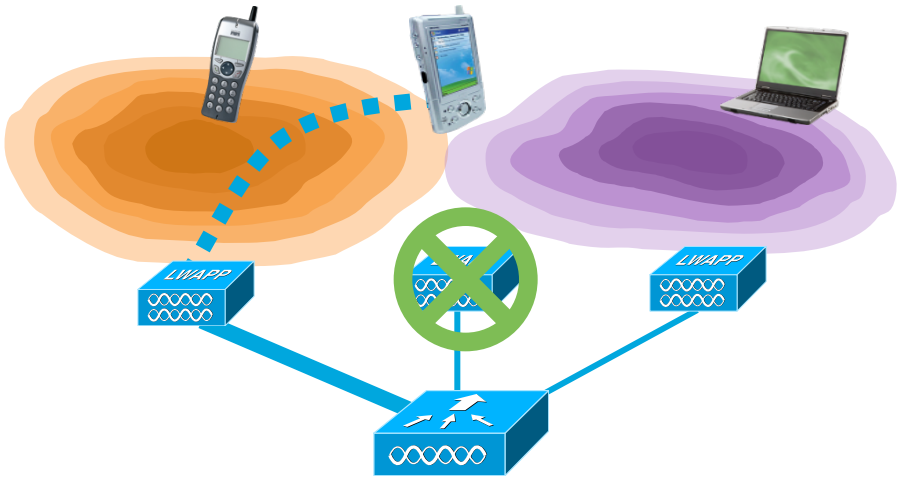
© 2011 Cisco and/or its affiliates. All rights reserved.

Radio Resource Management
Обнаружение и устранение дыр в покрытии

Нормальная работа



Отказ точки доступа обнаружен
Пустая зона покрытия заполнена



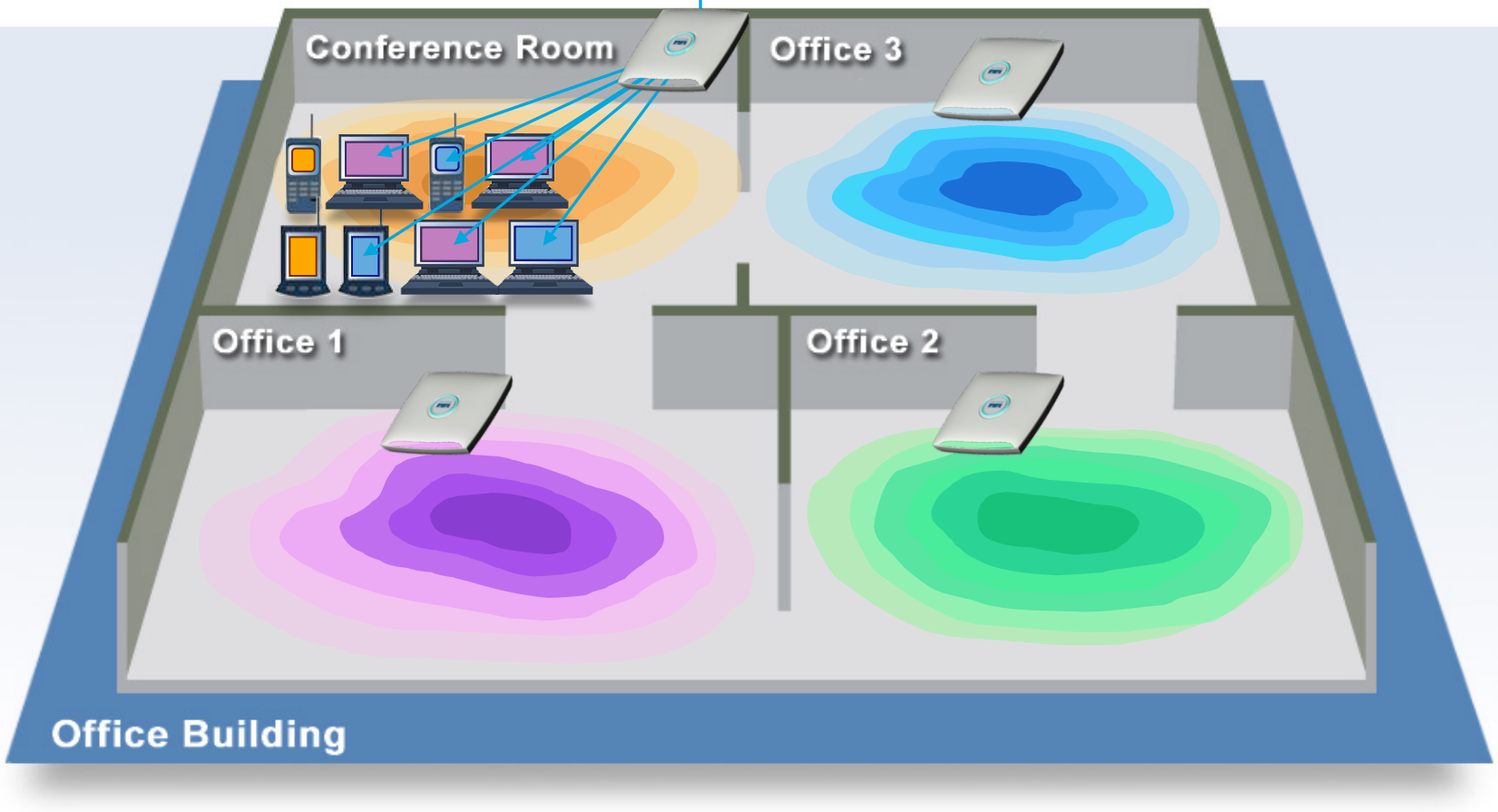
Как это происходит

- Нет единой точки отказа
- Автоматическое переключение уменьшает расходы на поддержку и восстановление
- Доступность беспроводной сети сравнима с проводной

© 2011 Cisco and/or its affiliates. All rights reserved.

Управление плотностью подключений

Решение проблем нагрузки на точки доступа в помещениях с плотным скоплением людей (залы совещаний, кафе)…



Мобильность и прозрачный роуминг

© 2011 Cisco and/or its affiliates. All rights reserved.

Прозрачный беспроводной роуминг

Роуминг подразумевает перемещение беспроводных клиентов между точками доступа

Mobility группа – это набор беспроводных контроллеров, которые настроены на роуминг между ними

Cisco WLC может принадлежать единой mobility группе.

Максимум 24 Cisco WLC может принадлежать одной mobility группе.

Роуминг поддерживается между mobility группами.

Два типа роуминга.

- Layer 2 (внутри подсети) роуминг
- Layer 3 (между подсетями) роуминг

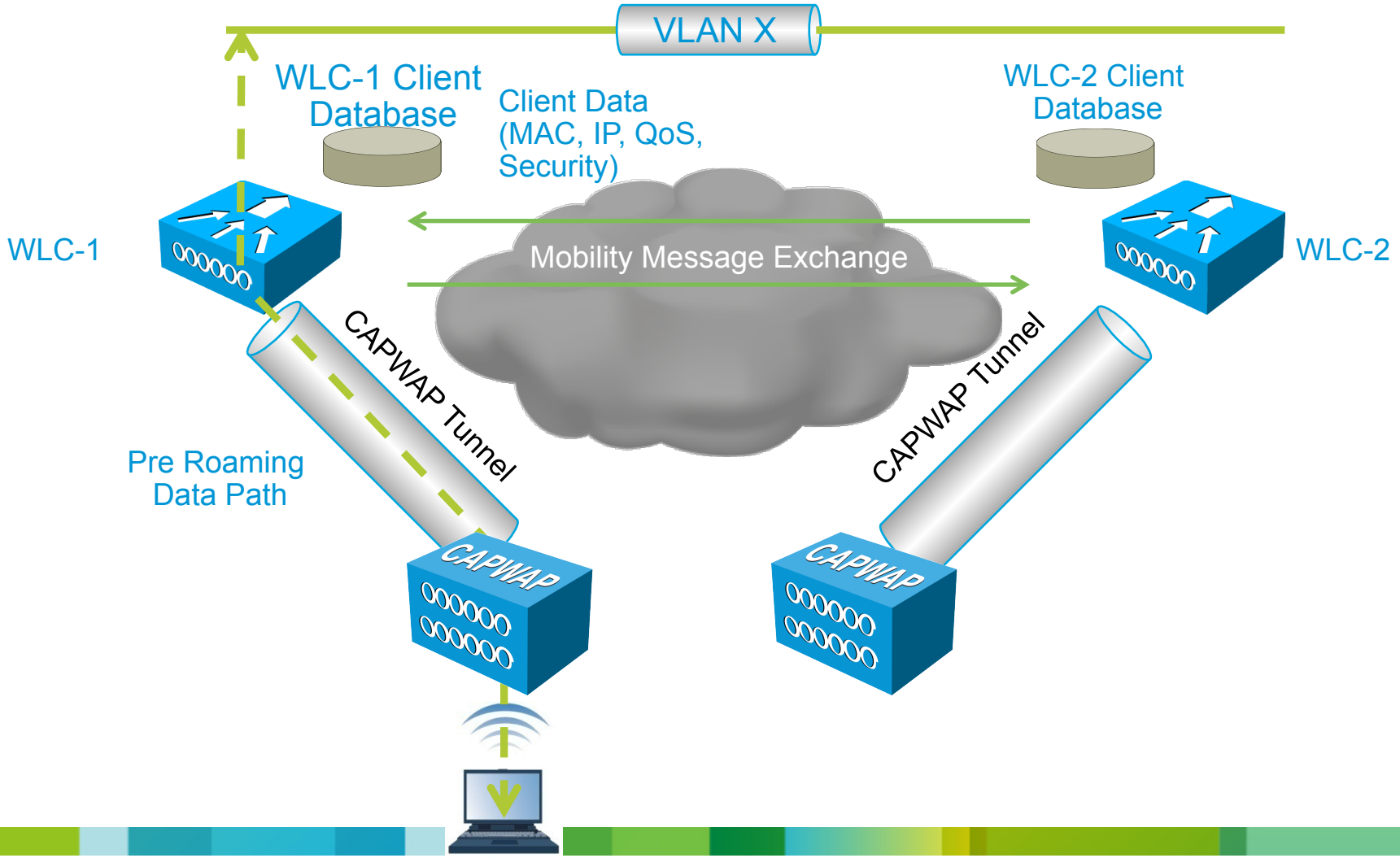
© 2011 Cisco and/or its affiliates. All rights reserved.

Layer 2 роуминг

- Один или несколько Cisco контроллеров находятся в одной подсети
- Роуминг прозрачный для клиента.
- Сессия сохраняется во время соединения с новой точкой доступа
- Клиент продолжает использовать прежний DHCP-присвоенный или статический IP адрес.
- Повторная аутентификация требуется, если клиент посылает DHCP discover с клиентским адресом или когда таймаут сессии исчерпан

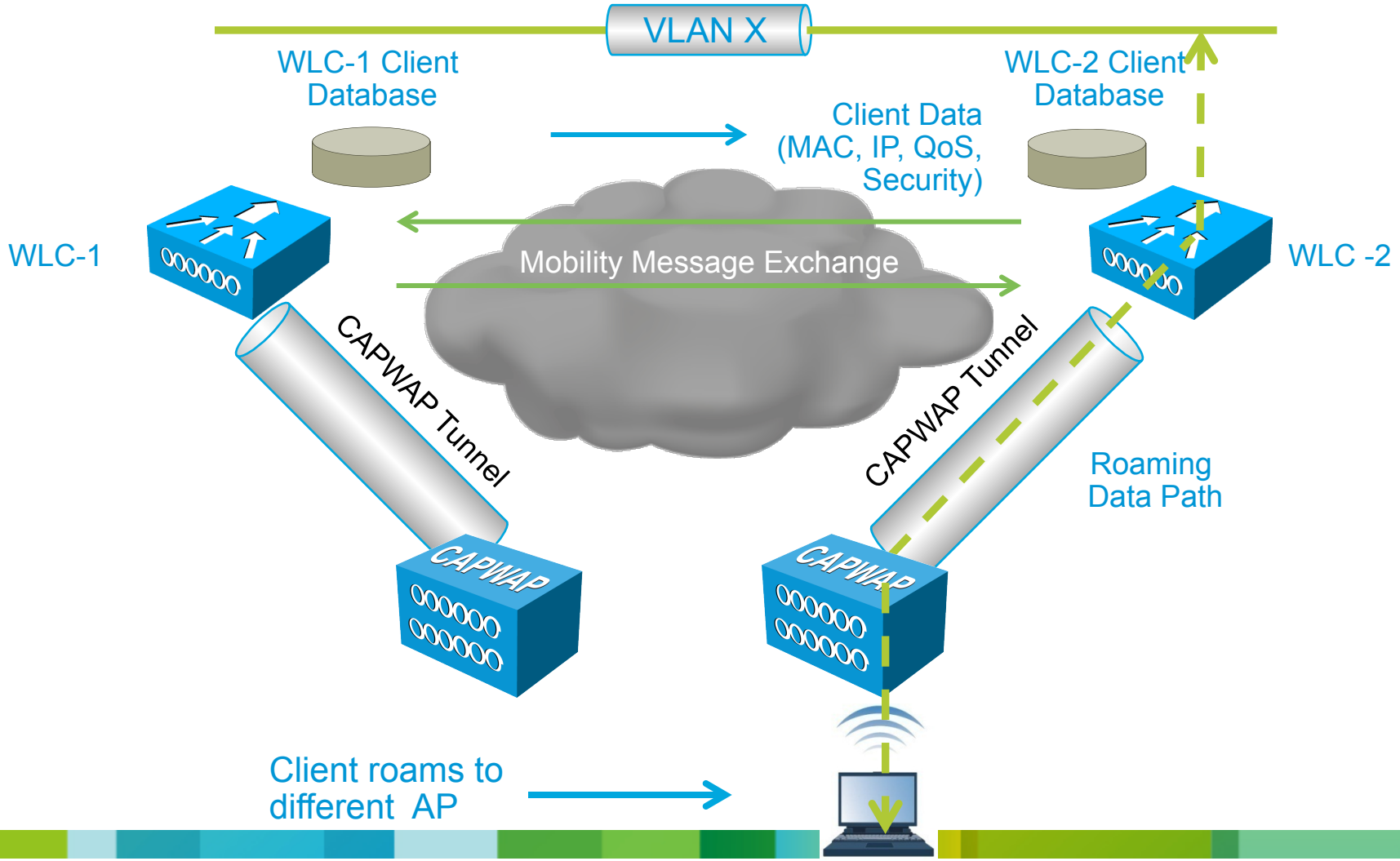
© 2011 Cisco and/or its affiliates. All rights reserved.

Клиентский роуминг в пределах подсети Layer 2 роуминг



© 2011 Cisco and/or its affiliates. All rights reserved.

Клиентский роуминг в пределах одной подсети
Layer 2 роуминг



© 2011 Cisco and/or its affiliates. All rights reserved.

Layer 3 роуминг

Несколько контроллеров в разных подсетях

Прозрачный для клиента.

Сессия сохраняется при смене точки доступа.

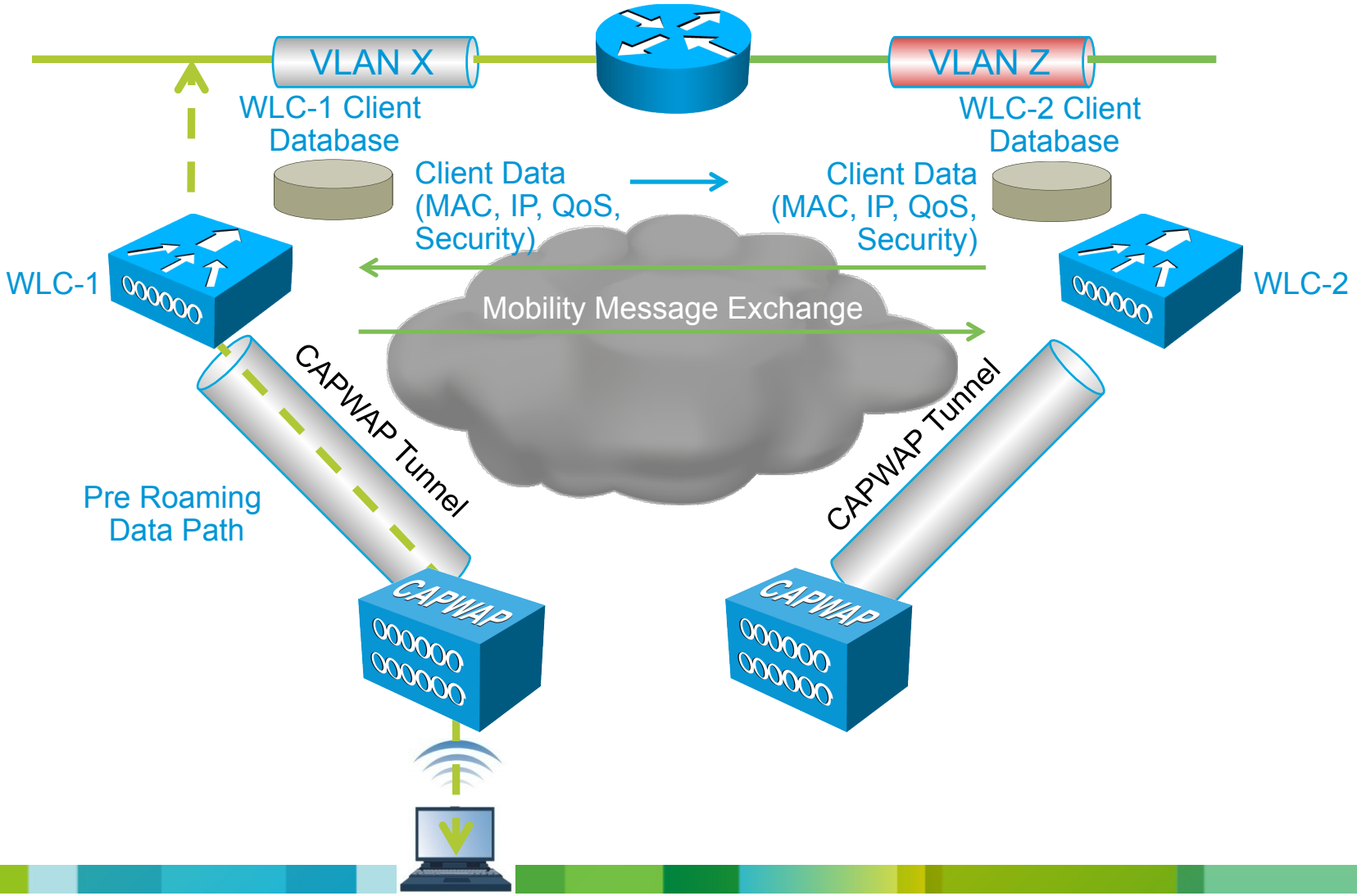
Туннель между родным и чужим контроллерами и специальная обработка клиентского трафика обоими WLC позволяет клиенту продолжать использовать тот же DHCP или статический IP адрес, пока сессия активна

Повторная аутентификация требуется, если клиент посылает DHCP discover с клиентским адресом или когда таймаут сессии исчерпан

Возможен благодаря симметричному туннелю между родным и чужим контроллерами.

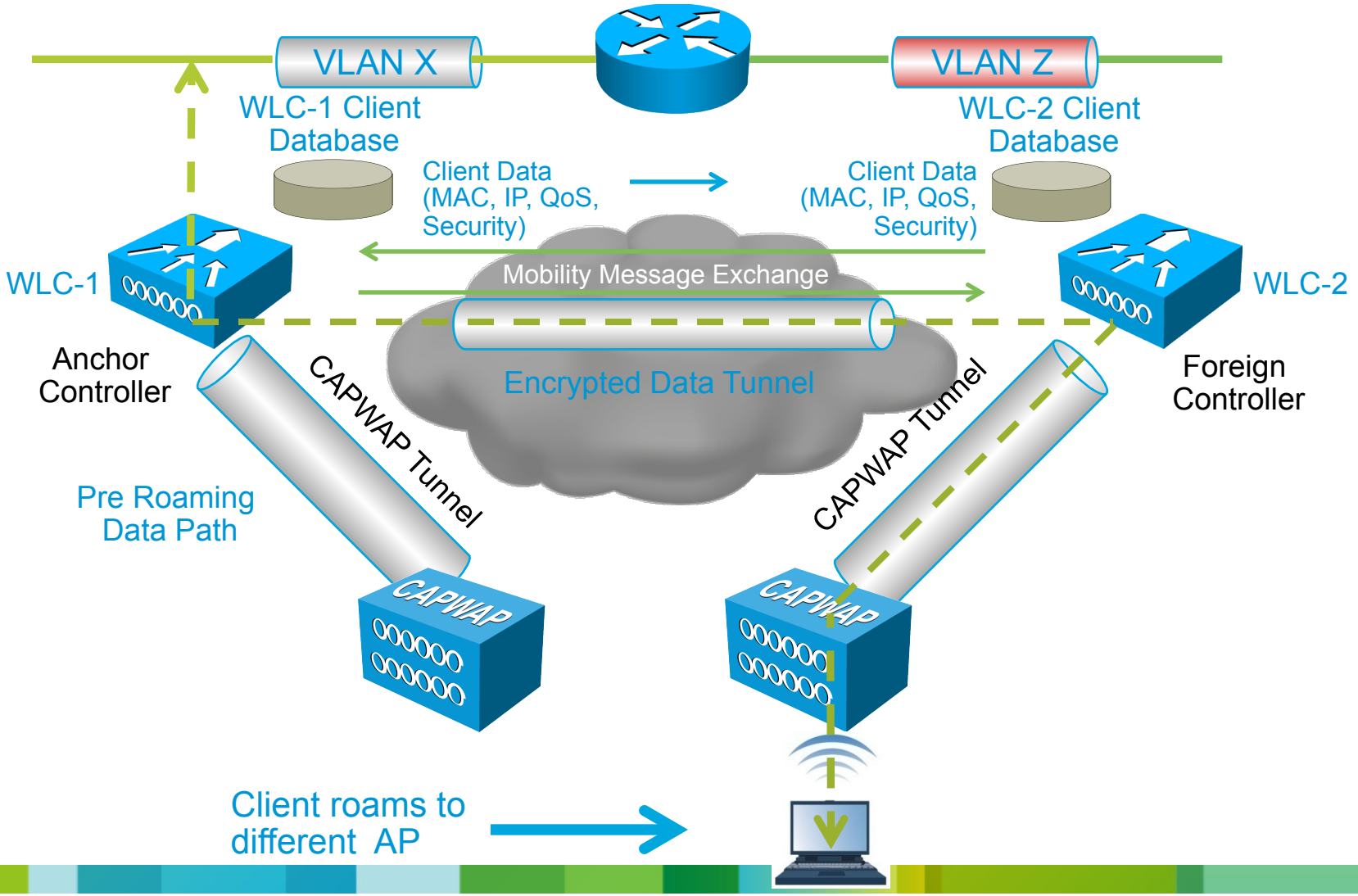
© 2011 Cisco and/or its affiliates. All rights reserved.

Клиент перемещается между подсетями Layer 3 Роуминг



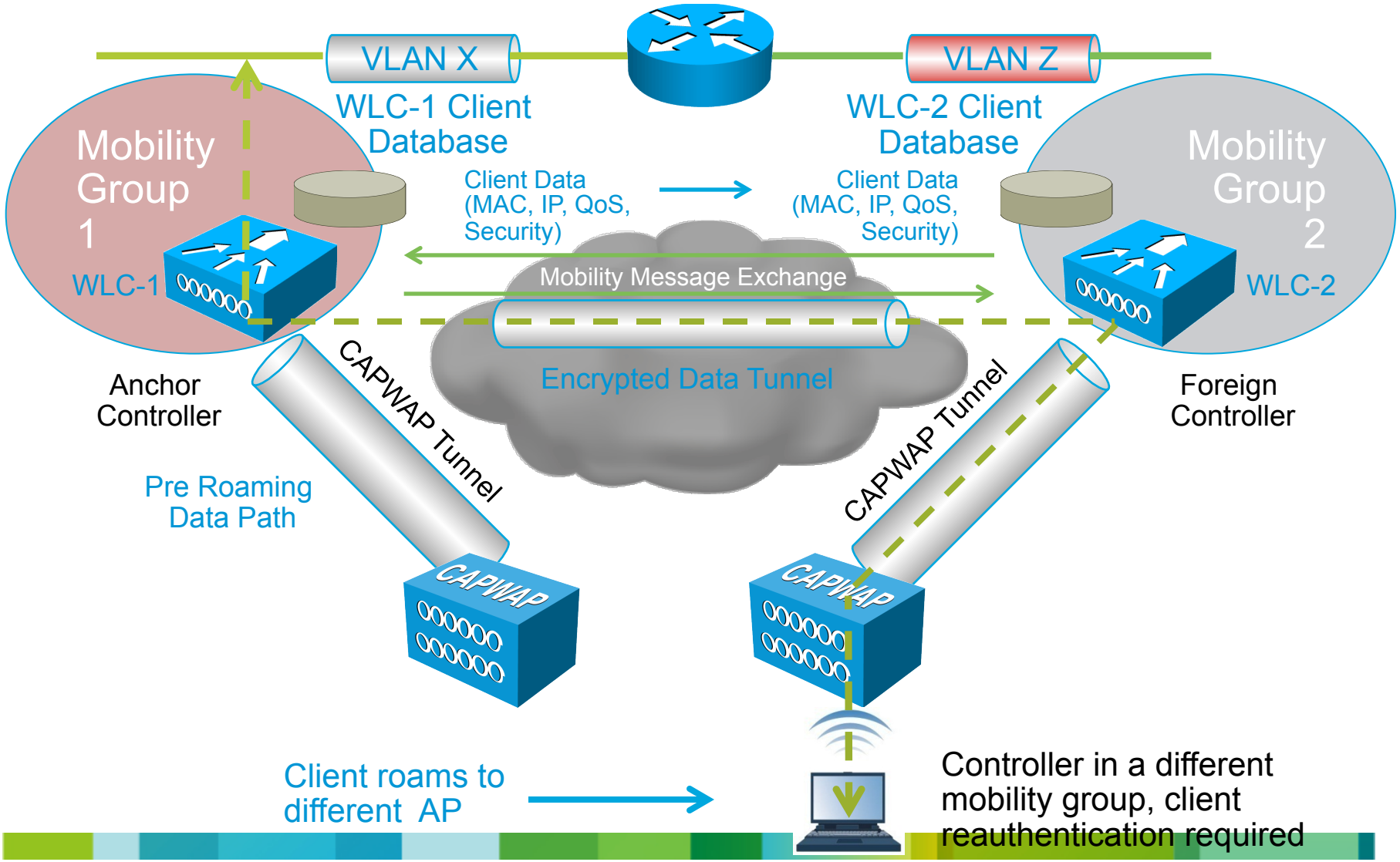
© 2011 Cisco and/or its affiliates. All rights reserved.

Клиент перемещается между подсетями Layer 3 Роуминг



© 2011 Cisco and/or its affiliates. All rights reserved.

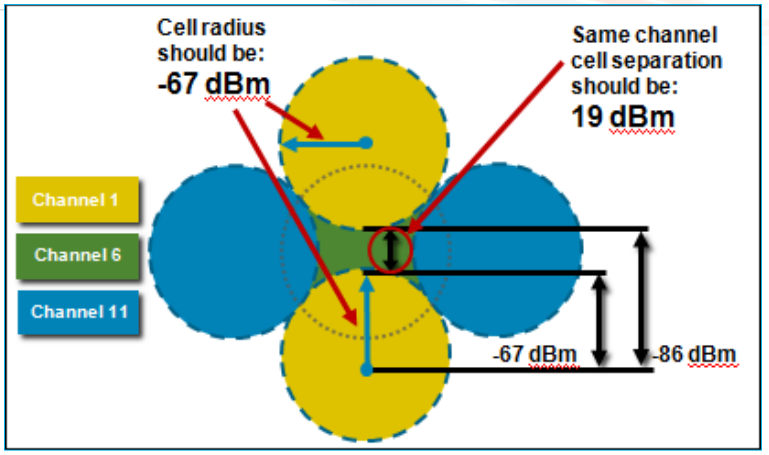
Клиентский роуминг между подсетями Layer 3 роуминг, разные Mobility группы

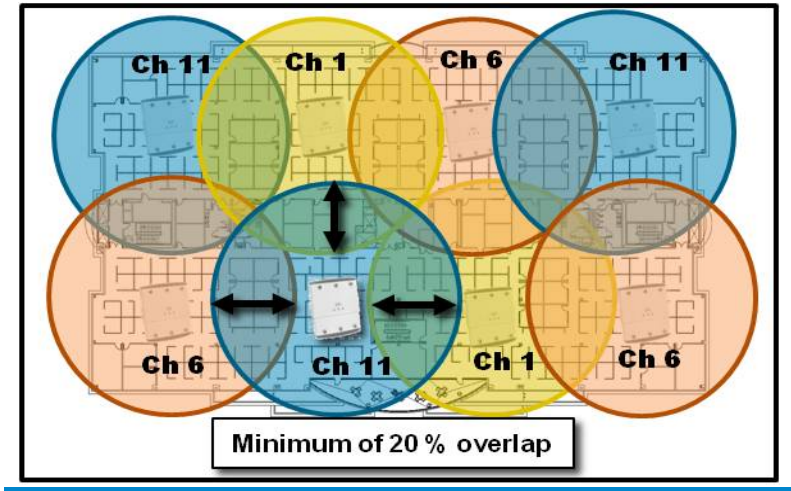


© 2011 Cisco and/or its affiliates. All rights reserved.

Внедрение голоса поверх Wi-Fi

- **Базовые VoWLAN требования:**
  - ✓ **Радиус зоны действия канала или мощность сигнала на границе -67 dBm** (или меньше) рекомендуется для минимзации потерь пакетов.
  - ✓ **Разделение одинаковых каналов с уровнем 19 dBm** для минимальной интерференции
  - ✓ **Пересечение несмежных каналов минимум на 20%** для обеспечения прозрачного роуминга при перемещении.
- **Требуется радиоисследования с участием каждого мобильного устройства**
- **Bluetooth устройства не рекомендуется ввиду интереференции на частоте 2.4 GHz**





Дополнительная информация - ***Voice over Wireless LAN 4.1 Design Guide*** :

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

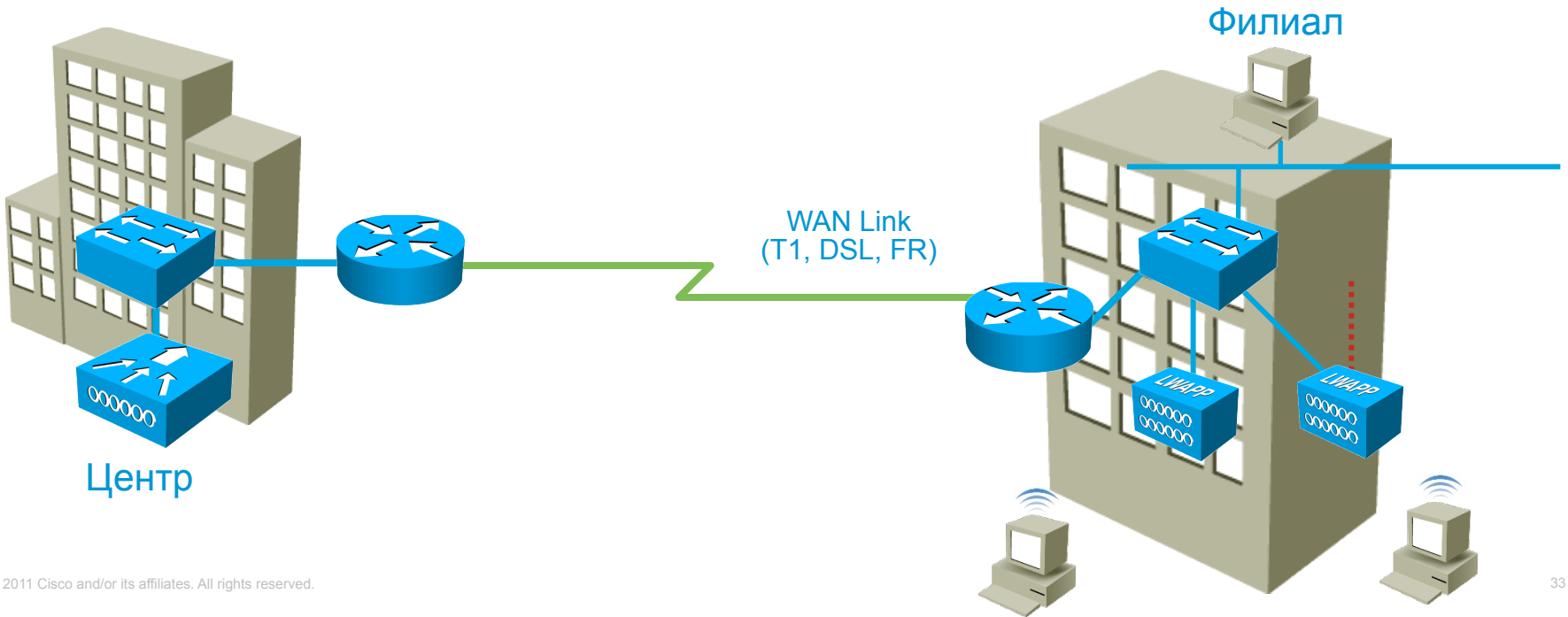
© 2011 Cisco and/or its affiliates. All rights reserved.

Расширение беспроводной сети к удаленным офисам

© 2011 Cisco and/or its affiliates. All rights reserved.

Удаленные беспроводные сети - примеры

- Большое количество удаленных объектов
- Установка контроллеров на малых удаленных объектах экономически нецелесообразна
- Необходим гостевой доступ
- Публичный открытый доступ в интернет
- WAN-каналы небольшой емкости



© 2011 Cisco and/or its affiliates. All rights reserved.

Flex-Connect (ex. H-REAP)

Беспроводной решение для удаленных объектов.

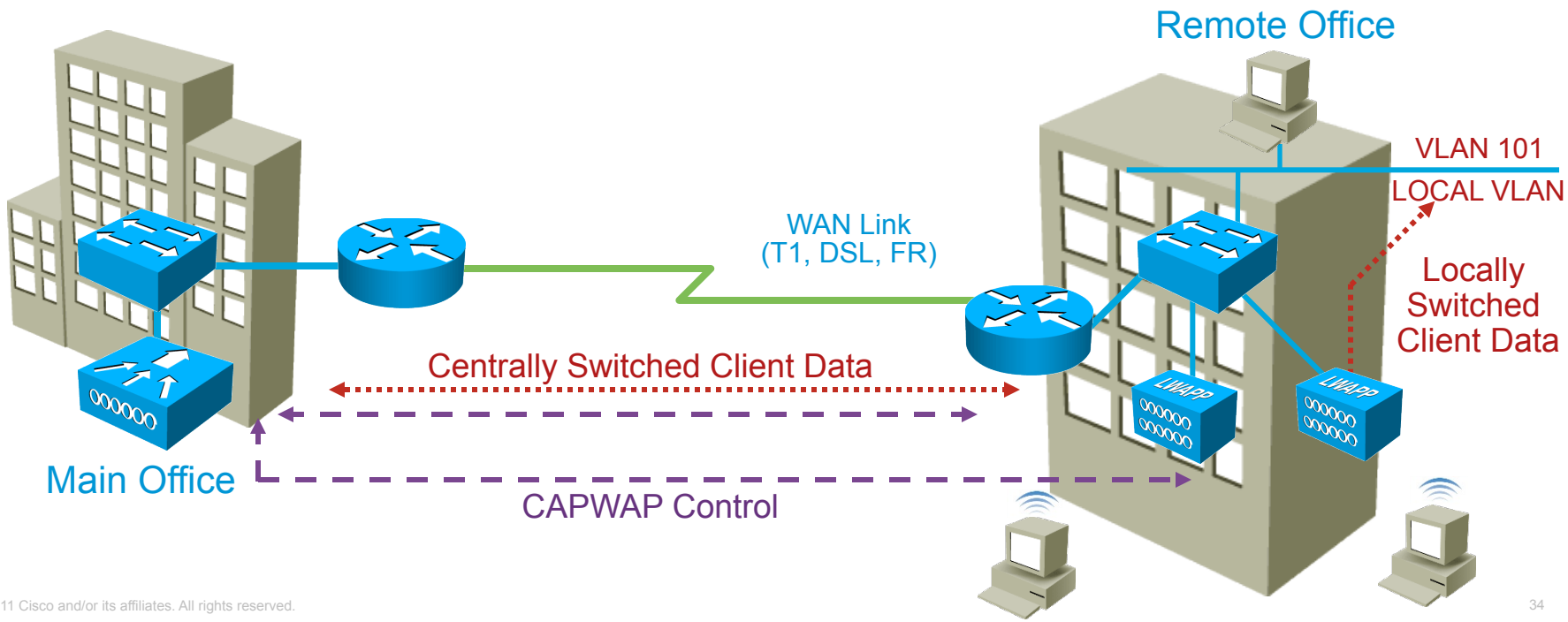
Точки доступа ассоциируютс с контроллером через WAN канал.

Позволяет внедрить беспроводные сети в филиале без установки WLC.

Клиентские данные коммутируются локально.

Аутентификация происходит через контроллер (через WAN).

Несколько вариантов локальной аутентификации при потери WAN-канала.



© 2011 Cisco and/or its affiliates. All rights reserved.

FlexConnect в Standalone Mode

- Standalone mode: Когда контроллер не доступен, точка доступа переключается в этот режим и проводит аутентификацию самостоятельно.
- Поддерживается ограниченный набор методово аутентификации в Standalone mode: Open, Shared WPA-PSK, Shared WPA2-PSK, WPA2 Enterprise: EAP-FAST.
  - Сети с центральной коммутацией перестают работать.
  - Сети с локальной коммутацией продолжают работать:
    - Аутентификация сетей с локальной коммутацией работает нормально
    - Существующие 802.1x аутентифицированные клиенты продожают работать до тех пор, пока не происходит их роуминг или же не проходит реаутентификация
- Не поддерживается в Standalone mode:
  - RRM, WIDS, LBS, AP modes
  - Web Auth, NAC

© 2011 Cisco and/or its affiliates. All rights reserved.

Инновационные технологии: оптимизация работы беспроводных клиентов

© 2011 Cisco and/or its affiliates. All rights reserved.

Типичные проблемы беспроводных сетей

- Как гарантировать совместимость массы устройств с беспроводной инфраструктурой?
- Как обеспечить бесшовный роуминг?
- Как оценить качество сигнала на стороне клиента?
- Как точно определить местоположение клиента на карте?
- Как обеспечить безопасную и гибкую аутентификацию?
- Как добиться оптимального качества сигнала на стороне клиента (SNR)?

© 2011 Cisco and/or its affiliates. All rights reserved.

Эволюция Cisco Compatible Extensions (CCX)

8 years of success in driving innovation
70% CCX features have become standard

LEAP, WPA, 802.1x,

LCCKM, Radio Measurement

LWME, Proxy ARP, WPA2, EAP,-FAST

CAC, Voide Metrics, Location

MFP, Client Reporting, Diagnostics

CCX Deprecation

Android + Video Support

CCX WiFi Direct

Clean Air, Enterprise MSAP

CCX Pre-.11ac, ad

CCX
IP Test & Certification Program
Under
Cisco Developer Network

V1 V2 V3 V4 V5

CCX Lite
(Services Modules)

2002 **2005** **2011** **2012**

Reliability Security

Support for mobile services

Service Centric Independence to access network

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Compatible Extensions (CCX)

- Проверенная и гарантированная совместимость большинства Wi-Fi клиентов с инфраструктурой Cisco
- Поддержка алгоритмов прозрачного роуминга (CCKM)
- Устранение неисправностей для каждого беспроводного соединения
- Управление мощностью передатчика клиента для оптимального качества соединения
- Более точное определение местоположения

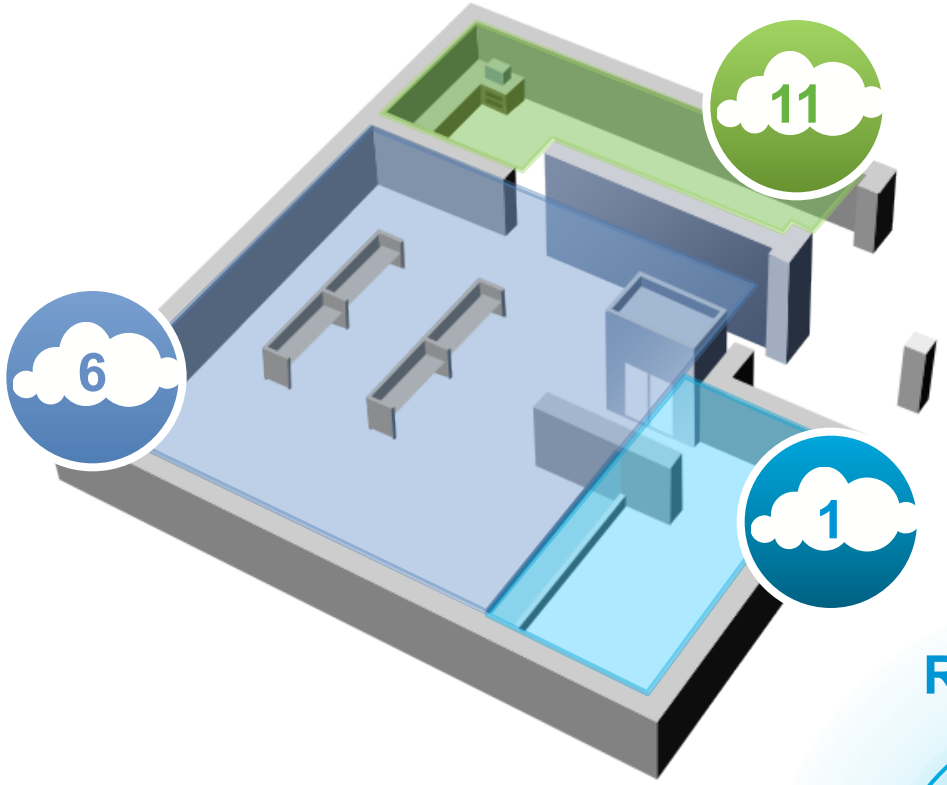
Детально: http://www.cisco.com/go/ccx

© 2011 Cisco and/or its affiliates. All rights reserved.

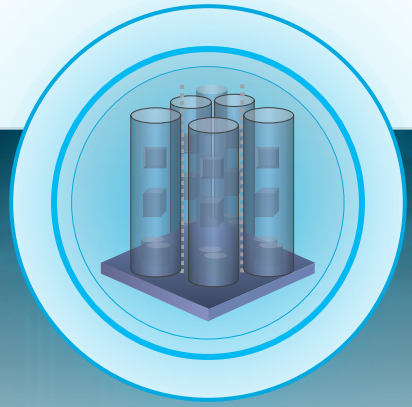
Инновационные технологии: оптимизация спектра с помощью Cisco CleanAir

© 2011 Cisco and/or its affiliates. All rights reserved.

Рабочая беспроводная сеть



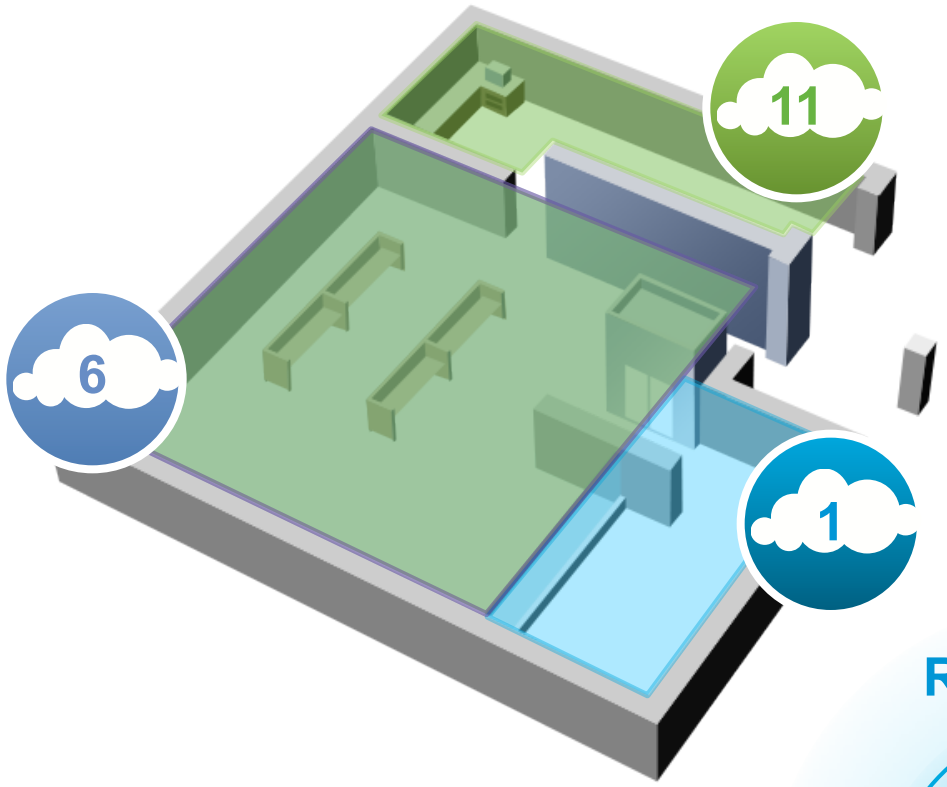
RRM



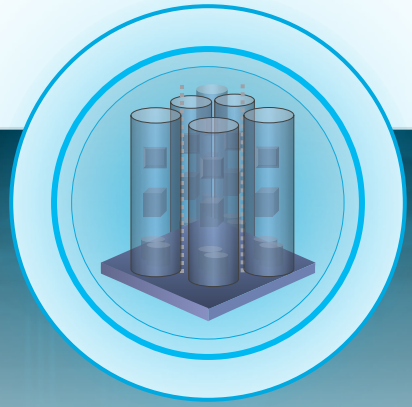
Wireless LAN Controller

Каналы 11, **6** и **1** оптимизированы для максимальной полосы пропускания и минимальной интерференции

Проблема: внезапно упала скорость



RRM



Wireless LAN Controller

Упала производительность в радиусе действия канала 6

Последствия переполненного спектра
Производительность под угрозой

Для пользователя

- Снижается покрытие и полоса пропускания
- Плохое качество голоса и видео

Для ИТ-менеджера

- Potential security breaches
- Звонки в службу поддержки
- Вырастает стоимость обслуживания

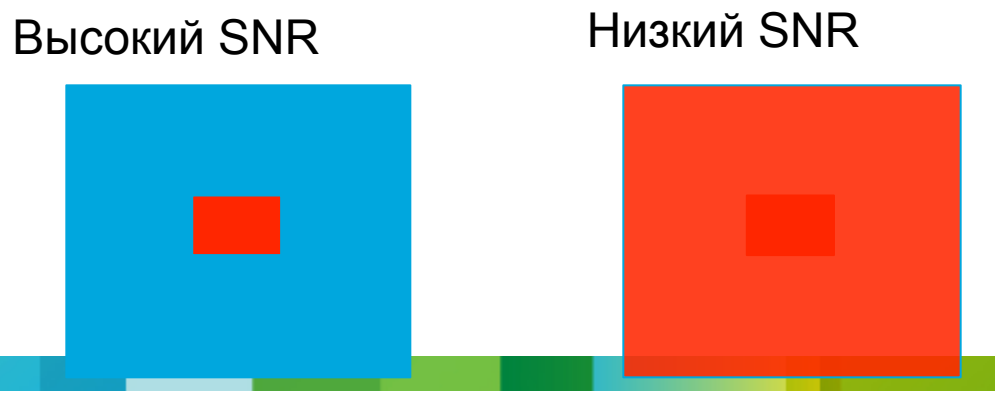
Interference Type		Throughput Reduction: Near (25 ft)	Throughput Reduction: Far (75 ft)
2.4 or 5 GHz Cordless Phones		100%	100%
Video Camera		100%	57%
Wi-Fi (busy neighbor)		90%	75%
Microwave Oven		63%	53%
Bluetooth Headset		20%	17%
DECT Phone		18%	10%

Source: FarPoint Group

© 2011 Cisco and/or its affiliates. All rights reserved.

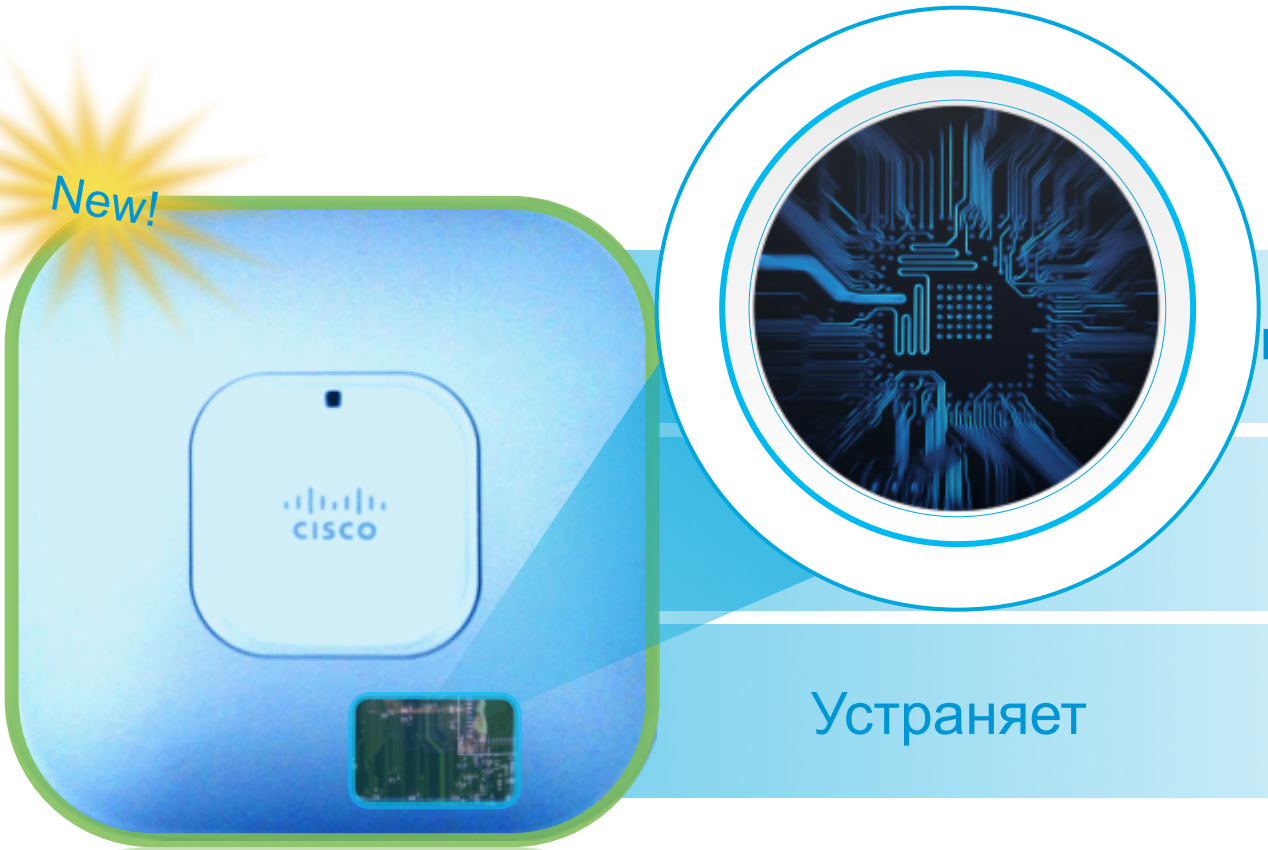
Как интерференция влияет на Wi-Fi?

- Коллизии - Другие устройства не участвуют в наших механизмах избежания коллизий
- Отсутсвие «уважения к Wi-Fi» – выливается в:
  - Поврежденных пакетах
  - Увеличение повторных передач
  - Меньшая доступная полоса пропускания
- SNR – Отношение сигнал/шум



© 2011 Cisco and/or its affiliates. All rights reserved.

Представляем CleanAir



и классифицирует

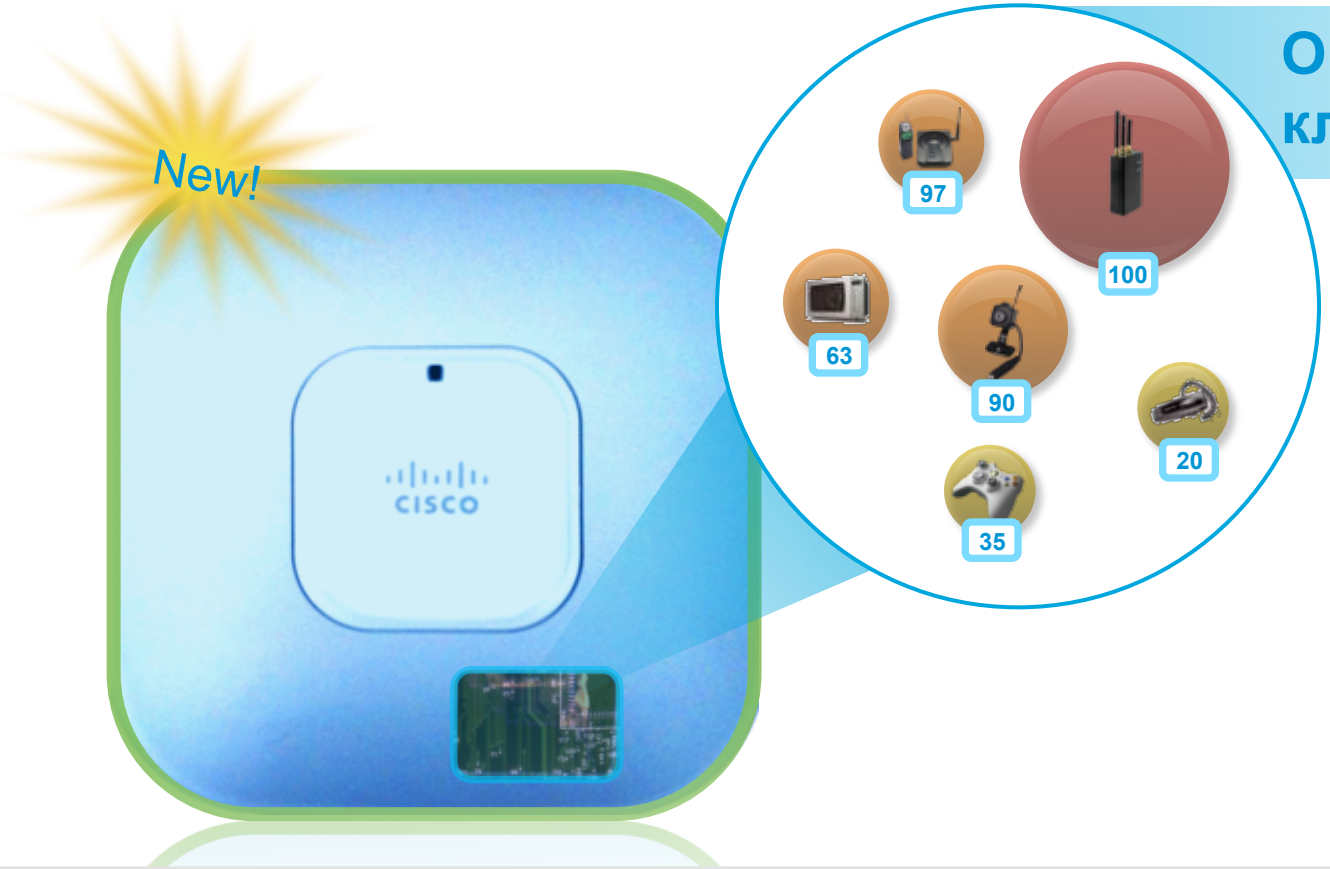
Устраняет

Cisco CleanAir

A system-wide feature that uses silicon-level intelligence to automatically mitigate the impact of wireless interference, optimize network performance and reduce troubleshooting costs

Reduces TCO with automated interference mitigation and troubleshooting

Что такое CleanAir?



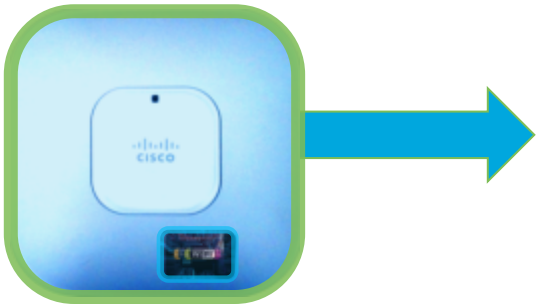
Определяет и классифицирует

- Идентифицирует многие источники помех
- Выявляет влияние на Wi-Fi производительность

Cisco CleanAir

High-resolution interference detection and classification logic built-in to Cisco's 802.11n Wi-Fi chip design. Inline operation with no CPU or performance impact.

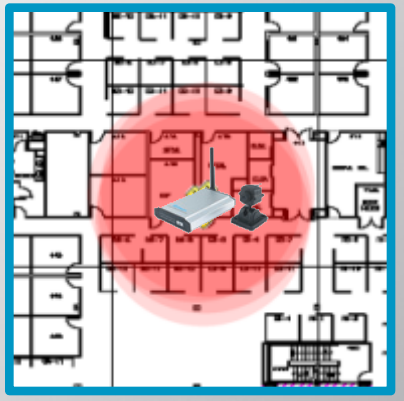
Что такое CleanAir?



- Классификация происходит точкой доступа
- Данные об интерференции высылаются на WLC для дальнейших действий
- WCS и MSE сохраняют данные об истории местоположения

Обнаруживает местоположение

Prime Infrastructure, MSE

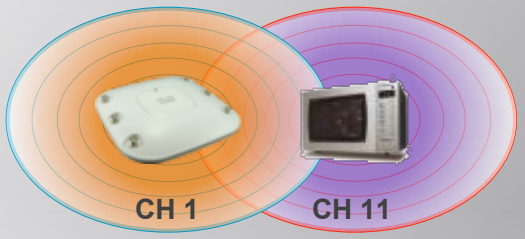


Visualize and Troubleshoot

Устраняет

Wireless LAN Controller

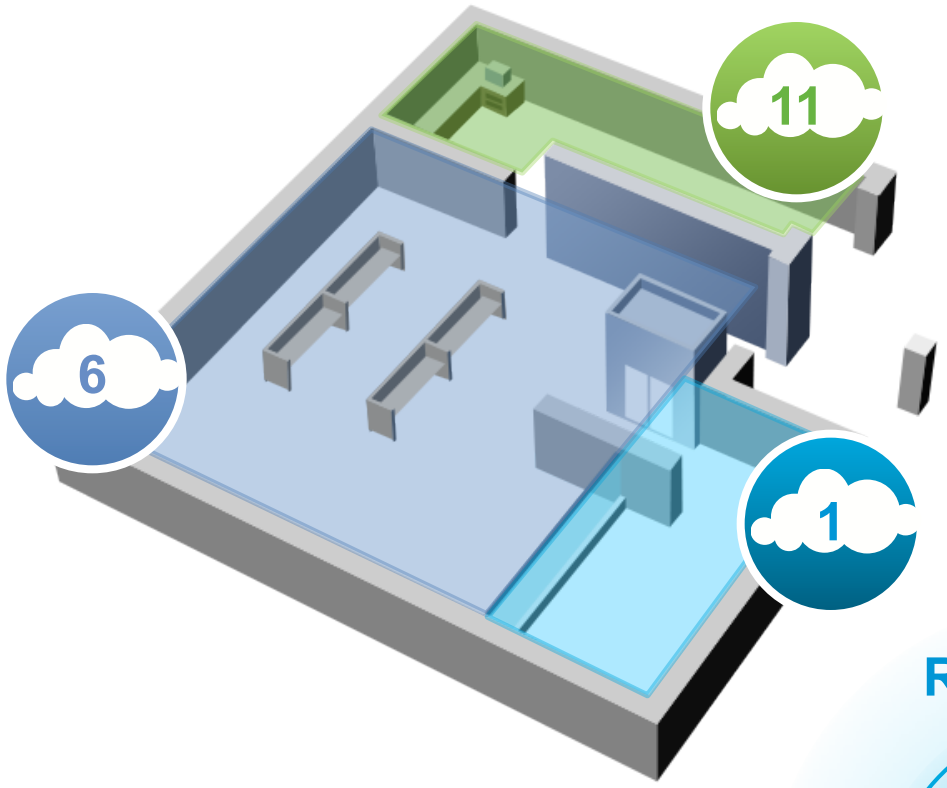
Maintain Air Quality



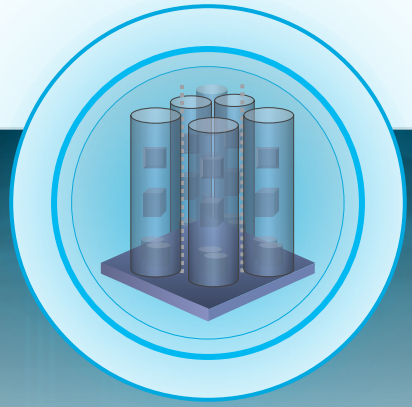
Cisco CleanAir

Cisco CleanAir Technology integrates interference information from the AP into the entire system.

Самолечение и оптимизация



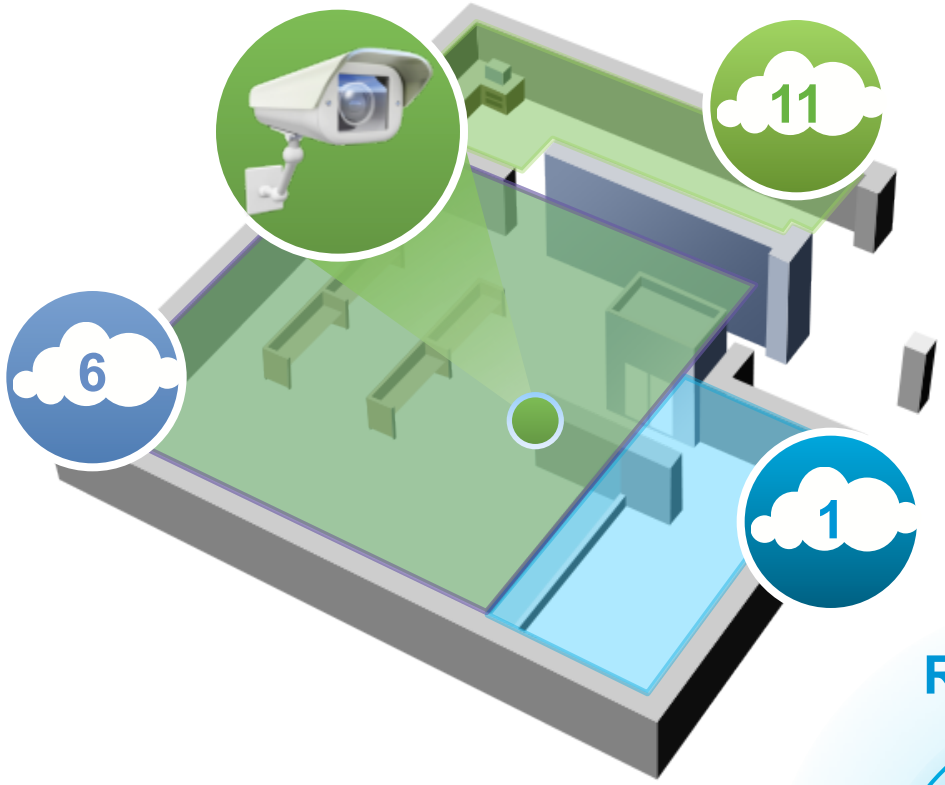
RRM



Wireless LAN Controller

Channels 11, **6** and **1** are optimized for maximum performance and minimum interference

Самолечение и оптимизация



RRM

Wireless LAN Controller

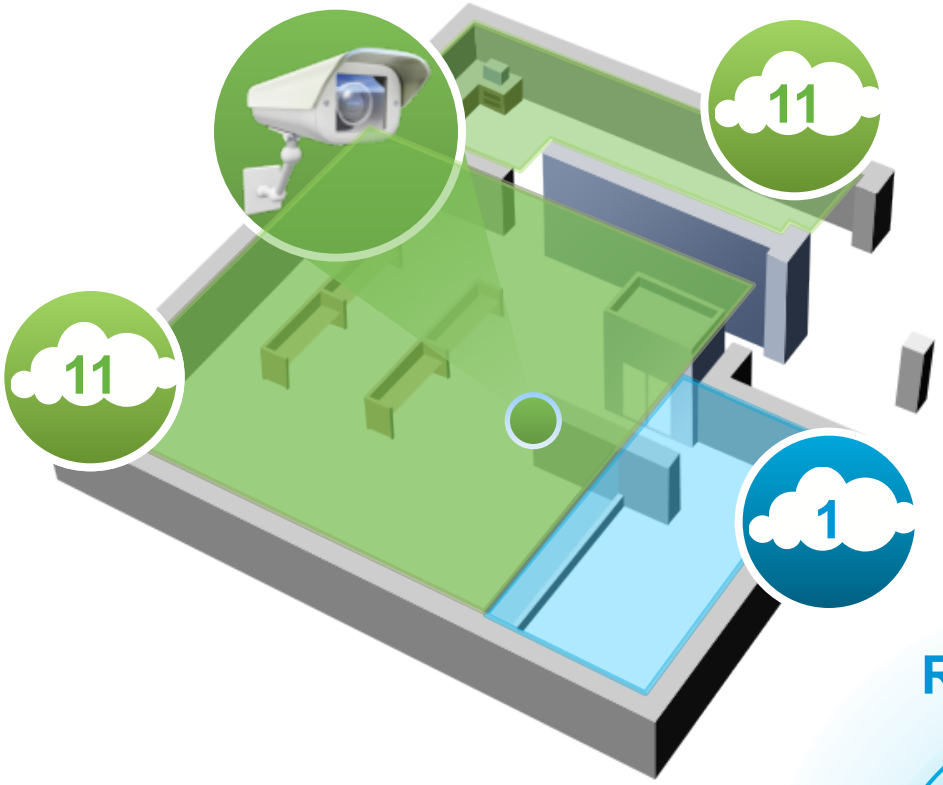
Channels 1, 6 and 11 are optimized for maximum performance

Channel 6 – Air Quality is not optimal

Scanning available channels to resolve conflict…

Channel 1 – Moving from preferred channels to resolve conflict…

Самолечение и оптимизация



Wireless LAN Controller

Conflict resolved. Information is being relayed to RRM. Conflicting channel is blocked from future use.

Channel 11 Conflict

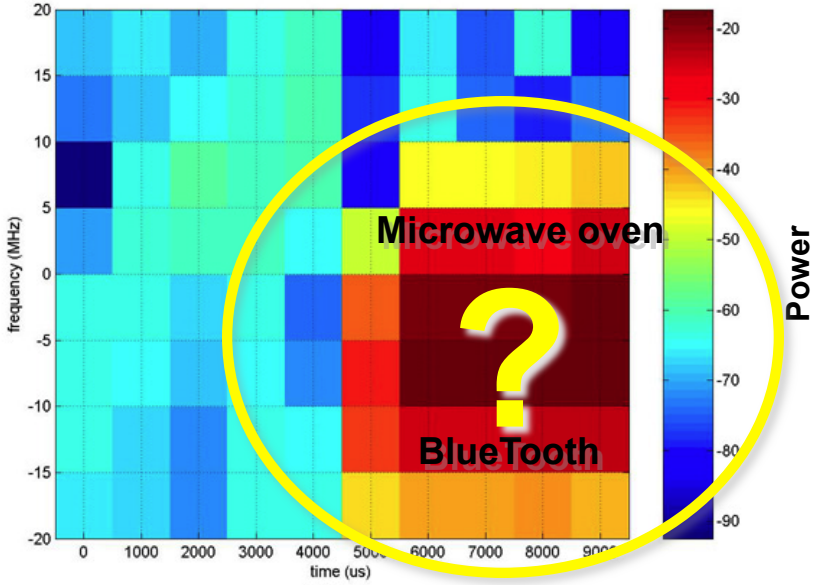
Ценность схемотехнической реализации интеллектуальных алгоритмов

Процесс устранения неполадок	Вариант A: Технология CleanAir	Вариант B: только программное решение
Сценарий: помехи вызваны камерой наблюдения и микроволновой печью		
Обнаружение помехи	Все AP обнаруживают 2 источника помех	Все AP обнаруживают спектр помехи
Классификация источника помехи	Определяются видеокамера и микроволновая печь	Нет возможности разделить несколько источников помех
Корреляционный анализ на всех точках доступа	Помеха анализируется на всех AP как сочетание двух воздействий	Нет – помеха считается уникальной для каждой AP
Оценка воздействия на AP и сеть в целом	Измеряется воздействие и уровень серьезности помехи от каждого источника	Измеряется только общая помеха
Уведомление ИТ-специалистов	Интеллектуальное уведомление об источниках и воздействии	Одно уведомление от каждой AP "обнаружена помеха"
Обнаружение местоположения камеры и печи	Местоположение источников точно указывается на плане	Поиск источников вручную
Устранение воздействия помехи	Интеллектуальная смена каналов в автоматическом режиме	Изменения вручную на основании ограниченного объема данных
Отчет о качестве радиосреды	Представление состояния Wi-Fi-сети для каждой AP	Нет

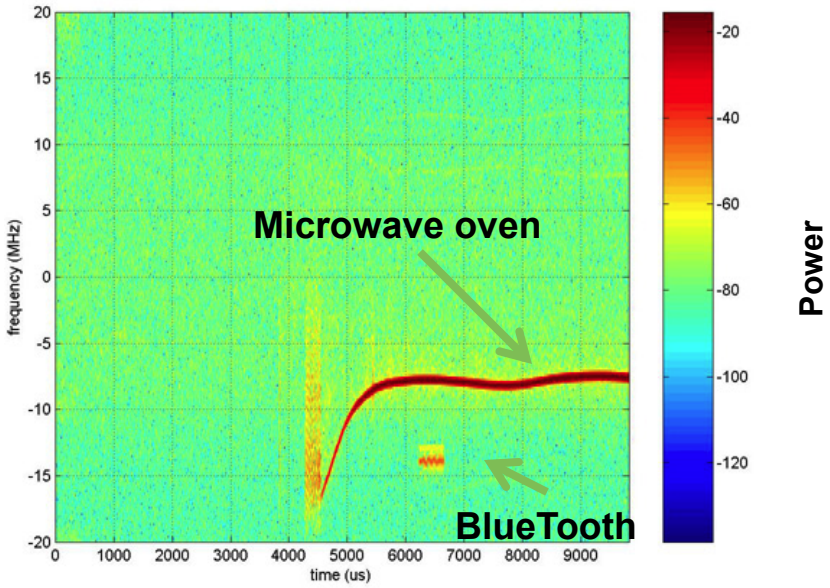
Высокое разрешение спектра

Спектральный анализ высокого разрешения

Типичный Wi-Fi чипсет
Дискретность разрешения 5 MHz



Cisco CleanAir Wi-Fi чипсет
Спектральное разрешение
78 to 156 KHz

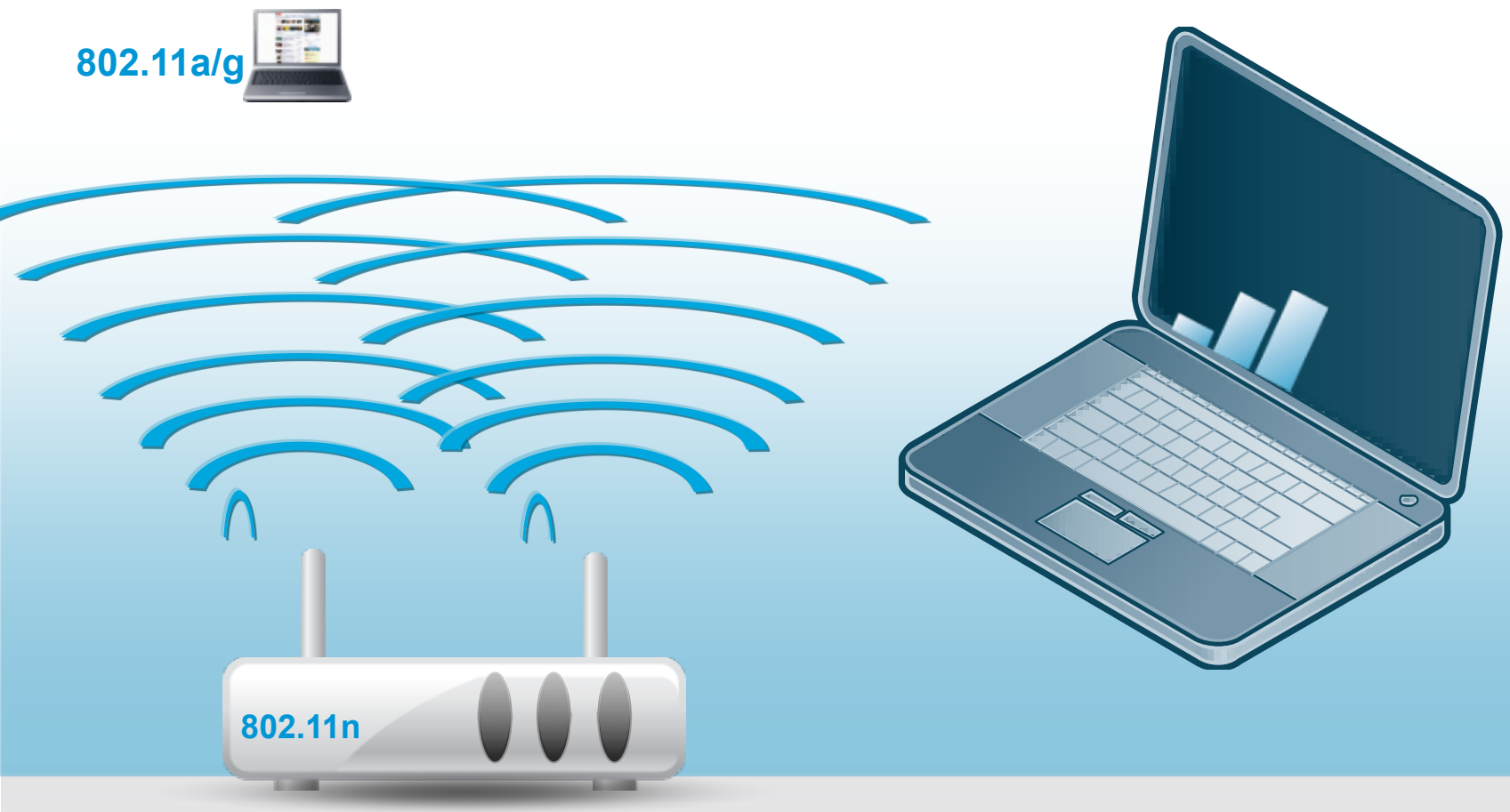


© 2011 Cisco and/or its affiliates. All rights reserved.

Инновационные технологии: Client-link

© 2011 Cisco and/or its affiliates. All rights reserved.

Стандартное решение 802.11n
радиосигнал не направлен в сторону клиента

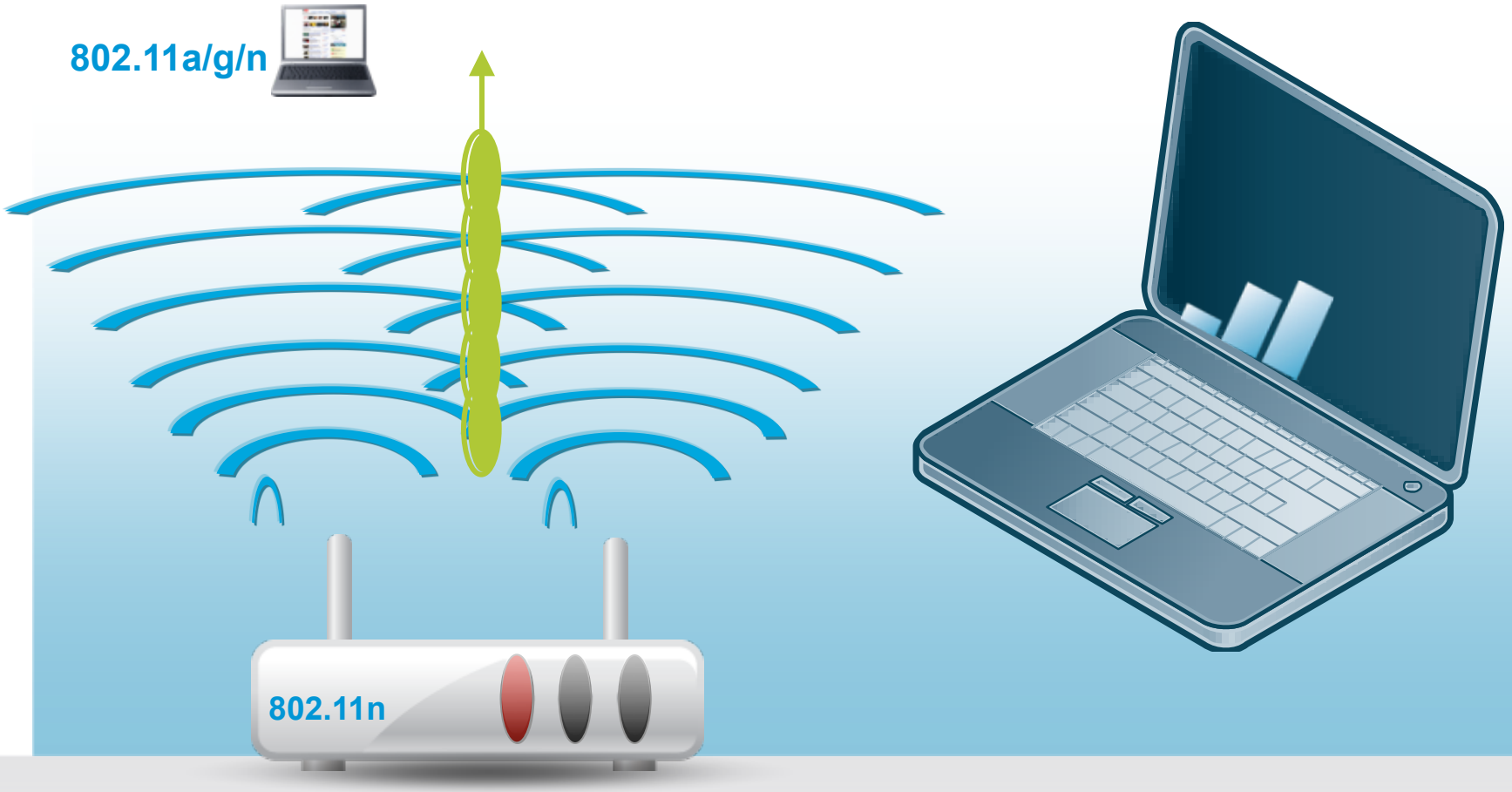


Соединение с 802.11a/g клиентов не оптимально, возможно появление «белых пятен» в радиопокрытии

© 2011 Cisco and/or its affiliates. All rights reserved.

Стандартное решение 802.11n

радиосигнал не направлен в сторону клиента

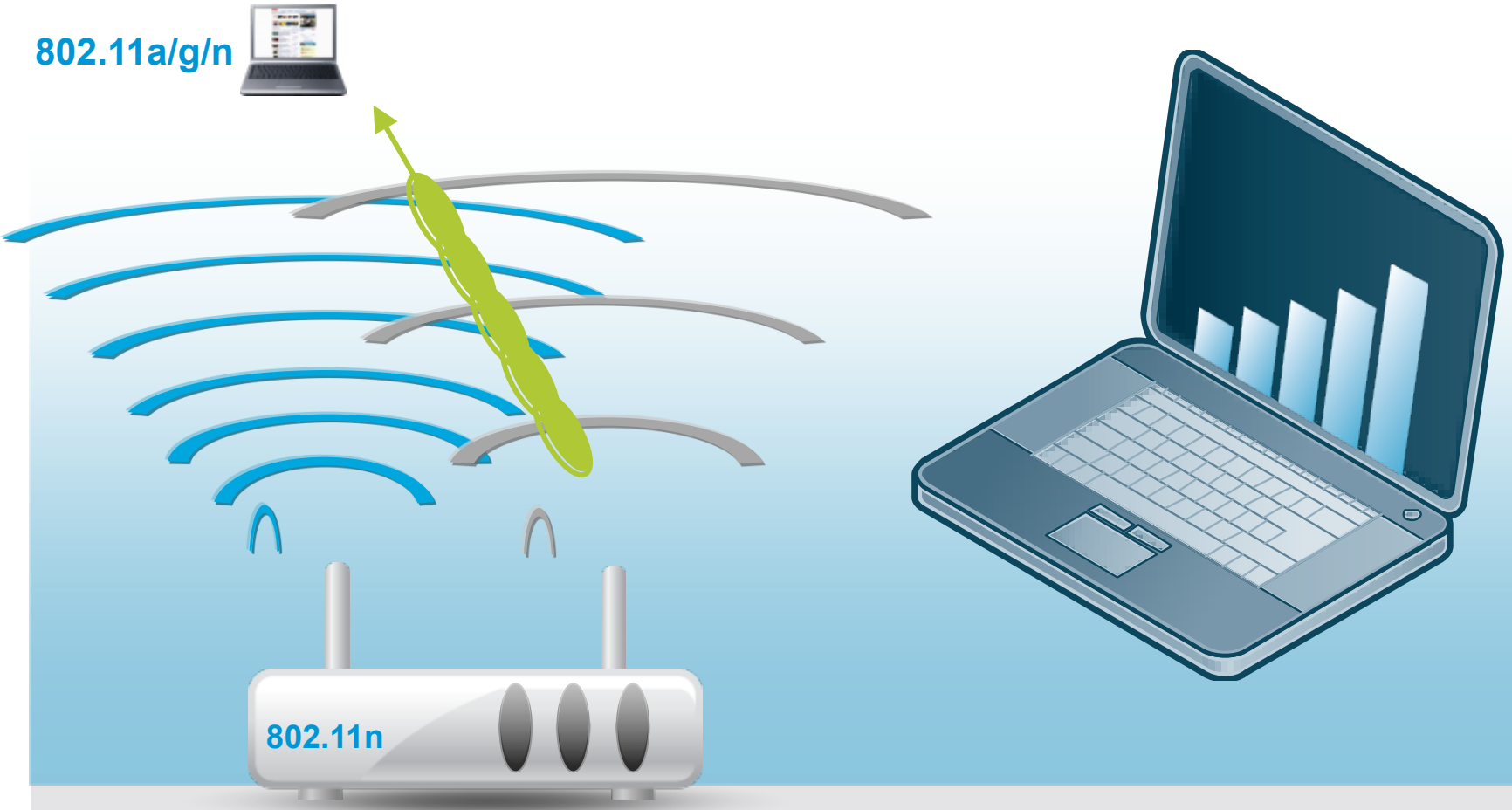


Соединение с 802.11a/g клиентов не оптимально, возможно появление «белых пятен» в радиопокрытии

© 2011 Cisco and/or its affiliates. All rights reserved.

Технология M-Drive с ClientLink

Инновационное решение Cisco : динамическое формирование диаграммы направленности



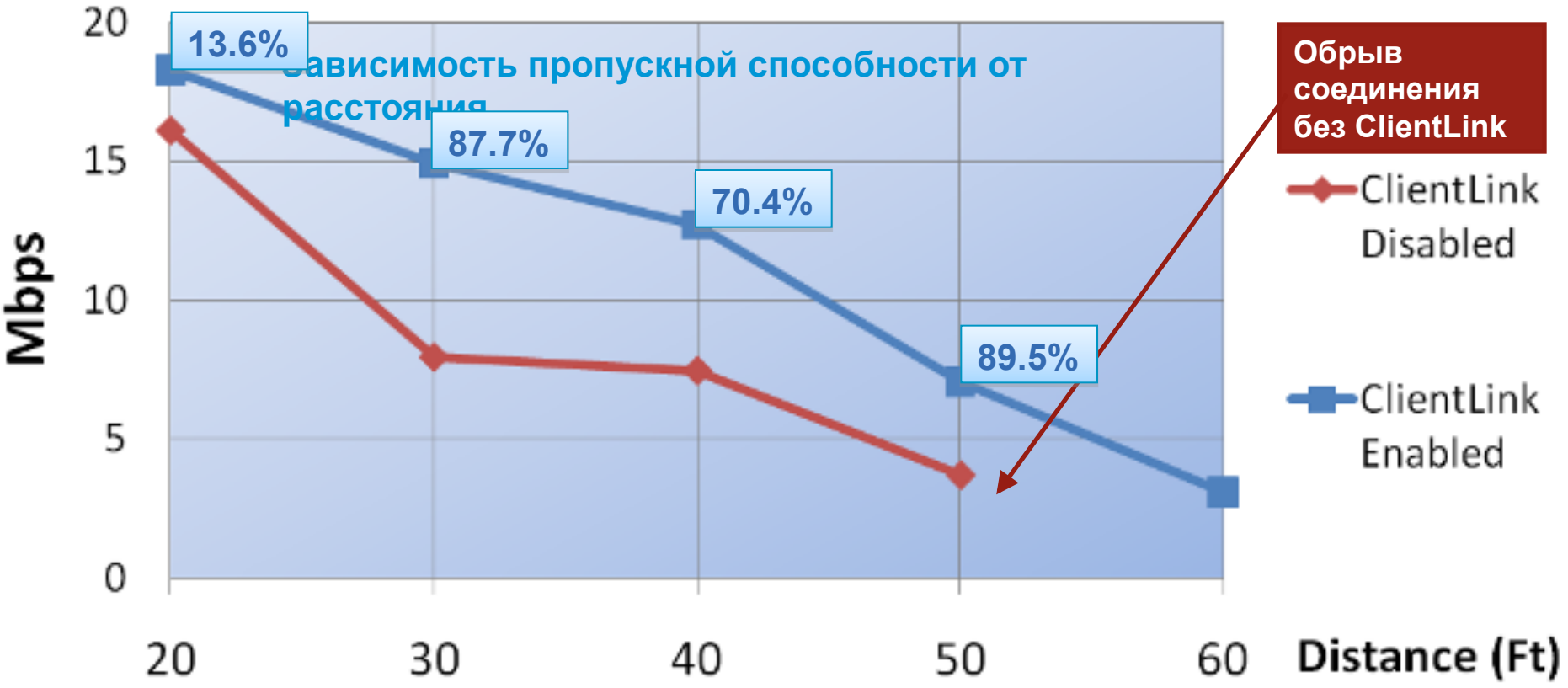
Интеллектуальная технология формирования диаграммы направленности фокусирует радиосигнал на принимающем клиенте, улучшая как производительность, так и качество покрытия для 802.11a/g/n устройств

© 2011 Cisco and/or its affiliates. All rights reserved.

Выгода №1: возрастание пропускной способности 11a/g устройств

Miercom

Увеличение пропускной способности до 65%



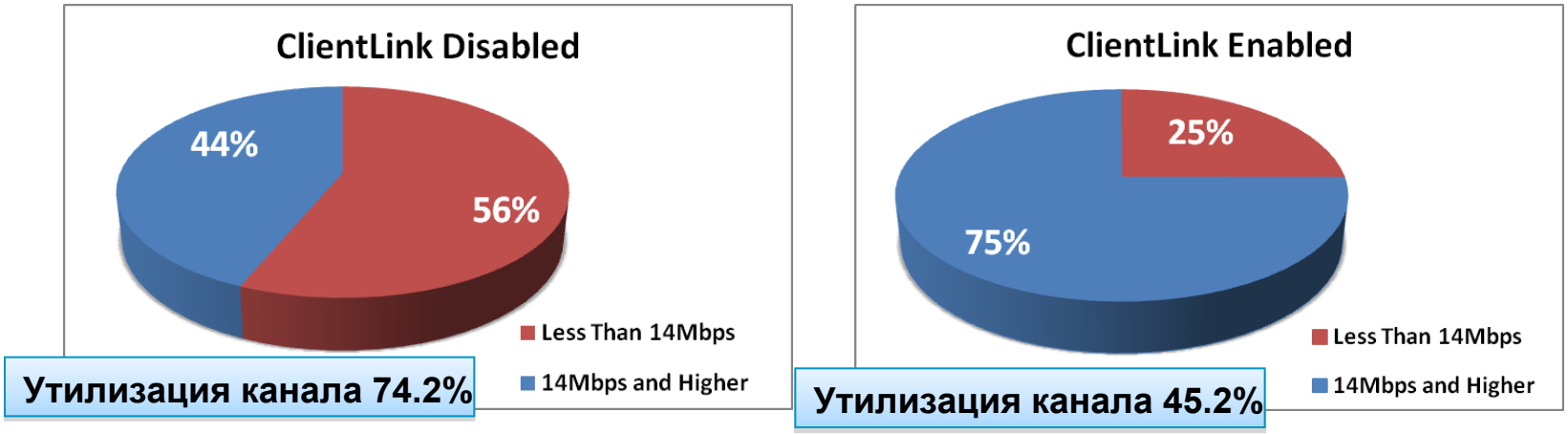
Тест: 802.11a/g устройства с 802.11n сетью
Источник: Miercom

© 2011 Cisco and/or its affiliates. All rights reserved.

Выгода: Увеличение емкости сети

Увеличение емкости канала до 27%

Miercom



- Большая скорость, меньше повторных передач = более эффективное использование радиоканала.
- Большая скорость 11a/g клиентов освобождает время для 11n устройств, тем самым увеличивая их производительность

Тест: производительность 802.11a/g устройства измерена для 16 вариантов положения антенны, сеть 802.11n
Источник: Miercom

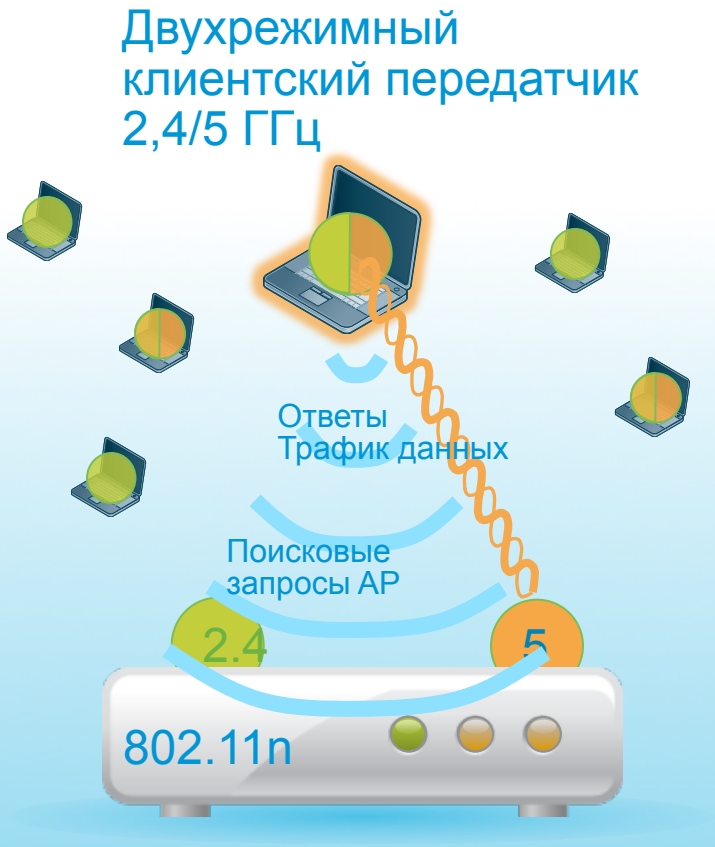
© 2011 Cisco and/or its affiliates. All rights reserved.

Инновационные технологии: BandSelect

© 2011 Cisco and/or its affiliates. All rights reserved.

BandSelect

Управляемый выбор полосы 5 ГГц для точки доступа



Множество двухрежимных клиентов подключаются на частоте 2,4 ГГц

Функция BandSelect позволяет двухрежимным клиентам подключаться на частоте 5 ГГц

Преимущество: оптимизация РЧ-использования

- Повышение эффективности использования диапазона 5 ГГц
- Высвобождение диапазона 2,4 ГГц для однорежимных клиентов

Оптимизация использования эфира за счет вывода клиентов с поддержкой 5 ГГц из каналов 2,4 ГГц

© 2011 Cisco and/or its affiliates. All rights reserved.

Инновационные технологии: VideoStream

© 2011 Cisco and/or its affiliates. All rights reserved.

Xoom, iPad, Galaxy Tab, Droid Charge, Cius & iPhone

© 2011 Cisco and/or its affiliates. All rights reserved.

Видео приложения предприятия

Потоковое видео

Живое вещание
•Обращения руководителей
•Видео-наблюдение

Чем выше качество видео, тем большая полоса пропускания расходуется

Совместная работа

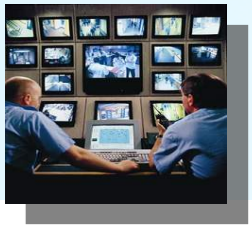
Совещания и обмен опытом
•Видеоконференции

Совместная работа на расстоянии

Видео-записи

Видео по запросу
- Записанные сессии

Увеличение количества приложений порождает множество потоков

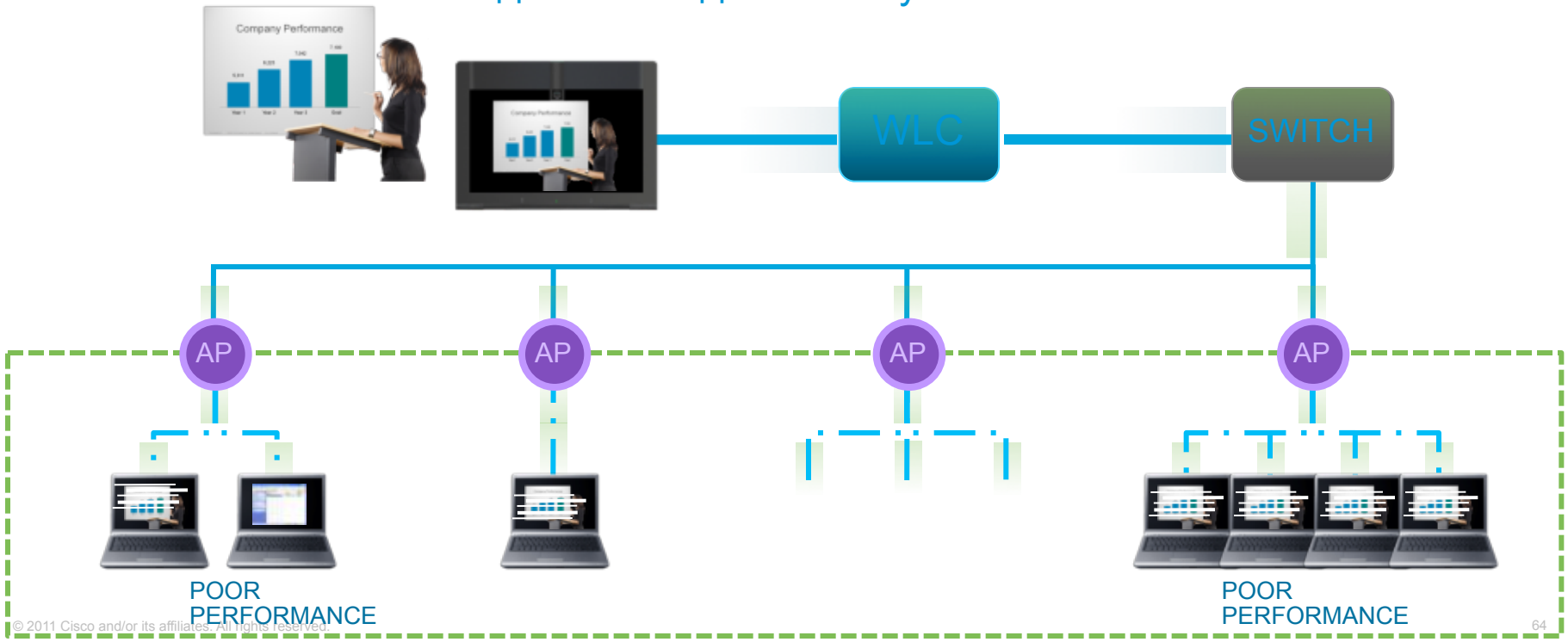


© 2011 Cisco and/or its affiliates. All rights reserved.

Сложности потокового видео
Ограничения радиосреды

- В радиосреде нет понятия мультикаста
- Видео заполняет радиоэфир и вызывает деградацию работы других пиложений – отсутствие качества обслуживания
- Невозможность доставлять видео высокого качества

Видео без надежного мультикаста



© 2011 Cisco and/or its affiliates. All rights reserved.

Технология VideoStream

Cisco VideoStream гарантирует надежную и постоянную доставку видео по беспроводной сети

© 2011 Cisco and/or its affiliates. All rights reserved.

Безопасность радиоэфира

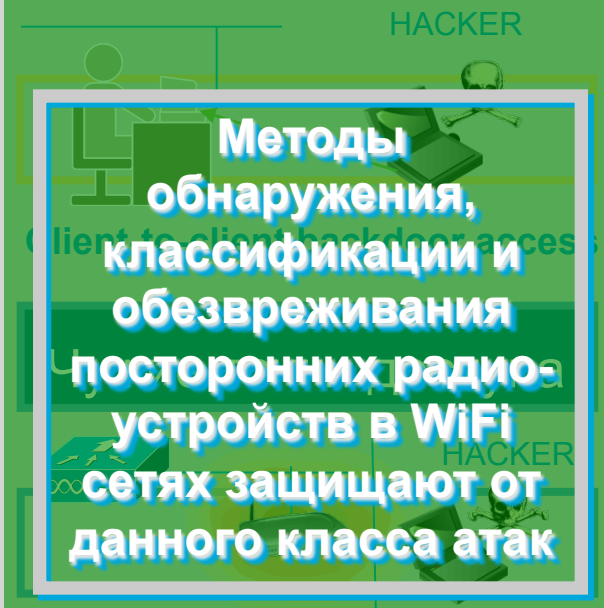
© 2011 Cisco and/or its affiliates. All rights reserved.

Введение

Проникновение в проводную ЛВС

Атаки на Wi-Fi сеть

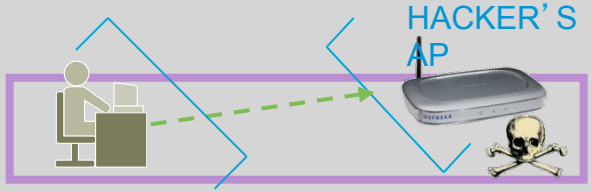
Одноранговые сети



Методы обнаружения, классификации и обезвреживания посторонних радио-устройств в WiFi сетях защищают от данного класса атак

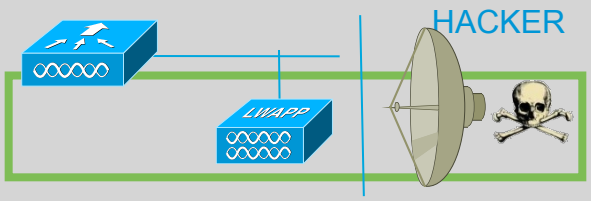
Доступ в ЛВС «с черного хода»

Wi-Fi приманки



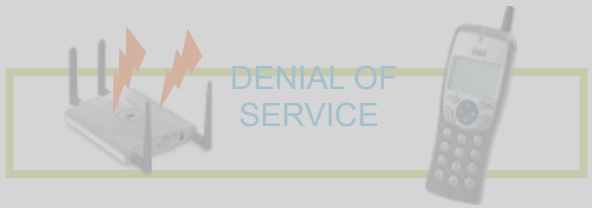
Connection to malicious AP

Разведывательные



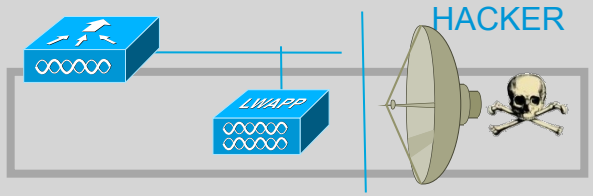
Seeking network vulnerabilities

Denial of Service



Service disruption

Взломы



Sniffing and eavesdropping

© 2011 Cisco and/or its affiliates. All rights reserved.

Посторонние устройства в корпоративных WiFi-сетях

Обнаружение, Классификация, Обезвреживание

© 2011 Cisco and/or its affiliates. All rights reserved.

Посторонние Wi-Fiустройства в корпоративных сетях

- Что относится к посторонним устройствам (ПУ) ?
  - Любое WiFi-устройство, находящееся в зоне радиовидимости нашей сети, которым мы не управляем
  - Большинство ПУ устанавливаются авторизованными пользователями (низкая цена, удобство, безграмотность)
- Когда ПУ опасны ?
  - Когда они обнаруживаются в проводном сегменте ЛВС
  - Одноранговые (ad-hoc) сети ПУ тоже могут представлять угрозу !
  - Когда установлены сторонними пользователями преднамеренно с целью злого умысла
- Что необходимо сделать?
  - Обнаружить [Detect]
  - Классифицировать (over-the-air и on-the-wire) [Classify]
  - Обезвредить (Shutdown, Contain, и т.д.) [Mitigate]

© 2011 Cisco and/or its affiliates. All rights reserved.

Примеры посторонних устройств

Сценарий 1:

Сотрудник приносит домашнюю точку доступа с целью организовать Wi-Fi в своем кабинете.

Точка доступа, не обладая богатым функционалом безопасности, включается в проводной сегмент сети.

Угроза:

«Легкая добыча» для злоумышленника. Обойдя слабые методы защиты, он подключается по WiFi к это точке доступа и автоматически попадает в проводную сеть организации.

© 2011 Cisco and/or its affiliates. All rights reserved.

Примеры посторонних устройств

Сценарий 2:

Департамент IT закупил несколько десятков сетевых принтеров и подключил их к сети организации.

Данные принтеры имеют Wi-Fi сетевую карту, которая включена по умолчанию и имеет базовые настройки безопасности.

Угроза:

Открытая дверь в сеть для любого злоумышленника через беспроводной интерфейс принтера.

© 2011 Cisco and/or its affiliates. All rights reserved.

Примеры посторонних устройств

Сценарий 3:

Компьютер сотрудника по умолчанию имеет включенный Wi-Fi интерфейс.

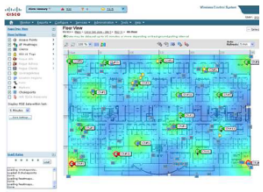
Угроза:

Злоумышленник может установить одноранговое Wi-Fi соединение с таким компьютером (типа точка-точка), скомпрометировать его, завладеть секретной информацией или же доступом к другим ресурсам организации.

© 2011 Cisco and/or its affiliates. All rights reserved.

Интегрированный комплекс безопасности Wi-Fi эфира

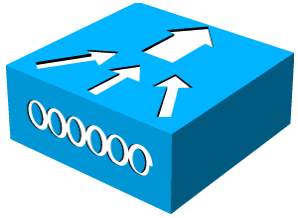
Capacity Management



RF Management

Security Management

Network Control System



Cisco WLC контроллер

Сервисы:

- Местоположение
- Безопасность
- Историческая отчетность

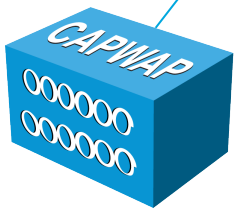
Проводная сеть

MSE

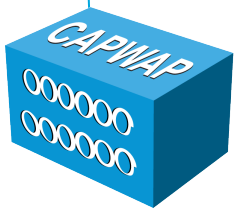
Безопасная радиосреда

Определение местоположения

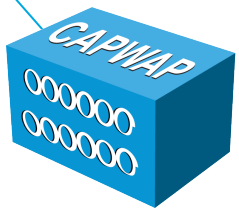
Централизированное управление



Monitor Mode AP



Monitor Mode AP



Rogue Detector

Точки доступа

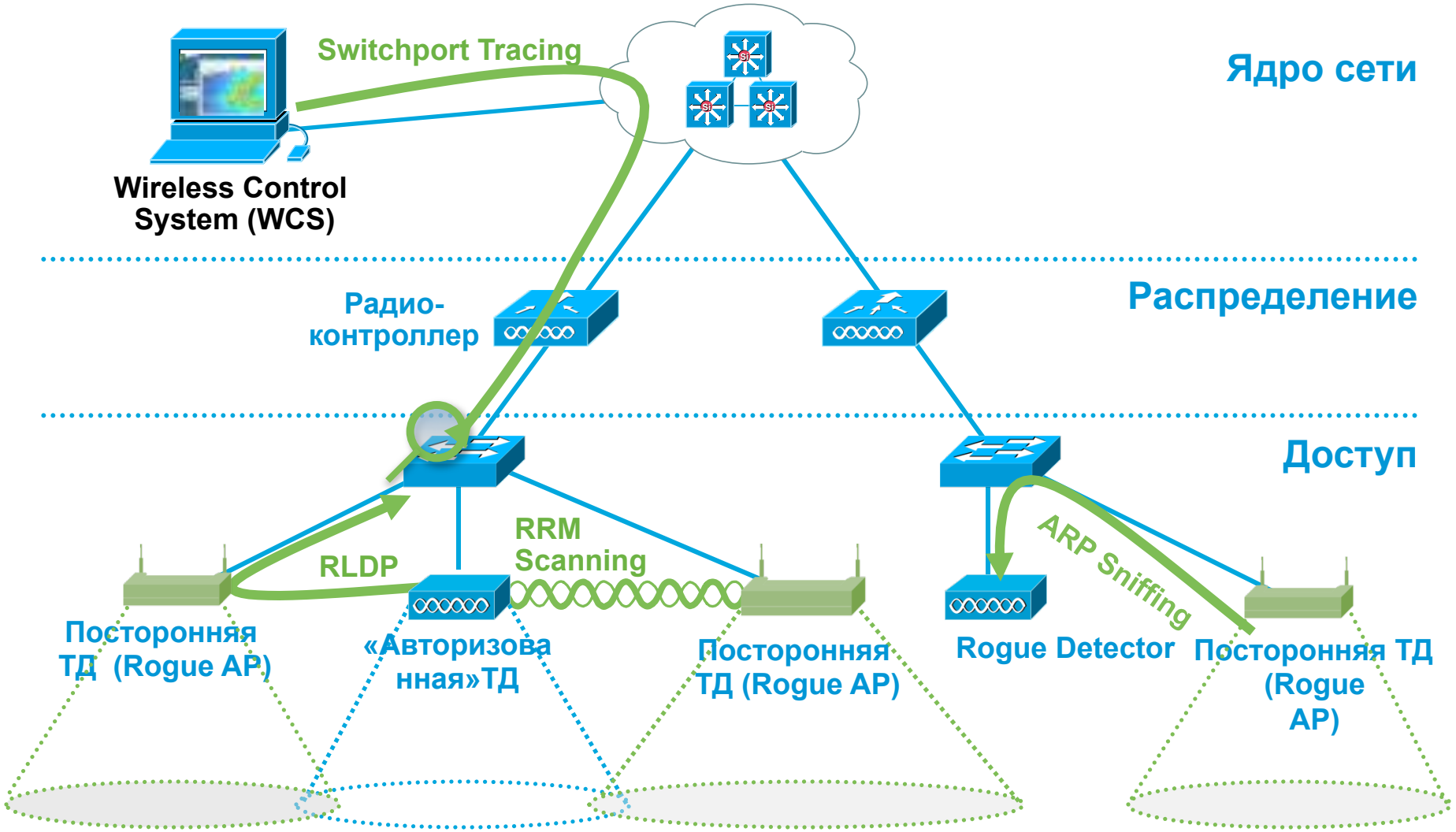
© 2011 Cisco and/or its affiliates. All rights reserved.

Этапы борьбы с посторонними Wi-Fi устройствами в корпоративных сетях

Обнаружение	Классификация	Обезвреживание
• обнаружение неинфраструктурных точек доступа (ТД), клиентов и одноранговых (ad-hoc) подключений • Обнаружение ПУ стандарта 802.11n	• Правила классификации ПУ, основанные на RSSI, SSID, клиентах и т.д. • Проверка нахождения ПУ в проводном сегменте ЛВС • Switch port tracing	• Отключение (shutdown) порта на коммутаторе • Обнаружение местоположения • Изоляция (containment) нарушителей в радио-эфире

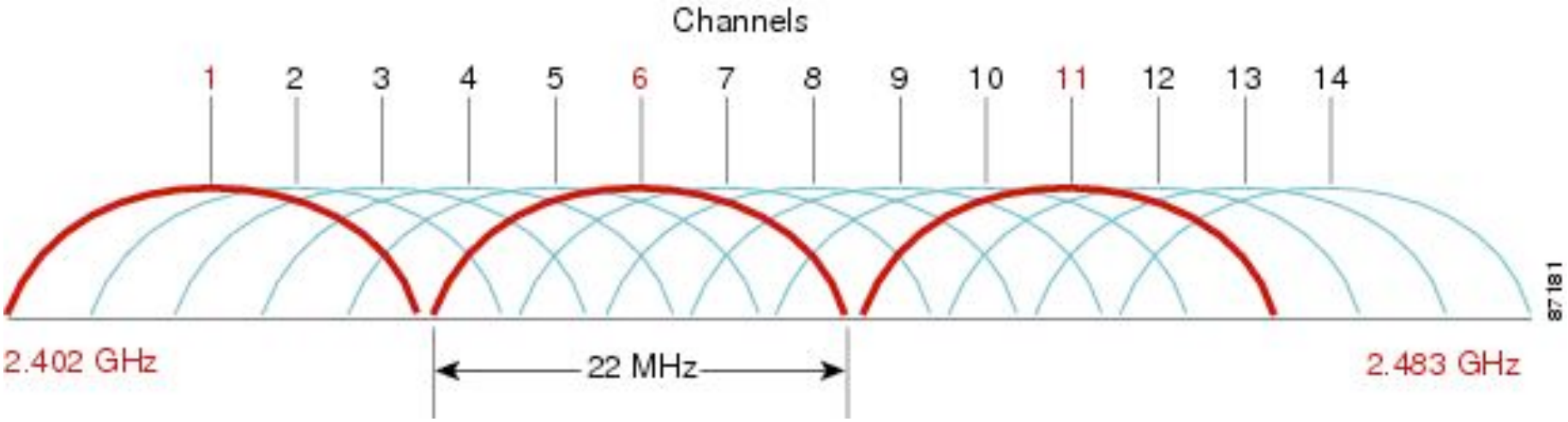
© 2011 Cisco and/or its affiliates. All rights reserved.

Схема борьбы с ПУ
Множество методов



© 2011 Cisco and/or its affiliates. All rights reserved.

Wi-Fi частоты в диапазоне 2.4Ghz

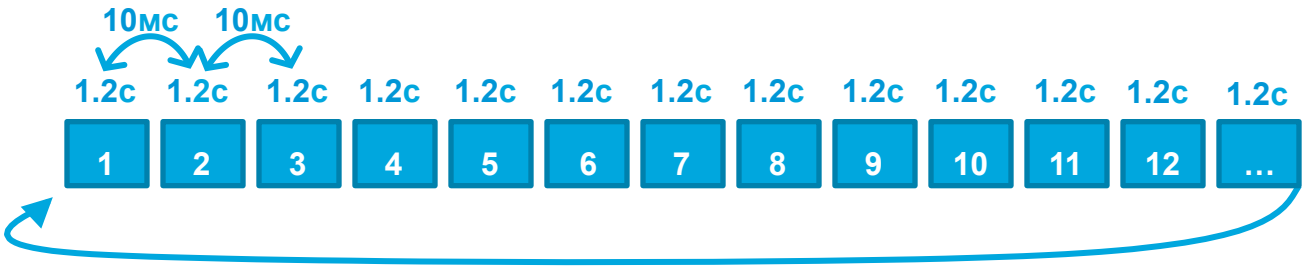


© 2011 Cisco and/or its affiliates. All rights reserved.

РЧ-алгоритм сканирования каналов
точка доступа в режиме Monitor Mode

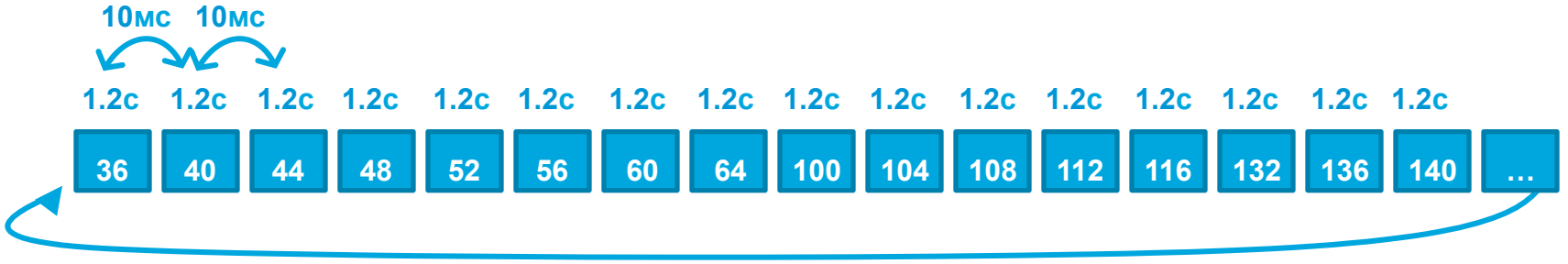
Detect

802.11b/g/n – Все каналы



- Общее время сканирования каждого канала ~10.7с ((180с / 1.2с) / 14кан) за период 180с

802.11a/n – Все каналы



- Общее время сканирования каждого канала ~6.8с ((180с / 1.2с) / 22кан) за период 180с

© 2011 Cisco and/or its affiliates. All rights reserved.

Правила классификации ПУ
Принцип

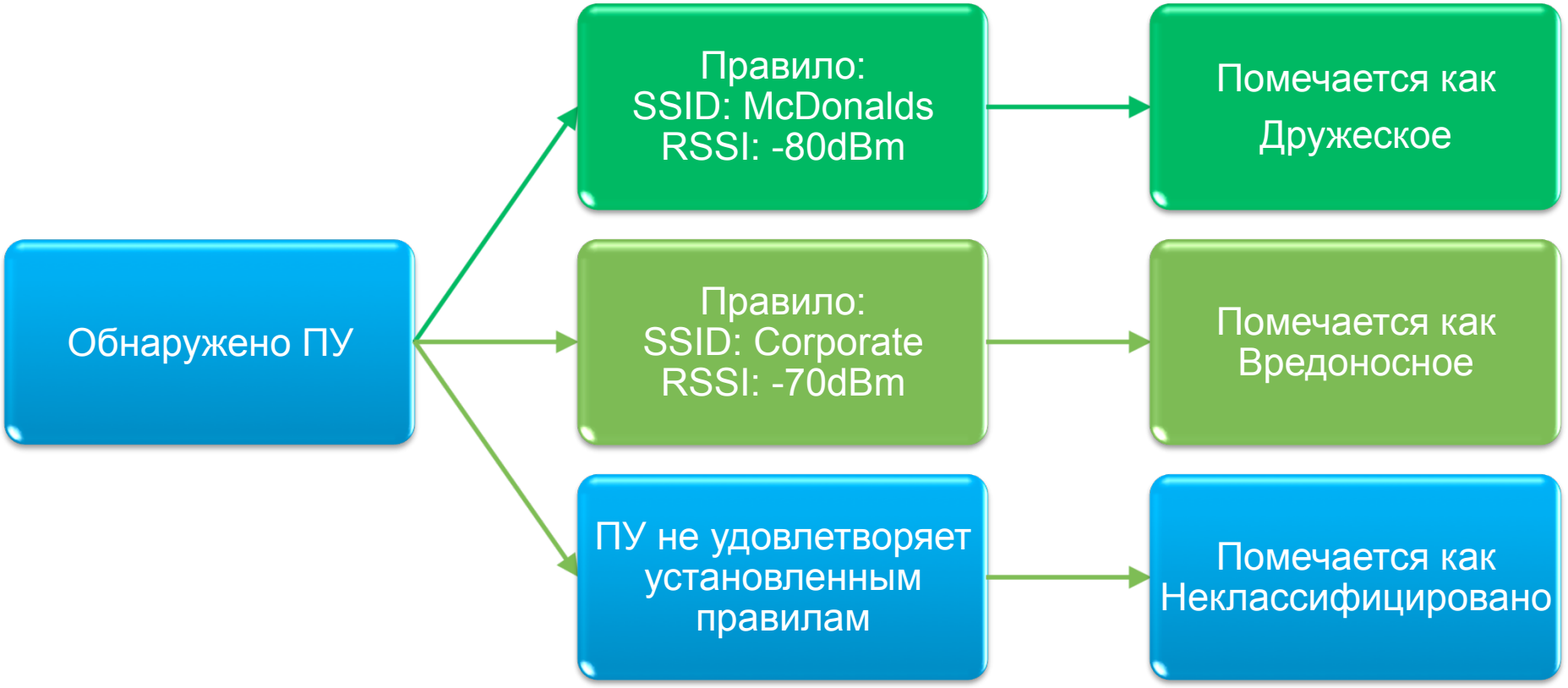
- **Классификация основана на степени опасности угрозы и действиях по обезвреживанию**
- **Правила классификации соотносятся с моделью рисков заказчика**

Низкий уровень → Высокий уровень

Вне сети	Внутри сети
Защищенный SSID	Открытый SSID
Неизвестный SSID	«наш» SSID
Слабый RSSI	Сильный RSSI
Удаленное расположение	На территории КЛВС
Нет клиентов	Привлекает клиентов

© 2011 Cisco and/or its affiliates. All rights reserved.

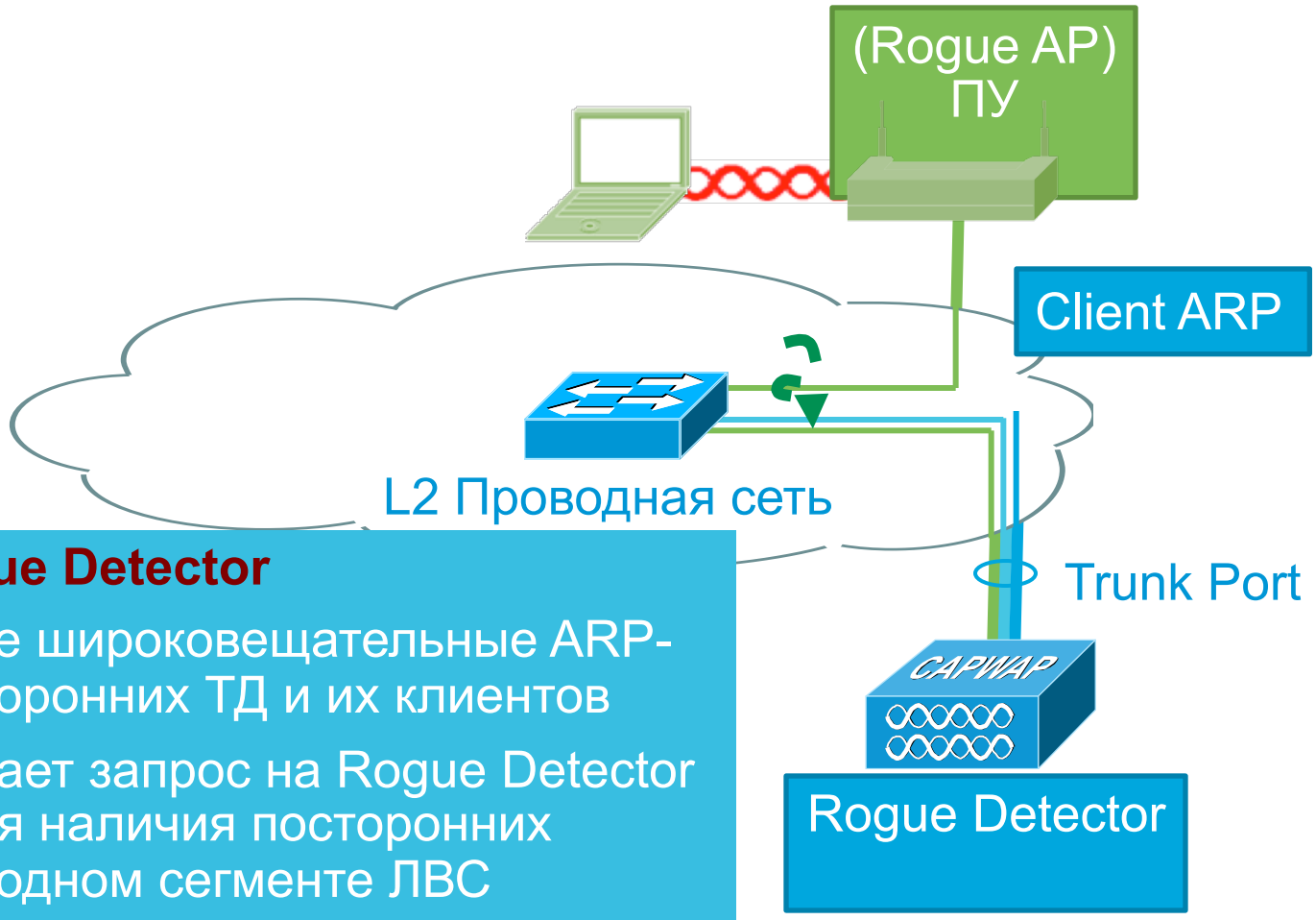
Правила классификации ПУ
Пример



Правила хранятся и выполняются на радио-контроллере

© 2011 Cisco and/or its affiliates. All rights reserved.

ТД в режиме Rogue Detector
Принципиальная схема работы



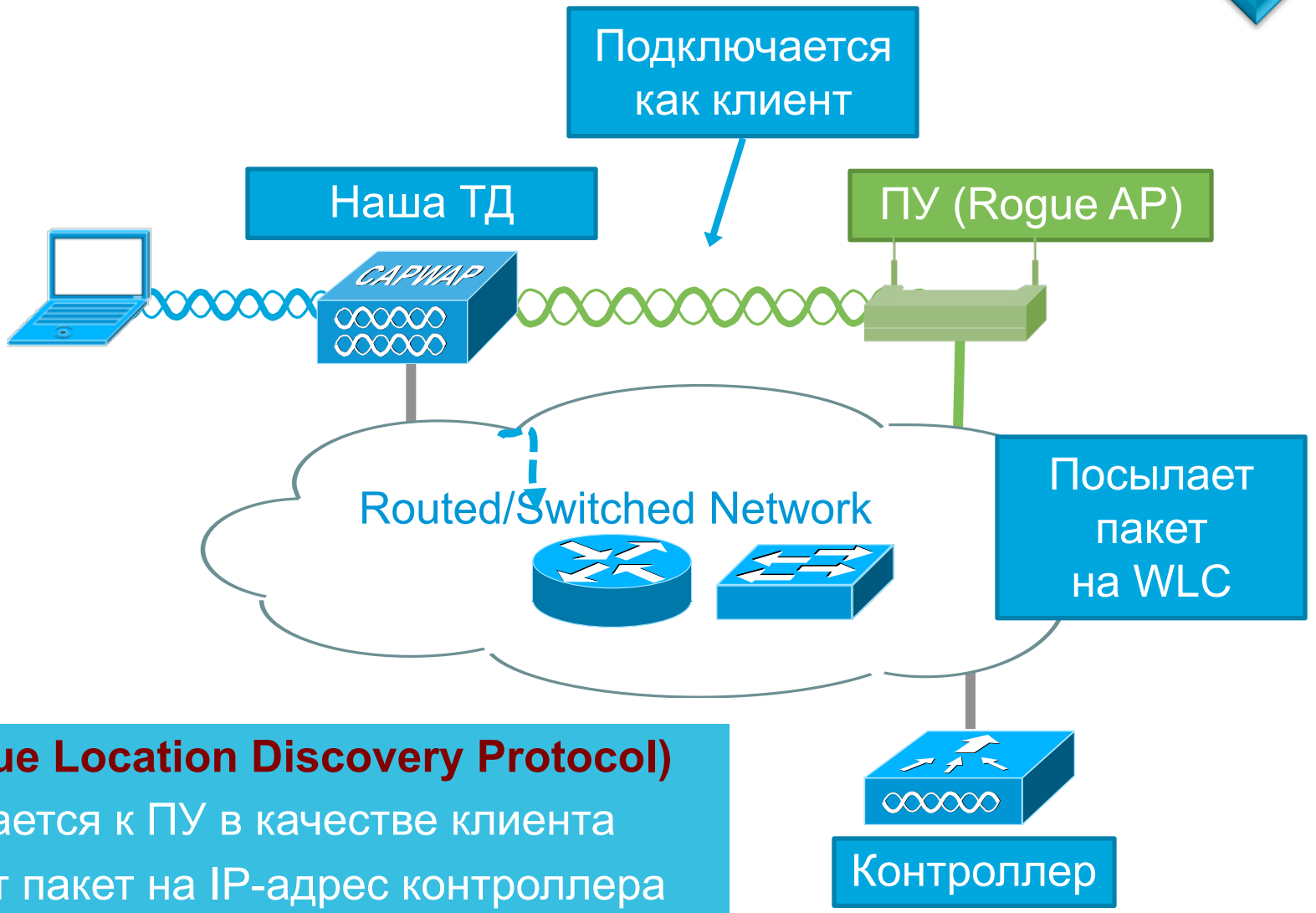
ТД в режиме Rogue Detector

- Отслеживает все широковещательные ARP-запросы от посторонних ТД и их клиентов
- Контроллер делает запрос на Rogue Detector для определения наличия посторонних клиентов в проводном сегменте ЛВС
- Не работает если посторонняя ТД настроена как NAT AP

Rogue Location Discovery Protocol

Принципиальная схема работы

Classify

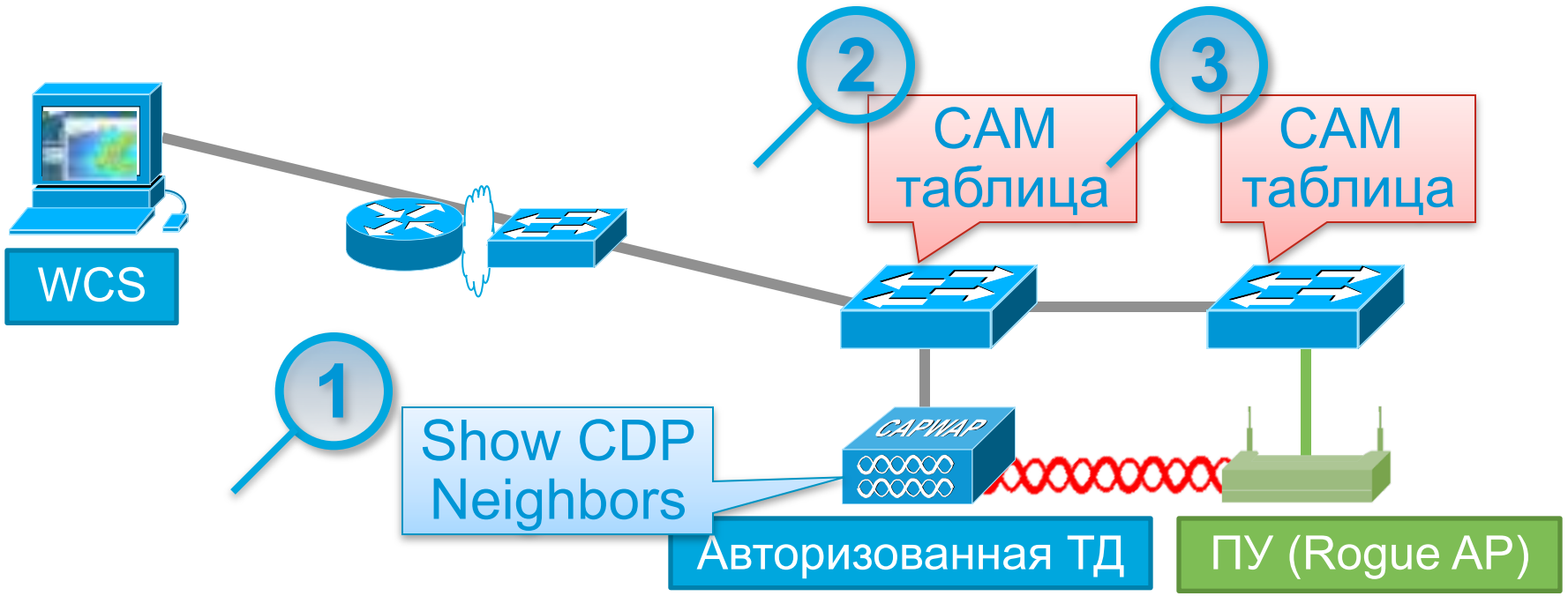


RLDP (Rogue Location Discovery Protocol)

- Подключается к ПУ в качестве клиента
- Посылает пакет на IP-адрес контроллера
- Работает только для ПУ с open SSID

© 2011 Cisco and/or its affiliates. All rights reserved.

Нахождение порта подключения
Принципиальная схема работы

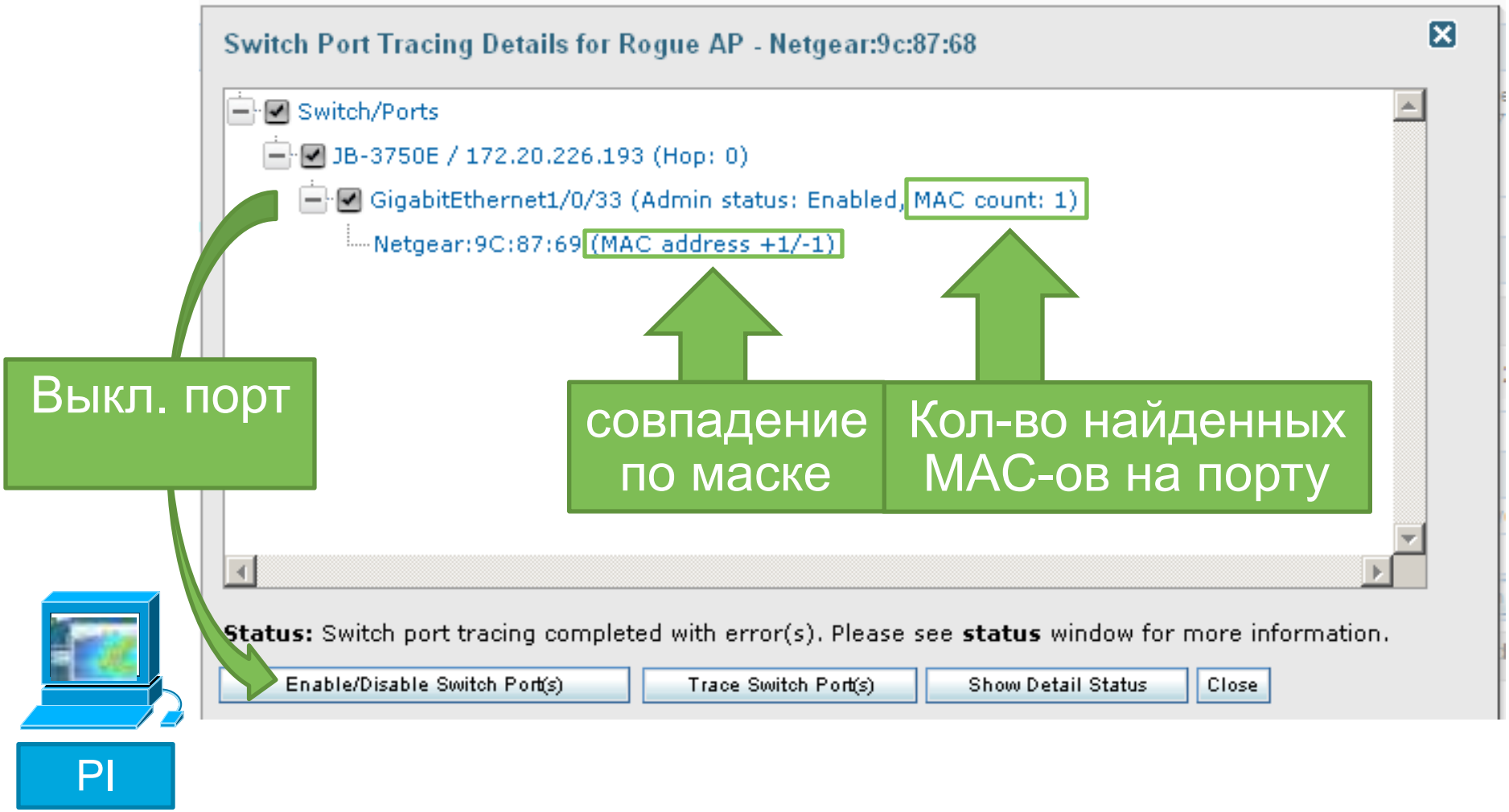


Cisco Prime Switchport Tracing

- Определяет CDP Neighbors для ТД, которая обнаружила ПУ
- Просматривает CAM-таблицы коммутаторов на предмет наличия в них mac-адресов ПУ или ПУ-клиентов
- Работает для ПУ с настройками Security и NAT

Cisco Prime Infrastructure Switchport Tracing

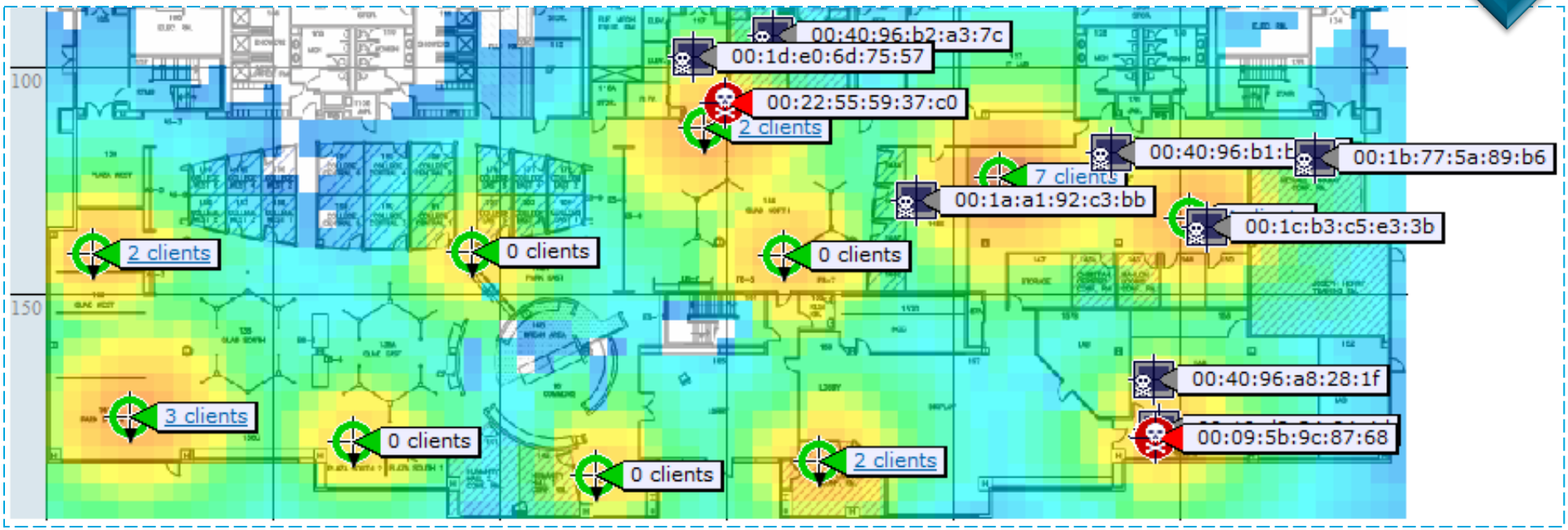
Как работает



© 2011 Cisco and/or its affiliates. All rights reserved.

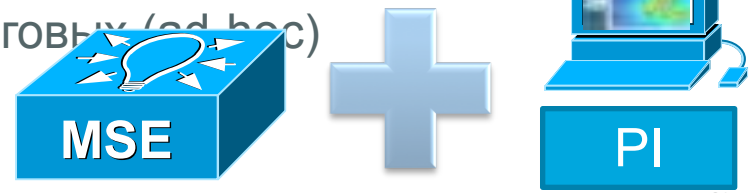
Определение местоположения ПУ
В реальном времени при помощи Cisco Prime и MSE

Mitigate



- Отслеживание множества ПУ в реальном времени (до лимитов определенных MSE)
- Хранение журнала с историей перемещений
- Отслеживание местоположения клиентов ПУ
- Отслеживание местоположения одноранговых (ad-hoc) подключений

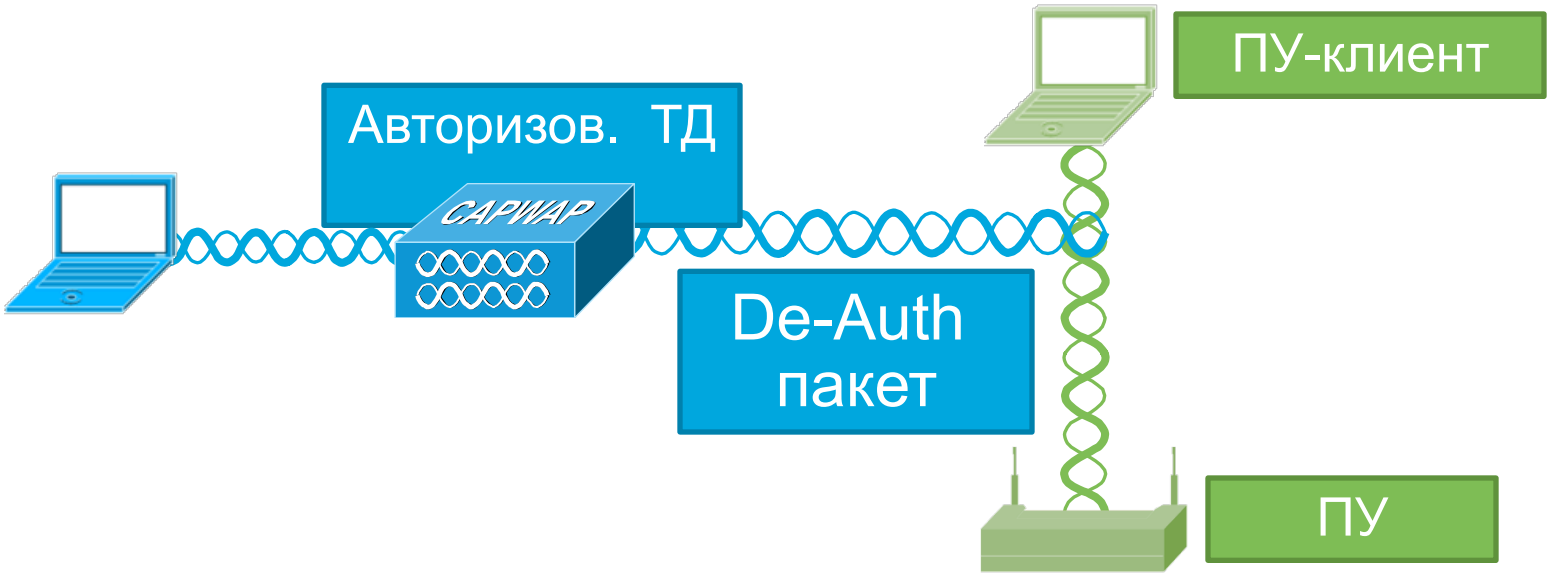
Rogue APs
Rogue Adhocs
Rogue Clients



© 2011 Cisco and/or its affiliates. All rights reserved.

Изоляция ПУ
Принципиальная схема работы

Mitigate

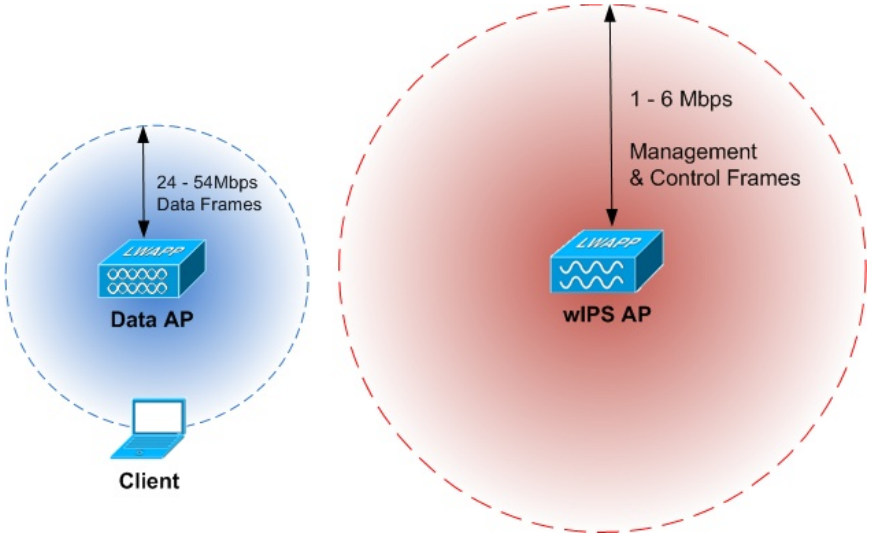


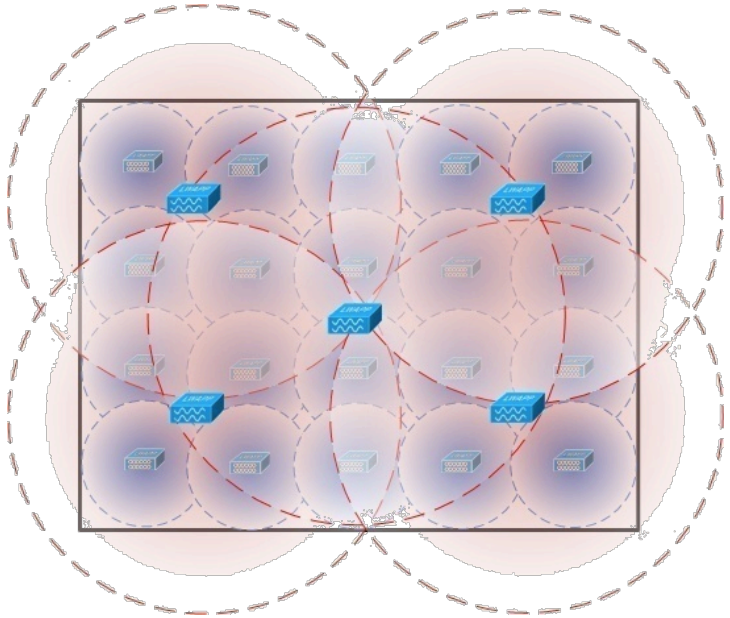
Изоляция посторонней точки доступа

- Посылка De-Authentication пакетов клиенту и ТД
- Возможность использования ТД в режимах Local Mode, Monitor Mode и H-REAP

© 2011 Cisco and/or its affiliates. All rights reserved.

ТД в Monitor Mode: радиус действия, размещение и плотность





Радиус действия

размещение, плотность

- **ТД в wIPS Monitor-mode не обслуживают клиентов, таким образом радиус их действия может быть шире**
  - **ТД обслуж. клиентов обычно покрывает 270-450 м2**
  - **wIPS ТД покрывает 1350–3150 м2**
- **Соотношение ТД wIPS monitor-mode к ТД local-mode зависит от дизайна сети, но можно предварительно исходить из соотношения 1:5**
- **wIPS ТД могут одновременно работать на обнаружение атак и опред. коорд.**
- **Cisco радио-управление обеспечив. максимальное покрытие**

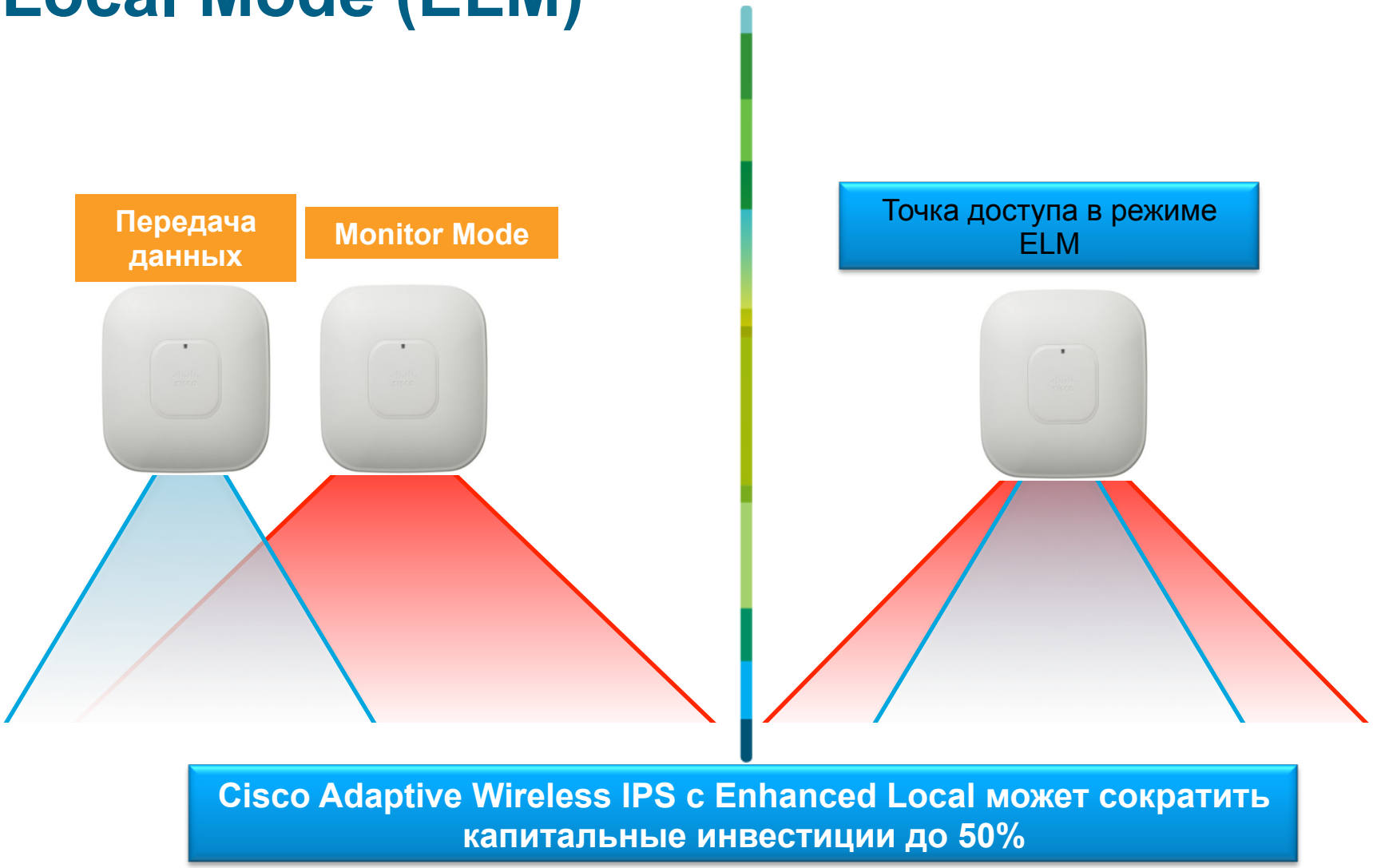
Сколько wIPS ТД необходимо ?

- Выбирается необходимый ‘security confidence level’
  - «Золотой»– Банки, Гос. учреждения, Retail
  - «Серебряный» – Предприятия
  - «Бронзовый» – Только для 2.4GHz
- Оценивается общий размер площади покрытия
  - Делим на рекомендуемую площадь (пример 18000 м2 / 1350 м2)
- Примеры:

Место размещ.	Размер	Уровень	Плотность	# ТД wIPS
Банковский офис	18000 м2	Золотой	1350м2	14
Офис предприятия	18000м2	Серебряный	1800м2	10
Склад	18000м2	Серебряный	2700м2	5

© 2011 Cisco and/or its affiliates. All rights reserved.

Определение ПУ с помощью Enhanced Local Mode (ELM)

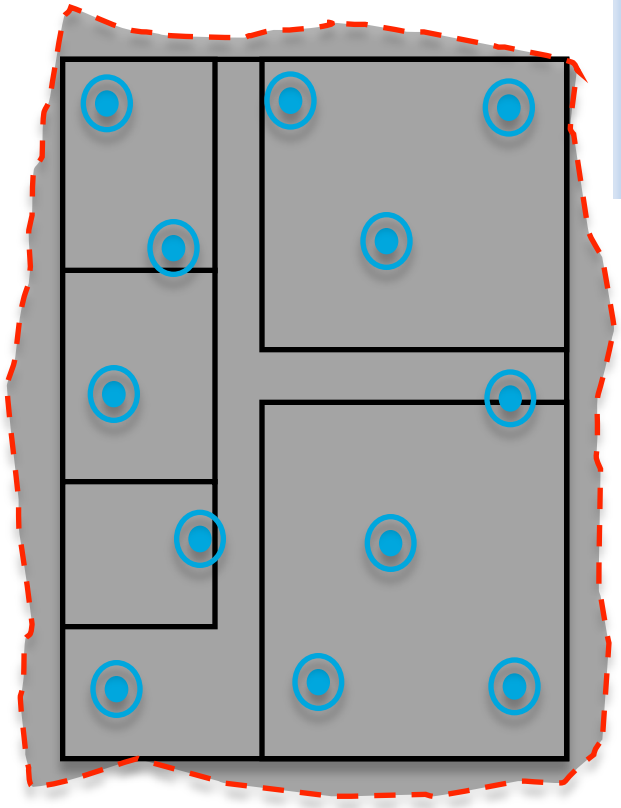


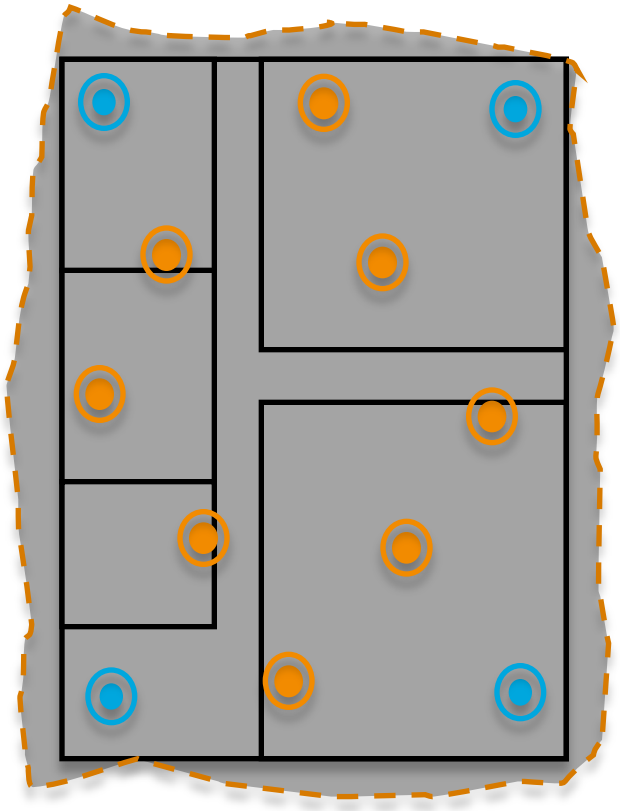
Cisco Adaptive Wireless IPS с Enhanced Local может сократить капитальные инвестиции до 50%

© 2011 Cisco and/or its affiliates. All rights reserved.

Определение ПУ с помощью Enhanced Local Mode (ELM)

PCI Requirement	
11.1	Identify rogue and unauthorized wireless devices





Cisco ELM AP

Cisco Monitor Mode AP

Cisco Data AP

© 2011 Cisco and/or its affiliates. All rights reserved.

А что если?

Сценарий:

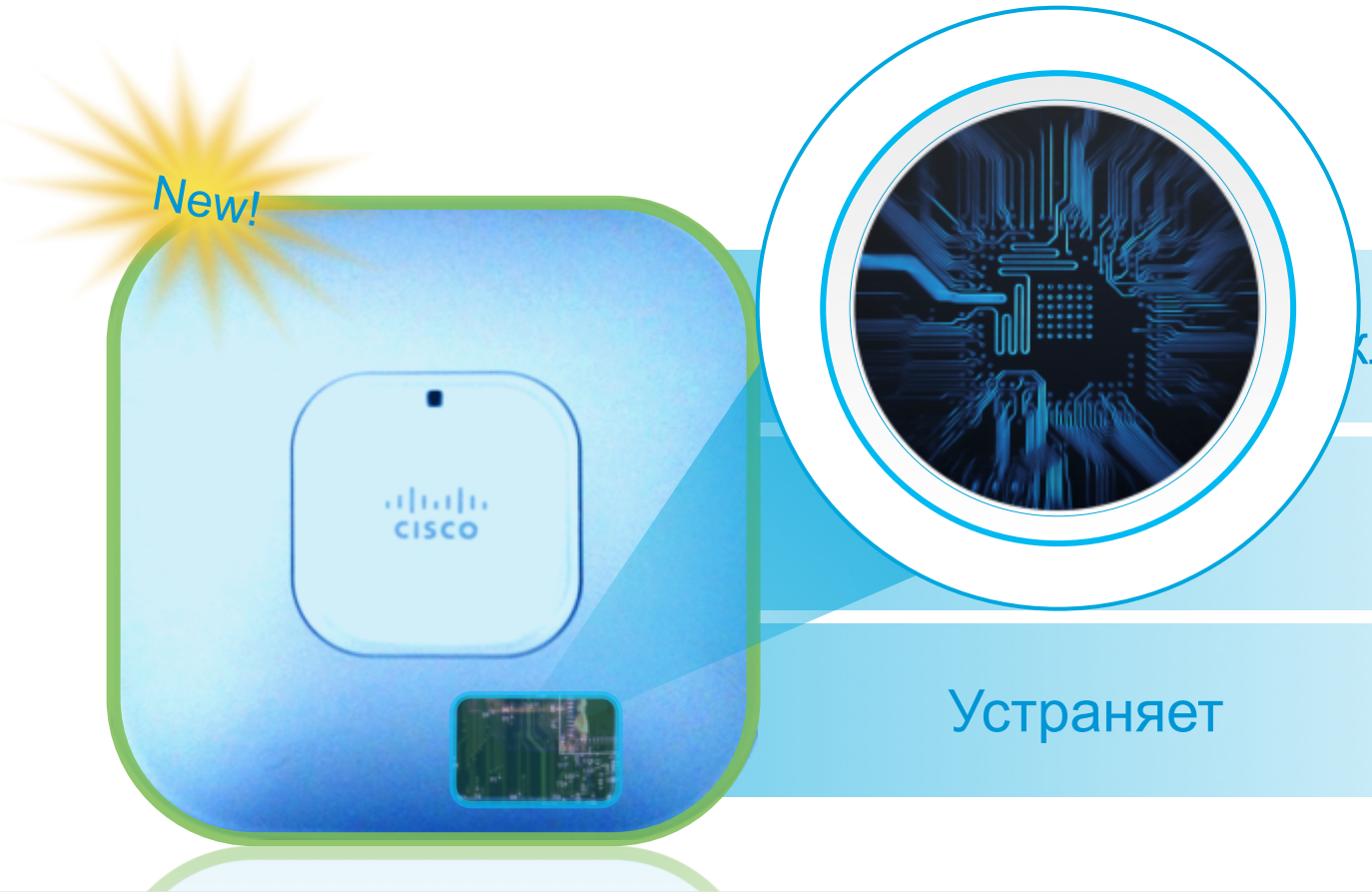
Злоумышленник использует точку доступа с прошивкой, которая использует нестандартные диапазоны частот?

Угроза:

Стандартные механизмы Wi-Fi безопасности не способны распознать такую активность.

© 2011 Cisco and/or its affiliates. All rights reserved.

Представляем CleanAir



классифицирует

Устраняет

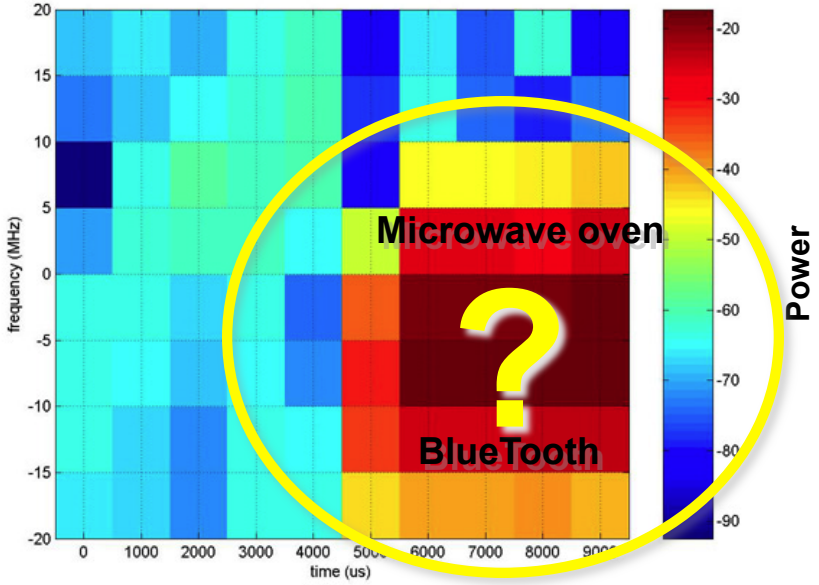
Cisco CleanAir

Обнаруживает нестандартные источники помех и угрозы

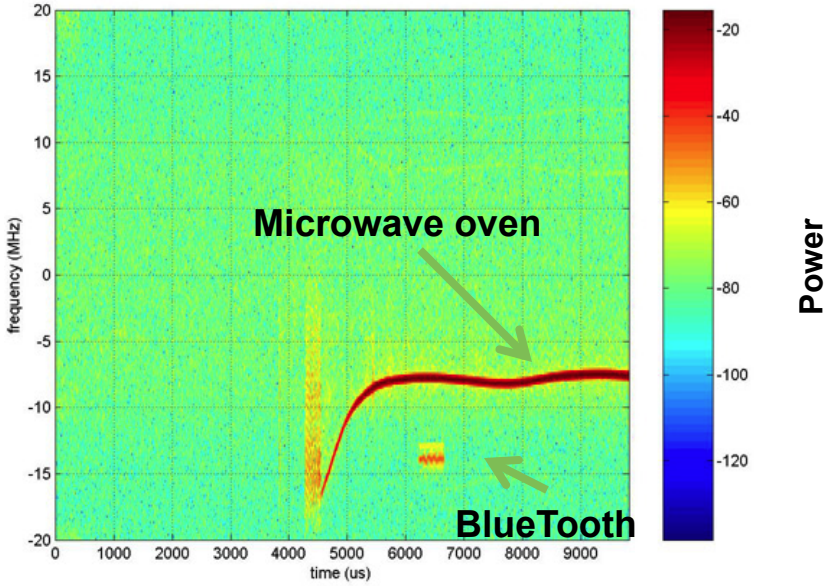
Высокое разрешение спектра

Спектральный анализ высокого разрешения

Типичный Wi-Fi чипсет
Дискретность разрешения 5 MHz



Cisco CleanAir Wi-Fi чипсет
Спектральное разрешение
78 to 156 KHz



© 2011 Cisco and/or its affiliates. All rights reserved.

Противодействие атакам на беспроводную сеть

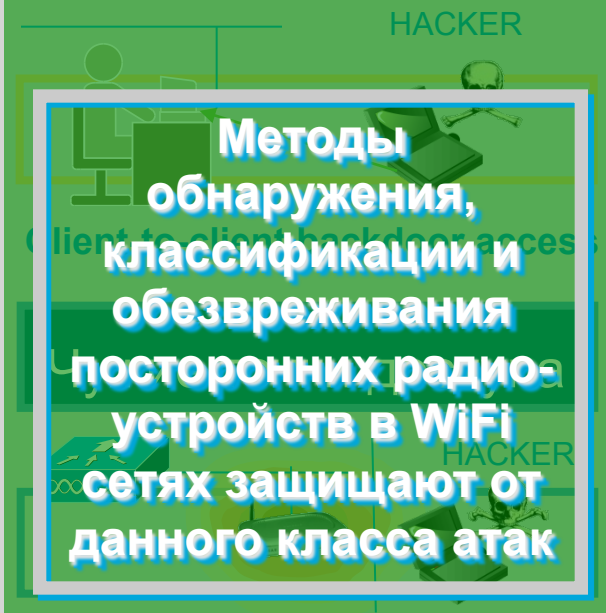
© 2011 Cisco and/or its affiliates. All rights reserved.

Атаки на Wi-Fi сеть

Проникновение в проводную ЛВС

Атаки на Wi-Fi сеть

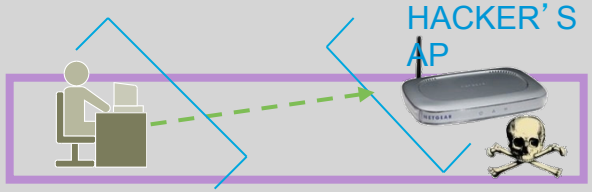
Одноранговые сети



Методы обнаружения, классификации и обезвреживания посторонних радио-устройств в WiFi сетях защищают от данного класса атак

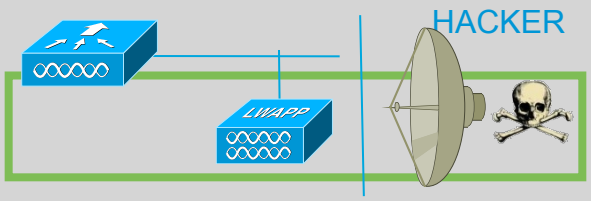
Доступ в ЛВС «с черного хода»

Wi-Fi приманки



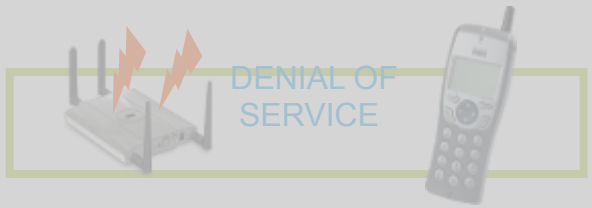
Connection to malicious AP

Разведывательные



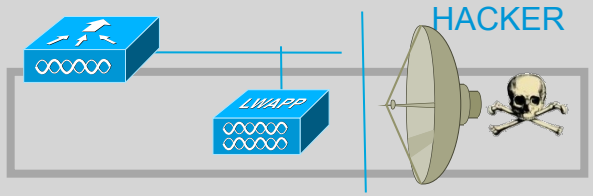
Seeking network vulnerabilities

Denial of Service



Service disruption

Взломы



Sniffing and eavesdropping

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco-алгоритмы обнаружения атак

Базовая IDS

- Встроено в ПО контроллера
- Использует ТД в режимах Local Mode и Monitor Mode

Адаптивная wIPS

- Требует MSE
- Использует ТД в режиме wIPS Monitor Mode

© 2011 Cisco and/or its affiliates. All rights reserved.

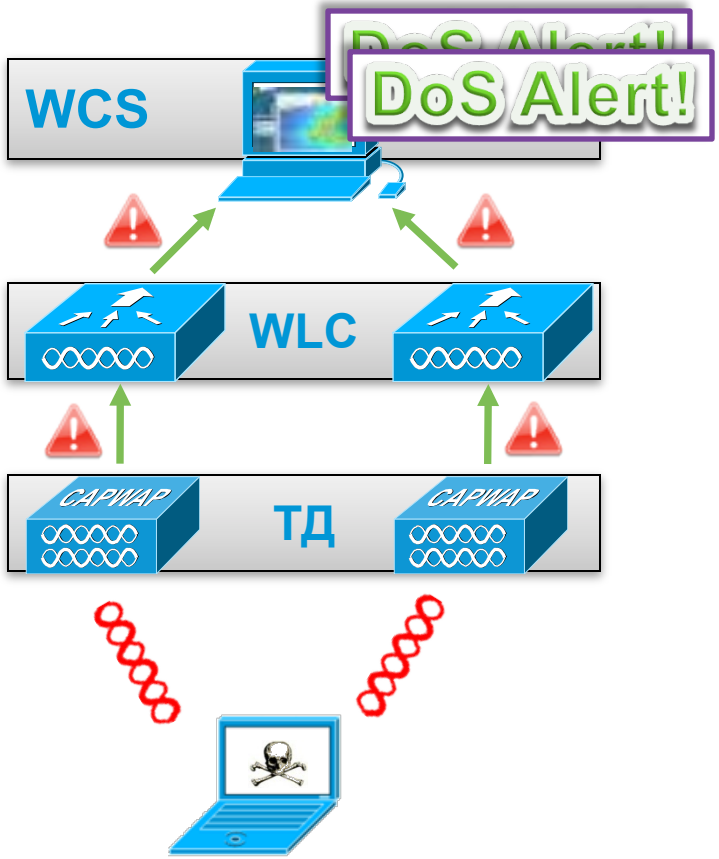
Отличия адаптивной wIPS от базовой IDS радио-контроллера

Корреляция сигналов тревоги	• Меньше ложных сигналов тревоги
Число атак	• Только 17 в базовой IDS контроллера
Криминалистика (Forensics)	• Захват пакетов атаки
Историческая отчетность	• Больше глубина архива

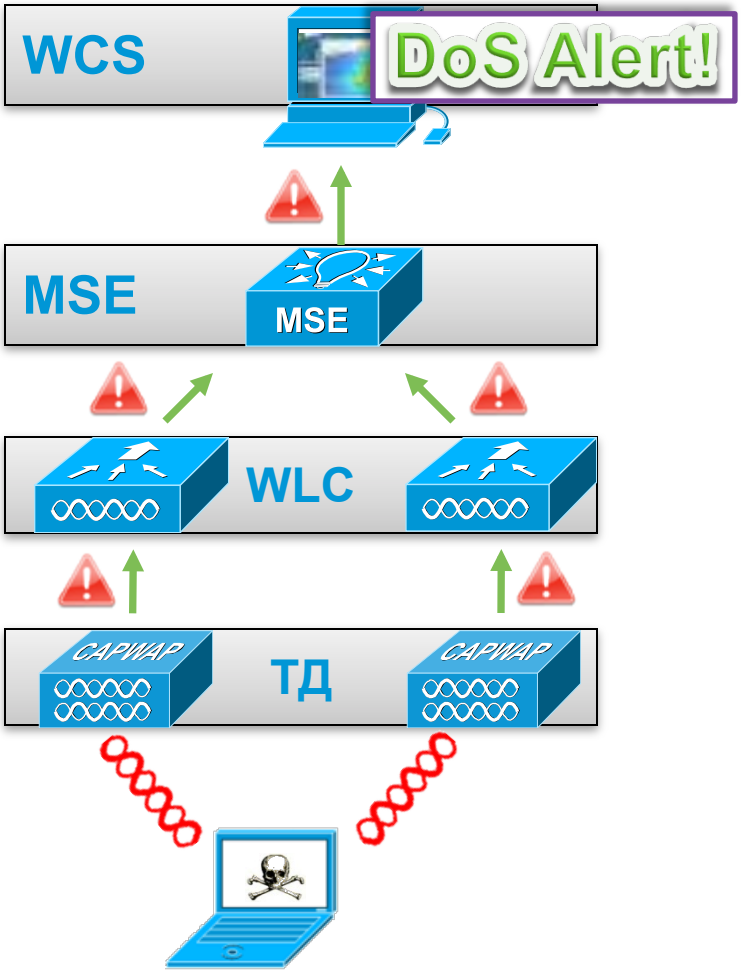
© 2011 Cisco and/or its affiliates. All rights reserved.

Адаптивная wIPS Отличие #1
Аггрегация и корреляция сигналов тревоги

Базовая IDS контроллера



Адаптивная wIPS



- Нет корреляции сигналов тревоги

© 2011 Cisco and/or its affiliates. All rights reserved.

Защита от DoS-аттак

© 2011 Cisco and/or its affiliates. All rights reserved.

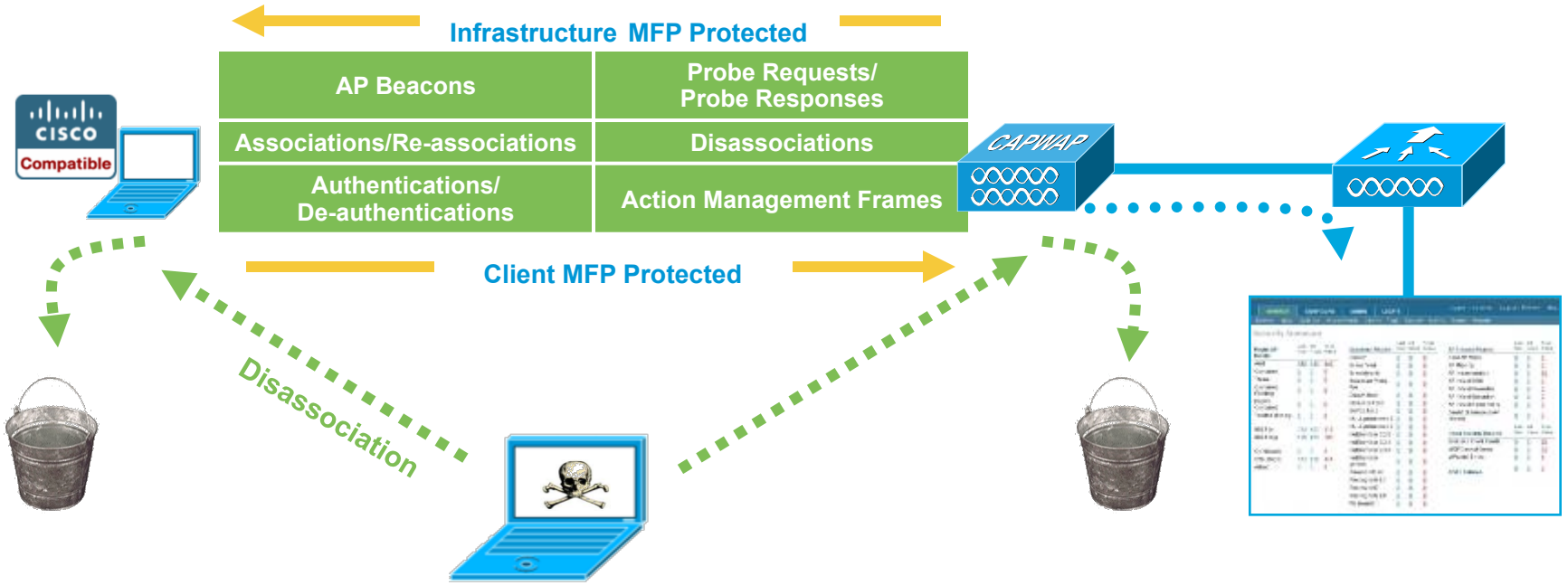
Защита кадров управления
Концепция

Проблема

- Кадры управления БЛВС не аутентифицируются, не шифруются и не подписываются
- Они - типичное направление атаки

Решение

- Вствить сигнатуру (Message Integrity Code/MIC) в кадры управления
- Клиенты и ТД используют MIC для проверки аутентичности кадров управления (КУ)
- ТД могут сразу же выявить постороннние/подмененные КУ



© 2011 Cisco and/or its affiliates. All rights reserved.

Польза от защиты кадров управления

- Защита от атак: от посторонних ТД, атак типа «посредник», других атак на кадры управления

  Увеличивает качество обнаружения посторонних ТД и использования IDS-сигнатур

- Предотвращение атак: Поддерживается на клиентах, способных расшифровывать сигнатуры (CCXv5-клиенты)

- Интеграция с другими решениями Cisco по security monitoring для определения «векторов атаки» — корреляция, основанная на правилах

- Предложен стандарт —IEEE 802.11w (~Дек 2009)

CCX: http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

© 2011 Cisco and/or its affiliates. All rights reserved.

Выводы

- Беспроводная инфраструктура Cisco с помощью инновационных технологий помогает осуществлять высокоскоростной, безопасный и надежный доступ большого количества Wi-Fi клиентских устройств в корпоративным приложениям и средствам совместной работы
- Программа Cisco Compatible Extensions – гарантирует проверенную и оптимальнуюсовместимость с подавляющим большинством клиентов
- Технологии Cisco CleanAir, Client-Link, BandSelect и VideoStream минимизируют негативное влияние помех, улучшают качество сигнала и способствуют эффективной работе видео-приложений

© 2011 Cisco and/or its affiliates. All rights reserved.

Выводы

- Угрозы со стороны беспроводного эфира существуют не зависимо от того, развернута ли Wi-Fi сеть в организации
- Необходимо принимать проактивные и реактивные меры для устранения этих угроз
- Решение Cisco предлагает единый интегрированный комплекс Wi-Fi безопасности, который позволяет выявлять, классифицировать и устранять посторонние беспроводные устройства
- Enhanced Local Mode, позволяющий работать точке доступа в режиме мониторинга и обслуживания клиентов, - защищает сеть от беспроводных атак и помогает сохранить инвестиции
- Cisco CleanAir может выявлять вредоносные посторонние устройства, работающие в нестандартных для Wi-Fi частотных диапазонах
- Management Frame Protection – защита от DoS атак

© 2011 Cisco and/or its affiliates. All rights reserved.

Thank you.