Руководство по развертыванию REAP в филиале компании

Содержание

Введение

Этот документ предоставляет сведения, который должен быть учтен, когда вы развертываете Точку доступа Удаленного Края (REAP). См. AP Удаленного Края (REAP) с Легковесными AP и Контроллерами беспроводной локальной сети (WLC) Пример конфигурации для основных сведений о конфигурации REAP.

Примечание: Функция REAP поддерживается до Выпуска 3.2.215 WLC. От Выпуска 4.0.155.5 WLC эту функциональность называют Гибридом REAP (H-REAP) с немногими усовершенствованиями до 7.0. x. x. От 7.2.103 выпусков эту функцию называют FlexConnect.

Традиционный протокол Cisco LWAPP (LWAPP) - базировал точки доступа (AP), (также

известный как LAP), такие как 1010, 1020, и AP серии 1200 и 1100 года, которые выполняют релиз 12.3 программного обеспечения Cisco IOS (7) JX или позже, обеспечивают централизованное управление и контроль через Контроллеры беспроводной локальной сети Cisco (WLC). Кроме того, эти LAP разрешают администраторам усиливать контроллеры как одиночные точки агрегации беспроводных данных.

В то время как эти LAP позволяют контроллерам выполнять дополнительные характеристики, такие как QoS и осуществление списка контроля доступа (ACL), требование контроллера, чтобы быть одиночной точкой входа и выхода для всего трафика беспроводного клиента может препятствовать, а не включить, способность соответственно удовлетворить пользовательские потребности. Когда ограниченная пропускная способность доступна по каналу WAN, в некоторых средах, таких как удаленные офисы, завершение всех пользовательских данных в контроллерах может доказать также использование пропускной способности, особенно. Кроме того, где ссылки между LAP и WLC подвержены простою, снова характерны с каналами WAN для удаленных офисов, использование LAP, которые полагаются на WLC для завершения пользовательских данных, приводит к разъединенной возможности беспроводного подключения во времена бездействия глобальной сети (WAN).

Вместо этого можно использовать архитектуру AP, где традиционная плоскость управления LWAPP усилена для выполнения задач, таких как управление динамической конфигурации, обновление программного обеспечения AP и беспроводное обнаружение несанкционированного доступа. Это позволяет беспроводным данным оставаться локальными, и беспроводная инфраструктура, которая будет централизованно управляема, и эластичное к бездействию глобальной сети (WAN).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

1030 введений архитектуры REAP

REAP Cisco 1030 разделяет плоскость управления LWAPP от плоскости беспроводных данных для обеспечения удаленной функциональности. WLC Cisco все еще используются для централизованного управления и управления таким же образом как обычные LAP. Различие - то, что все пользовательские данные соединены локально в AP. Доступ к локальным сетевым ресурсам производится в перерывах связи WAN. Рисунок 1 иллюстрирует базовую архитектуру REAP.

Рисунок 1: Основной REAP архитектурная схема

Примечание: Посмотрите Приложение A для списка основных отличий в функциональности REAP по сравнению с традиционными LAP.

Когда должны Использоваться AP REAP?

Cisco 1030 AP REAP должна использоваться прежде всего при этих двух условиях:

- Если ссылка между LAP и WLC подвержена простою, 1030 REAP может использоваться, чтобы позволить пользователям беспроводной связи непрерывный доступ к данным во время отказа соединения.
- Если все пользовательские данные должны быть завершены локально, что означает в проводном порту AP (в противоположность тому, чтобы быть завершенным в контроллере, как данные для всех других LAP), 1030 REAP может использоваться для учета центрального управления через интерфейс контроллера и/или Wireless Control System (WCS). Это позволяет данным оставаться локальными.

Где плотность покрытия или пользователя требует больше чем двух или три 1030 AP REAP на одиночном узле, рассмотрите развертывания 2006 или 2106 WLC. Эти контроллеры могут поддержать до 6 LAP любого типа. Это может оказаться более финансово жизнеспособным, и предоставить надмножество функций и функциональности по сравнению с развертываниями ТОЛЬКО ДЛЯ REAP.

Как со всеми AP серии 1000, одиночные 1030 AP покрывают приблизительно 5,000 квадратных футов. Это зависит от характеристик распространения радиочастот (RF) на каждом узле и нужного количества пользователей беспроводной связи и их потребностей пропускной способности. В наиболее распространенных развертываниях одиночный AP серии 1000 может поддержать 12 пользователей в 512 Кбит/с на 802.11b и 12 пользователей в 2 Мбит/с на 802.11a, одновременно. Как со всеми основанными на 802.11 технологиями, разделен доступ к среде. Поэтому, когда больше пользователей присоединяется к беспроводному AP, пропускная способность разделена соответственно. Снова, когда пользовательская плотность увеличивается и/или повышение требований пропускной способности, полагайте, что добавление локального WLC экономит стоивший для каждого пользователя и увеличивает функциональность.

Примечание: Можно настроить 1030 REAPs для работы тождественно к другим LAP. Поэтому, когда WLC добавлены для масштабирования размера инфраструктур WLAN удаленных узлов, существующие инвестиции REAP могут продолжить быть усиленными.

Разверните REAP

Поскольку 1030 REAP разработан, чтобы быть размещенным в удаленные узлы далеко от инфраструктуры WLC, традиционные, нулевые сенсорные LAP методов использовали обнаруживать и присоединяться, контроллеры (такие как параметр DHCP 43) обычно не используются. Вместо этого LAP должен сначала быть запущен, чтобы позволить 1030

соединяться с WLC назад в центральном узле.

Воспламенение является процессом, где LAP дают список WLC, с которыми они могут соединиться. После того, как соединенный с одиночным WLC, LAP сообщают обо всех контроллерах в группе мобильности и оборудуют всей информацией, должен был присоединиться к любому контроллеру в группе. См. Развертывание Контроллеров беспроводной локальной сети Cisco 440X Series для получения дополнительной информации о группах мобильности, распределении нагрузки и резервировании контроллера.

Для выполнения этого в центральном узле, таком как Network Operations Center (NOC) или ЦОД, REAPs должен быть связан с проводной сетью. Это позволяет им обнаруживать одиночный WLC. После того, как соединенный с контроллером, LAP загружают Версию операционной системы LAP, которая соответствует инфраструктуре WLAN. Затем IP-адреса всех WLC в группе мобильности переданы AP. Это позволяет AP, когда включено на их удаленных узлах, чтобы обнаружить и присоединиться к наименее используемому контроллеру из их списков, если возможность подключения с помощью IP-адреса доступна.

Примечание: Параметр DHCP 43 и Поиск в системе доменных имен (DNS) работает с REAPs, также. См. Развертывание Контроллеров беспроводной локальной сети Cisco 440X Series для получения информации о том, как настроить DHCP или DNS на удаленных узлах, чтобы позволить AP находить центральные контроллеры.

В это время этим 1030 можно дать статические адреса при желании. Это гарантирует, что схема IP-адресации совпадает с целевым удаленным узлом. Кроме того, названия WLC могут быть вводом для детализации, который три контроллера каждый LAP попытается подключить. Если эти три отказывают, автоматические функциональные возможности балансировки нагрузки LWAPP позволяют LAP выбирать наименее загруженный AP из остающегося списка контроллеров в кластере. Редактирование конфигурации LAP может быть сделано через интерфейс командной строки (CLI) WLC или GUI, или с большей простотой, через WCS.

Примечание: 1030 REAPs требует WLC, с которыми они соединяются для работы в режиме LWAPP Уровня 3. Это означает, что контроллерам нужно дать IP-адреса. Кроме того, WLC требуют, чтобы сервер DHCP был доступен на каждом удаленном узле, или статические адреса должны быть назначены во время процесса воспламенения. Функциональные возможности DHCP, встроенные в контроллеры, не могут использоваться для обеспечения адресов LAP 1030-х или их пользователям.

Прежде чем вы выключите эти 1030 LAP, чтобы послать к удаленным узлам, гарантировать, что каждый 1030 установлен в режим REAP. Это очень важно, потому что по умолчанию для всех LAP должен выполнить обычный, локальная функциональность, и 1030-е должны собираться выполнить функциональность REAP. Это может быть сделано на уровне LAP через CLI контроллера или GUI, или с большей простотой, через шаблоны WCS.

Основные функции воспламенения REAP

После того, как 1030 REAPs связан с WLC в группе мобильности, где REAPs соединяется с, когда размещено в удаленные узлы, эта информация может быть предоставлена:

Требуемые параметры настройки REAP

- Список IP-адресов для WLC в группе мобильности (предоставленный автоматически на соединение контроллера/AP)
- Режим AP REAP (AP должны быть настроены для работы в режиме REAP для выполнения функциональности REAP),

Дополнительные параметры настройки REAP

- Статически назначенные IP - адреса (дополнительная установка вводят на основе на AP),
- Основные, вторичные, и третичные названия WLC (дополнительная установка вводят на основе на AP или через шаблоны WCS),
- Название AP (дополнительная информационная установка вводят на основе на AP),
- Сведения о размещении AP (дополнительная информационная установка вводят на основе на AP или через шаблоны WCS),

Требования ссылки REAP К КОНТРОЛЛЕРУ

Когда вы планируете развернуть REAPs, несколько основных требований нужно помнить. Эти требования касаются скорости и задержки каналов WAN, которые пересечет трафик управления LWAPP REAP. 1030 LAP предназначены, чтобы использоваться через каналы WAN, такие как туннель IP-безопасности, Frame Relay, DSL (PPPoE non) и выделенные линии.

Примечание: 1030 реализаций LWAPP REAP принимают 1500-байтовый путь MTU между AP и WLC. Любая фрагментация, которая имеет место в пути из-за под1500байтового MTU, приводит к непредсказуемым результатам. Поэтому 1030 LAP не подходят для сред, таких как PPPoE, где маршрутизаторы заранее фрагментировати пакеты к под1500 байтам.

Задержка канала WAN особенно важна, потому что каждые 1030 LAP передают, по умолчанию, пульсирующие сообщения назад к контроллерам каждые 30 секунд. После того, как пульсирующие сообщения потеряны, LAP передают 5 последовательных тактовых импульсов, один раз во второй. Если ни один не успешен, LAP решает, что подключение контроллера разъединено, и 1030-е возвращаются к автономному режиму REAP. В то время как 1030 LAP могут терпеть большие задержки между собой и WLC, необходимо гарантировать, что задержка не превышает 100 мс между LAP и контроллером. Это происходит из-за клиентских таймеров, которые ограничивают клиентов периода времени, ждут, прежде чем таймеры решают, что отказала аутентификация.

Ограничения REAP

Несмотря на то, что 1030 AP разработаны, чтобы быть управляемыми централизованно и предоставить услугу беспроводной локальной сети во время простоев канала WAN, существуют некоторые различия между тем, какие услуги REAP предлагает с подключением WLC и что это может предоставить, когда разъединено подключение.

WLAN

В то время как 1030 REAP может поддержать до 16 WLAN (беспроводные профили, которые содержат Идентификатор набора сервисов [SSID] каждый, наряду со всей безопасностью,

QoS и другой политикой), каждый с его собственным Множественным ID Набора Основного сервиса (MBSSID), 1030 REAP может только поддержать первый WLAN, когда прервано подключение с контроллером. Во времена простоя канала WAN списаны все WLAN кроме первого. Поэтому WLAN 1 должен быть предназначен как основной WLAN, и политика безопасности должна быть запланирована соответственно. Безопасность на этом первом WLAN особенно важна, потому что, если канал WAN сбои, Проверка подлинности RADIUS бэкэнда - также. Это вызвано тем, что такой трафик пересекает плоскость контроллера LWAPP. Поэтому никаким пользователям не предоставляют беспроводной доступ.

Рекомендуется, чтобы локальная проверка подлинности / метод шифрования, такой как часть предварительного общего ключа Защищенного доступа по протоколу Wi-Fi (WPA-PSK), использовалась на этом первом WLAN. Протокол WEP достаточен, но не рекомендуется из-за известной уязвимости безопасности. Когда WPA-PSK (или WEP) используется, должным образом настроенные пользователи могут все еще получить доступ к ресурсам локальной сети, даже если канал WAN не работает.

Примечание: Все основанные на RADIUS методы безопасности требуют, чтобы сообщения аутентификации были переданы через плоскость управления LWAPP назад к центральному узлу. Поэтому все основанные на RADIUS сервисы недоступны во время бездействия глобальной сети (WAN). Это включает, но не ограничено, основанная на RADIUS проверка подлинности MAC, 802.1X, WPA, WPA2, и 802.11i.

1030 REAP может только находиться на одиночной подсети, потому что она не может выполнить маркировку "VLAN 802.1q". Поэтому трафик на каждом SSID завершается в той же подсети на проводной сети. Это означает, что, в то время как беспроводной трафик мог бы быть сегментирован по воздуху между SSIDs, трафик пользователя не разделен на проводной стороне.

Безопасность

1030 REAP может предоставить всю политику безопасности уровня 2, поддерживаемую основанной на контроллере архитектурой глобальной сети (WAN) Cisco. Это включает всю аутентификацию Уровня 2 и типы шифрования, такие как WEP, 802.1X, WPA, WPA2, и 802.11i. Как сообщили ранее, большая часть этой политики безопасности требует подключения WLC для аутентификации бэкэнда. WEP и WPA-PSK полностью внедрены на уровне AP и не требуют Проверки подлинности RADIUS бэкэнда. Поэтому, даже если канал WAN не работает, пользователи могут все еще соединиться. Клиентское исключение перечисляет функцию, предоставленную в Cisco WLCis, поддерживаемый с 1030 LAP. Если подключение назад к контроллеру доступно, фильтрация по MAC-адресам функционирует на 1030.

Примечание: Когда AP находится в автономном режиме, REAP не поддерживает PSK WPA2.

Вся политика безопасности уровня 3 не доступна с 1030 LAP. Эта политика безопасности включает web-аутентификацию, основанное на контроллере завершение VPN, ACL и одноранговое блокирование, потому что они внедрены в контроллере. Passthrough VPN действительно работает для клиентов, которые соединяются с внешними концентраторами VPN. Однако функция контроллера, которая позволяет только трафик, предназначенный для указанного концентратора VPN (только passthrough VPN) не делает.

!--- преобразования сетевых адресов (NAT)

WLC, к которым подключение REAPs не может находиться позади границ NAT. Однако REAPs на узлах пультов ДУ может находиться позади коробки NAT, предоставил порты, используемые для LWAPP (порты 12222 и 12223 UDP) переданы 1030-м. Это означает, что каждый REAP должен иметь статический адрес для переадресации портов для работы надежно, и что только одиночный AP может находиться позади каждого экземпляра NAT. Причина для этого состоит в том, что только экземпляр VRF одного порта может существовать на IP-адрес NAT, что означает, что только один LAP может работать позади каждого сервиса NAT над удаленными узлами. Непосредственный NAT может работать со множественным REAPs, потому что порты LWAPP могут быть переданы для каждого внешнего IP - адреса каждому внутреннему IP-адресу (статический IP-адрес REAP).

Качество обслуживания (QOS)

Назначение приоритета пакетов на основе 802.1p биты приоритета не доступны, потому что REAP не может выполнить 802.1q маркировка. Это означает, что не поддерживаются Мультимедиа Wi-fi (WMM) и 802.11e. Назначение приоритета пакетов на основе SSID и Идентификационных Сетей Ядер поддерживается. Однако назначение VLAN через Основанные на идентичности Сети не работает с REAP, потому что это не может выполнить 802.1q маркировка.

Роуминг и клиентское распределение нагрузки

В средах, где больше, чем одиночный REAP присутствует и где мобильность межAP ожидается, каждый LAP должен быть в той же подсети. Мобильность уровня 3 не поддерживается в 1030 LAP. Как правило, это не ограничение, потому что удаленные офисы обычно не используют достаточно LAP для потребности такой гибкости.

Агрессивное клиентское распределение нагрузки предоставлено через весь REAPs в узлах с больше, чем одиночный AP, когда восходящее подключение контроллера доступно (только балансирует нагрузку, включен на хост-контроллере).

Управление радиоресурсами (RRM)

Когда подключение к контроллерам присутствует, 1030 LAP получают динамический канал и выходную мощность от механизма RRM в WLC. Когда канал WAN не работает, RRM не функционирует, и канал и параметры настройки питания не изменены.

Постороннее обнаружение и функциональность IDS

Архитектура REAP поддерживает все постороннее обнаружение и подпись обнаружения несанкционированного доступа (IDS), которые совпадают с подписью обнаружения несанкционированного доступа (IDS) обычных LAP. Однако, когда подключение потеряно с центральным контроллером, вся собранная информация не разделена. Поэтому видимость в домены RF удаленных узлов потеряна.

Сводка ограничения REAP

Когда соединение с WLC через канал WAN не доступно, таблица в Приложении B суммирует возможности REAP во время нормальной работы и.

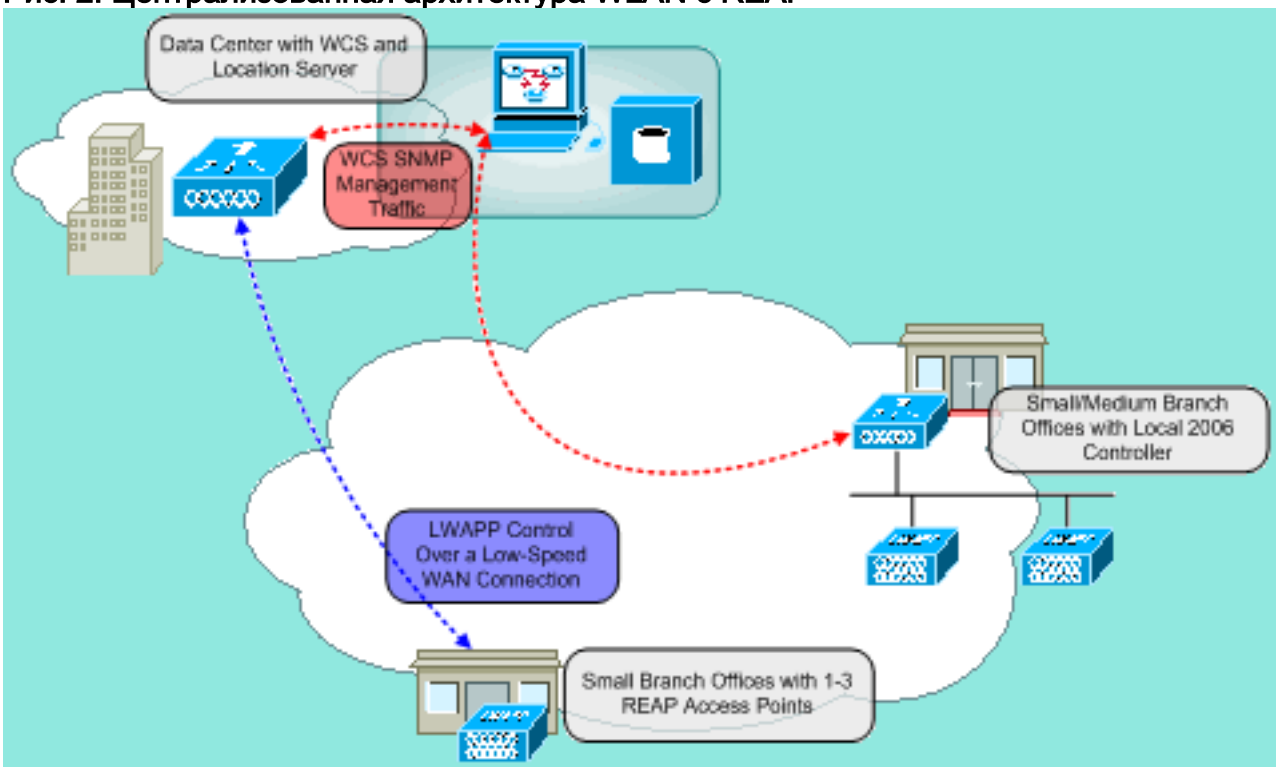
Управляйте REAP и центральной архитектурой WLAN

1030 управления REAP является не другим, чем тот из обычных LAP и WLC. Менеджмент и конфигурация все сделаны на уровне контроллера, или через CLI каждого контроллера или через веб-GUI. Конфигурация в масштабе системы и сетевая видимость предоставлены через WCS, где всеми контроллерами и AP (REAP или иначе) можно управлять как единая система. Когда подключение КОНТРОЛЛЕРА REAP разрушено, возможности управления также разрушены.

Централизованная архитектура WLAN с REAP

Рисунок 2 показывает, как каждая часть централизованной архитектуры LWAPP сотрудничает для совещания множества потребностей беспроводной сети. Менеджмент и службы определения местоположения предоставлены централизованно через WCS и 2700 Устройств определения местоположения.

Рис. 2: Централизованная архитектура WLAN с REAP



Приложение A

Каковы основные различия между архитектурой REAP и обычными LAP?

- Если параметр DHCP 43 или Разрешение DNS не доступен на удаленных узлах, эти 1030 должны сначала быть запущены в центральной АТС. Затем это послано к узлу назначения.
- После сбоя соединений WAN только первый WLAN остается активным.Политика безопасности, которая требует RADIUS, откажет.Аутентификация/Шифрование, которая использует WPA-PSK, рекомендуется для WLAN 1. WEP работает, но не рекомендуется.
- Никакое шифрование Уровня 3 (Только шифрование уровня 2)
- WLC, с которыми соединяется REAPs, не могут находиться позади границ NAT. Однако

REAPs может, если каждый внутренний статический IP-адрес REAP имеет и порты LWAPP (12222 и 12223) переданный им.**Примечание:** Преобразование адресов портов (PAT) / NAT с перегрузкой не поддерживается, потому что исходный порт трафика LWAPP, который происходит из LAP, может изменяться в течение долгого времени. Это ломает ассоциацию LWAPP. Та же проблема может возникнуть с реализациями NAT для REAP, где адрес порта изменяется, такие как PIX/ASA мог бы, который зависит от конфигурации.

- Только сообщения управления LWAPP пересекают канал WAN.
- Трафик данных соединен в Порту Ethernet 1030.
- 1030 LAP не выполняют маркировку 802.1Q (VLAN). Поэтому беспроводной трафик от всего SSIDs завершается на той же проводной подсети.

Приложение Б

Каковы различия в функциональности между обычными и автономными режимами REAP?

		REAP (обычный режим)	REAP (автономный режим)
Протоколы	IPv4	Да	Да
	IPv6	Да	Да
	Все другие протоколы	Да (только если клиент является также IP, включил),	Да (только если клиент является также IP, включил),
	Прокси - протокол преобразования адресов IP	Нет	Нет
WLAN	Количество SSIDs	16	1 (первый)
	Присвоение динамического канала	Да	Нет
	Динамическое управление питанием	Да	Нет
	Балансировка динамической нагрузки	Да	Нет

Сети VLAN	Несколько интерфейсов	Нет	Нет
	Поддержка 802.1Q	Нет	Нет
WLAN Security	Постороннее обнаружение AP	Да	Нет
	Список исключения	Да	Да (только существующие участники)
	Одноранговое блокирование	Нет	Нет
	Система обнаружения вторжений (IDS)	Да	Нет
Безопасность уровня 2	Аутентификация протокола управления доступом к среде передачи (MAC)	Да	Нет
	802.1x	Да	Нет
	WEP (64/128/152bits)	Да	Да
	WPA-PSK	Да	Да
	PSK WPA2	Да	Нет
	EAP WPA	Да	Нет
	EAP WPA2	Да	Нет
Безопасность уровня 3	Web-аутентификация	Нет	Нет
	IPSec	Нет	Нет

	L2TP	Нет	Нет
	Passthrough VPN	Нет	Нет
	Списки управления доступом	Нет	Нет
QoS	Профили QoS	Да	Да
	Нисходящее QoS (очереди взвешенного алгоритма кругового обслуживания)	Да	Да
	802.1p поддержка	Нет	Нет
	Договоры пропускной способности для каждого пользователя	Нет	Нет
	WMM	Нет	Нет
	802.11e (будущее)	Нет	Нет
	Замена Профиля QoS AAA	Да	Нет
Mobility	Внутриподсеть	Да	Да
	Межподсеть	Нет	Нет
DHCP	Внутренний сервер DHCP	Нет	Нет
	Внешний сервер DHCP	Да	Да

Топология	Прямое подключение (2006)	Нет	Нет

Дополнительные сведения

- Пример конфигурации удаленного AP (REAP) с легкими APs и контроллерами беспроводной LAN (WLC)
- Балансировка нагрузки и переход в аварийный режим системы AP в объединенных беспроводных сетях
- Развертывание контроллеров беспроводной локальной сети Cisco 440X Series
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Cisco Systems – техническая поддержка и документация