Внутреннее руководство развертывания ячеистой сети

Содержание

Введение

Облегченная точка доступа 1242/1131 представляет собой устройство инфраструктуры Wi-Fi с двумя беспроводными каналами для особых применений в помещениях. Это продукт на основе протокола LWAPP. Это предоставляет радио на 2.4 ГГц и радио на 5.8 ГГц, совместимое с 802.11b/g и 802.11a. Одно радио может использоваться для локального (клиентского) доступа для точки доступа (AP), и второе радио может быть настроено для беспроводного обратного рейса. LAP1242/LAP1131 поддерживает P2P, P2MP и тип сетки архитектур.

Удостоверьтесь, что прочитали руководство прежде, чем делать попытку любой из установок.

Этот документ описывает развертывания Беспроводной полносвязной сети Предприятия для внутренней сетки. Этот документ позволит беспроводным конечным пользователям понять основные принципы Внутренней Сетки, где настроить внутреннюю сетку, и как настроить внутреннюю сетку. Внутренняя сетка является подмножеством Беспроводной полносвязной сети Cisco Enterprise, развернутой с помощью контроллеров беспроводной локальной сети и легковесных AP.

Внутренняя сетка является подмножеством архитектуры сетки Предприятия, развернутой на Унифицированной беспроводной архитектуре. Сегодня внутренняя сетка пользуется спросом. В то время как второе радио (как правило, 802.11a) используется к трафику клиента обратного рейса, с внутренней сеткой, одним из радио (как правило, 802.11b/g) и/или проводное Соединение Ethernet используется для соединения с клиентами. Обратный рейс может быть одним переходом или по множественным переходам. Внутренняя сетка приносит эти значения вам:

- Не имея необходимость выполнить проводное соединение Ethernet к каждому AP.
- Порт коммутатора Ethernet не требуется для каждого AP.
- Сетевое подключение, где провода не могут предоставить подключение.
- Гибкость в развертываниях – не ограниченный 100 м от Коммутатора Ethernet.
- Легкий развернуть оперативную беспроводную сеть.

Магазины розничной торговли больших коробок очень привлечены к внутренней сетке из-за сохранений затрат при проводном соединении, а также по причинам, ранее упомянутым.

Специалисты по материально-техническим ресурсам используют его n, выполняющие материально-технические ресурсы значат ритейлеров, производственные установки и другие компании. Они хотят быстро развернуть временную сеть Wi-Fi в клиентском узле сети для включения подключения в реальном времени для их карманных устройств. Образовательные Семинары, конференции, производство и гостеприимство являются некоторыми местами, где необходима внутренняя архитектура сетки.

Когда вы закончите читать это руководство, вы поймете, где использовать и как настроить внутреннюю сетку. Вы также поймете, что внутренняя сетка в приложениях NEMA НЕ является заменой для наружной сетки. Далее, вы также поймете превосходство внутренней

сетки по гибкости роли ссылки (сетка одного перехода) используемый автономными AP.

Предположения:

Вы ознакамливаетесь с единой беспроводной сетью Cisco (UWN), архитектурой и продуктами. Вы ознакамливаетесь с Cisco Наружные продукты Сетки и часть терминологии, используемой для сетей сетки.

Глоссарий акронимов	
LWAPP	Упрощенный протокол точки доступа – контроль и протокол туннелирования данных между AP и Контроллером беспроводной локальной сети.
Контроллер беспроводной локальной сети / Контроллер / WLC	Контроллер беспроводной локальной сети – устройства Cisco, которые централизуют и упрощают управление сетью WLAN путем сворачивания большого числа управляемых оконечных точек в одиночную, унифицированную систему, учета унифицированной интеллектуальной информационной системы сети WLAN.
RAP	Точка Доступа к корневому каталогу / точка доступа Крыши – устройства беспроводной связи Cisco действует как мост между контроллером и другими беспроводными AP. AP, которые соединены проводом к контроллеру.
MAP	AP сетки – устройство беспроводной связи Cisco, которое соединяется с RAP или MAP по воздуху на 802.11a радио и также клиенты сервисов по 802.11b/g радио.
Родитель	AP (любой RAP/MAP), который предоставляет

	доступ к другим AP по воздуху на 802.11a радио.
Соседний узел	Все AP в Сети с ячеистой структурой являются соседними узлами и имеют соседние узлы. RAP не имеет соседнего узла, поскольку он соединил проводом к контроллеру.
Потомок	AP дальше от контроллера всегда является потомком. У потомка будут один родитель и много соседних узлов в сети с ячеистой структурой. Если родитель умрет, то следующий соседний узел с лучшим значением простоты будет выбран родитель.
SNR	Отношение сигнала к шуму
BGN	Имя группы моста
EAP	Расширяемый протокол проверки подлинности
PSK	Pre-shared-key *
AWPP	Адаптивный беспроводной протокол пути

Обзор

Точка доступа Ячеистой сети в помещении Cisco является устройством, относящимся к инфраструктуре Wi-Fi с двумя радио для выбранных внутренних развертываний. Это продукт на основе протокола LWAPP. Это предоставляет радио на 2.4 ГГц и радио на 5.8 ГГц, совместимое с 802.11b/g, 802.11a стандарты. Одно радио (802.11b/g) может использоваться для локального (клиентского) доступа для AP, и второе радио (802.11a) может быть настроено для беспроводного обратного рейса. Это предоставляет внутреннюю архитектуру сетки, где другие узлы (радио) говорят друг с другом через обратный рейс и также предоставляют доступ локального клиента. Этот AP может также использоваться для архитектур с использованием мостов точка - много точек и "точка-точка". Беспроводное решение для Ячеистой сети в помещении идеально для большого внутреннего покрытия, поскольку у вас могут быть высокие скорости передачи данных и хорошая надежность с минимальной инфраструктурой. Это основные существенные функции, начатые с первого выпуска этого продукта:

- Используемый во Внутренней среде для 3 чисел переходов. Максимальные 4.
- Релейный узел и хост к клиентам конечного пользователя. 802.11a радио используется

в качестве интерфейса обратного рейса и 802.11b/g радио для обслуживания клиентов.
- Внутренняя безопасность AP сетки – EAP и PSK поддерживаются.
- MAP LWAPP в среде ячеистой сети связываются с контроллерами таким же образом по сравнению с подключенными Ethernet AP.
- Мостовое соединение двухточечного беспроводного соединения.
- Беспроводное мостовое соединение точка - много точек.
- Оптимальный родительский выбор. SNR, ПРОСТОТА и BGN
- Усовершенствования BGN. NULL и Режим по умолчанию.
- Локальный доступ.
- Породите черную распечатку. Список исключения.
- Сам заживающий с AWPP.
- Мостовое соединение Ethernet.
- Основная поддержка Голоса от этих 4.0 выпусков.
- Динамический выбор частоты.
- Анти-скручивание – BGN По умолчанию и аварийное переключение DHCP.

Примечание: Эти функции не будут поддерживаться:

- 4.9 Канал общественной безопасности ГГц
- Маршрутизация вокруг интерференции
- Фоновое сканирование
- Универсальный доступ
- Поддержка моста подключения для рабочих групп

Внутреннее программное обеспечение сетки

Внутреннее программное обеспечение Сетки является специальным релизом, поскольку оно концентрируется на внутренних AP, особенно внутренней сетке. В этом выпуске у нас есть и Внутренний APs working в Автономном режиме и также в мостовом режиме. Некоторые опции, которые доступны в 4.1.171.0 выпусках, не реализованы в этом выпуске. Улучшения были сделаны к интерфейсу командной строки (CLI), графический интерфейс пользователя (GUI – web-браузер) и на самом механизме состояний. Цель для этих улучшений состоит в том, чтобы получить полезную информацию с вашей точки зрения относительно этого нового продукта и его функциональной жизнеспособности.

Внутренняя сетка определенные усовершенствования:

- **Внутренняя среда** – Внутренняя сетка внедрена с помощью LAP1242s и LAP1131. Они внедрены во внутренних средах, где Кабель Ethernet не доступен. Реализация легка и быстрее для обеспечения зоны охвата беспроводного соединения удаленным областям в здании (например, Розничные Распределительные центры, Образование для Семинаров/конференций, Производства, Гостеприимства).
- **Усовершенствования Имени группы моста (BGN)** – Чтобы позволить администратору сети организовывать сеть Внутренних AP Сетки в пользователя, задали секторы, Cisco предоставляет механизм под названием Имя группы моста или BGN. BGN, действительно название сектора, заставляет AP соединяться с другими AP с тем же BGN. В конечном счете AP не находит подходящего сектора, совпадающего с его BGN, AP работает в режиме по умолчанию и выбирает лучшего родителя, который отвечает на BGN по умолчанию. Эта функция уже получила большую оценку от поля, поскольку это борется против скрученных условий AP (если кто-то неправильно сконфигурировал BGN). В 4.1.171.0 выпусках ПО AP, при использовании BGN по умолчанию, не

действуют в качестве внутреннего узла сетки и не имеют никакого доступа клиента. Это находится в режиме обслуживания для доступа через контроллер, и если администратор не исправит BGN, то AP перезагрузит после 30 минут.

- **Улучшения безопасности** - Безопасность на внутреннем коде сетки по умолчанию настроена для EAP (Расширяемый протокол аутентификации). Это определено в RFC3748. Несмотря на то, что протокол EAP не ограничен беспроводными локальными сетями и может использоваться для проводной аутентификации LAN, он чаще всего используется в беспроводных локальных сетях. То, когда EAP вызван 802.1X, включило NAS (Сервер доступа к сети) устройство, такое как Точка беспроводного доступа a/b/g 802.11, современные методы EAP могут предоставить механизм безопасной аутентификации и выполнить согласование о безопасном PMK (Попарный Главный ключ) между клиентом и NAS. PMK может тогда использоваться для беспроводного сеанса с шифрованием, который использует TKIP или CCMP (на основе AES) шифрование.До 4.1.171.0 выпусков ПО вне помещения сцепитесь, AP использовали PMK/BMK для присоединения к контроллеру. Это было процессом с тремя циклами. Теперь циклы уменьшены для более быстрой конвергенции.Общая задача внутренней безопасности сетки должна предоставить:Нулевая сенсорная конфигурация для инициализации безопасности.Конфиденциальность и аутентификация для фреймов данных.Обоюдная проверка подлинности между сетью и узлами.Способность использовать стандартные методы EAP для аутентификации узлов точки доступа ячеистой сети в помещении.Разъединение LWAPP и внутренней безопасности сетки.Обнаружение, маршрутизация и синхронизация механизмов улучшены от текущей архитектуры для размещения требуемых элементов для поддержки новых протоколов безопасности.Внутренние AP сетки обнаруживают другие AP сетки путем сканирования и прислушивания к бесплатным соседним обновлениям от других AP сетки. Любой RAP или внутренние MAP, связанные с сетью, объявляют базовые параметры безопасности в их кадрах NEIGH_UPD (во многом как кадры неисправность 802.11).Как только эта фаза закончена, логическое соединение между точкой доступа ячеистой сети в помещении и корневой точкой доступа установлено.
- **Усовершенствования WCS**Были добавлены внутренние Сигналы тревоги Сетки.Внутренние Отчёты о Сетке могут генерироваться, показывая счетчик переходов, худший SNR, и т.д.Тестирование канала (Родитель Потомку, Потомок Родителю) может быть выполнено между узлами, который показывает очень интеллектуальную информацию.Отображенная информация AP намного больше, чем более ранние.У каждого есть опция, чтобы также просмотреть потенциальные соседние узлы.Контроль исправности улучшен и более удобен для доступа.

Поддерживаемые программные и аппаратные средства

Существует минимальное оборудование и требование к программному обеспечению для внутренней сетки:

- AP LWAPP Cisco AIR-LAP1242AG-A-K9 и AIR-LAP1131AG-A-K9 поддерживают внутреннюю конфигурацию сетки.
- Программное обеспечение Cisco Mesh Release 2 поддерживает Сетку Предприятия (Внутренние и Наружные продукты). Это может быть установлено на Cisco Controller, Cisco 440x/210x и WISMs только.

- Программное обеспечение Cisco Enterprise Mesh Release 2 может быть загружено от Cisco.com.

Внутренний по сравнению с вне помещения

Это некоторые существенные различия между внутренней и наружной сеткой:

	Внутренняя сетка	Наружная сетка
Среда	Внутренний ONLY, аппаратные средства, внутренние оцененный	Наружный ONLY, Бурные аппаратные средства
Аппаратные средства	Внутренний AP с помощью LAP1242 и LAP1131AG	Наружный AP с помощью LAP15xx и LAP152x
Уровни мощности	2,4 ГГЦ: 20dbm 5.8 Ghz:17dbm	2,4 ГГЦ: 28dbm 5.8 Ghz:28dbm
Размеры ячейки	Приблизительно 150 футов	Приблизительно 1000 футов
Высота реализации	В 12 футах от основы	30-40ft от основы

!--- конфигурацию

Удостоверьтесь, что рассмотрели руководство полностью прежде, чем запустить любую реализацию, особенно при получении новых аппаратных средств.

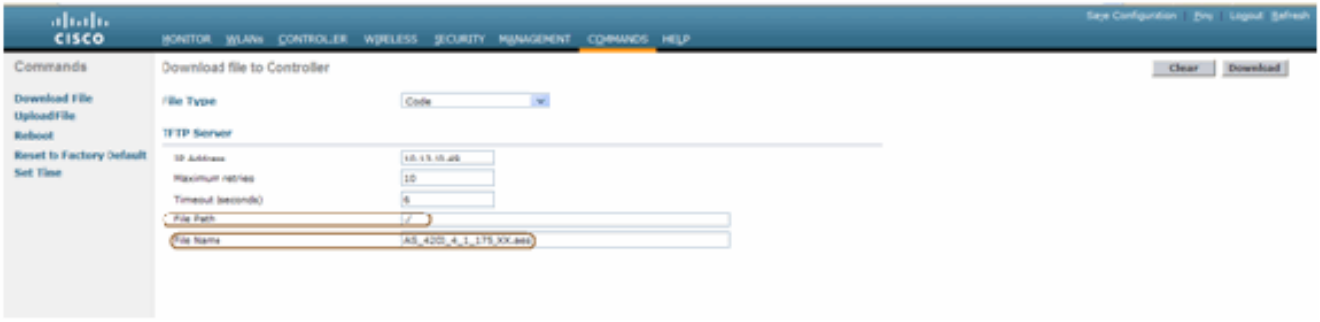
Режим L3 контроллера

Внутренние AP сетки могут быть развернуты как сеть L3.

Обновите контроллер к последнему коду

Выполните следующие действия:

1. Для обновления Выпуска 2 Сетки на ячеистой сети в помещении ваша сеть должна работать 4.1.185.0 или Сетка Release1, доступный на Cisco.com.
2. Загрузите последний код для Контроллера к вашему серверу TFTP. От интерфейса Графического интерфейса контроллера нажмите **Commands> файл Download**.
3. Выберите Тип файла как **код** и дайте IP-адрес своего сервера TFTP. Определите путь и название
   файла.



   Примечание: Используйте Сервер TFTP, который поддерживает передачи Размера файла на больше чем 32 МБ. Например, **tftpd32**. Под помещенным Путем к файлу **“. /”** как показано.
4. Закончено устанавливая новую микропрограмму, используйте **команду show sysinfo** в CLI, чтобы проверить, что установлена новая
   микропрограмма.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version.............................. 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

   Примечание: Официально, Cisco не поддерживает Переходы на более ранние версии для контроллеров.

MAC-адрес

Это является обязательным для использования фильтрации по MAC-адресам. Эта функция сделала Cisco Внутренним решением для Сетки как реальное “Нулевое Касание”. В отличие от предыдущих версий, экран Mesh больше не будет иметь опции MAC Filtering.

Примечание: Фильтрация по MAC-адресам включена по умолчанию.

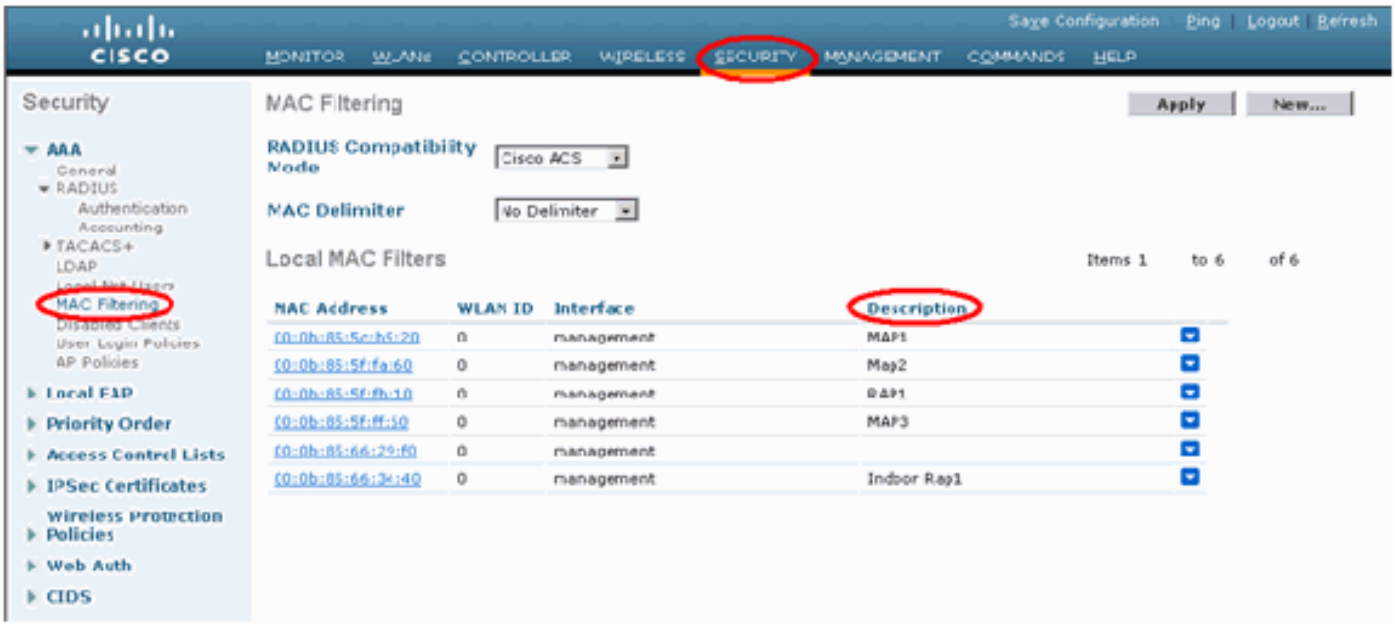
Рекордный MAC-адрес к радио

В текстовом файле сделайте запись MAC-адресов всех радио точки доступа ячеистой сети в помещении, которые вы развертываете в своей сети. MAC-адрес может быть найден в конце AP. Это помогает вам для будущего тестирования, поскольку большинство команд CLI требует MAC-адреса AP, или имена введены с командой. Можно также поменять имя AP к чему-то, более легко помнил, такой как, “создавая тип AP номера переходной приставки номера: последние четыре шестнадцатеричных символа MAC-адреса”.

Введите MAC-адрес и названия радио в контроллере

Cisco Controller ведет внутренний список MAC-адреса авторизации AP. Контроллер только отвечает на запросы на обнаружение от внутренних радио, которые появляются на списке авторизации. Введите MAC-адреса всех радио, которые вы склонны использовать в вашей сети на Контроллере.

На интерфейсе Графического интерфейса контроллера перейдите **к Безопасности** и щелкните **по фильтрации по MAC-адресам** на левой части экрана. Нажмите **New** для ввода MAC-адресов как показано здесь:



Кроме того, введите имена радио для удобства в соответствии с **Описанием** (таких как местоположение, AP #, и т.д.), Описание может также использоваться для того, где Радио были установлены для легкой ссылки любое время.

Включите фильтрацию по MAC-адресам

Фильтрация по MAC-адресам включена по умолчанию.

Можно также сделать выбор Режима безопасности как EAP или PSK на той же странице.

От графического интерфейса пользователя (GUI) коммутатора используйте этот путь:

Путь Графического интерфейса пользователя (GUI): **Беспроводные сети> Внутренняя Сетка**

Режим безопасности может ONLY быть проверенным на CLI этой командой:

```
(Cisco Controller) > show network
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3 внутреннее развертывание ячеистой сети

Для Ячеистой сети в помещении L3 настройте IP-адреса для радио, если вы не намереваетесь использовать сервер DHCP (внутренний или внешний).

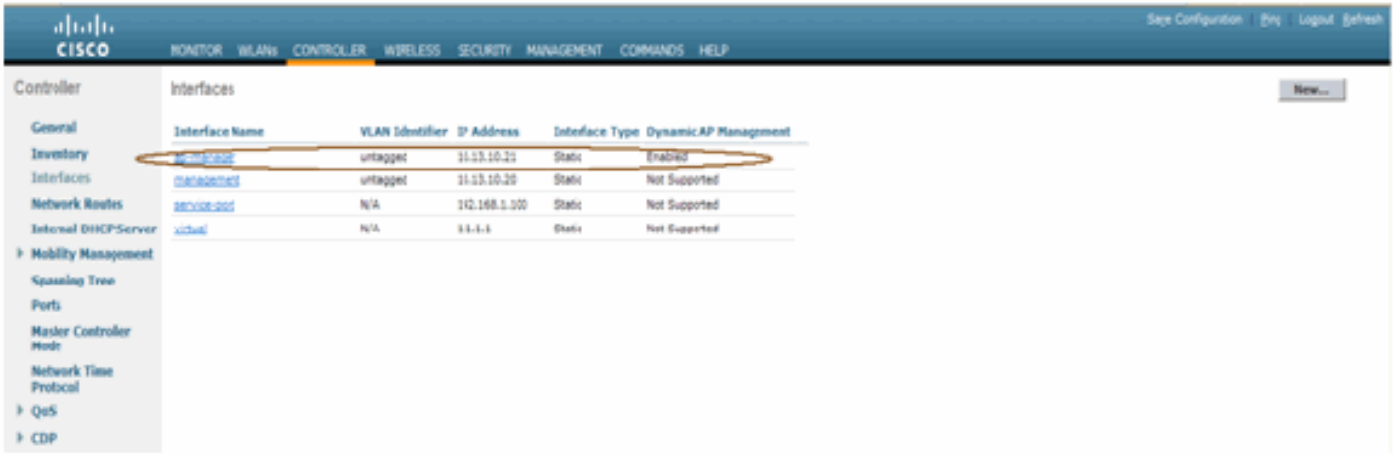
Для Ячеистой сети в помещении L3, если вы хотите использовать сервер DHCP, настраивают контроллер в режиме L3. Сохраните конфигурацию и перезагрузите Контроллер. Удостоверьтесь вы Опция configure 43 на сервере DHCP. После того, как Контроллер перезапустил, недавно соединился, AP получат свой IP-адрес от сервера DHCP.

Определите интерфейсы на контроллере

AP Manager

Для развертываний L3 необходимо определить **AP - диспетчера**. Менеджер AP действует как IP - адрес источника для связи от Контроллера до AP.

Путь: **Контроллер> Интерфейсы> менеджер AP> редактирует**.



Интерфейсу менеджера точки доступа нужно назначить IP-адрес в той же подсети и VLAN как ваш интерфейс управления.

Радио-роли

Существует две основных радио-роли, возможные с этим решением:

- Точка доступа к корневому каталогу (RAP) - радио, с которым вы хотите соединиться с Контроллером (через коммутатор) возьмет роль RAP. RAP имеют проводное, поддерживающее LWAPP соединение с Контроллером. RAP является родительским узлом к любому мостовому соединению или ячеистой сети в помещении. Контроллер может иметь один или несколько RAP, каждый порождающий те же или другие беспроводные сети. Может быть несколько RAP для той же ячеистой сети в помещении для резервирования.
- Внутренняя точка доступа для полносвязных сетей (MAP) - радио, которое не имеет никакого проводного соединения с Контроллером, берет роль точки доступа ячеистой сети в помещении. Этот AP раньше назвали AP вершины полюса. MAP имеют беспроводное соединение (через интерфейс обратного рейса) к, возможно, другим MAP и наконец к RAP и таким образом к контроллеру. MAP могут также иметь проводное Подключение по технологии Ethernet к LAN и служить оконечной точкой моста для той LAN (использующий P2P или соединение P2MP). Это может произойти одновременно, если настроено должным образом как мост Ethernet. Клиенты сервиса MAP на полосе, не используемой для Интерфейса Обратного рейса.

Режим по умолчанию для AP является MAP.

Примечание: Радио-роли могут быть установлены через GUI или CLI. AP перезагрузят после изменения роли.

Примечание: Можно использовать CLI Контроллера, чтобы предварительно сконфигурировать радио-роли на AP, если AP физически связан с коммутатором, или вы видите AP на коммутаторе как RAP или MAP.

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Имя группы моста

Имена группы моста (BGN) управляют ассоциацией AP. BGN могут логически сгруппировать радио для предотвращения двух сетей на том же канале от связи друг с другом. Если у вас есть несколько RAP в вашей сети в том же секторе (область), эта установка также полезна. BGN является строкой максимума десяти знаков.

Установленное на заводе имя группы моста назначено в стадии производства (ПУСТОЕ ЗНАЧЕНИЕ). Это не видимо вам. В результате даже без определенного BGN, радио могут все еще присоединиться к сети. Если у вас есть два RAP в вашей сети в том же секторе (для большей емкости), рекомендуется настроить эти два RAP с тем же BGN, но на других каналах.

Примечание: Имя группы моста может быть установлено от CLI Контроллера и GUI.

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

После настройки BGN AP перезагрузит.

Примечание: BGN должен быть настроен очень тщательно на действующей сети. Необходимо всегда запускать с самого дальнего узла (последний узел) и двигать RAP. Причина состоит в том, что, если вы начинаете настраивать BGN где-нибудь посреди мультиперехода, тогда узлы вне этой точки будут отброшены, поскольку эти узлы будут иметь другой BGN (старый BGN).

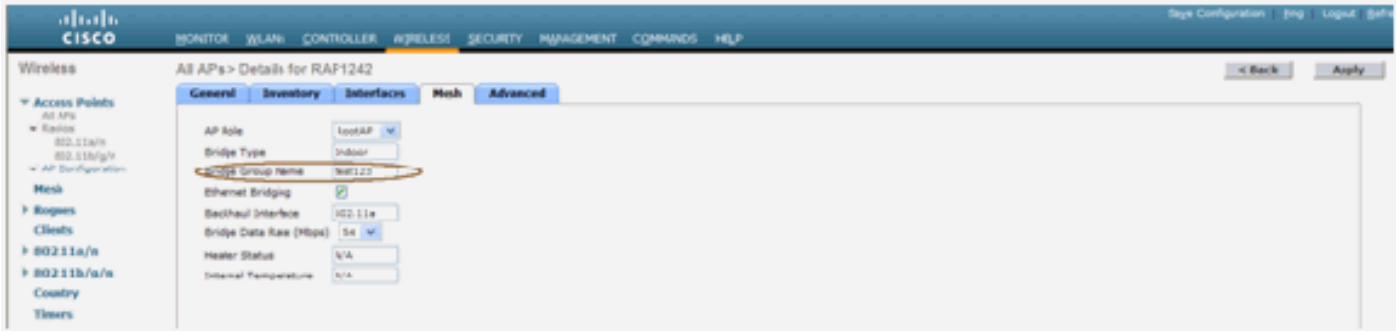
Можно проверить BGN путем запуска этой команды CLI:

(Cisco Controller) **> show ap config general** *<apname>*

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-A3
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ................................... Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation........... Disabled
Console Login Name............................... 
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

Кроме того, можно настроить или проверить BGN с помощью Графического интерфейса контроллера:

Путь: **Беспроводные сети> Все AP> Подробные данные**.



Вы видите, что Сведения о среде AP также отображены с этим новым выпуском.

Конфигурация безопасности

Внутренний режим безопасности сетки по умолчанию является EAP. Это означает, что, пока вы не настраиваете эти параметры на своем Контроллере, не присоединятся ваши MAP:

Внутренний CLI конфигурации EAP сетки

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index      Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Если необходимо остаться в режиме PSK, используйте эту команду для возвращения к режиму PSK:

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

Внутренние команды показа EAP Сетки

В режиме EAP можно проверить эти **команды показа** для проверки аутентификации MAP:

```
(Cisco Controller) >show network

RF-Network Name............................. jaggi123
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode..................... Disable
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Enable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Disable
Bridge Security Mode........................ EAP  otherwise PSK
Mesh Multicast Mode......................... 802.11b/g/n
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Mobile Peer to Peer Blocking................ Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
--More-- or (q)uit
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
```

```
(Cisco Controller) >show wlan 0
```

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500L1EAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ........................................... Disabled
   IP Security Passthru........................... Disabled
   Web Based Authentication....................... Disabled
   Web-Passthrough................................ Disabled
   Conditional Web Redirect....................... Disabled
   Auto Anchor.................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching......................... Disabled
   Infrastructure MFP protection.................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP..................................... Optional
   Tkip MIC Countermeasure Hold-down Timer........ 60

 Mobility Anchor List
 WLAN ID      IP Address       Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

(Cisco Controller) >**show advanced eap**

Внутренние команды отладки EAP Сетки

Для отладки любых проблем режима EAP используйте эти команды в Контроллере:

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

Установка

Предварительные условия

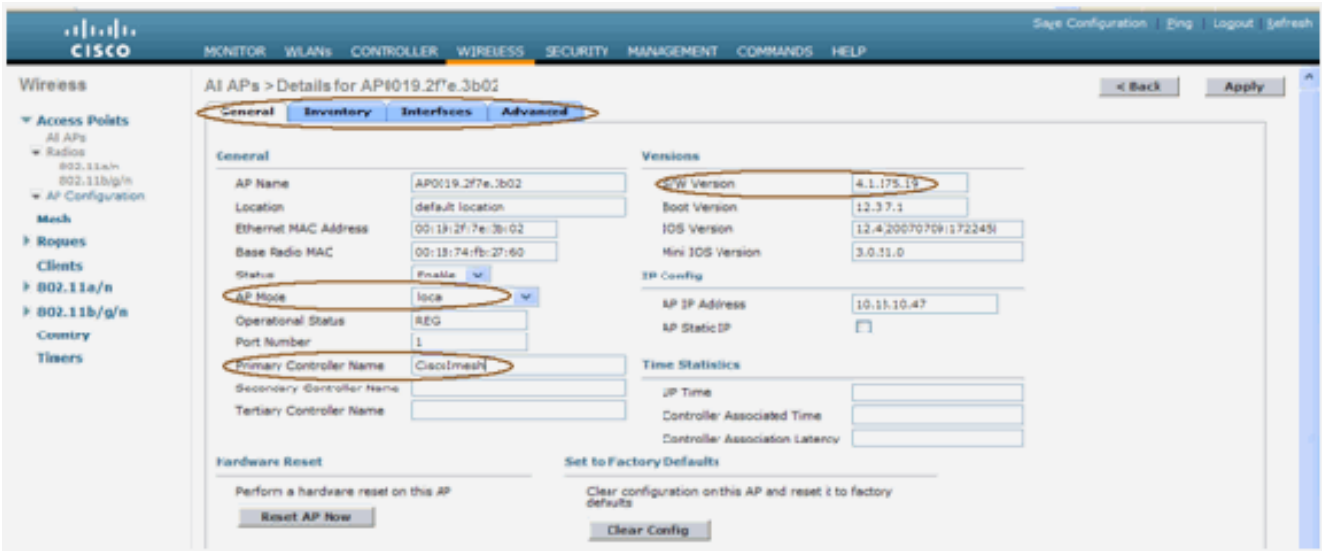
Контроллер должен выполнять рекомендуемую версию кода. Нажмите **Monitor** для проверки Версии программного обеспечения. То же может быть проверено через CLI.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

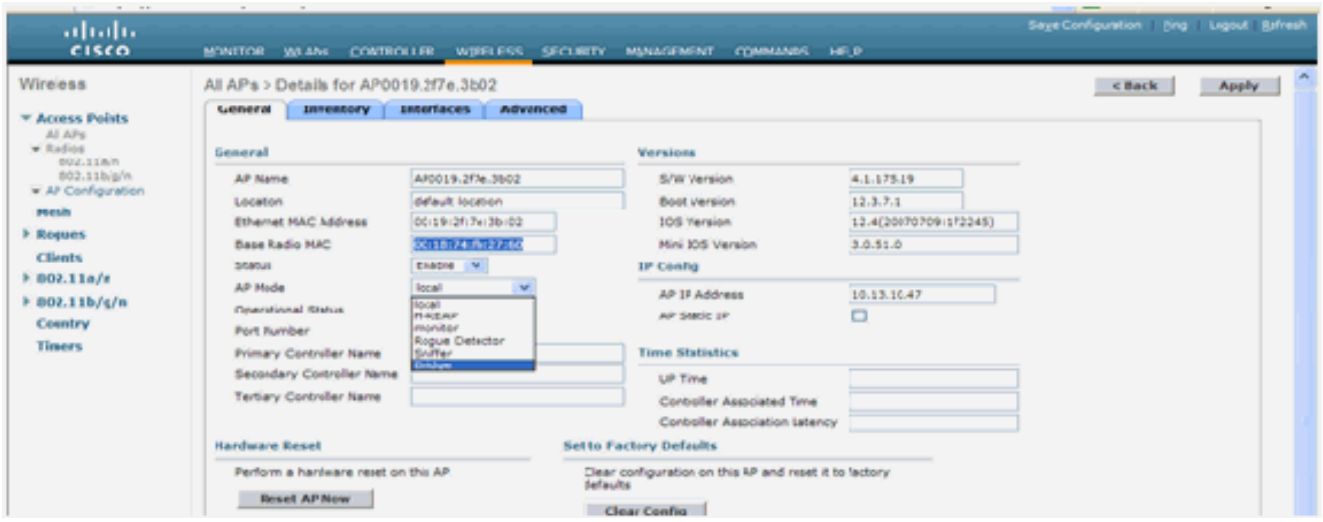
Системы как сервер DHCP, сервер ACS и сервер WCS должны быть достижимыми.

Установка

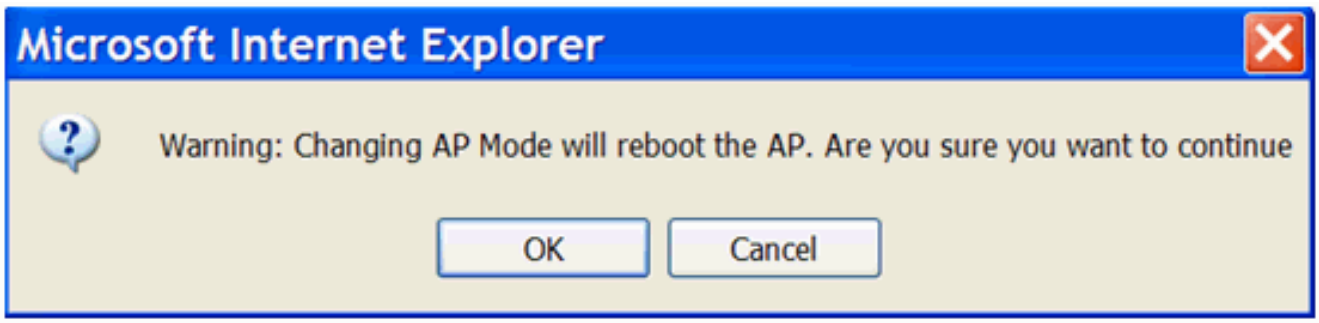
1. Подключите все LAP (1131AG/1242AG) с сетью Уровня 3 в той же подсети как Управление IP-адресами. Все AP присоединятся к контроллеру как AP в Автономном режиме. В этом режиме, главном AP с названием Главного контроллера, названием Вспомогательного контроллера и названием Третичного контроллера.



2. Перехватите MAC-адрес Базовой радиостанции AP (например, 00:18:74: fb: 27:60).
3. Добавьте MAC-адрес AP для AP для участия в мостовом режиме.
4. Нажмите **Security> MAC-filtering> New**.
5. Добавьте скопированный MAC-адрес и назовите AP в списке фильтров MAC и списке точек доступа.
6. Выберите **Bridge** из списка **Режима AP**.



7. Это побудит вас подтверждать, поскольку это перезагрузит AP.



8. AP перезагрузит и присоединится к контроллеру в Мостовом режиме. Новое окно AP будет иметь дополнительную вкладку: СЕТКА. Нажмите вкладку **MESH**, чтобы проверить роль, тип моста, имя группы моста, Мостовое соединение Ethernet, назад буксировать интерфейс, скорость передачи данных моста, и т.д.

9. В этом окне обратитесь к списку роли AP и выберите соответствующую роль. В этом случае роль по умолчанию является MAP.Имя группы моста пусто по умолчанию.Обратный интерфейс трофея 802.11a.Скорость передачи данных моста (т.е. Назад буксируйте, скорость передачи данных) 24 Мбит/с.
10. Подключите AP, который вы хотите как RAP к контроллеру. Разверните радио (MAP) в желаемых местоположениях. Включите радио. Должна существовать возможность видеть все радио на
    контроллере.

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model             Ethernet MAC       Location          Port  Country
-----------------   -----  -----------------    ----------------   ---------------   ----  -------
RAP1242              2     AIR-LAP1242AG-A-K9   00:18:74:fa:7d:1f  default location  1     US
LAP1242-1            2     AIR-LAP1242AG-A-K9   00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2            2     AIR-LAP1242AG-A-K9   00:14:1b:59:07:af  default location  1     US
```

11. Попытайтесь иметь условия линии прямой видимости между узлами. Если условия линии прямой видимости не существуют, создайте документы Зоны Френеля для получения near-line-of-site условий.
12. Если у вас есть несколько контроллеров, подключенных к той же ячеистой сети в помещении, то необходимо задать имя главного контроллера на каждом узле. В противном случае контроллер, который замечен сначала, будет взят в качестве основного.

Питание и конфигурация канала

Канал обратного рейса может быть настроен на RAP. MAP настроятся на канал RAP. Локальный доступ может быть настроен независимо для MAP.

От GUI Коммутатора придерживайтесь пути: **Беспроводные сети> 802.11a радио> настраивают**.

Примечание: Уровень Мощности передатчика по умолчанию на обратном рейсе является самым высоким уровнем мощности (Уровень 1), и Управление радиоресурсами (RRM) ВЫКЛЮЧЕНО по умолчанию.

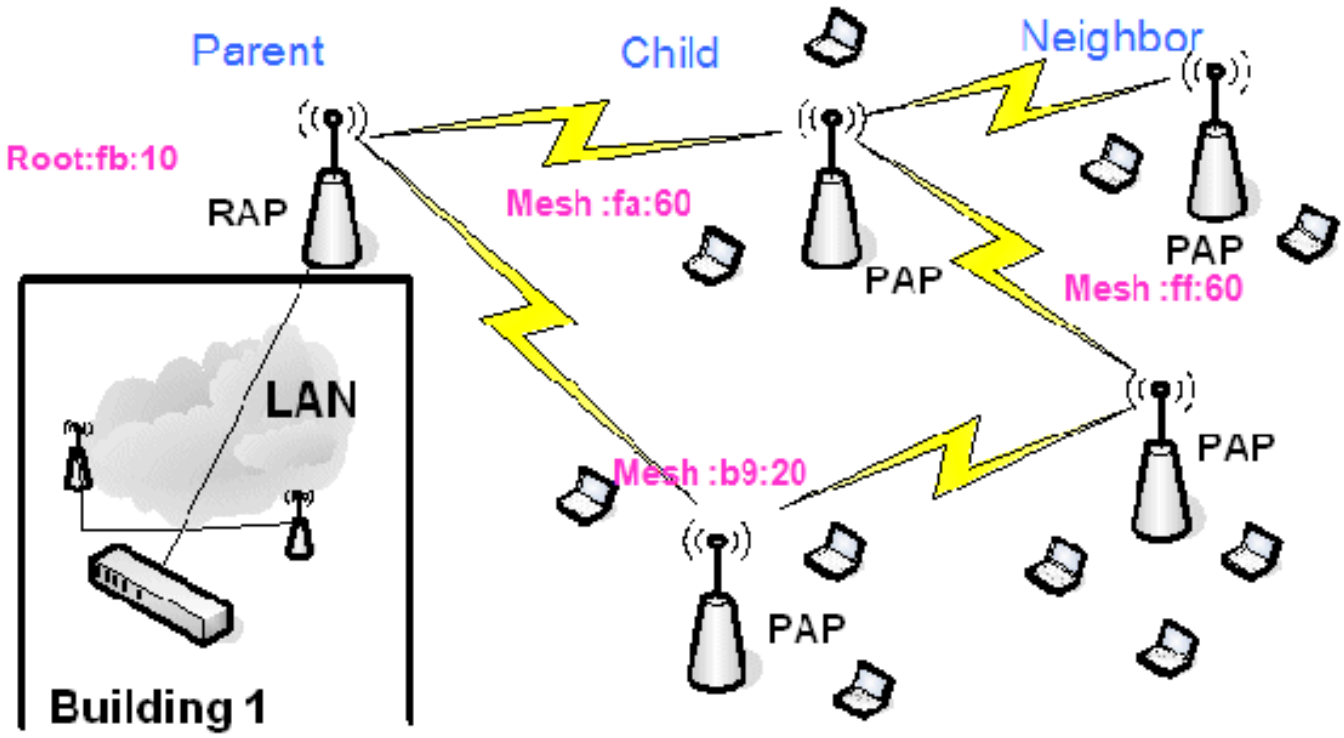
Если вы располагаете RAP, мы рекомендуем использовать альтернативные соседние каналы на каждом RAP. Это уменьшит помехи от соседних каналов.

Проверка RF

В ячеистой сети в помещении мы должны проверить Родительско - дочерние отношения между узлами. **Переход** является беспроводным соединением между этими двумя радио. Родительско - дочерние отношения изменяются, когда вы перемещаетесь через сеть. Это зависит от того, где вы находитесь в ячеистой сети в помещении.

Радио ближе к контроллеру в беспроводном соединении (переход) является **Родителем** радио с другой стороны перехода. Во множественной системе перехода существует структура древовидного типа, где узел, связанный с Контроллером, является RAP **(Родитель)**. Непосредственный узел с другой стороны первого перехода является **Потомком**, и последующие узлы во втором переходе и далее являются **Соседними узлами** к тому определенному Родителю.

Рисунок 1: Две сети перехода



На рисунке 1 названия AP упомянуты для удобства. В выстреле следующего экрана исследуется **RAP (fb:10)**. Этот узел видит (в действительном развертывании) Внутренние AP Сетки **(fa:60 и b9:20)** как потомки и **MAP ff:60 как соседний узел**.

От графического интерфейса пользователя (GUI) коммутатора придерживайтесь пути: **Беспроводные сети> Все AP> Rap1> Соседняя Информация**.

Гарантируйте, что Родительско-дочерние Отношения установлены и поддержаны правильно для вашей Ячеистой сети в помещении.

Проверьте соединения

покажите, что Сетка является информативной командой для проверки взаимосвязанности в сети.

Необходимо дать эти команды в каждом узле (AP) с помощью CLI Контроллера и загрузить результаты, одним словом, или текстовый файл к узлу загрузки.

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

В вашей ячеистой сети в помещении выберите множественную ссылку перехода и выполните эти команды, запускающиеся с RAP. Загрузите результат команд к узлу загрузки.

В следующем разделе все эти команды были выполнены для Двух Ячеистых сетей в помещении Перехода, показанных на рисунке 1.

Покажите внутренний путь сетки

Эта команда покажет вам MAC-адреса, радио-роли узлов, Сигнала к Отношениям сигнал/шум (SINR) в dBs для Канала от абонента к оператору/Нисходящей линии (SNRUp, SNRDown), и SNR Ссылки в дБ для отдельного пути.

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------  ------- ------ -------- -------- -------  -----
RAP1242          is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------  ------- ------ -------- -------- -------  -----
LAP1242-1          56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242            56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242          is a Root AP.
```

Покажите внутреннюю сводку соседнего узла сетки

Эта команда покажет вам MAC-адреса, родительско - дочерние отношения и Канал от абонента к оператору/Нисходящую линию SNRs в дБ.

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------  ------- ------ -------- -------- -------  -----
LAP1242-2          56      0      0        0        0x860    BEACON
LAP1242-1          56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------  ------- ------ -------- -------- -------  -----
LAP1242-2          56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242            56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

К этому времени должна существовать возможность видеть отношения между узлами вашей сети и проверить подключение RF путем наблюдения SNR оценивают для каждой

ссылки.

Безопасность консольного доступа AP

Эта функция дает усиленную безопасность консольному доступу AP. Консольный кабель для AP требуется, чтобы использовать эту функцию.

Они поддерживаются:

- CLI для продвижения user-id/комбинации пароля к указанному AP:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- Команда CLI для продвижения сочетания имени пользователя и пароля ко всем AP зарегистрировалась к Контроллеру:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

С этими командами идентификатор пользователя/комбинация пароля, выдвинутый от контроллера, является персистентным через повторную загрузку на AP. Если AP очищен от контроллера, нет никакого режима безопасности доступа. AP генерирует trap-сообщение SNMP с успешной регистрацией в системе. AP будет также генерировать trap-сообщение SNMP на сбое регистрационного имени консоли в течение трех раз подряд.

Мостовое соединение Ethernet

Из соображений безопасности Порт Ethernet на MAP отключен по умолчанию. Это может быть включено только путем настройки Мостового соединения Ethernet на RAP и соответствующих MAP.

В результате Мостовое соединение Ethernet должно быть включено для двух сценариев:

- Когда вы хотите использовать внутренние узлы сетки в качестве мостов.
- Когда вы хотите подключить любое Устройство ethernet (такое как ПК/Портативный ПК, видеокамера и т.д.) на MAP с помощью его Порта Ethernet.

Путь: **Беспроводные сети>** Щелчок любой AP> **Сетка**.

Существует команда CLI, которая может использоваться для настройки расстояния между

узлами, делающими Мостовое соединение. Попытайтесь подключить Устройство ethernet как Видеокамера в каждом переходе и посмотрите производительность.

Усовершенствование имени группы моста

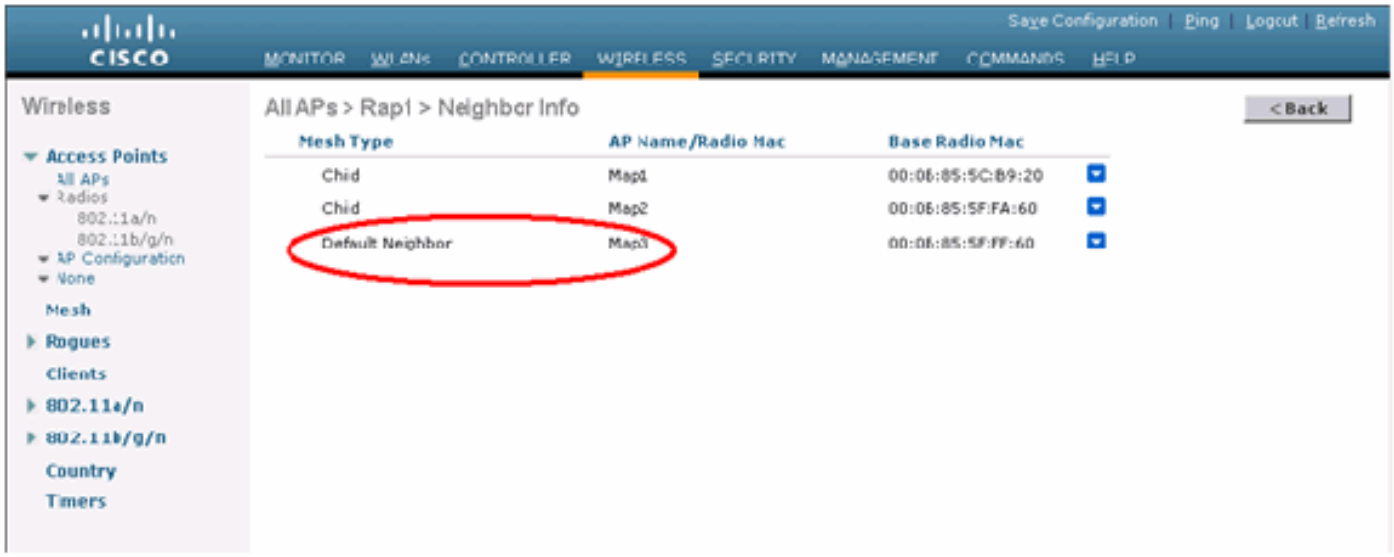
Возможно, что AP неправильно настроен с “bridgegroupname”, для которого это не было предназначено. В зависимости от организации сети этот AP может или может не быть в состоянии протянуться и найти его корректный сектор/дерево. Если это не может достигнуть совместимого сектора, это может стать скрученным.

Для восстановления такого скрученного AP понятие 'по умолчанию' bridgegroupname было представлено с 3.2.xx.x код. Основная идея - то, что AP, который неспособен соединиться с любым другим AP с его настроенным bridgegroupname, пытается соединиться с “по умолчанию” (слово) как bridgegroupname. Все выполнение узлов 3.2.xx.x и более позднее программное обеспечение принимает другие узлы с этим bridgegroupname.

Эта функция может также помочь в добавлении нового узла или неправильного настроенного узла к рабочей сети.

Если вы имеете рабочую сеть, берете предварительно сконфигурированный AP с другим BGN и заставляете его присоединиться к сети. Вы будете видеть этот AP в контроллере с помощью BGN “по умолчанию” после добавления его MAC-адреса в контроллере.

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



AP с помощью BGN по умолчанию может действовать как обычная Точка доступа ячеистой сети в помещении, привязывающая клиентов и формирующая Внутренние отношения отцов и детей Сетки.

Момент этот AP с помощью BGN по умолчанию находит другого родителя с корректным BGN, это переключится к нему.

Журналы - сообщения, системные, AP и trap-сообщение

Журналы сообщений

Включите уровень создания отчетов для журналов сообщений. От CLI контроллера выполните эту команду:

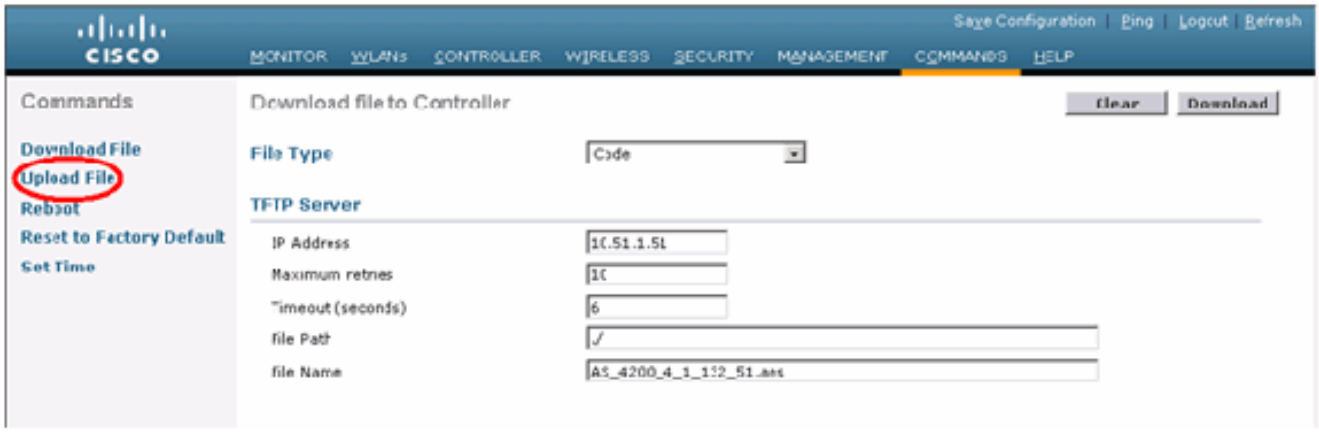
```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

Для наблюдения Журналов сообщений выполните эту команду от CLI Контроллера:

```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

Для загрузки Журналов сообщений используйте интерфейс Графического интерфейса контроллера:

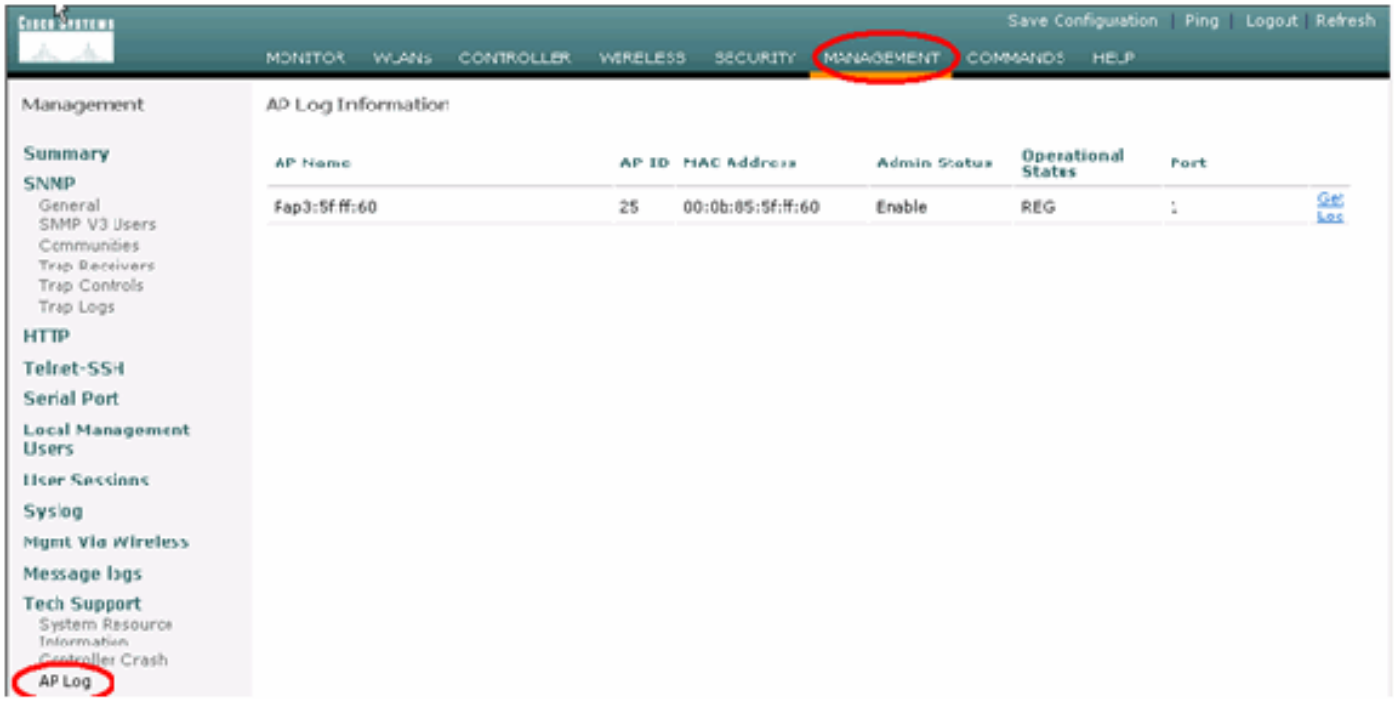
1. Нажмите **Commands>**
   Upload.



2. Введите свою информацию о сервере TFTP. Эта страница даст вам различные варианты для загрузки, и вы хотите, чтобы были переданы эти файлы:Журнал сообщенийЖурнал событийЖурнал trap-сообщенияФайл катастрофического отказа (если таковые имеются)Для проверки для файлов Катастрофического отказа нажмите **Management> Controller Crash**.

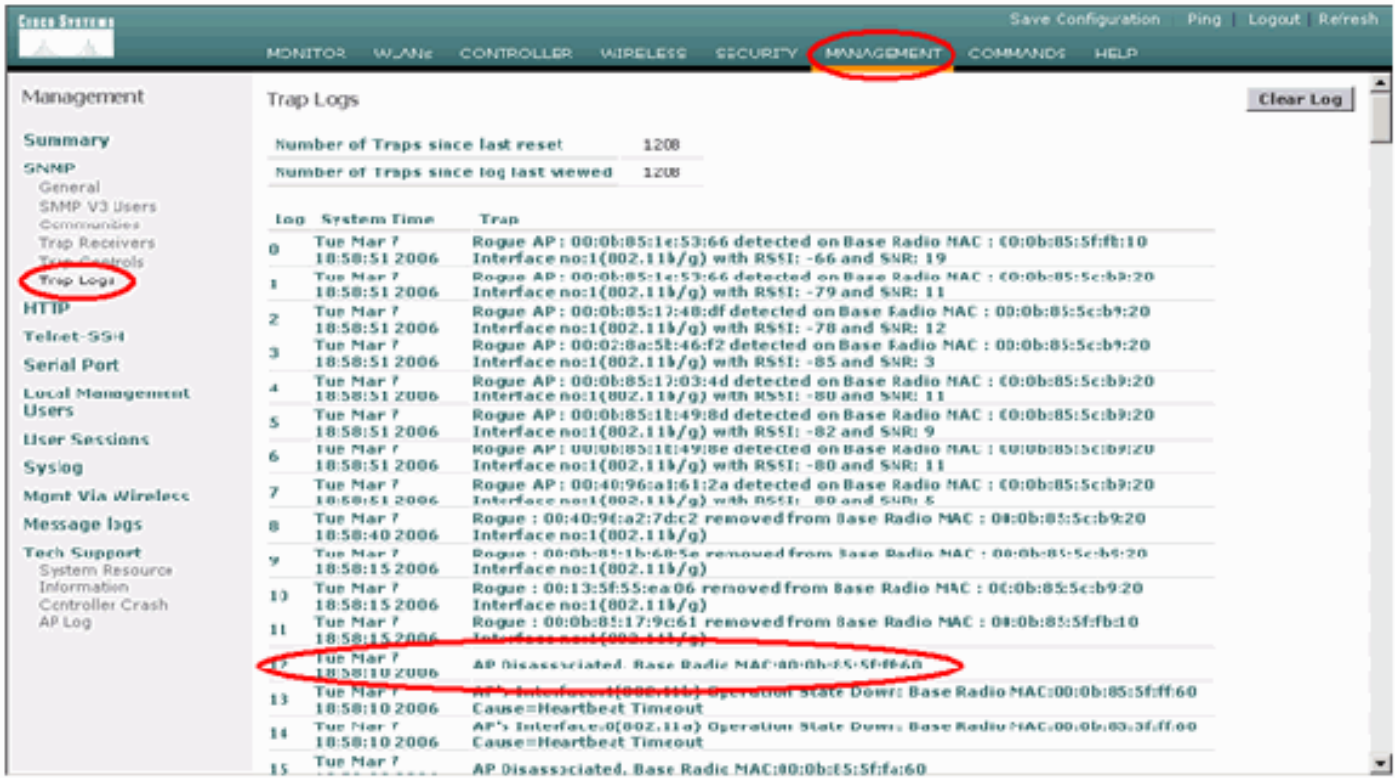
Журналы AP

Перейдите к этой странице GUI на контроллере для проверки журналов AP для локального AP, если таковые имеются:



Журналы trap-сообщения

Перейдите к этой странице GUI Контроллера и проверьте Журналы Trap-сообщения:



Производительность

Проверка сходимости запуска

Конвергенция является временем, потраченным RAP/MAP для установления стабильного соединения LWAPP с контроллером беспроводной локальной сети, запускающимся со времени, когда это сначала загрузилось, как перечислено здесь:

Проверка сходимости	Время согласования (min:sec)			
	RAP	MAP1	MAP2	MAP3
Обновление образа	2:34	3:50	5:11	6:38
Перезагрузка контроллера	0:38	0:57	1:12	1:32
Включите ячеистую сеть в помещении	2:44	3:57	5:04	6:09
Перезагрузка RAP	2:43	3:57	5:04	6:09
MAP возражает		3:58	5:14	6:25
Изменение MAP родителя (тот же канал)		0:38		

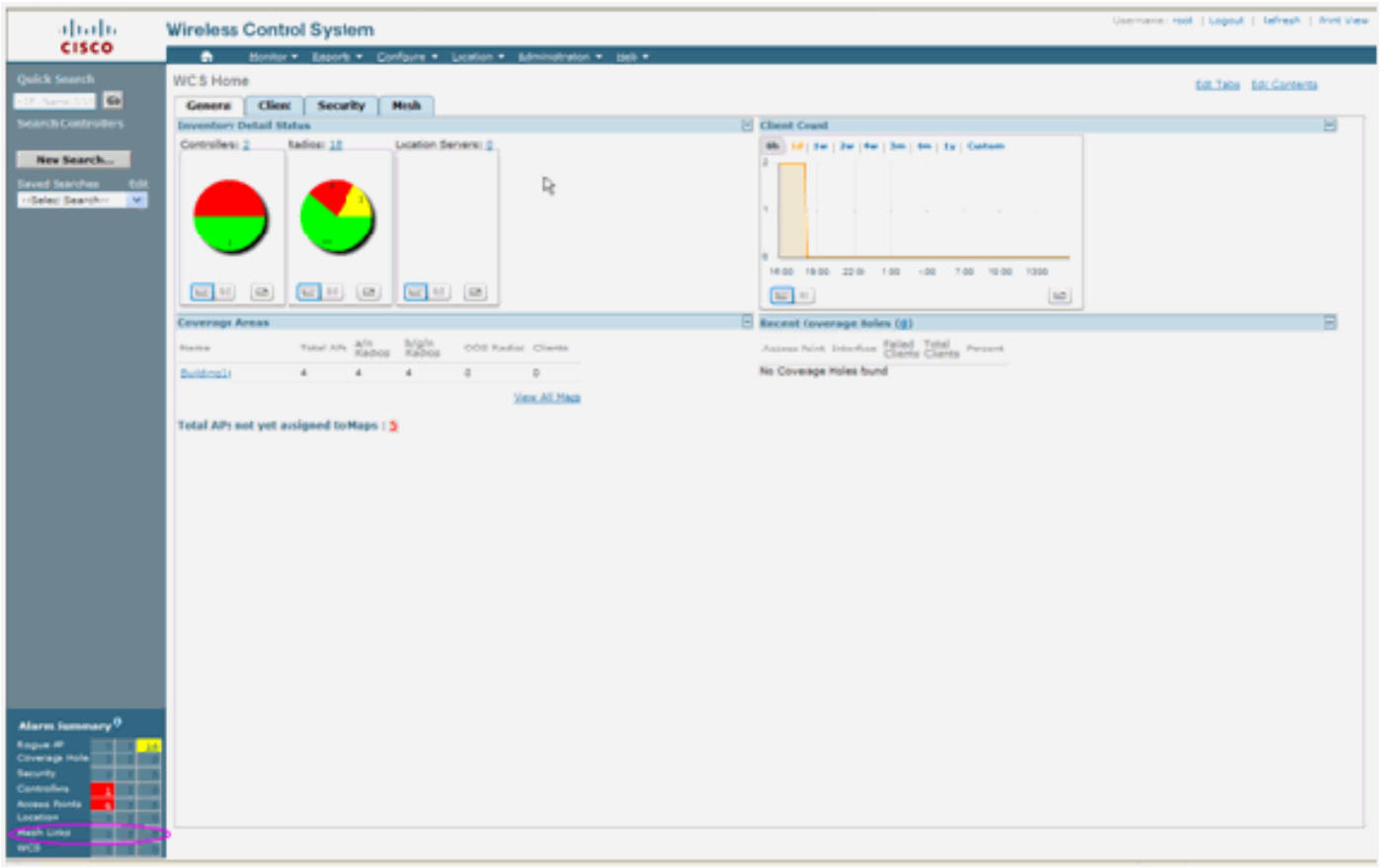
WCS

Внутренние сигналы тревоги сетки

WCS будет генерировать эти сигналы тревоги и события, отнесенные к ячеистой сети в помещении на основе trap-сообщений от Контроллера:

- Плохой SNR ссылки
- Измененный родитель
- Потомок переместился
- Изменения MAP часто порождают
- Событие консольного порта
- Сбой авторизации MAC
- Ошибки проверки подлинности
- Потомок исключил Родителя

Нажмите **Mesh Links**. Это покажет все сигналы тревоги, отнесенные внутренним каналам ячеистой сети.



Эти Сигналы тревоги применяются к внутренним каналам ячеистой сети:

- Если SNR ссылки падает ниже 12 дБ, плохой SNR ссылки - Этот сигнал тревоги генерируется. Пользователь не может изменить этот порог. Если плохой SNR будет обнаружен на ссылке обратного рейса для потомка/родителя, то trap-сообщение будет генерироваться. Trap-сообщение будет содержать значение SNR и MAC-адреса. Важность сигнала является Главной. SNR (сигнал к шуму), соотношение важно, потому что силы высокого сигнала недостаточно для обеспечения хорошей производительности получателя. Входящий сигнал должен быть более сильным, чем какой-либо шум или интерференция, которая присутствует. Например, если существует сильная интерференция или высокий уровень шума, возможно иметь силу высокого сигнала и все еще иметь плохую беспроводную производительность.
- Родитель изменился - Этот сигнал тревоги генерируется, когда потомок переместился к другому родителю. Когда родитель будет потерян, потомок присоединится к другому родителю, и потомок передаст trap-сообщение, содержащее и MAC-адреса старого родительского и нового родителя к WCS. Важность сигнала: Информационный.
- Потомок переместился - Этот сигнал тревоги генерируется, когда WCS добирается, Потомок потерял trap-сообщение. То, когда родительский AP обнаружил свою потерю потомка и не способный связаться с тем потомком, он передаст Потомку, потеряло trap-сообщение WCS. Trap-сообщение будет содержать дочерний MAC-адрес. Важность сигнала: Информационный.
- Родитель MAP часто изменялся - Этот сигнал тревоги генерируется, если Точка доступа ячеистой сети в помещении часто изменяет своего родителя. Когда родительский счетчик изменений MAP превысит порог в данной продолжительности, это передаст trap-сообщение к WCS. Trap-сообщение будет содержать число раз изменений MAP и продолжительность времени. Например, если будет 5 изменений в течение 2 минут, то trap-сообщение будет передаваться. Важность сигнала: Информационный.

- Когда потомок поместил в черный список родителя, дочерний Исключенный Родитель - Этот сигнал тревоги генерируется. Когда потомок был не в состоянии аутентифицироваться в Контроллере после фиксированного номера попыток, потомок может поместить в черный список родителя. Потомок помнит помещенного в черный список родителя и когда потомок присоединится к сети, она передаст trap-сообщение, которое содержит Помещенный в черный список Родительский MAC-адрес и продолжительность периода черного списка.

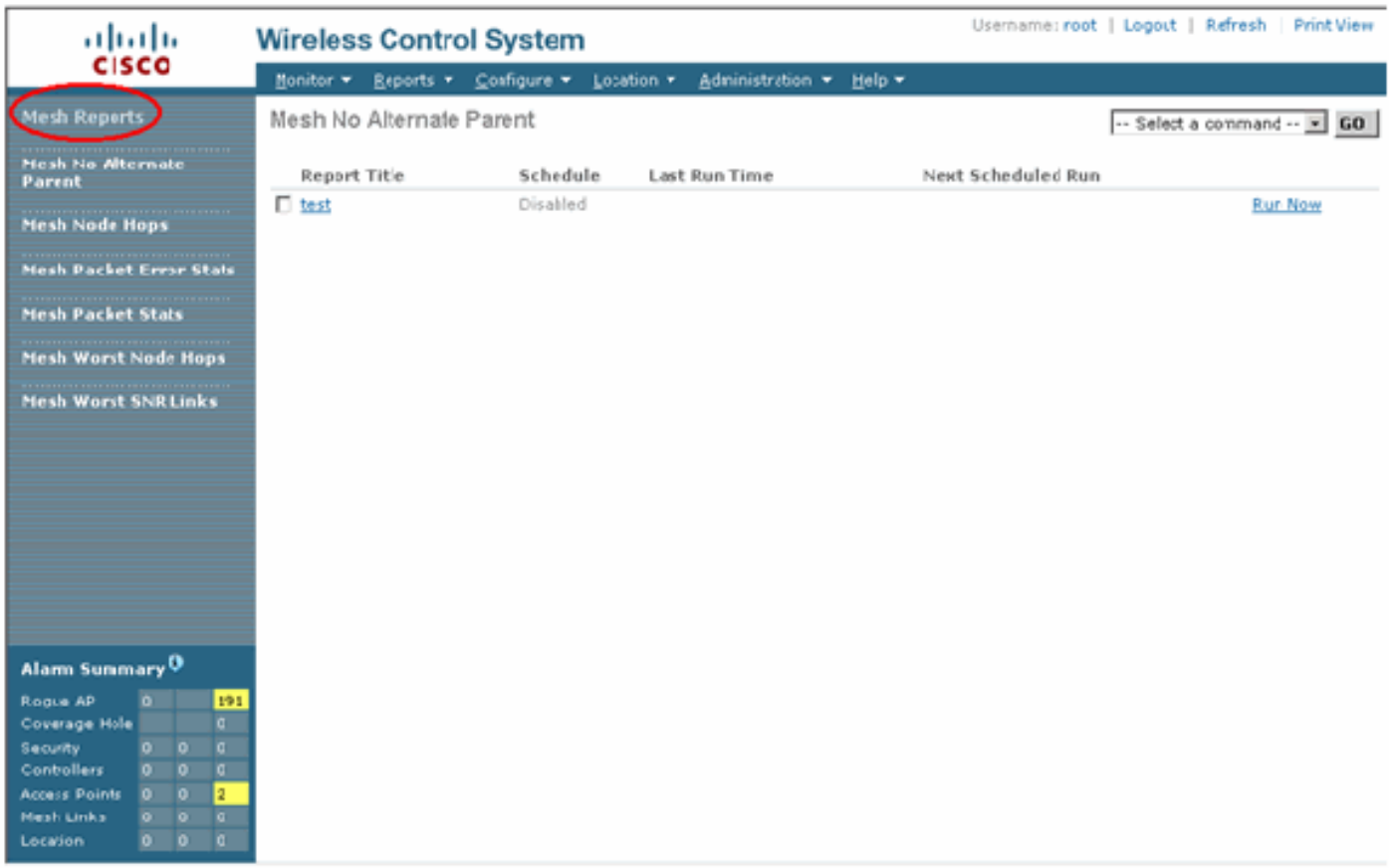
Сигналы тревоги кроме внутренних каналов ячеистой сети:

- Доступ Консольного порта - консольный порт предоставляет способность к клиенту изменить имя пользователя и пароль для восстановления скрученного наружного AP. Однако для предотвращения любого доступа авторизованного пользователя к AP WCS должен передать сигнал тревоги, когда кто-то пытается войти. Этот сигнал тревоги требуется, чтобы обеспечивать защиту, поскольку AP физически уязвим, в то время как расположено на открытом воздухе. Этот сигнал тревоги будет генерироваться, если пользователь успешно вошел к консольному порту AP, или если он отказал три раза подряд.
- Сбой авторизации MAC - Этот сигнал тревоги генерируется, когда AP пытается присоединиться к Внутренней Сетке, но не в состоянии аутентифицироваться, потому что это не находится в списке фильтров MAC. WCS получит trap-сообщение от Контроллера. Trap-сообщение будет содержать MAC-адрес AP, который не прошел авторизацию.

Отчёт о сетке и статистика

Мы переносим расширенный отчёт и платформу статистики от 4.1.185.0:

- Никакой альтернативный путь
- Переходы узла сетки
- Пакетный ошибочный Stats
- Пакетный Stats
- Худший переход узла
- Худшие ссылки SNR



Никакой альтернативный путь

Точка доступа ячеистой сети в помещении, как правило, имеет несколько соседних узлов. В случае, что точка доступа ячеистой сети в помещении высвобождает свою родительскую ссылку, AP должен быть в состоянии найти альтернативного родителя. В некотором случае, если не будет никаких показанных соседних узлов, то AP не будет в состоянии перейти к любым другим родителям, если это высвободит своих родителей. Важно для пользователя знать, какие AP не имеют альтернативных родителей. Это списки отчета все AP, которые не имеют никаких других соседних узлов кроме текущего родителя.

Внутренние переходы узла сетки

Этот отчёт показывает количество переходов далеко от Корневой точки доступа (RAP). Можно создать отчёт на основе этих критериев:

- AP контроллером
- AP полом

Коэффициенты пакетных ошибок

Ошибки пакета могут быть вызваны интерференцией и отбрасыванием пакета. Вычисление коэффициента пакетных ошибок основывается на переданных пакетах и пакетах, успешно переданных. Коэффициент пакетных ошибок измерен на ссылке обратного рейса и собран для обоих соседних узлов и родителя. AP периодически передает данные пакета к Контроллеру. Как только родитель изменяется, AP отсылает собранную информацию ошибки пакета в Контроллер. WCS опрашивает информацию об ошибке пакета от Контроллера каждые 10 минут по умолчанию и хранит его в базе данных в течение максимум 7 дней. В WCS коэффициент пакетных ошибок показывают как график. График

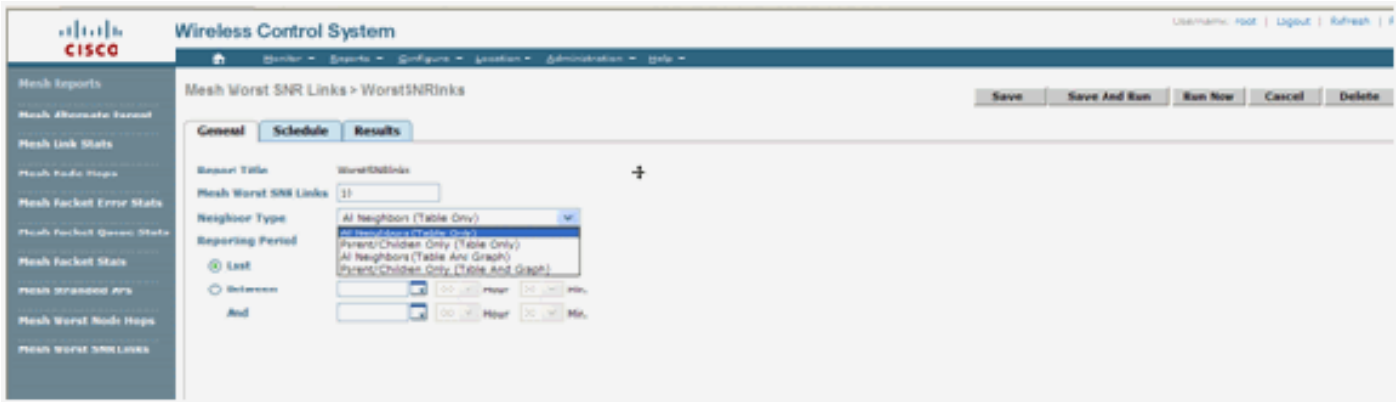
ошибки пакета основывается на исторических данных, хранивших в базе данных.

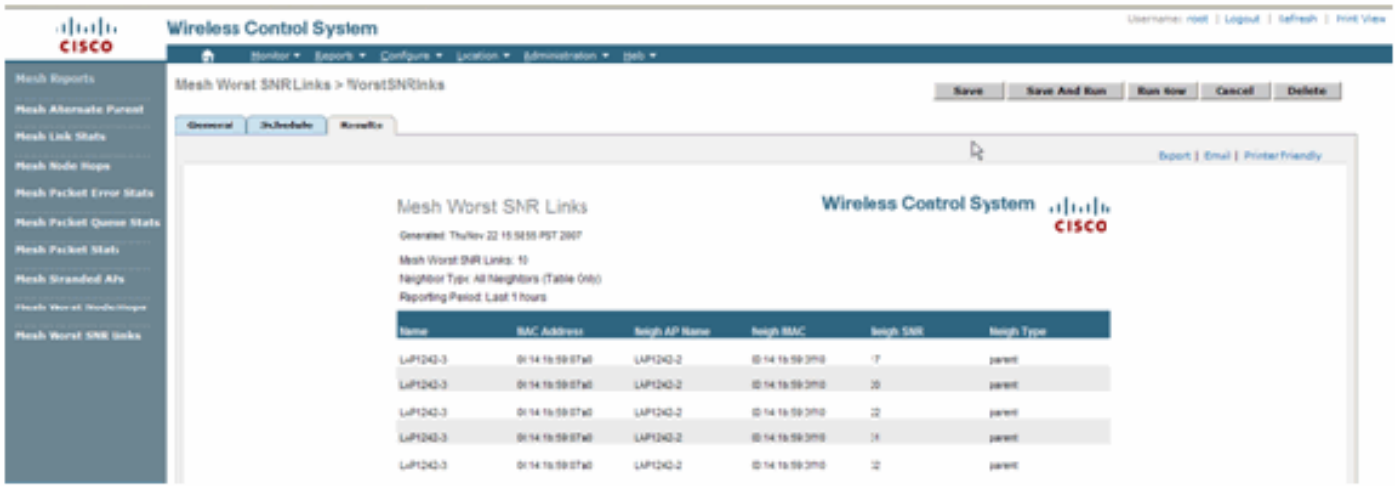
Пакетный Stats

Этот отчёт показывает значения счетчика соседних общих пакетов передачи и Соседних Общих пакетов, успешно переданных. Можно создать отчёт на основе определенных критериев.

Худшие ссылки SNR

Шумовые проблемы могли бы произойти в разное время, и шум мог бы увеличиться на других скоростях или продлиться в течение других промежутков времени. Следующий рисунок предоставляет способность создать отчёт и для Радио a и для b/g, а также выборочных интерфейсов. Списки отчета 10 худших SNR связываются по умолчанию. Можно выбрать из 5 до 50 худших ссылок. Отчёт может генерироваться в течение прошлого 1 часа, прошлых 6 часов, в последний день, продлиться 2 дня и до 7 дней. Данные опрошены каждые 10 минут по умолчанию. Данные сохранены в базе данных в течение максимальных семи дней. Соседние критерии Выбора типа могут быть Всеми Соседними узлами, Родителем/Потомками только.

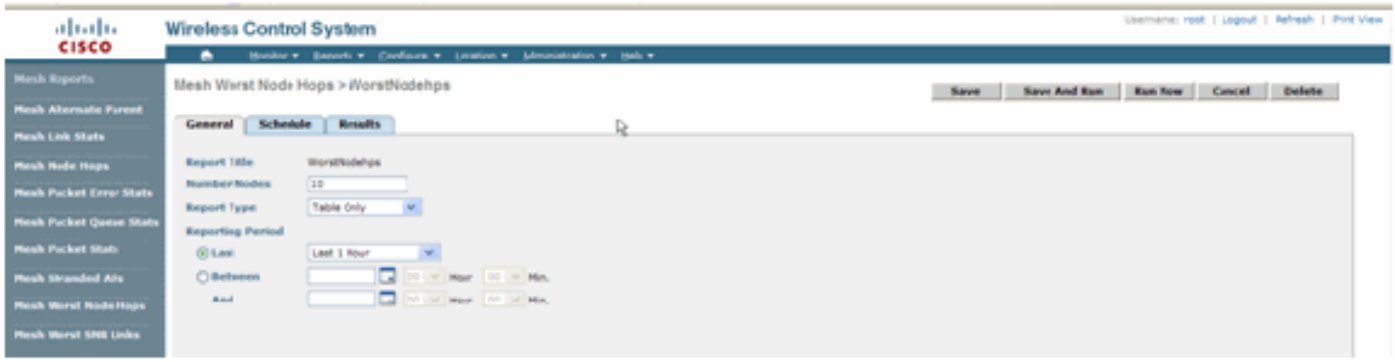




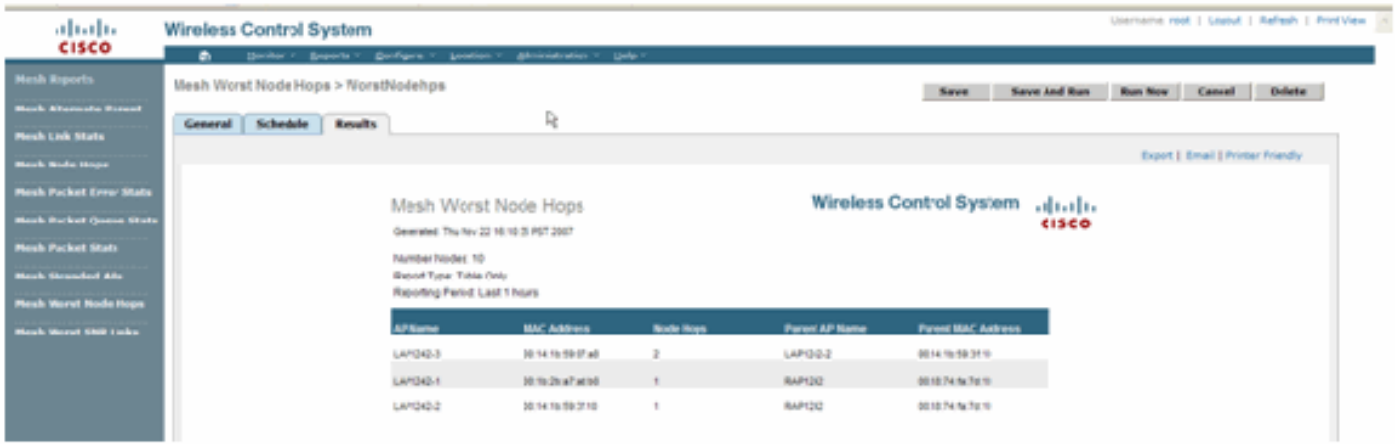
Худшие переходы узла

Это списки отчета the10 худшие AP переходов по умолчанию. Если AP являются слишком многими переходами далеко, ссылки могли бы быть очень слабыми. Пользователь может изолировать AP, которые имеют много переходов далеко от Корневой точки доступа и принимают соответствующие меры. Можно принять решение изменить это **Количество** критериев **Узлов** между 5 и 50. Критерии фильтра **Типа отчета** на этом рисунке могут быть

Таблицей Только или Таблицей и Графиком:



Эти данные показывают результат для последнего отчёта:



Статистика безопасности

Внутренние статистические данные Безопасности Сетки отображены на Странице сведений о точке доступа под информационным разделом Мостового соединения. Когда дочерний внутренний узел сетки связывается или аутентифицируется с родительским Внутренним узлом Сетки, запись во Внутренней таблице Статистической величины MeshNodeSecurity создана. Когда Внутренний узел Сетки разъединяет с Контроллером, записи удалены.

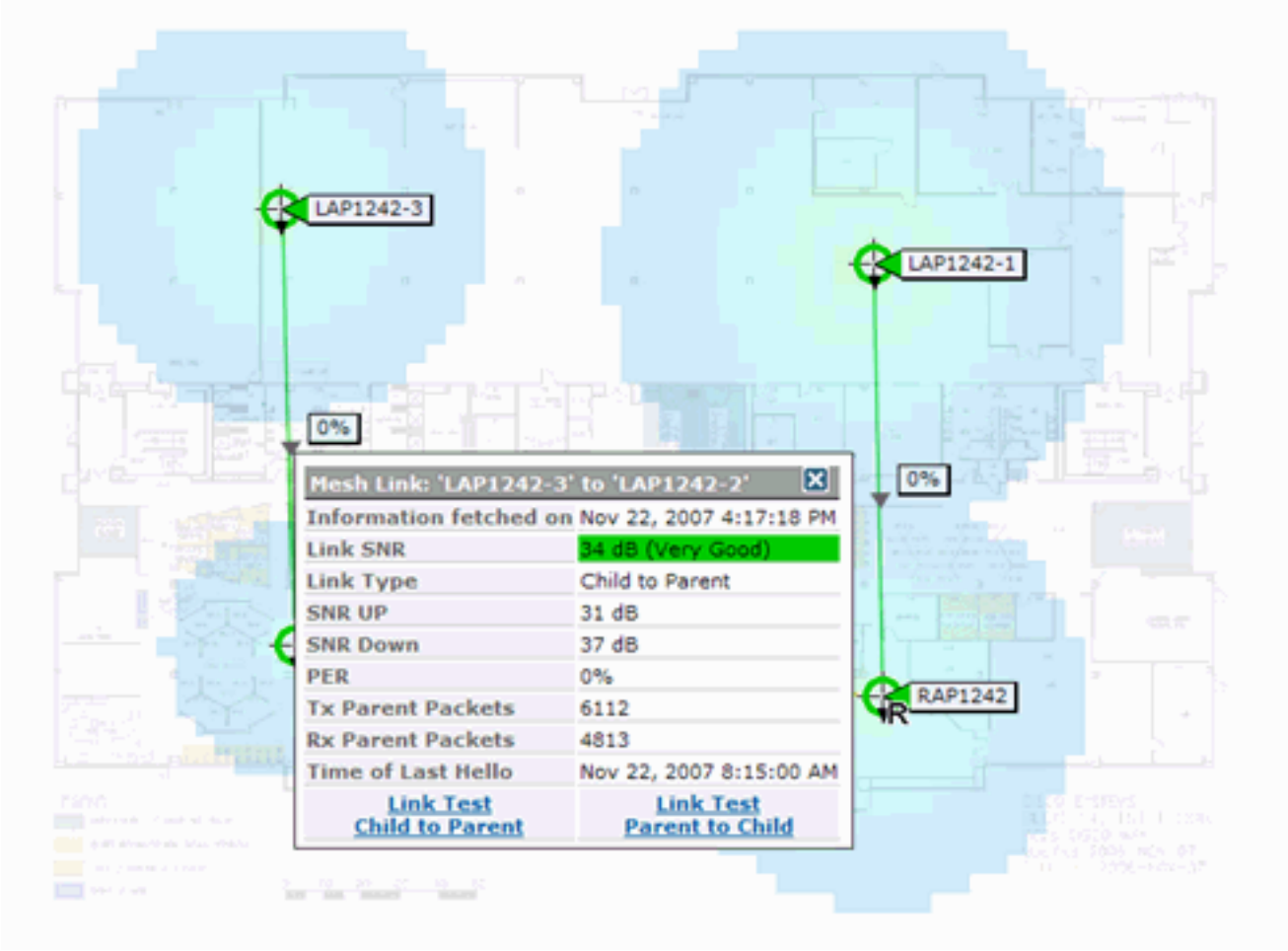
Тестирование канала

Тестирование канала ОТ AP К AP поддерживается на WCS. Можно выбрать любые два AP и вызвать тестирование канала между двумя.

Если те AP являются соседними узлами RF, то тестирование канала может иметь результат. Результат показывают в диалоговом окне на самой карте без завершенного обновления страницы. От диалогового окна можно избавиться легко.

Однако, если те 2 AP не являются соседними узлами RF, то WCS не пытается выяснить путь между 2 AP, чтобы сделать тест сложного соединения объединения.

Когда мышь отодвинута стрелка на ссылке между этими двумя узлами, это окно появляется:



Тестирование канала узла - узла

Программное средство Тестирования канала по требованию программное средство для проверки качества канала между любыми двумя AP. В WCS эта опция добавлена на Странице сведений о точке доступа.

На Странице сведений о точке доступа, под вкладкой **Indoor Mesh Link**, где ссылки перечислены рядом с ним, существует ссылка для выполнения тестирования канала.

Программное средство Тестирования канала CLI Контроллера имеет дополнительные параметры ввода: Размер пакета, пакеты тестирования Общего размера канала, продолжительность теста и скорость Канала передачи данных. Тестирование канала имеет значения по умолчанию для этих дополнительных параметров. MAC-адреса для Узлов являются единственными обязательными параметрами ввода.

Программное средство Тестирования канала тестирует силу, пакет, переданный и пакет, полученный между узлами. Ссылка для Тестирования канала отображена на сведениях отчета AP. При щелчке на ссылку существует всплывающий экран, показывая результаты Тестирования канала. Тестирование канала только будет применимо к Родительскому Потомку и среди соседних узлов.

Выходные данные Link Test генерируют переданные Пакеты, полученные Пакеты, Ошибочные пакеты (блоки по diff причинам), SNR, Минимальный уровень шума и RSSI.

Тест Lnk предоставляет эту подробную информацию о GUI как минимум:

- Переданные пакеты тестирования канала
- Полученные пакеты тестирования канала
- Уровень сигнала в ДБм
- Отношение сигнала к шуму

По требованию ссылки соседнего узла AP

Это - новая характеристика в Карте WCS. Можно щелкнуть по Mesh AP, и всплывающее окно с подробной информацией появляется. Можно тогда нажать **View Mesh Neighbors**, который выбирает сведения о соседях для выбранного AP и отображает таблицу со всеми соседними узлами к выбранной точке доступа ячеистой сети в помещении.

Обзорная Ссылка Соседнего узла Сетки отображает все соседние узлы к выделенному AP. Этот снимок показывает всем соседним узлам, Типу соседних узлов и значению SNR.

Эхо - тест (ping test)

Эхо - тест (ping test) по требованию, программное средство использовало пропинговывать между Контроллером и AP. Программное средство Эхо - теста (ping test) доступно и в Странице сведений о точке доступа и в MAP. Щелкните по ссылке **Эхо - теста (ping test) Выполнения** или в Странице сведений о точке доступа или от информации AP MAP для инициирования эхо-запроса от Контроллера до текущего AP.

Заключение

Сетка предприятия (т.е. внутренняя сетка) являются расширением покрытия беспроводной связи Cisco к местам, где проводной ethernet не может предоставить подключение. Гибкость и управляемость беспроводной сети выполнены с сеткой Предприятия.

Большинство соединенных проводом AP функций предоставляет, предоставлен внутренней топологией сетки. Сетка предприятия может также сосуществовать с проводными AP на том же контроллере.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация