Пример конфигурации узловой сети контроллера беспроводной LAN

Содержание

Введение

В этом документе приведен пример базовой конфигурации для создания двухточечного мостового канала с использованием ячеистой сети. В примере используются две облегченные точки доступа (lightweight access point, LAP). Одна точка LAP работает как точка доступа на крыше (roof-top access point, RAP), а другая — как точка доступа на столбе (pole-top access point, PAP), и они подключены к контроллеру беспроводной локальной сети Cisco (Cisco Wireless LAN (WLAN) Controller (WLC)). Точка доступа RAP подключена к WLC через коммутатор Cisco Catalyst.

См. Пример конфигурации Сети с ячеистой структурой Контроллера беспроводной локальной сети для Версий 5.2 и позже для выпуска 5.2 WLC и более поздних версий

Предварительные условия

- WLC настроен для главной операции.
- Контроллер WLC настроен в режиме "Уровень 3".

- Настроен коммутатор для WLC.

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Основные сведения о конфигурации точек LAPи контроллеров Cisco WLC
- Основные сведения о протоколе облегченных точек доступа (LWAPP).
- Сведения о конфигурации внешнего сервера DHCP и/или сервера доменных имен (сервера DNS)
- Сведения о базовой конфигурации коммутаторов Cisco

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- WLC Cisco серии 4402, который выполняет микропрограммное обеспечение 3.2.150.6
- Два (2) Cisco Aironet LAP серии 1510
- Коммутатор уровня 2 Cisco

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Общие сведения

Облегченные внешние точки доступа Cisco Aironet 1510 для ячеистых сетей

Cisco Aironet Легковесный Наружный AP Сетки серии 1510 является беспроводным устройством, разработанным для доступа беспроводного клиента и мостового соединения точка-точка, мостового соединения точка - много точек и возможности беспроводного подключения сетки точка - много точек. Внешняя точка доступа является автономным устройством, которое можно устанавливать на стене или свесе, на крыше или на уличном фонарном столбе.

Устройство AP1510 взаимодействует с контроллерами, чтобы обеспечить централизованное и масштабируемое управление, высокую безопасность и мобильность. Предназначенное для поддержки развертываний с нулевой конфигурацией, устройство AP1510 легко и безопасно подключается к ячеистой сети и доступно для управления сетью и ее контроля через графически интерфейс или интерфейс командной строки (CLI) контроллера.

Устройство AP1510 оснащено двумя одновременно работающими радиомодулями: 2,4-гигагерцовым модулем, используемым для клиентского доступа, и 5-гигагерцовым модулем, используемым для транзита данных на другие устройства AP1510. Трафик клиента по беспроводной локальной сети проходит через радиомодуль точки доступа, используемый для транзита данных, или ретранслируется через другие устройства AP1510, пока не достигнет места Ethernet-подключения к контроллеру.

Точка доступа RAP

RAP имеют проводное соединение с WLC Cisco. Они используют интерфейс беспроводного транзита данных для связи с соседними точками доступа PAP. Точки доступа RAP являются родительскими узлами для любой мостовой или ячеистой сети и соединяют мостовые и ячеистые сети с проводными сетями. Поэтому для любого сегмента мостовой или смешанной сети может быть только одна RAP.

Примечание: При использовании сетевого решения сетки для мостового соединения LAN-LAN не подключайте RAP непосредственно с WLC Cisco. Между Cisco WLC и RAP должен находиться коммутатор или маршрутизатор, так как контроллеры Cisco WLC не переадресуют Ethernet-трафик, поступающий из порта с включенной поддержкой протокола LWAPP. Точки доступа RAP могут работать по протоколу LWAPP в режиме "Уровень 2" или "Уровень 3".

Точка доступа PAP

PAP не имеют никакого проводного соединения с WLC Cisco. Они могут быть полностью беспроводными и поддерживать клиентов, которые обмениваются информацией с другими PAP или RAP, либо их можно использовать для подключения периферийных устройств или проводной сети. По умолчанию в целях безопасности порт Ethernet отключен, но для PAP его необходимо включать.

Примечание: Cisco Aironet 1030 Удаленных Граничных LAP поддерживают развертывания одного перехода, в то время как Легкий вес Cisco Aironet серии 1500 Наружные AP поддерживают и одиночный - и развертывания мультиперехода. Таким образом, точки доступа Cisco Aironet 1500 Series Lightweight Outdoor AP можно использовать в качестве точек доступа RAP, а также точек доступа PAP для одного или нескольких переходов от контроллера Cisco WLC.

Функции, не поддерживаемые на сетях с ячеистой структурой

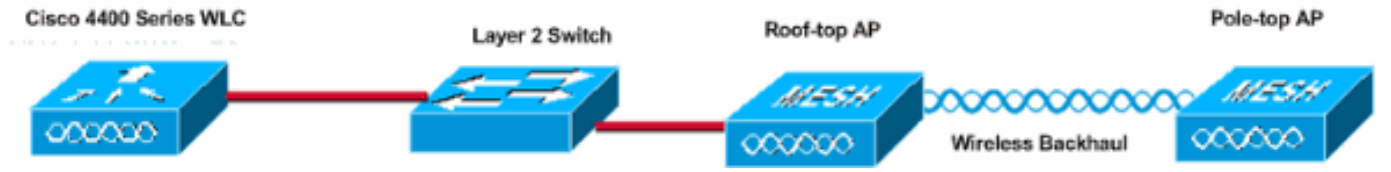
Эти функции контроллера не поддерживаются на сетях с ячеистой структурой:

- Поддержка мультистраны
- Основанный на загрузке CAC (Сети с ячеистой структурой поддерживают только основанный на пропускной способности, или статический, CAC.)
- Высокая доступность (быстрое биение и основное обнаружение присоединяются к таймеру),
- EAP-FASTv1 и аутентификация 802.1X
- EAP-FASTv1 и аутентификация 802.1X
- Локально значительный сертификат
- Услуги на основе определения местоположения

Последовательность запуска точек доступа

Этот список описывает то, что происходит, когда RAP и PAP запускают:

- Весь трафик проходит через точку доступа RAP и контроллер Cisco WLC, прежде чем отправляется в локальную сеть.
- Когда включается точка доступа RAP, к ней автоматически подключаются точки доступа PAP.
- Подключенный канал использует общий секрет, чтобы сформировать ключ, используемый для шифрования AES в канале.
- Как только удаленная точка доступа PAP подключается к RAP, точки доступа в ячеистой сети могут передавать трафик данных.
- Пользователи могут изменять общий секрет или настраивать точки доступа в ячеистой сети с помощью интерфейса командной строки (CLI) Cisco, веб-интерфеса пользователя контроллера Cisco или системы Cisco Wireless Control System (Cisco WCS). Компания Cisco рекомендует изменить общий секрет.



Настройка

Выполните следующие шаги, чтобы настроить контроллер WLC и точки доступа для мостового соединения типа "точка-точка".

1. Включите функцию Zero Touch Configuration на контроллере WLC.
2. Добавление MIC в список авторизованных точек доступа.
3. Настройка параметров мостового соединения для точек доступа.
4. Проверка конфигурации.

Включение функции "Zero Touch Configuration" (включена по умолчанию)

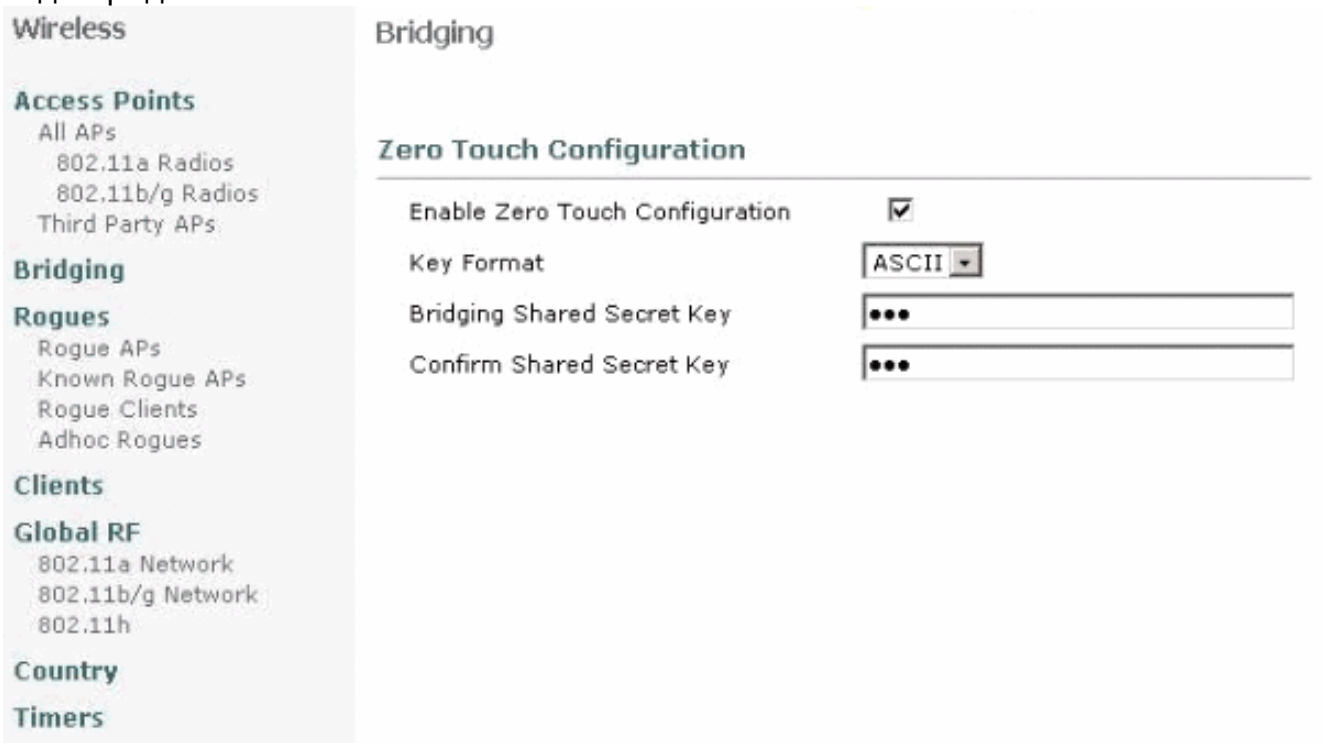
Конфигурация графического интерфейса пользователя (GUI)

Включите Нулевую Сенсорную Конфигурацию, позволяет AP получить общий секретный ключ от контроллера, когда это регистрируется в WLC. Если снять этот флажок, контроллер не предоставит общий секретный ключ, и точки доступа будут использовать стандартный предварительный общий ключ для надежных соединений. Значение по умолчанию включено (или выбрано). В графическом пользовательском интерфейсе WLC выполните следующие действия:

Примечание: Нет никакого условия для Нулевой Сенсорной конфигурации в версии 4.1 WLC и позже.

1. Выберите **Wireless> Bridging** и нажмите **Enable Zero Touch Configuration**.
2. Выберите формат ключа.
3. Введите общий секретный ключ для мостового соединения.

4. Еще раз введите общий секретный ключ для мостового соединения в поле для подтверждения.



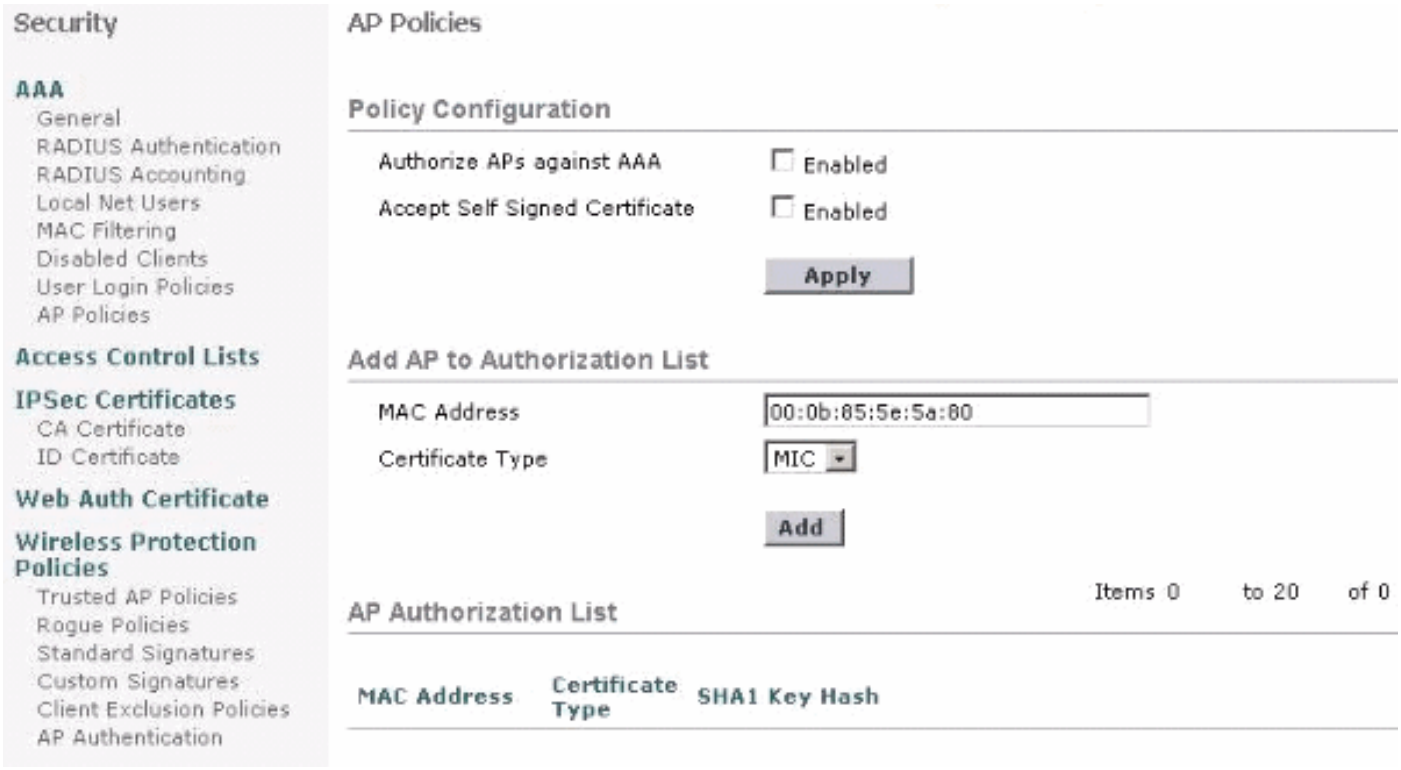
Конфигурация интерфейса командой строки CLI

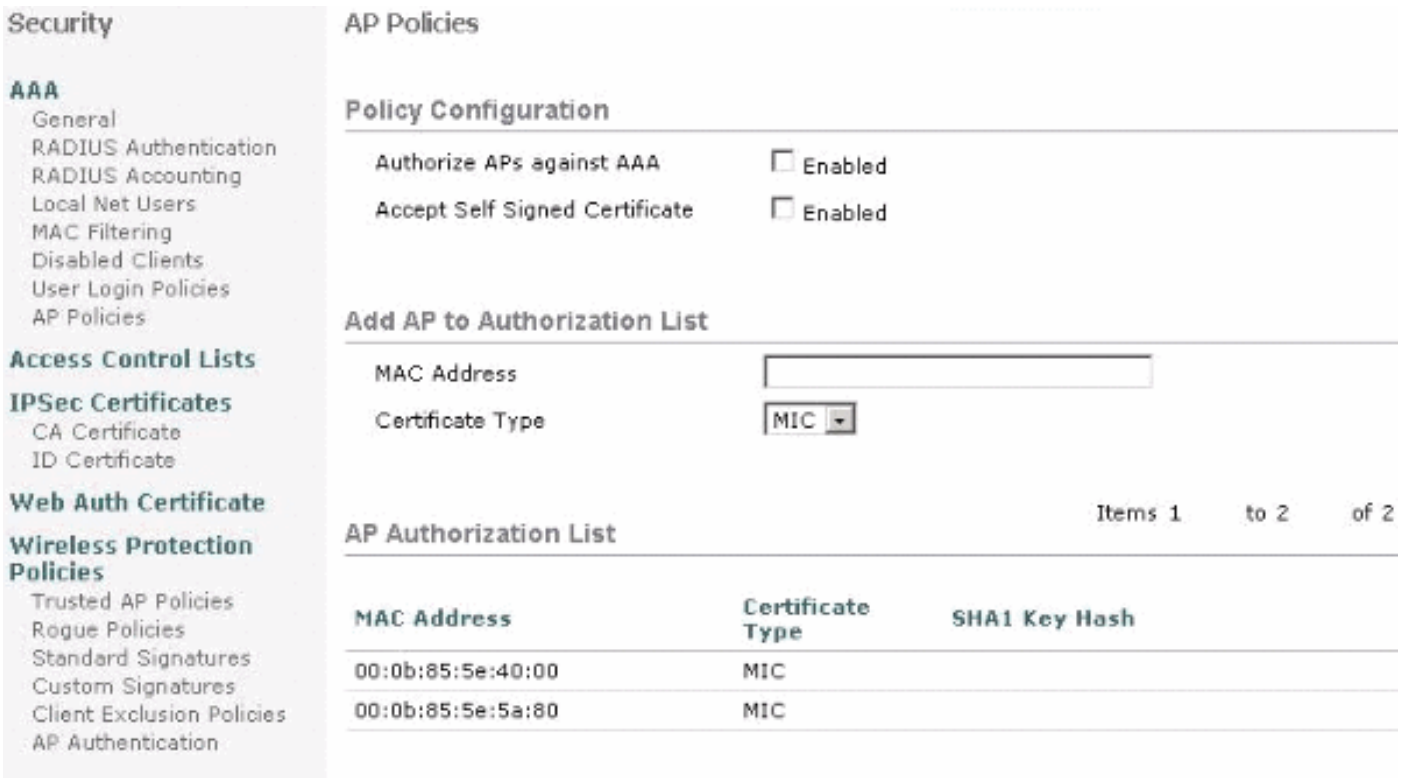
Выполните эти шаги от CLI:

1. **Введите команду config network zero-config enable, чтобы включить функцию Zero Touch Configuration.**`(Cisco Controller) >`**`config network zero-config enable`**
2. Выполните **команду config network bridging-shared-secret <string>** для добавления общего секретного ключа мостового соединения.`(Cisco Controller) >`**`config network bridging-shared-secret Cisco`**

Добавление MIC в список авторизованных точек доступа

Следующим шагом будет добавление точки доступа в список авторизованных точек доступа в WLC. Чтобы сделать это, выберите **Security> AP Policies**, войдите, MAC-адрес AP под Добавляют AP к Списку авторизации и **нажмите Add**.





В этом примере обе точки доступа (RAP и PAP) добавляются в список авторизованных точек доступа в контроллере.

Конфигурация интерфейса командой строки CLI

Выполните **команду config auth-list add mic <AP mac>** для добавления MIC к списку авторизации.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00 (Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80

!--- конфигурацию
```

В данном документе используется следующая конфигурация:

Cisco WLC 4402

```
(Cisco Controller) >show run-config Press Enter to
continue... System Inventory Switch
Description..............................  Cisco
Controller Machine
Model.................................. WLC4402-12
Serial Number.................................
FLS0943H005 Burned-in MAC
Address........................... 00:0B:85:40:CF:A0
Crypto Accelerator 1............................ Absent
Crypto Accelerator 2............................ Absent
Power Supply 1.................................. Absent
Power Supply 2.................................
Present, OK Press Enter to continue Or <Ctl Z> to abort
System Information Manufacturer's
Name............................. Cisco Systems, Inc
Product Name.................................... Cisco
Controller Product
Version................................ 3.2.150.6 RTOS
Version..................................... 3.2.150.6
Bootloader Version.............................
3.2.150.6 Build
Type..................................... DATA + WPS
System Name.....................................
lab120wlc4402ip100 System
Location................................ System
Contact................................. System
ObjectID.............................
1.3.6.1.4.1.14179.1.1.4.3 IP
Address.....................................
192.168.120.100 System Up
Time................................. 0 days 1 hrs 4
mins 6 secs Configured
Country.............................. United States
Operating Environment...........................
Commercial (0 to 40 C) Internal Temp Alarm
Limits...................... 0 to 65 C Internal
Temperature........................... +42 C State of
802.11b Network........................ Disabled State
of 802.11a Network......................... Disabled
Number of WLANs................................. 1 3rd
Party Access Point Support................... Disabled
Number of Active Clients........................ 0
Press Enter to continue Or <Ctl Z> to abort Switch
Configuration 802.3x Flow Control
Mode......................... Disable Current LWAPP
Transport Mode..................... Layer 3 LWAPP
Transport Mode after next switch reboot.... Layer 3 FIPS
prerequisite features...................... Disabled
Press Enter to continue Or <Ctl Z> to abort Network
Information RF-Network Name.....................
airespacerf Web Mode.....................................
Enable Secure Web Mode..........................
Enable Secure Shell (ssh).......................
Enable Telnet...................................
Enable Ethernet Multicast Mode..................
Disable Mode: Ucast User Idle
Timeout.......................... 300 seconds ARP Idle
Timeout.......................... 300 seconds ARP
Unicast Mode........................... Disabled Cisco
AP Default Master..................... Disable Mgmt Via
```

```
Wireless Interface..................... Enable Bridge AP
Zero Config....................... Enable Bridge Shared
Secret....................... youshouldsetme Allow Old
Bridging Aps To Authenticate...... Disable Over The Air
Provisioning of AP's.......... Disable Mobile Peer to
Peer Blocking................. Disable Apple Talk
............................... Disable AP Fallback
............................... Enable Web Auth
Redirect Ports ..................... 80 Fast SSID Change
.......................... Disabled Press Enter to
continue Or <Ctl Z> to abort Port Summary STP Admin
Physical Physical Link Link Mcast Pr Type Stat Mode Mode
Status Status Trap Appliance POE -- ------- ---- -------
---------- ---------- ------ ------- --------- ------- 1
Normal Forw Enable Auto 1000 Full Up Enable Enable N/A 2
Normal Forw Enable Auto 1000 Full Up Enable Enable N/A
Mobility Configuration Mobility Protocol
Port........................... 16666 Mobility Security
Mode........................... Disabled Default
Mobility Domain........................... airespacerf
Mobility Group members configured................. 3
Switches configured in the Mobility Group MAC Address IP
Address Group Name 00:0b:85:33:a8:40 192.168.5.70
<local> 00:0b:85:40:cf:a0 192.168.120.100 <local>
00:0b:85:43:8c:80 192.168.5.40 airespacerf Interface
Configuration Interface
Name................................... ap-manager IP
Address.....................................
192.168.120.101 IP
Netmask.....................................
255.255.255.0 IP
Gateway.....................................
192.168.120.1
VLAN........................................
untagged Active Physical
Port............................. 1 Primary Physical
Port............................. 1 Backup Physical
Port............................. Unconfigured Primary
DHCP Server............................... 192.168.1.20
Secondary DHCP Server...........................
Unconfigured
ACL.........................................
Unconfigured AP
Manager..................................... Yes
Interface Name..................................
management MAC
Address.....................................
00:0b:85:40:cf:a0 IP
Address.....................................
192.168.120.100 IP
Netmask.....................................
255.255.255.0 IP
Gateway.....................................
192.168.120.1
VLAN........................................
untagged Active Physical
Port............................. 1 Primary Physical
Port............................. 1 Backup Physical
Port............................. Unconfigured Primary
DHCP Server............................... 192.168.1.20
Secondary DHCP Server...........................
Unconfigured
ACL.........................................
Unconfigured AP
```

```
Manager..................................... No
Interface Name.............................
service-port MAC
Address.....................................
00:0b:85:40:cf:a1 IP
Address.....................................
192.168.250.100 IP
Netmask.....................................
255.255.255.0 DHCP
Protocol.................................... Disabled AP
Manager..................................... No
Interface Name.............................
virtual IP
Address..................................... 1.1.1.1
Virtual DNS Host Name.......................
Disabled AP
Manager..................................... No WLAN
Configuration WLAN
Identifier.................................. 1 Network
Name (SSID).............................
lab120wlc4402ip100
Status......................................
Enabled MAC
Filtering................................... Enabled
Broadcast SSID..............................
Enabled AAA Policy
Override.............................. Disabled Number
of Active Clients.......................... 0
Exclusionlist Timeout.......................... 60
seconds Session
Timeout................................. 1800 seconds
Interface...................................
management WLAN
ACL.........................................
unconfigured DHCP
Server...................................... Default
Quality of Service.............................. Silver
(best effort)
WMM.........................................
Disabled
802.11e.....................................
Disabled Dot11-Phone Mode
(7920)......................... Disabled Wired
Protocol.................................... None IPv6
Support..................................... Disabled
Radio Policy................................... All
Radius Servers
Authentication..............................
192.168.1.20 1812 Security 802.11
Authentication:........................ Open System
Static WEP Keys............................. Enabled
Key Index:..................................... 1
Encryption:.................................... 104-bit
WEP 802.1X..................................
Disabled Wi-Fi Protected Access (WPA1).................
Disabled Wi-Fi Protected Access v2 (WPA2).............
Disabled IP Security....................................
Disabled IP Security Passthru..........................
Disabled L2TP..........................................
Disabled Web Based Authentication......................
Disabled Web-Passthrough...............................
Disabled Auto Anchor....................................
Disabled Cranite Passthru..............................
Disabled Fortress Passthru.............................
```

```
Disabled RADIUS Configuration Vendor Id Backward
Compatibility.................. Disabled Credentials
Caching............................ Disabled Call
Station Id Type.......................... IP Address
Administrative Authentication via RADIUS.........
Enabled
Keywrap.....................................
Disabled Load Balancing Info Aggressive Load
Balancing....................... Enabled Aggressive
Load Balancing Window.................. 0 clients
Signature Policy Signature
Processing.......................... Enabled Spanning
Tree Switch Configuration STP
Specification..................... IEEE 802.1D STP Base
MAC Address................... 00:0B:85:40:CF:A0
Spanning Tree Algorithm................. Disable STP
Bridge Priority................... 32768 STP Bridge
Max. Age (seconds).......... 20 STP Bridge Hello Time
(seconds)........ 2 STP Bridge Forward Delay
(seconds)..... 15 Spanning Tree Port Configuration STP
Port ID.............................. 8001 STP Port
State............................. Forwarding STP Port
Administrative Mode................. 802.1D STP Port
Priority.......................... 128 STP Port Path
Cost......................... 4 STP Port Path Cost
Mode..................... Auto STP Port
ID................................ 8002 STP Port
State............................. Forwarding STP Port
Administrative Mode................. 802.1D STP Port
Priority.......................... 128 STP Port Path
Cost......................... 4 STP Port Path Cost
Mode..................... Auto
```

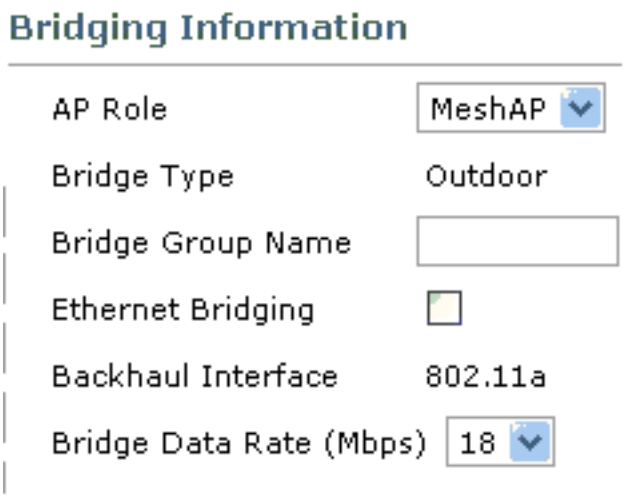
Настройка параметров мостового соединения для точек доступа

Этот раздел предоставляет инструкции по тому, как настроить роль AP в сети с ячеистой структурой и отнесенных параметрах мостового соединения. Эти параметры можно настроить с помощью GUI или CLI.

1. **Щелкните Wireless, а затем в разделе "Access Points" выберите All APs.** Появится страница "All APs".
2. Щелкните **по Подробной** ссылке для своего AP1510 для доступа к странице All APs> Details

На этой странице Режим AP под Общим автоматически собирается Соединить для AP, которые имеют функциональность моста, такую как AP1510. На указанной странице эти сведения также представлены в разделе "Bridging Information". В разделе "Bridging Information" выберите один из следующих параметров, чтобы указать роль этой точки доступа в ячеистой сети:

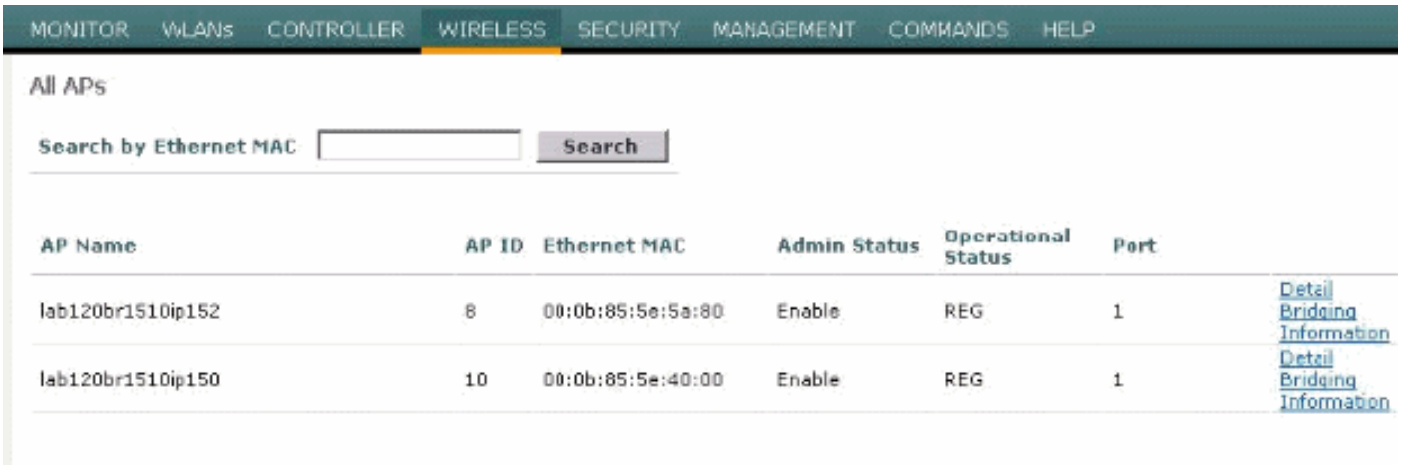
- **MeshAP. Выберите этот параметр, если у точки AP1510 есть беспроводное подключение к контроллеру.**
- **RootAP. Выберите этот параметр, если у точки AP1510 есть проводное подключение к контроллеру.**



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

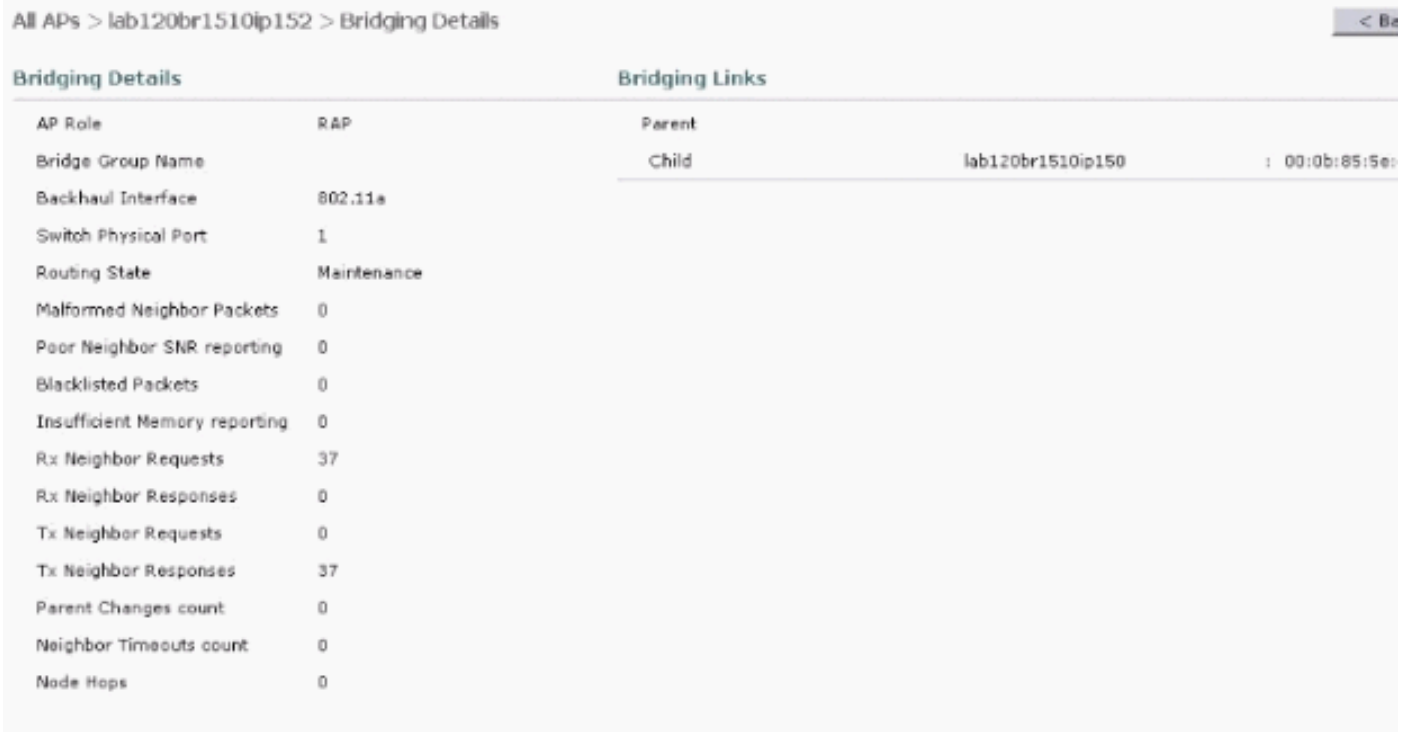
После того как точки доступа будут зарегистрированы в WLC, они станут доступны для просмотра на вкладке "Wireless" в верхней части интерфейса контроллера WLC:



В интерфейсе командной строке можно использовать команду show ap summary для проверки регистрации точек доступа на контроллере беспроводной локальной сети:

```
(Cisco Controller) >show ap summary AP Name Slots AP Model Ethernet MAC Location Port ----------
-------- ----- ---------- ---------------- ---------------- ---- lab120br1510ip152 2 OAP1500
00:0b:85:5e:5a:80 default_location 1 lab120br1510ip150 2 OAP1500 00:0b:85:5e:40:00
default_location 1 (Cisco Controller) >
```

В графическом щелкните Bridging Details, чтобы проверить роль точки доступа:



На CLI можно использовать **show mesh path <AP Cisco>** и **команды show mesh neigh <Cisco AP>**, чтобы проверить, что AP зарегистрировались в WLC:

```
(Cisco Controller) >show mesh path lab120br1510ip152 00:0B:85:5E:5A:80 is RAP (Cisco Controller) >show mesh neigh lab120br1510ip152 AP MAC : 00:0B:85:5E:40:00 FLAGS : 160 CHILD worstDv 255, Ant 0, channel 0, biters 0, ppiters 10 Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0 adjustedEase 0, unadjustedEase 0 txParent 0, rxParent 0 poorSnr 0 lastUpdate 1150103792 (Mon Jun 12 09:16:32 2006) parentChange 0 Per antenna smoothed snr values: 0 0 0 0 Vector through 00:0B:85:5E:40:00 (Cisco Controller) >
```

Устранение неполадок

`Mesh APs doesn't associate to the WLC` является одной из наиболее распространенных проблем, замеченных в Развертывании ячеистой сети. Проверьте следующее:

1. Проверьте, что MAC-адрес точки доступа добавлен в Списке фильтров Mac в WLC. Это может быть замечено под **Безопасностью> фильтрация Mac**.
2. Проверьте общий секретный ключ между RAP и MAP. Когда существует несоответствие в ключе, вы видите это сообщение в WLC." `LWAPP Join-Request AUTH_STRING_PAYLOAD, invalid BRIDGE key hash AP 00:0b:85:68:c1:d0"` **Примечание:** Всегда пытайтесь использовать **Разрешать Нулевые Сенсорные Параметры конфигурации** при наличии для версии. Это автоматически настраивает ключ для AP Сетки и избегает неверных конфигураций.
3. RAP не передают широковещательных сообщений на своем Радиоинтерфейсе. Поэтому настройте сервер DHCP для передачи IP-адресов через индивидуальную рассылку так, чтобы MAP мог передать их IP-адреса RAP. В противном случае используйте статическое ip для MAP.
4. Или оставьте Имя группы моста в значениях по умолчанию или удостоверьтесь, что Имена группы моста настроены точно то же на MAP и соответствующем RAP.

Это проблемы, которые являются определенными, чтобы Поймать в сети точки доступа. Для проблем с подключением, которые распространены между WLC и точкой доступа, обратитесь для Устранения проблем Облегченной точки доступа, Не Присоединяющейся к

Контроллеру беспроводной локальной сети.

Команды для устранения неполадок

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Для устранения неполадок WLC можно использовать следующие команды:

- **состояние debug pem позволяет** — Используемый настроить менеджера политики доступа параметры отладки.
- **события debug pem позволяют** — Используемый настроить менеджера политики доступа параметры отладки.
- **сообщение debug dhcp включает** — Показывает отладку сообщений DHCP, к которым обмениваются и от сервера DHCP.
- **debug dhcp packet enable** — Показывает отладку подробных данных пакета DHCP, которые передаются и от сервера DHCP.

Вот несколько дополнительных команд debug, которые можно использовать для устранения неполадок:

- **debug lwapp errors enable** — Показывает отладку Ошибок lwapp.
- **debug pm pki enable** отладку сообщений сертификата, которые передают между AP и WLC.

Следующие выходные данные команды WLC debug lwapp events enable показывают регистрацию точки LAP в контроллере WLC:

```
(Cisco Controller) >debug lwapp events enable Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00
Received LWAPP JOIN REQUEST from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1' Mon Jun
12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce 00:0B:85:40:CF:A0 rxNonce
00:0B:85:5E:40:00 Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00
Successfully added NPU Entry for AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101,
Switch Port: 12223, intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop MAC:
00:0b:85:5e:40:00 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Join-Reply to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP
event for AP 00:0b:85:5e:40:00 slot 0 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP
event for AP 00:0b:85:5e:40:00 slot 1 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP
CONFIGURE REQUEST from AP 00:0b:85:5e:40:00 to 00:0b:85:40:cf:a3 Mon Jun 12 09:04:59 2006:
00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00 -- static 1,
192.168.120.150/255.255.255.0, gtw 192.168.120.1 Mon Jun 12 09:04:59 2006: spamVerifyRegDomain
RegDomain set for slot 0 code 0 regstring -A regDfromCb -A Mon Jun 12 09:04:59 2006:
spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -A Mon Jun 12
09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret
airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to AP 00:0b:85:5e:40:00
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100' Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100' Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00
associated. Last AP failure was due to Link Failure, reason: STATISTICS_INFO_RES Mon Jun 12
09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00 Mon
Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event
Response to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00
apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0 Mon Jun
12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 0!
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP
00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT
```

```
from AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission
of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006:
00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP
00:0b:85:5e:40:00 slot 1 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event
for AP 00:0b:85:5e:40:00 slot 1! Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP
CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00
Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00
```

Дополнительные сведения

- Руководство по развертыванию сетевого решения сетки Cisco
- Краткое руководство по началу работы: Легкий вес Cisco Aironet серии 1500 вне помещения поймал в сети точки доступа
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация