Пример конфигурации удаленного AP (REAP) с легкими APs и контроллерами беспроводной LAN (WLC)

Содержание

Введение

Возможности точки доступа удаленного края (REAP), начатые с единой беспроводной сети Cisco (UWN), позволяют удаленные развертывания точек доступа облегченного Cisco (LAP) от беспроводной локальной сети (WLAN) контроллер (WLC). Это делает их идеальными для филиала компании и небольших розничных местоположений. Этот документ объясняет способ развертывания сети WLAN на основе REAP с использованием LAP серии Cisco 1030 и контроллеров WLC 4400.

Предварительные условия

Требования

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

- Знание WLC и как настроить основные параметры WLC
- Знание режима работы REAP в LAP Cisco 1030

- Знание конфигурации внешнего сервера DHCP и/или сервера Системы доменных имен (DNS)
- Знание понятий Защищенного доступа по протоколу Wi-Fi (WAP)

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет релиз микропрограммы 4.2
- LAP Cisco 1030
- Маршрутизаторы двух Cisco серии 2800, которые выполняют релиз 12.2 программного обеспечения Cisco IOS (13) T13
- Cisco Aironet 802.11a/b/g Клиентский адаптер, который выполняет релиз микропрограммы 3.0
- Версия 3.0 утилиты Cisco Aironet Desktop Utility

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

В режиме REAP точка доступа LAP может находится на другом конце канала WAN и при этом связываться с WLC и выполнять функции обычной LAP. Режим REAP поддерживается в настоящий момент только LAP серии 1030.

Для обеспечения этой функциональности 1030 REAP разделяет уровень управления Протокола LWAPP от плоскости беспроводных данных. WLC Cisco все еще используются для централизованного управления и управления таким же образом, что обычные основанные на LWAPP точки доступа (AP) используются, в то время как все пользовательские данные соединены локально в AP. Доступ к локальным сетевым ресурсам производится в перерывах связи WAN.

AP REAP поддерживают два режима работы:

- Обычный режим REAP
- Автономный режим

Когда канал WAN между AP REAP и WLC подключен, LAP установлен в обычном режиме REAP. Когда LAP работают в обычном режиме REAP, они могут поддержать до 16 WLAN.

Когда канал WAN между WLC и LAP выключается, ПОДДЕРЖИВАЮЩИЙ REAP LAP переключается на автономный режим. Если WLAN настроен или с Протоколом WEP или с каким-либо методом локальной проверки подлинности, в то время как в автономном

режиме, LAP REAP могут поддержать только один WLAN независимо без WLC. В этом случае WLAN, который поддерживает AP REAP, является первым WLAN, который настроен на AP, WLAN 1. Это вызвано тем, что большинство других методов аутентификации должно передать информацию к и от контроллера и, когда канал WAN не работает, эта операция не возможна. В автономном режиме LAP поддерживают минимальный набор функций. Эта таблица показывает набор функций, что LAP REAP поддерживает, когда это находится в автономном режиме по сравнению с функциями, которые LAP REAP поддерживает в обычном режиме (когда канал WAN подключен, и связь к WLC подключена):

Функции, что LAP REAP поддержки в обычном режиме REAP и в автономном режиме

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

Таблица показывает, что несколько интерфейсов VLAN не поддерживаются на LAP REAP в

режимах Both. Несколько интерфейсов VLAN не поддерживаются, потому что LAP REAP могут только находиться на одиночной подсети, потому что они не могут выполнить маркирование VLAN IEEE 802.1Q. Поэтому трафик на каждых из идентификаторов наборов сервисов (SSIDs) завершается в той же подсети как проводная сеть. В результате трафик данных не разделен на проводной стороне даже при том, что беспроводной трафик может быть сегментирован по воздуху между SSIDs.

См. Руководство по развертыванию REAP в Филиале компании для получения дополнительной информации о развертываниях REAP, и как управлять REAP и его ограничениями.

Настройка

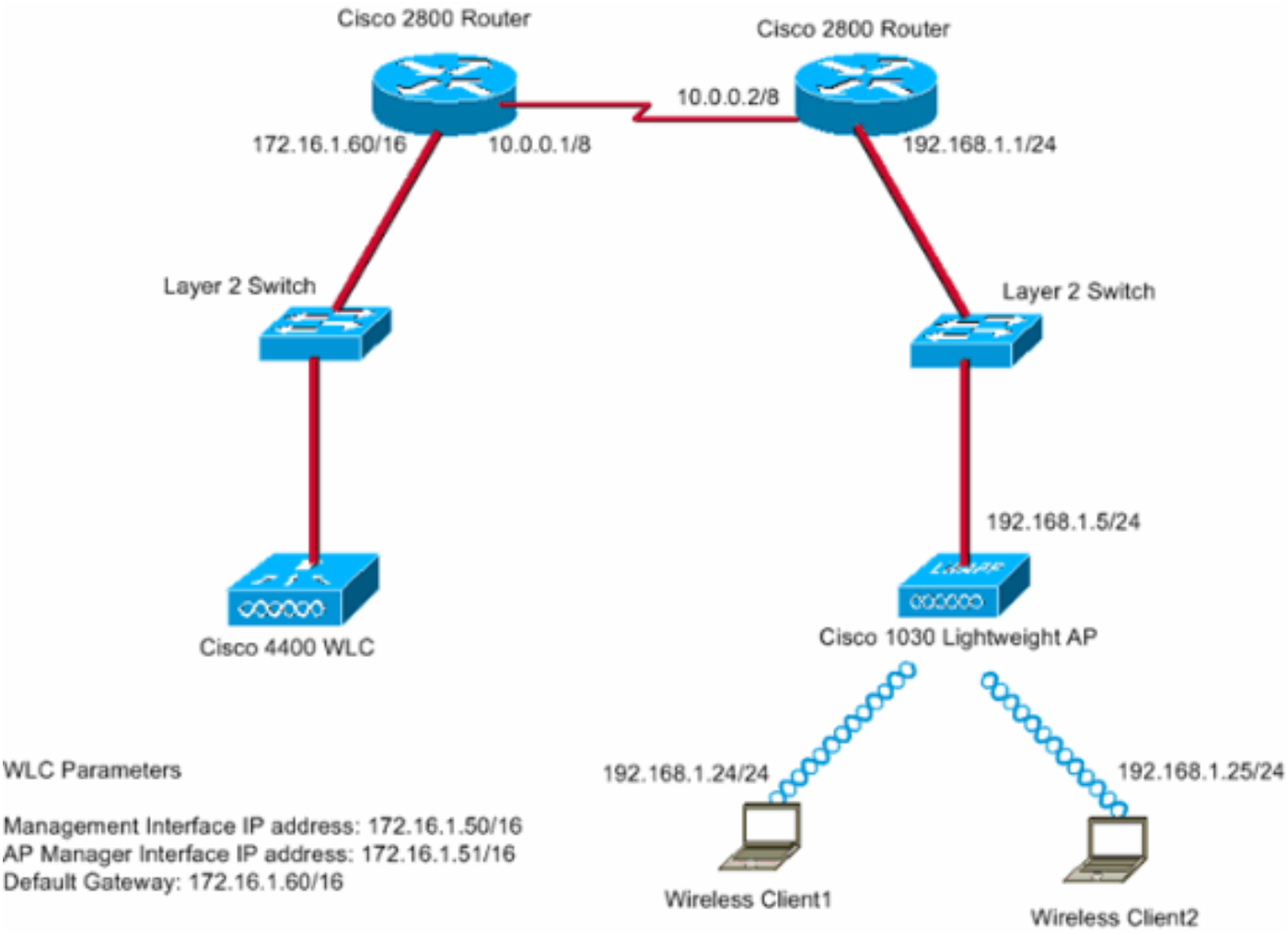
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Для настройки устройств для реализации сетевой установки, выполните эти шаги:

1. Настройте WLC для главной операции и настройте WLAN.
2. Главный AP для установки на удаленном узле.
3. Настройте эти 2800 маршрутизаторов для установления канала WAN.
4. Разверните LAP REAP на удаленном узле.

Схема сети

В настоящем документе используется следующая схема сети:



Главный офис соединяется с филиалом компании с использованием выделенной линии. Выделенная линия завершается на маршрутизаторах серии 2800 в каждом конце. Данный пример использует Протокол OSPF для данных маршрутов на канале WAN с инкапсуляцией PPP. 4400 WLC находятся в главном офисе, и 1030 LAP должны быть развернуты в удаленном офисе. 1030 LAP должны поддержать два WLAN. Вот параметры для WLAN:

- **WLAN 1**SSID — **SSID1**Аутентификация — **Открытый**Шифрование **(предварительный общий ключ WPA [WPA-PSK])**
- **WLAN 2**SSID — **SSID2**Аутентификация — **протокол EAP**Шифрование**Примечание:** Для WLAN 2 конфигурация в этом документе использует WPA (аутентификация 802.1x и TKIP для шифрования).

Необходимо настроить устройства для этой настройки.

Настройте WLC для главной операции и настройте WLAN

Чтобы настроить WLC для выполнения основных операций, используйте мастер запуска конфигурации в интерфейсе командной строки (CLI). Также можно использовать GUI для настройки WLC. В данном документе описан способ выполнения конфигурации на контроллере WLC с помощью мастера запуска конфигурации в CLI.

После первоначальной загрузки WLC, он напрямую подключается к мастеру запуска конфигурации. Чтобы настроить основные параметры, используется мастер запуска конфигурации. Можно запустить мастер в CLI или GUI. Ниже приведен пример мастера запуска конфигурации:

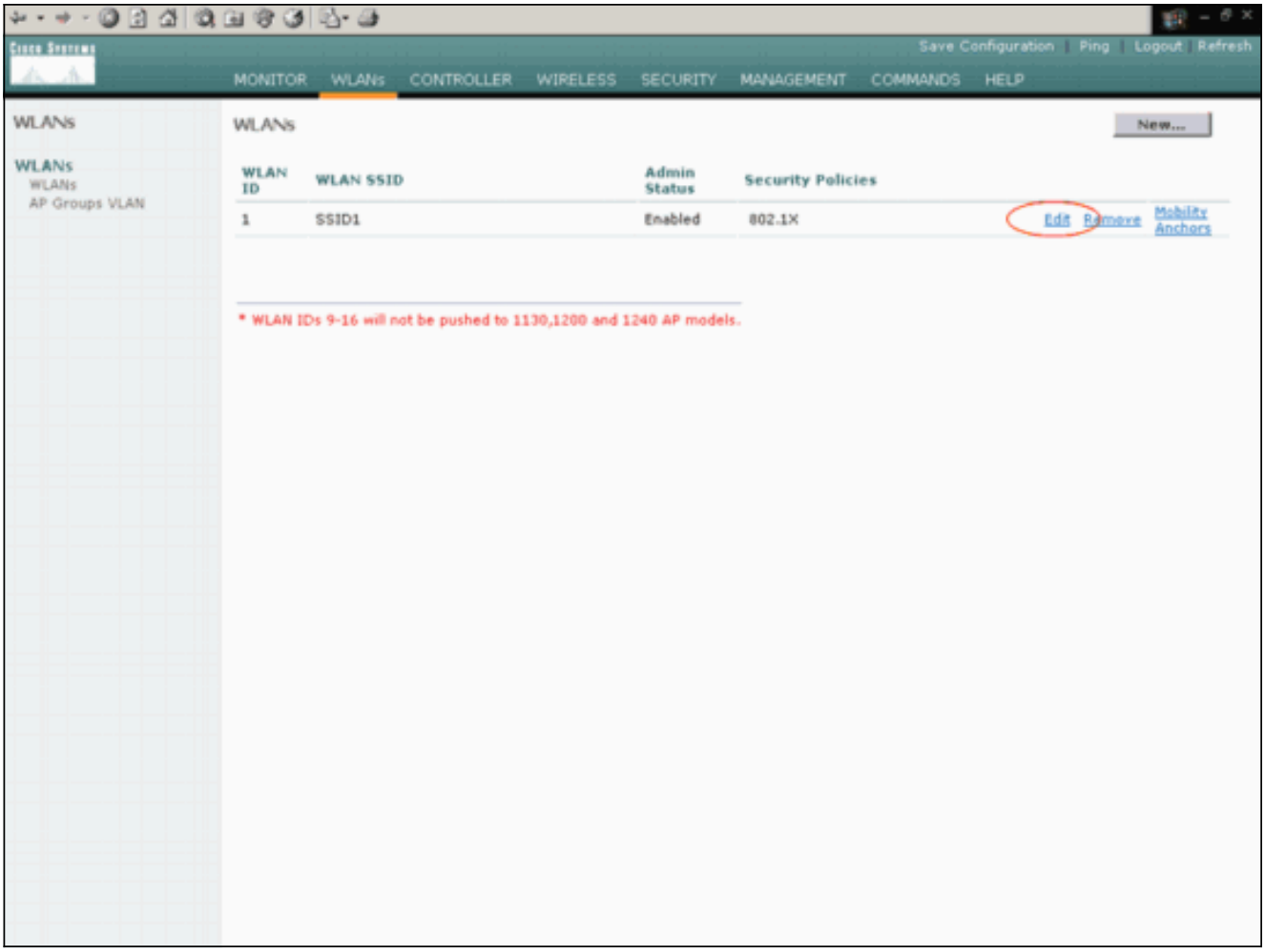
```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice Enter Administrative User Name (24 characters max):
admin Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
172.16.1.50 Management Interface Netmask: 255.255.0.0 Management Interface Default Router:
172.16.1.60 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 172.16.1.1 AP Manager Interface IP
Address: 172.16.1.51 AP-Manager is on Management subnet, using same values AP Manager Interface
DHCP Server (172.16.1.1): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: Main
Network Name (SSID): SSID1 Allow Static IP Addresses [YES][no]: Yes Configure a RADIUS Server
now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please
see documentation for more details. Enter Country Code (enter 'help' for a list of countries)
[US]: Enable 802.11b Network [YES][no]: Yes Enable 802.11a Network [YES][no]: Yes Enable 802.11g
Network [YES][no]: Yes Enable Auto-RF [YES][no]: Yes Configuration saved! Resetting system with
new configuration...
```

Данный пример настраивает эти параметры на WLC:

- Имя системы
- Management Interface IP Address
- AP Manager Interface IP Address
- Номер порта интерфейса управления
- Идентификатор сети VLAN интерфейса управления
- Имя мобильной группы
- SSID
- Другие параметры

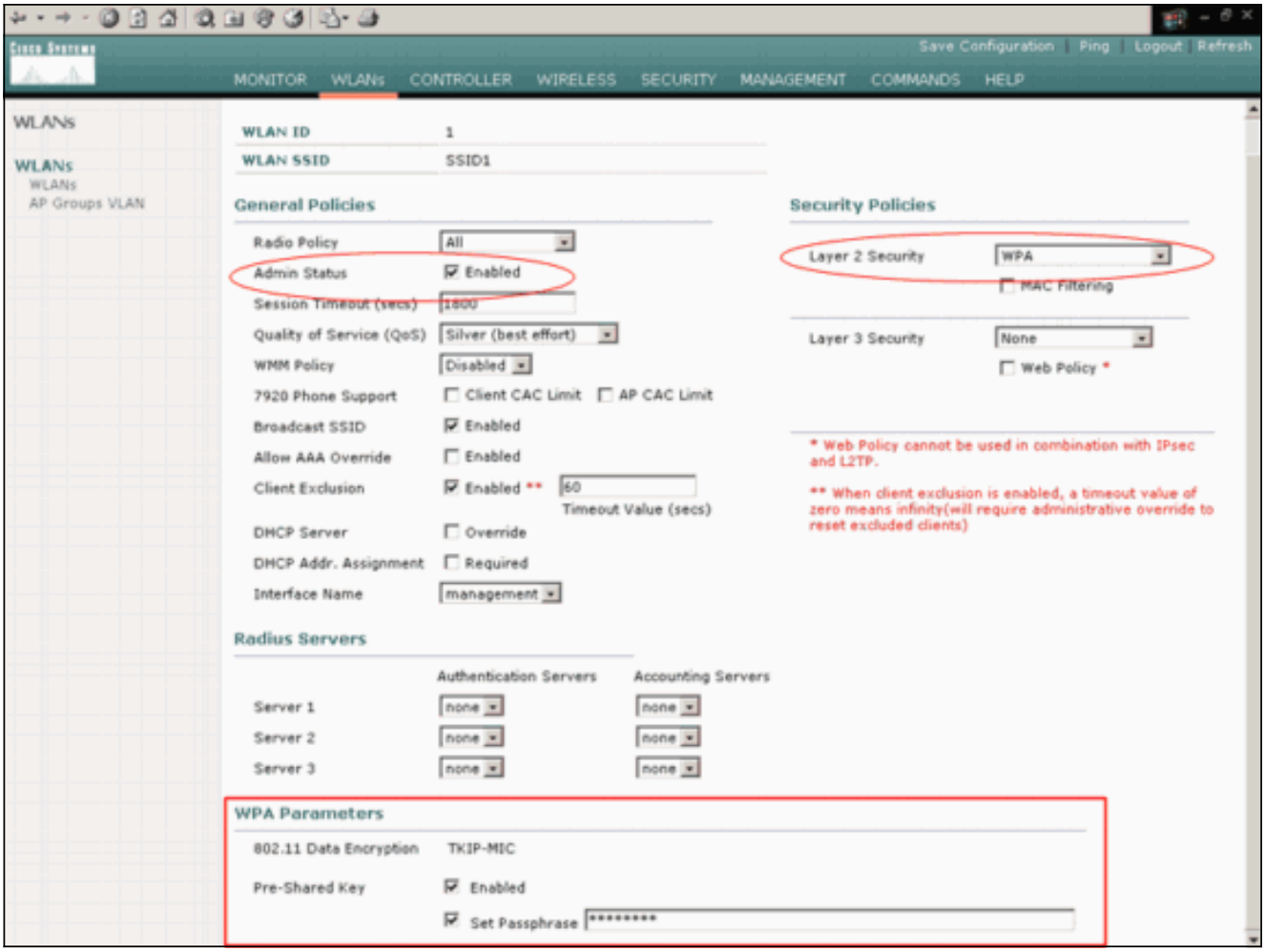
Эти параметры используются для устанавливания WLC для главной операции. Поскольку выходные данные WLC в этом разделе показывают, WLC использует 172.16.1.50 в качестве IP-адреса интерфейса управления и 172.16.1.51 как IP-адрес интерфейса менеджера точки доступа. Для настройки этих двух WLAN для сети выполните эти шаги на WLC:

1. От GUI WLC нажмите **WLAN** в меню наверху окна.Откроется окно WLAN. Это окно перечисляет WLAN, которые настроены на WLC. Поскольку вы настроили один WLAN с использованием мастера загрузочной конфигурации, необходимо настроить другие параметры для этого WLAN.
2. Нажмите **Edit** для SSID1 WLAN.Например:



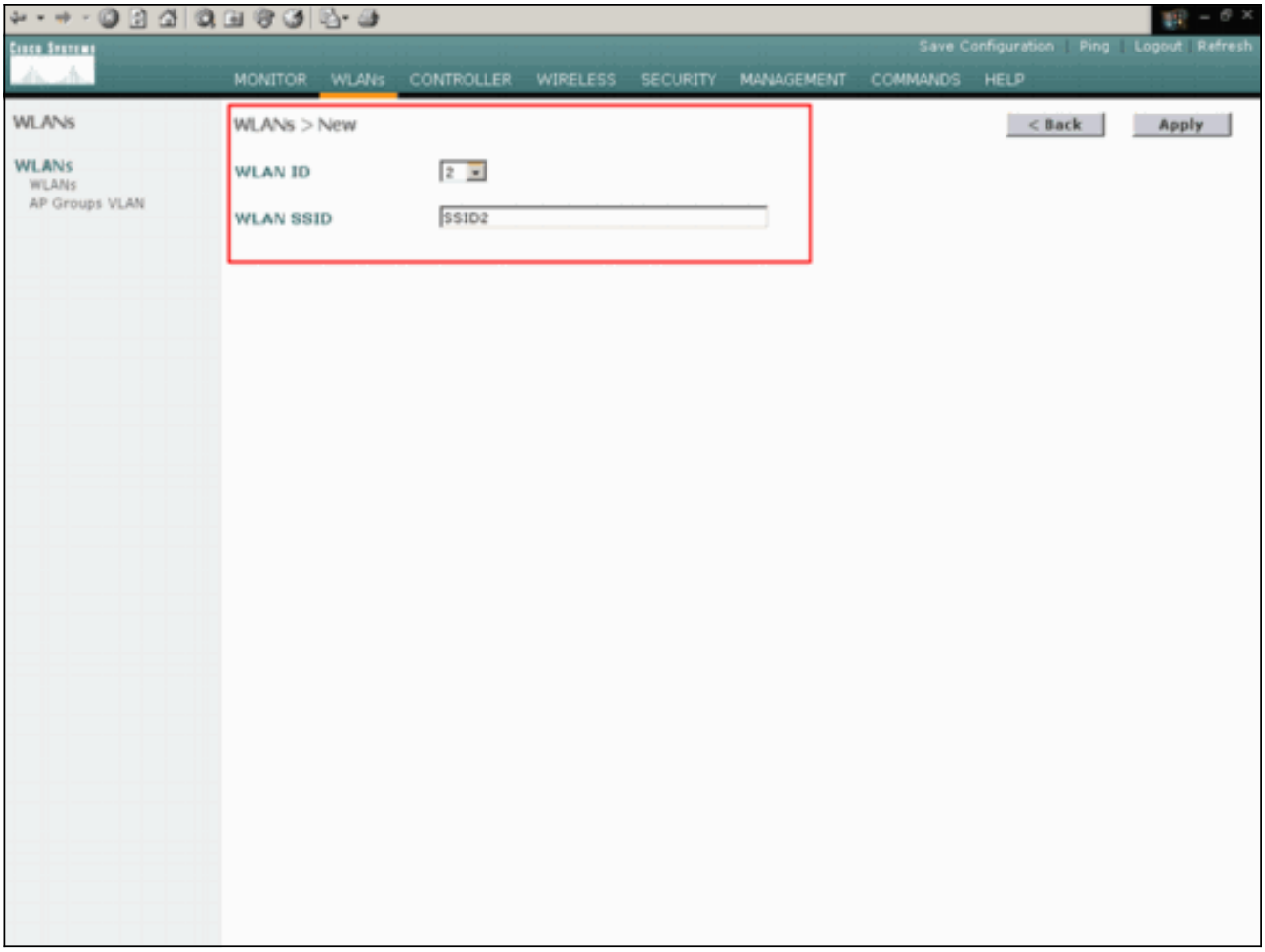
WLAN> Окно редактирования появляются. В этом окне можно настроить параметры, которые являются определенными для WLAN, который включает Общую политику, Политику безопасности, сервер RADIUS и других.

3. Сделайте эти выборы в WLAN> Окно редактирования:В области General Policies проверьте флажок **Enabled** около Административного статуса для включения этого WLAN.Выберите **WPA** из раскрывающегося меню безопасности уровня 2 для использования WPA для WLAN 1.Определите параметры WPA у основания окна.Для использования WPA-PSK на WLAN 1 проверьте флажок **Enabled** около Предварительного общего ключа в области WPA Parameters и введите пароль для WPA-PSK. WPA-PSK Будет использовать TKIP для шифрования.**Примечание:** Пароль WPA-PSK должен совпасть с паролем, который настроен на клиентском адаптере для WPA-PSK для работы.**Щелкните "Применить".**Например:



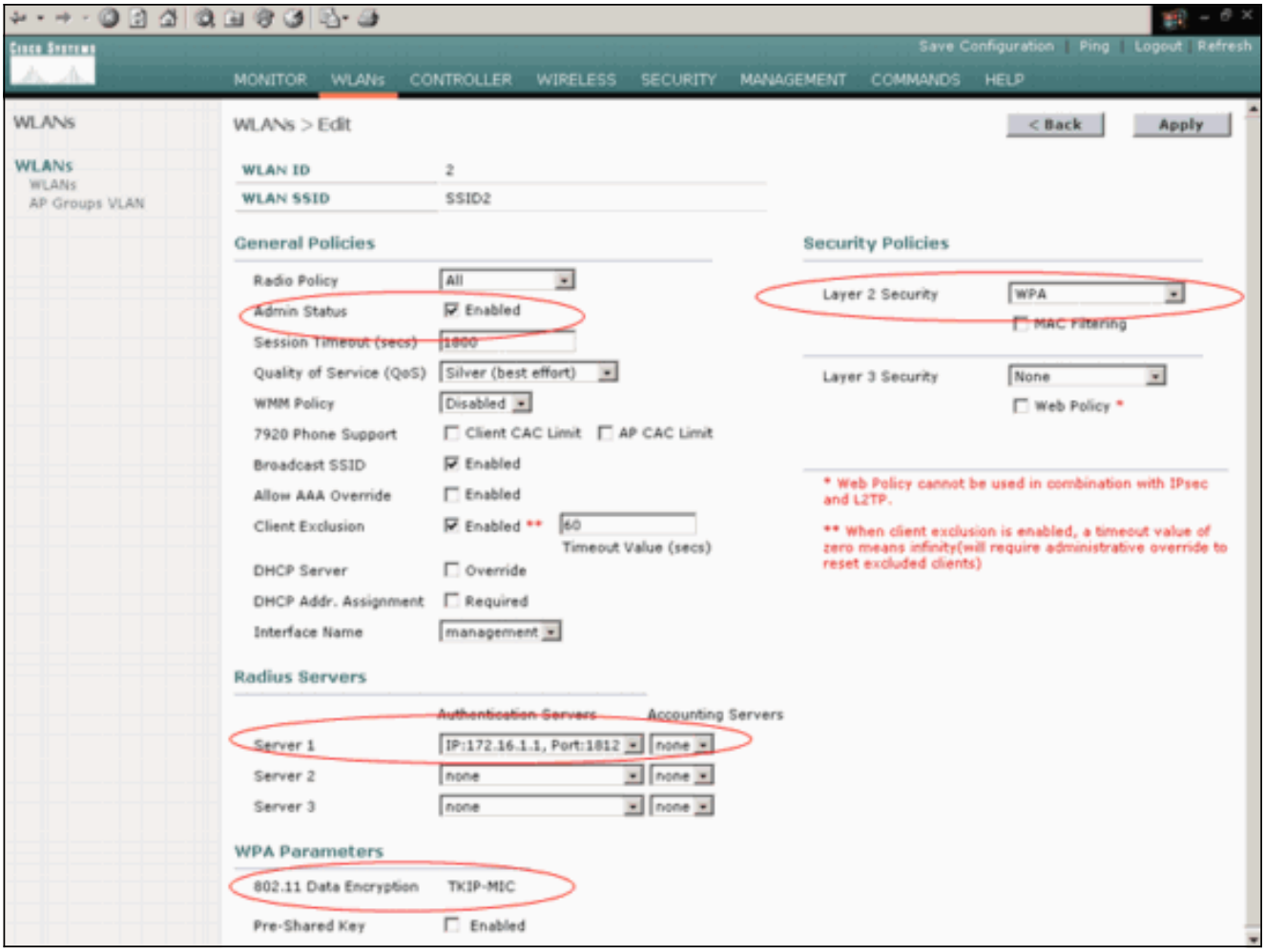
Вы настроили WLAN 1 для шифрования WPA-PSK.

4. Для определения WLAN 2 нажмите **New** в окне WLANs.WLAN> Новое окно появляется.
5. В WLAN> Новое окно, определите ИДЕНТИФИКАТОР WLAN и SSID WLAN, и нажмите **Apply**.Например:



Окно WLANs> Edit для второго WLAN появляется.

6. Сделайте эти выборы в WLAN> Окно редактирования:В области General Policies проверьте флажок **Enabled** около Административного статуса для включения этого WLAN.Выберите **WPA** из раскрывающегося меню безопасности уровня 2 для настройки WPA для этого WLAN.В области серверов RADIUS выберите соответствующий сервер RADIUS для использования для аутентификации клиентов.**Щелкните "Применить".**Например:



Примечание: Этот документ не объясняет, как настроить серверы RADIUS и Аутентификацию eap. Для получения информации о том, как настроить Аутентификацию eap с WLC, обратитесь к Аутентификации eap с Контроллерами беспроводной локальной сети (WLC) Пример конфигурации.

Главный AP для установки на удаленном узле

Воспламенение является процессом, которым LAP получают список контроллеров, с которыми они могут соединиться. LAP сообщают обо всех контроллерах в группе мобильности, как только они соединяются с одиночным контроллером. Таким образом LAP изучают всю информацию, в которой они нуждаются для присоединений к любому контроллеру в группе.

Чтобы к началу СПОСОБНЫЙ К REAP AP, подключите AP с проводной сетью в главном офисе. Это соединение позволяет AP обнаруживать одиночный контроллер. После того, как LAP присоединяется к контроллеру в главном офисе, AP загружает версию операционной системы (OS) AP, которая соответствует инфраструктуре WLAN и конфигурации. IP-адреса всех контроллеров в группе мобильности переданы AP. Когда AP имеет всю информацию, в которой требуется, AP может быть связан в удаленном местоположении. Если возможность подключения с помощью IP-адреса доступна, AP может тогда обнаружить и присоединиться к наименее используемому контроллеру из списка.

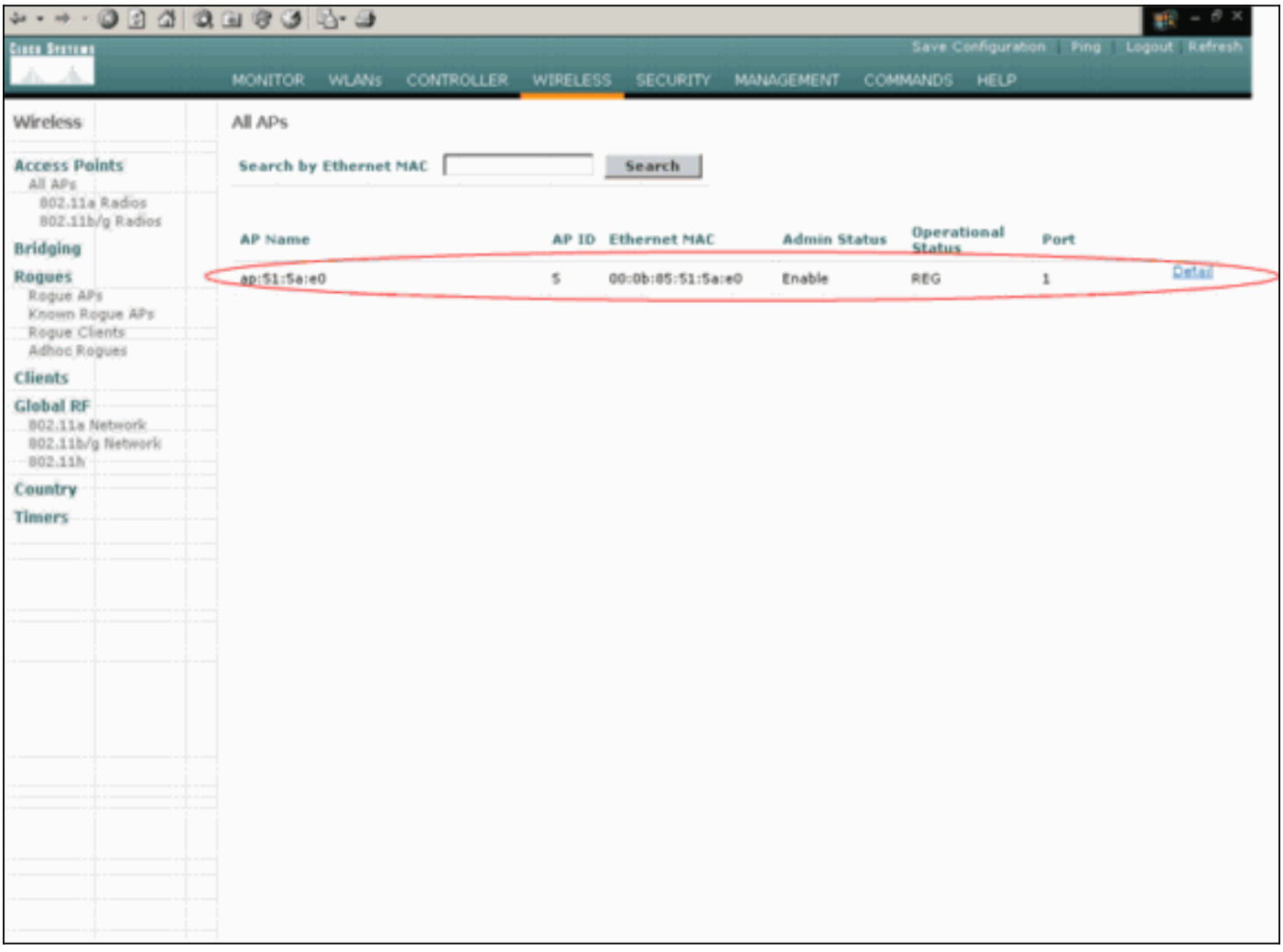
Примечание: Удостоверьтесь, что вы устанавливаете AP в режим "REAP", прежде чем вы выключите их для отправления их удаленным узлам. Можно установить режим на уровне AP через CLI контроллера или GUI, или с использованием шаблонов Wireless Control System (WCS). AP собираются выполнить обычную, "локальную" функциональность по умолчанию.

LAP могут использовать любой из этих методов для обнаружения контроллера:

- **Обнаружение уровня 2**
- **Обнаружение уровня 3**С использованием широковещания локальной подсетиС использованием параметра DHCP 43С использованием сервера DNSC использованием По беспроводной связи инициализации (OTAP)С использованием внутреннего сервера DHCP**Примечание:** Для использования внутреннего сервера DHCP LAP должен соединиться непосредственно с WLC.

Этот документ предполагает, что LAP регистрирует к WLC в использовании параметра DHCP 43 механизма обнаружения. Для получения дополнительной информации об использовании параметра DHCP 43 для регистрации LAP к контроллеру, а также другим механизмам обнаружения, обращаются к [регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC)](#).

После того, как LAP обнаруживает контроллер, вы видите, что AP зарегистрирован к контроллеру в Беспроводном клиенте Windows WLC. Например:

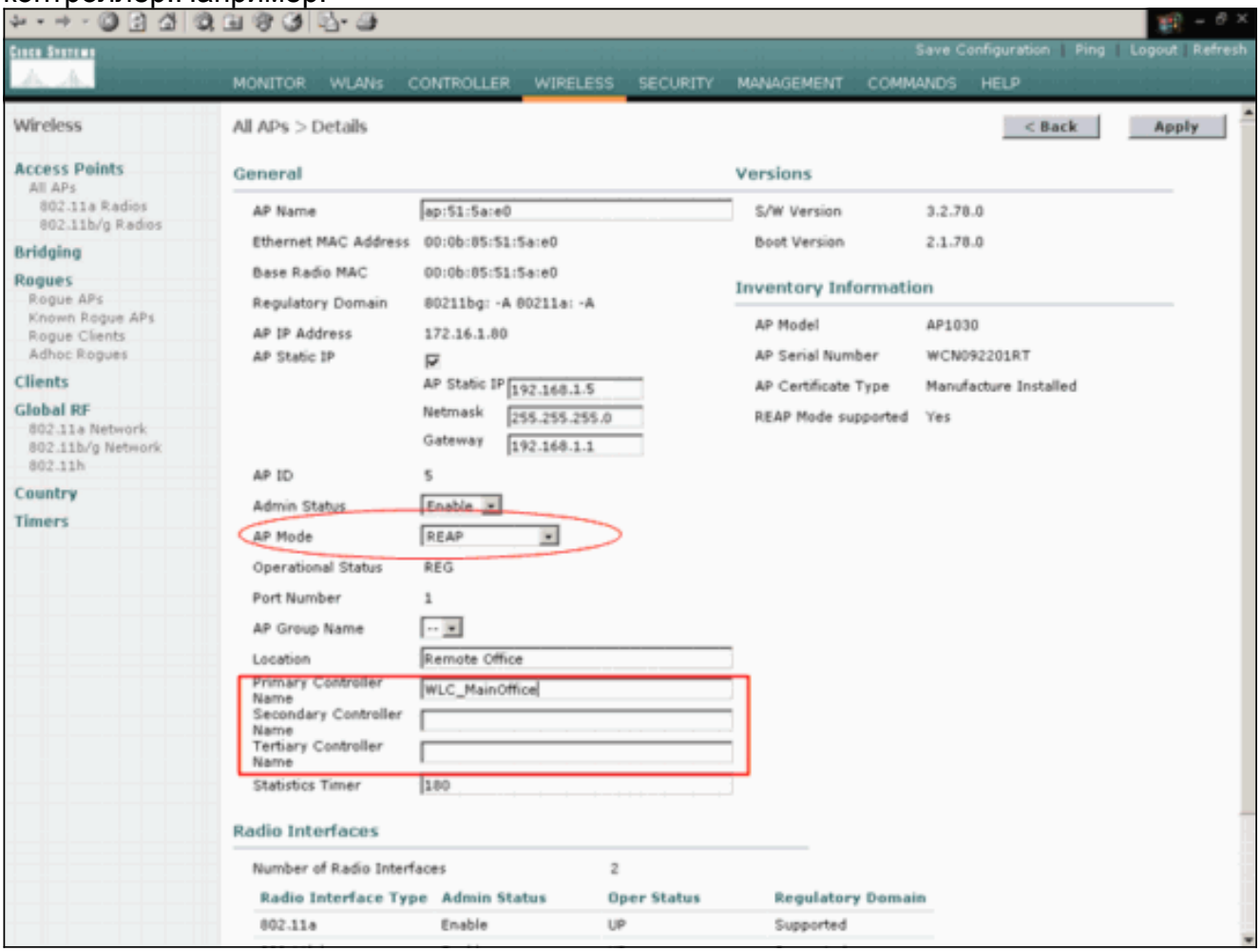


Выполните эти шаги для настройки LAP для обычного режима REAP:

1. **В графическом интерфейсе пользователя WLC нажмите Wireless.**Все окно Все APs появляется. Это окно перечисляет AP, которые зарегистрированы к WLC.
2. Выберите AP, который необходимо настроить для режима REAP и нажать **Detail**.Окно All APs> Detail для определенного AP появляется. В этом окне можно настроить различные параметры AP, которые включают:Название APIP-адрес (который можно

изменить на помехи),Административный статусПараметры безопасностиРежим APСписок WLC, с которыми может соединиться APДругие параметры

3. Выберите **REAP** из раскрывающегося меню Режима AP.Этот режим только доступен на СПОСОБНЫХ К REAP AP.
4. Определите названия контроллера, которые AP будут использовать, чтобы зарегистрировать и нажать **Apply**.Можно определить до трех названий контроллера (основной, вторичный, и третичный). AP ищут контроллер в том же заказе, который вы предоставляете в этом окне. Поскольку данный пример использует только один контроллер, пример определяет контроллер как главный контроллер.Например:



Вы установили AP для режима REAP, и можно развернуть его на удаленном узле.

Примечание: В окне данного примера вы видите, что IP-адрес AP изменен на помехи, и статический IP - адрес 192.168.1.5 назначен. Это присвоение происходит, потому что это - подсеть, которая будет использоваться в удаленном офисе. Таким образом, вы используете IP-адрес от сервера DHCP, 172.16.1.80, только во время этапа воспламенения. После того, как AP зарегистрирован к контроллеру, вы изменяете адрес на статический IP - адрес.

Настройте эти 2800 маршрутизаторов для установления канала WAN

Для установления канала WAN данный пример использует два маршрутизатора серии 2800 с OSPF к сведениям о маршруте между сетями. Вот является конфигурация обоих маршрутизаторами для примера сценария в этом документе:

Головной офис

```
MainOffice#show run Building configuration... Current
configuration : 728 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname MainOffice ! ! ip
subnet-zero ! ! ! ! interface Ethernet0 ip address
172.16.1.60 255.255.0.0 !--- This is the interface which
acts as the default gateway to the WLC. ! interface
Virtual-Template1 no ip address ! interface Serial0 no
ip address ! interface Serial1 !--- This is the
interface for the WAN link. ip address 10.0.0.1
255.0.0.0 encapsulation ppp !--- This example uses PPP.
Use the appropriate !--- encapsulation for the WAN
connection. ! router ospf 50 !--- Use OSPF to route data
between the different networks. log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0 network 172.16.0.0
0.0.255.255 area 0 ! ! ip classless ip http server ! ! !
line con 0 line aux 0 line vty 0 4 ! end
```

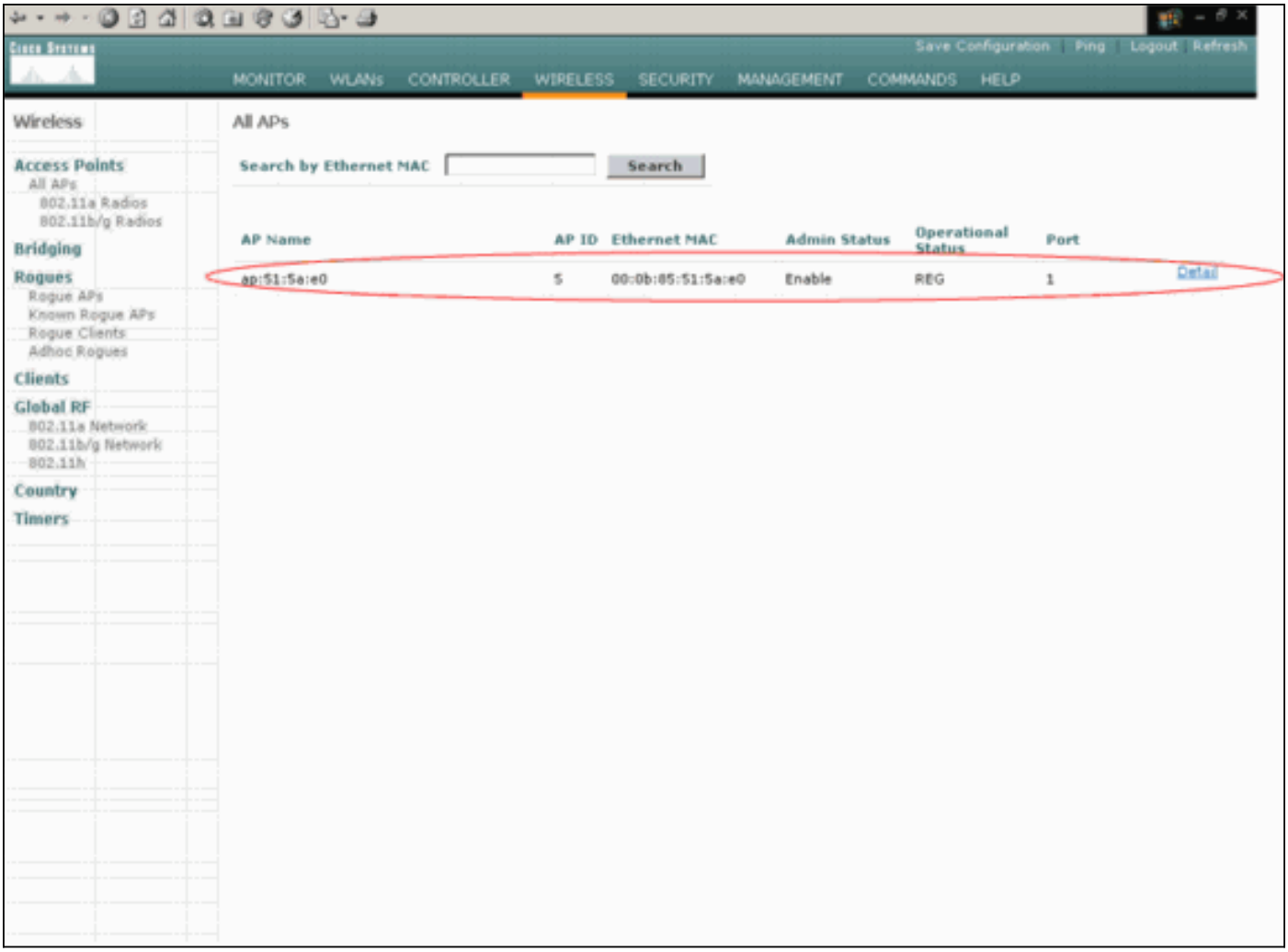
Офис филиала

```
BranchOffice#show run Building configuration... Current
configuration : 596 bytes ! version 12.2 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
BranchOffice ! ! ip subnet-zero ! ! ! ! interface
Ethernet0 ip address 192.168.1.1 255.255.255.0 !--- This
is the interface which acts as the default gateway to
the LAP. ! interface Serial0 no ip address ! interface
Serial1 !--- This is the interface for the WAN link. ip
address 10.0.0.2 255.0.0.0 encapsulation ppp clockrate
56000 ! router ospf 50 !--- Use OSPF to route data
between the different networks. log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0 network
192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

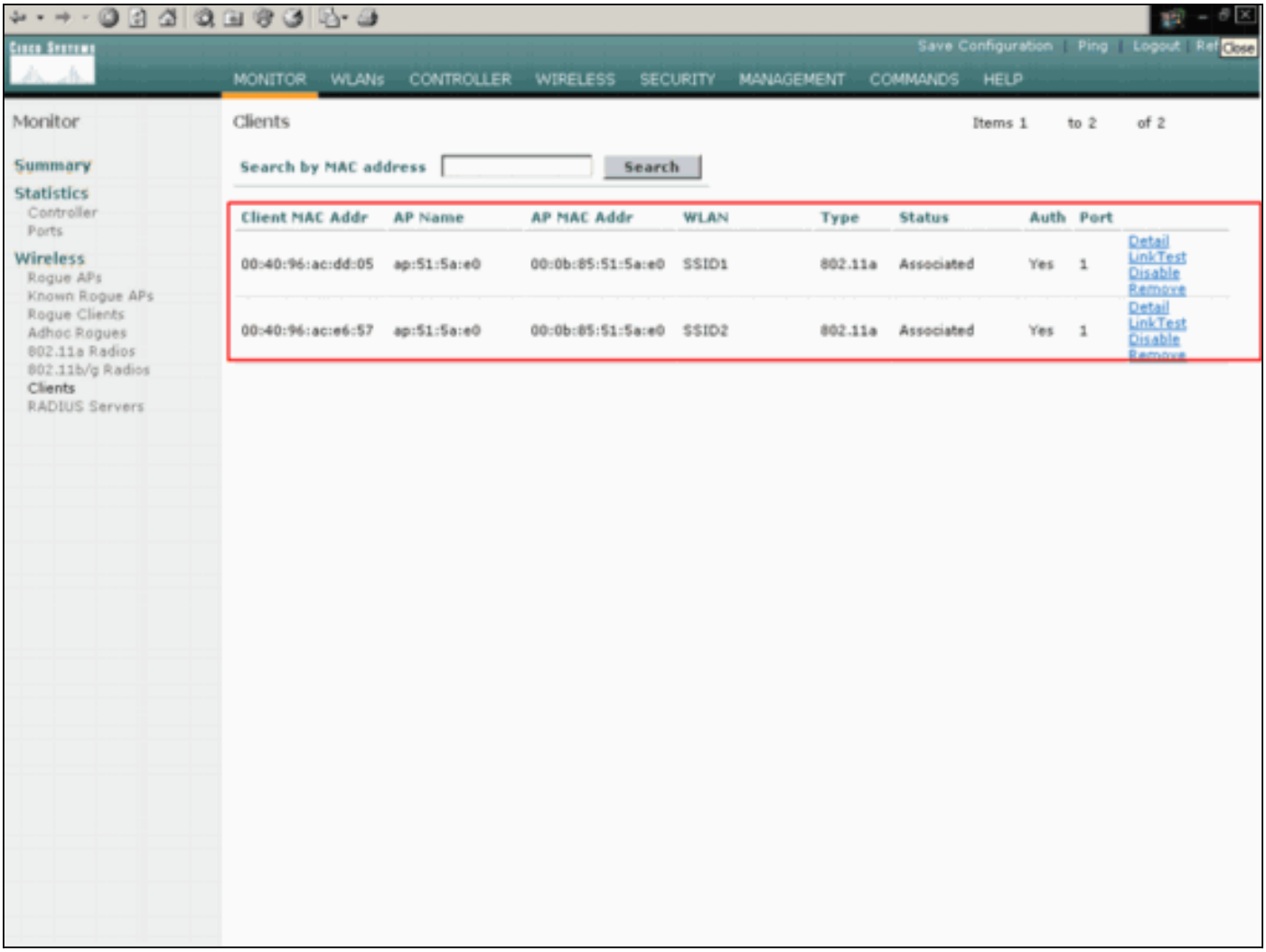
Разверните AP REAP на удаленном узле

Теперь, когда вы настроили WLAN на WLC, запущенных LAP, и установили канал WAN между главным офисом и удаленным офисом, вы готовы развернуть AP на удаленном узле.

После того, как вы включаете AP на удаленном узле, AP ищет контроллер в заказе, который вы настроили на этапе воспламенения. После того, как AP находит контроллер, регистры AP с контроллером. Например. От WLC вы видите, что AP присоединился к контроллеру на порту 1:



Клиенты, которые имеют **SSID1** SSID, и для которого WPA-PSK включен, партнер к AP на WLAN 1. Клиенты, которые имеют **SSID SSID2**, и которым включили аутентификацию 802.1x, партнера к AP на WLAN 2. Вот пример, который показывает двум клиентам. Один клиент связан с WLAN 1, и другой клиент связан с WLAN 2:



Проверка

Используйте этот раздел, чтобы подтвердить, что ваша конфигурация REAP работает должным образом.

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

Переведите канал WAN в нерабочее состояние. Когда канал WAN не работает, AP теряет подключение с WLC. WLC тогда вычеркивает из списка AP из своего списка. Например:

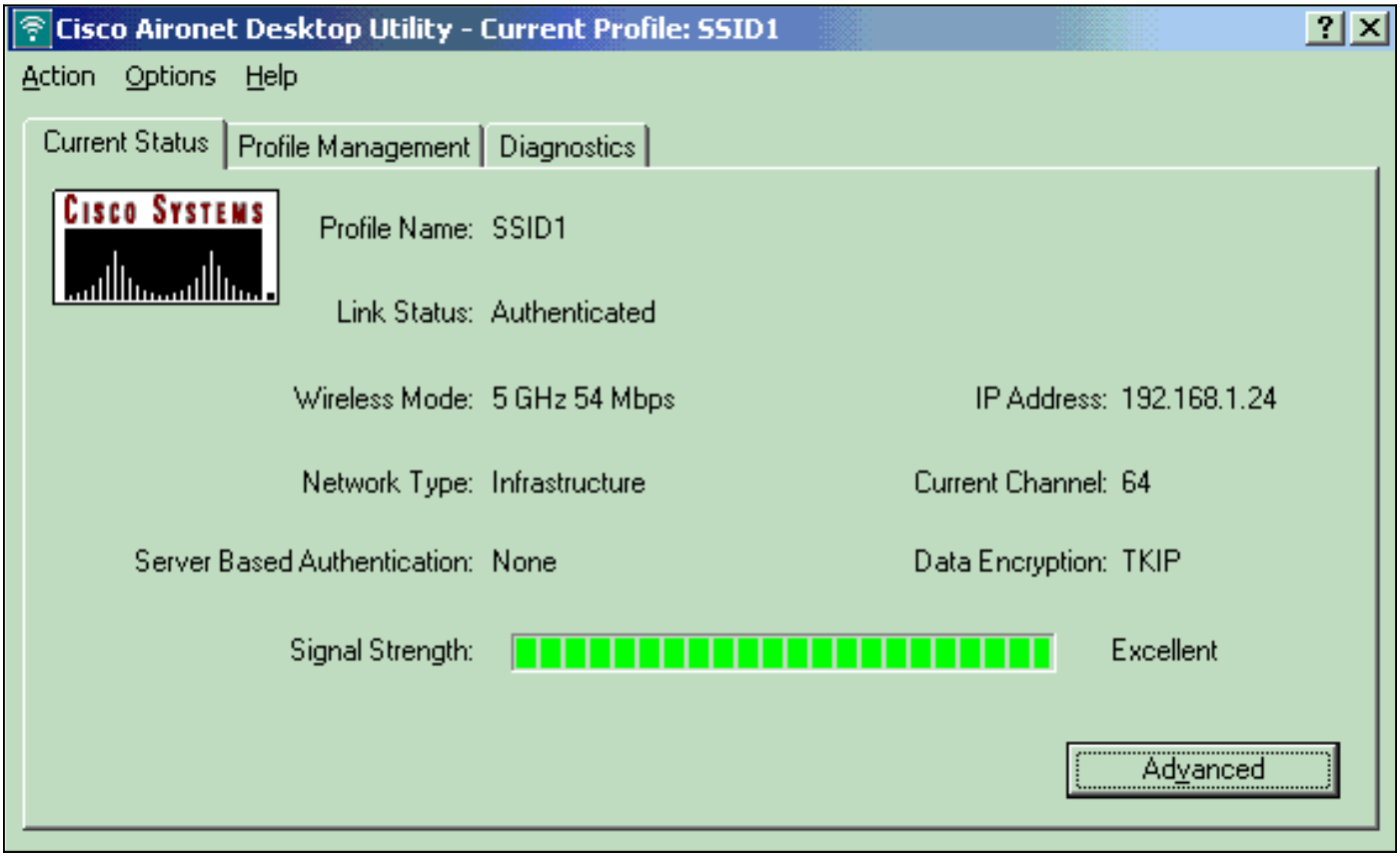
```
(Cisco Controller) >debug lwapp events enable Wed May 17 15:04:22 2006: Did not receive
heartbeat reply from AP 00:0B:85:51:5A:E0 Wed May 17 15:04:22 2006: Max retransmissions reached
on AP 00:0B:85:51:5A:E0 (CONFIGURE_COMMAND, 1) Wed May 17 15:04:22 2006:
apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May
17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP
00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down
LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17 15:04:22 2006:
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP 00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0! Wed May 17
15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006:
Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1! Wed May 17 15:04:22 2006: Deregister
LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

От выходных данных **команды debug lwapp events enable** вы видите, что WLC вычеркивает из списка AP, потому что WLC не получил ответ биения от AP. Ответ биения подобен

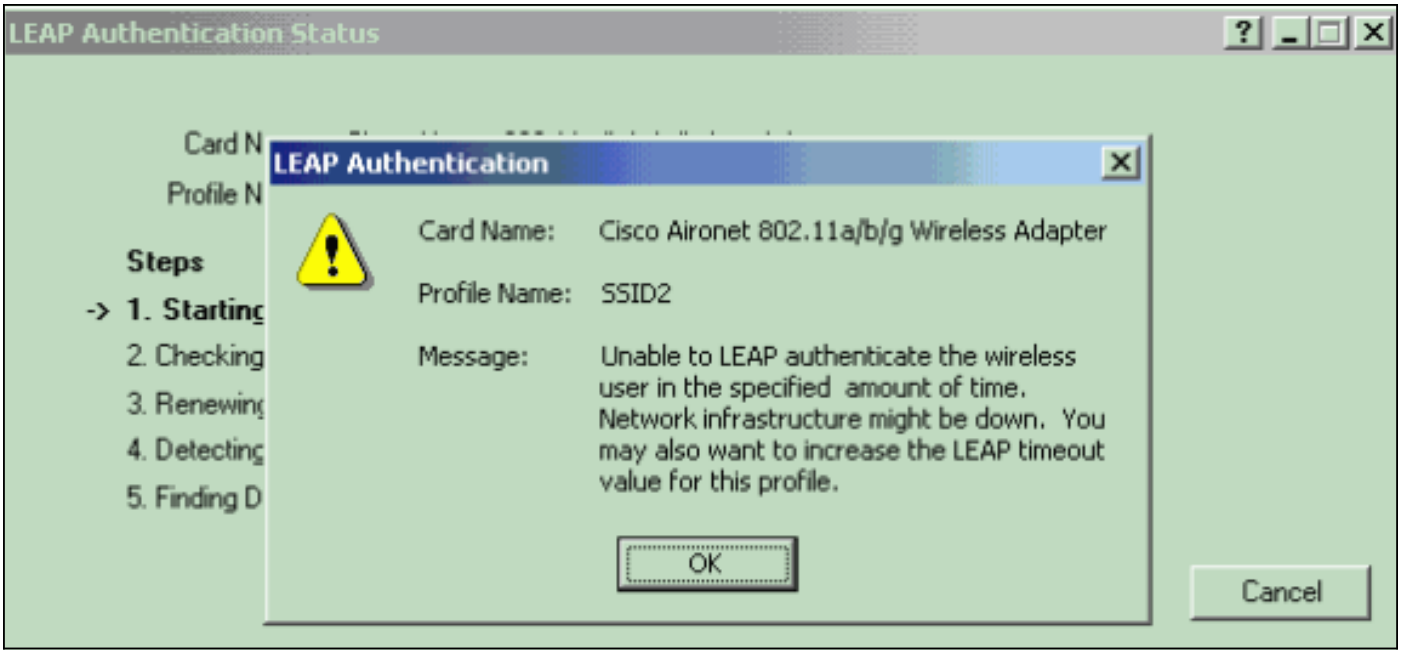
сообщениям поддержки активности. Контроллер пробует пять последовательных пульсов, 1 секунда независимо. Если WLC не получает ответ, WLC вычеркивает из списка AP.

Когда AP находится в автономном режиме, вспышках индикатора питания AP. Клиенты, которые связываются к первому WLAN (WLAN 1), все еще привязаны к AP, потому что клиенты в первом WLAN настроены для шифрования WPA-PSK только. LAP обрабатывает само шифрование в автономном режиме. Вот пример, который показывает статус (когда канал WAN не работает) клиента, который связан с WLAN 1 с SSID1 и WPA-PSK:

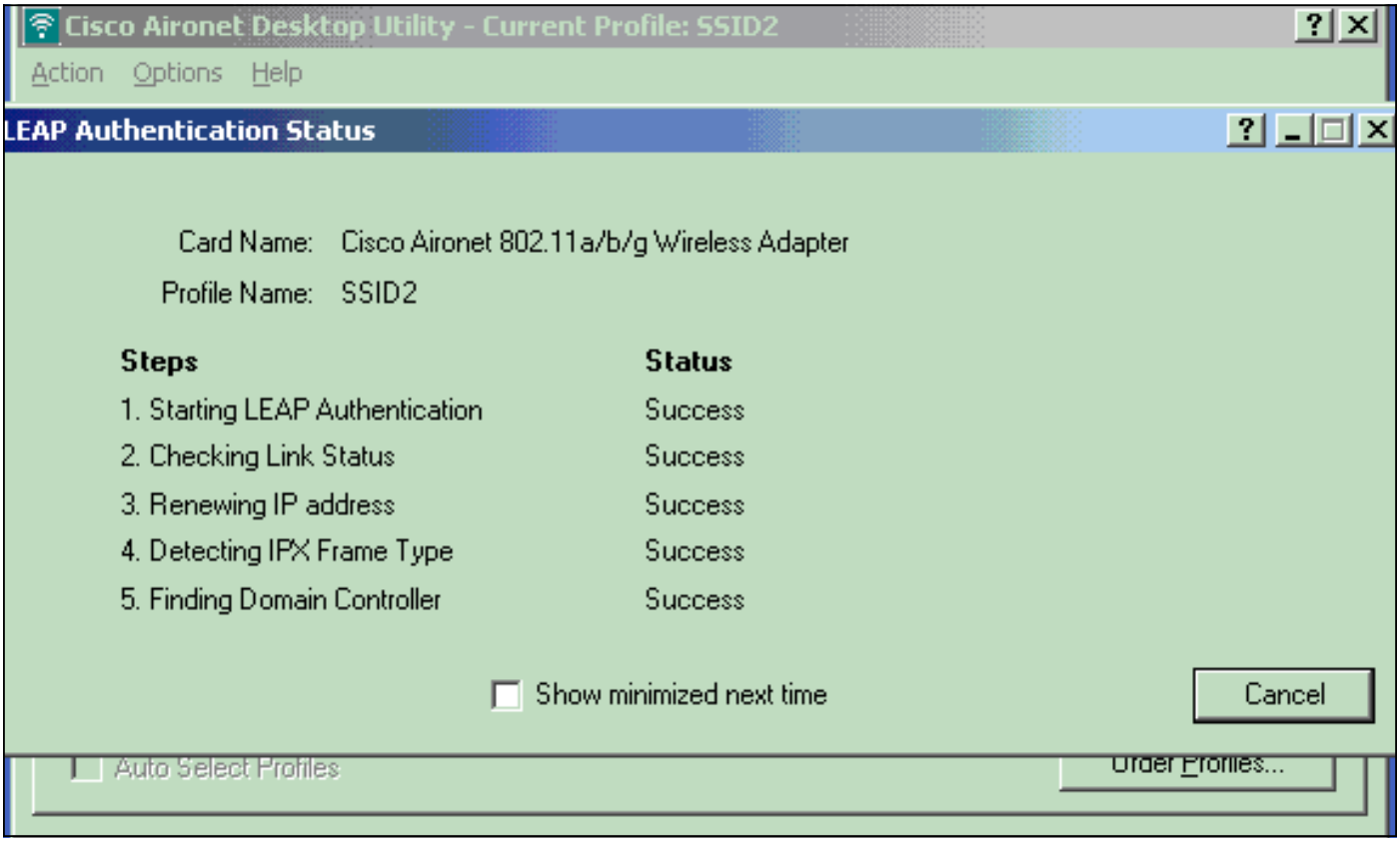
Примечание: TKIP является шифрованием, которое используется с WPA-PSK.



Клиенты, которые связаны с WLAN 2, разъединены, потому что WLAN 2 использует Аутентификацию eap. Это разъединение происходит, потому что клиенты, которые используют Аутентификацию eap, должны связаться с WLC. Вот образец окна, который показывает, что Аутентификация eap отказывает, когда канал WAN не работает:



После того, как канал WAN подключен, коммутаторы AP назад к обычному режиму REAP и регистрируется в контроллере. Клиент, который использует Аутентификацию eap также, подходит. Например:



Этот пример выходных данных **команды debug lwapp events enable** на контроллере показывает эти результаты:

```
(Cisco Controller) >debug lwapp events enable Wed May 17 15:06:40 2006: Successful transmission
of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed May 17 15:06:52 2006: Received
LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to 00:0b:85:33:84:a0 on port '1' Wed May 17 15:06:52
2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500, remote debug mode is 0 Wed
May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51) Switch IP:
172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP Port: 5550, next hop
MAC: 00:d0:58:ad:ae:cb Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply
```

```
to AP 00:0b:85:51:5a:e0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0
slot 0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17
15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Команды для устранения неполадок

Можно использовать эти **команды отладки** для устранения проблем конфигурации.

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

- **debug lwapp events enable** последовательность событий, которые происходят между LAP и WLC.
- **debug lwapp errors enable** — Отображает ошибки, которые происходят в подключении LWAPP.
- **debug lwapp packetenable** отладку трассировки Пакета lwapp.
- **адрес debug mac** — Включает отладку MAC для клиента, которого вы задаете.

Дополнительные сведения

- Руководство по развертыванию REAP в филиале компании
- Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Пример конфигурации при отказе контроллера WLAN для "облегченных" точек доступа
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация