Настройка беспроводных доменных служб

Содержание

Общие сведения

Данный документ описывает основные понятия беспроводных доменных служб (WDS). В этом документе также описывается настройка одной точки доступа (AP) или модуля Wireless LAN Services Module (WLSM) как WDS и как минимум одной другой точки как точки доступа к инфраструктуре. Описанная в этом документе процедура является руководством по WDS — функциональным службам, с помощью которых клиент получает возможность присоединяться к точке доступа WDS или инфраструктурной точке доступа. Задача этого документа — создать базу, на основе которой можно настроить Fast Secure Roaming или добавить в сеть модуль решений для беспроводных сетей беспроводных сетей (WLSE), получив возможность использовать его функции.

Предварительные условия

Требования

Перед использованием этой настройки убедитесь в выполнении следующих предварительных условий:

- Основательные знания беспроводных сетей и вопросов их безопасности
- Знания современных методов обеспечения безопасности расширенного протокола аутентификации (EAP).

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям программного и аппаратного обеспечения:

- Точки доступа с ПО Cisco IOS®
- ПО Cisco IOS выпуск 12.3(2)JA2 и выше
- Модуль служб беспроводных сетей LAN серии Catalyst 6500

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с пустой (стандартной) настройкой и IP-адресом на интерфейсе BVI1, поэтому модуль доступен с GUI ПО Cisco IOS или через интерфейс командной строки (CLI). При работе в активной сети необходимо осознавать потенциальное воздействие любой команды.

Условные обозначения

Обратитесь к разделу Технические советы Cisco. Условные обозначения для получения дополнительных сведений об условных обозначениях в документах.

Беспроводные доменные службы

WDS - это новая функция точек доступа в ПО Cisco IOS, являющаяся основой модуля WLSM серии Catalyst 6500. WDS - это центральная функция, обеспечивающая работу таких функций, как:

- Быстрый и безопасный роуминг
- Взаимодействие WLSE
- Радиоуправление

Необходимо установить соединение между точками доступа, участвующими в WDS, и модулем WLSM до выполнения любой другой функции, основанной на WDS. Одной из целей WDS является устранение необходимости в проверке учетных данных пользователя сервером аутентификации и уменьшение времени, которое необходимо для аутентификации клиента.

Для использовния WDS необходимо обозначить одну точку доступа или модуль WLSM как WDS. Точка доступа WDS должна использовать имя пользователя и пароль WDS для установления соединения с сервером аутентификации. Сервер аутентификации может быть внешним сервером RADIUS или функцией локального сервера RADIUS в точке доступа WDS. WLSM должен быть связан с сервером аутентификации, даже если его аутентификация на сервере не требуется.

Другие точки доступа, называемые инфраструктурными, взаимодействуют с WDS. Перед регистрацией инфраструктурные точки доступа должны аутентифицировать себя с WDS. Группа сервера инфраструктуры на WDS определяет аутентификацию инфраструктуры.

Аутентификацию клиента определяет одна или несколько групп сервера клиента на WDS.

Когда клиент пытается связаться с инфраструктурной точкой доступа, точка доступа передает учетные данные на WDS для проверки. Если WDS видит эти учетные данные впервые, то он обращается к серверу аутентификации для проверки учетных данных. После этого WDS кэширует учетные данные, следовательно, нет надобности обращаться к серверу аутентификации при повторной проверке подлинности этого пользователя. Примером повторной аутентификации могут служить:

- Повторный вход
- Роуминг
- Когда пользователь включает устройство клиента

Любой протокол аутентификации EAP на основе RADIUS можно тоннелировать через WDS, например:

- Упрощенный EAP (LEAP)
- Защищенный EAP (PEAP)
- Управление безопасностью транспортного уровня протокола расширенной аутентификации (EAP-TLS)

- Гибкая аутентификация через безопасное туннелирование протокола расширенной аутентификации (EAP-FAST)

Аутентификация MAC-адреса также может туннелироваться к внешнему серверу аутентификации или согласно локальному списку точки доступа WDS. WLSM не поддерживает аутентификацию MAC-адреса.

Примечание: Аутентификация MAC-адреса несовместима с WPA-PSK. Эта проблема возникает из-за того, что при аутентификации локального MAC удаляется строка настройки, содержащая пароль WPA-PSK ASCII. Обратитесь к разделу WPA Настройка адаптера клиента через Windows CE .NET для получения дополнительной информации о WPA-PSK.

WDS и инфраструктурные точки доступа взаимодействуют через многоадресный протокол, который называют протоколом управления контекстом беспроводных ЛВС (WLCCP). Маршрутизация данных многоадресных сообщений невозможна, поэтому WDS и связанные с ней инфраструктурные точки доступа должны быть в одной и той же IP-подсети и на одном и том же сегменте LAN. Между WDS и WLSE протокол WLCCP использует TCP и протокол датаграмм пользователя (UDP) в порту 2887. В случае, если WDS и WLSE находятся в разных подсетях, такой протокол, как протокол преобразования сетевых адресов (NAT) не может преобразовывать пакеты.

Текущая рекомендация - одна точка доступа WDS на 30 инфраструктурных точек доступа. WSLM может обрабатывать до 300 инфраструктурных точек доступа.

Примечание: Cisco рекомендует использовать на инфраструктурных точках доступа ту же версию ПО IOS, что и на устройстве WDS. Если вы используете устаревшую версию IOS, точки доступа могут некорректно провести аутентификацию устройства WDS. Кроме этого, Cisco рекомендует использовать последнюю версию ПО IOS. Последнюю версию ПО IOS можно найти на странице Беспроводные устройства .

Точка доступа является устройством уровня 2. Поэтому она не обладает мобильностью устройств уровня 3, когда точка доступа настроена как устройство WDS. Мобильность устройств уровня 3 достигается путем настройки WLSM как устройства WDS. Обратитесь к разделу *Архитектура мобильности уровня 3* официального документа Модуль служб беспроводных сетей LAN серии Catalyst 6500 Cisco: для получения дополнительной информации.

Поэтому при настройке точки доступа как устройства WDS не нужно использовать команду **mobility network-id**. Эта команда используется для настройки мобильности уровня 3, и необходимо иметь WLSM в качестве устройства WDS для правильной настройки мобильности уровня 3. При неправильном использовании команды **mobility network-id** возможно появление следующих симптомов:

- Беспроводной клиент не может установить соединение с точкой доступа.
- Беспроводной клиент может установить соединение с точкой доступа, но не получает IP-адрес от сервера DHCP.
- Беспроводной телефон не аутентифицирован при развертывании передачи голоса через WLAN.
- Не происходит аутентификация EAP. При настроенной команде **mobility network-id** точка доступа пытается организовать туннель общей инкапсуляции маршрутов (GRE) для передачи пакетов EAP. Если туннель не установлен, пакеты не будут переданы.
- Точка доступа, настроенная как устройство WDS, работает неправильно, настройка WDS не работает вообще.

  Примечание: Вы не можете настроить Cisco Aironet 1300 AP/Bridge как мастер WDS. 1300 AP/Bridge не поддерживает эту функцию. 1300 AP/Bridge может участвовать в сети WDS как инфраструктурное устройство, в котором какая-либо другая точка доступа или WLSM настроена как мастер WDS.

Настройка

WDS представляет настройку в упорядоченном, модульном виде. Каждый последующий шаг основан на предыдущем. WDS опускает такие параметры настройки, как пароли, удаленный доступ и настройки радио, и концентрируется на самом важном.

В этом разделе представлены сведения по настройке функций, описанных в данном документе.

Примечание: Используйте Средство поиска команды (только для зарегистрированных пользователей) для получения дополнительной информации о командах, упомянутых в этом разделе.

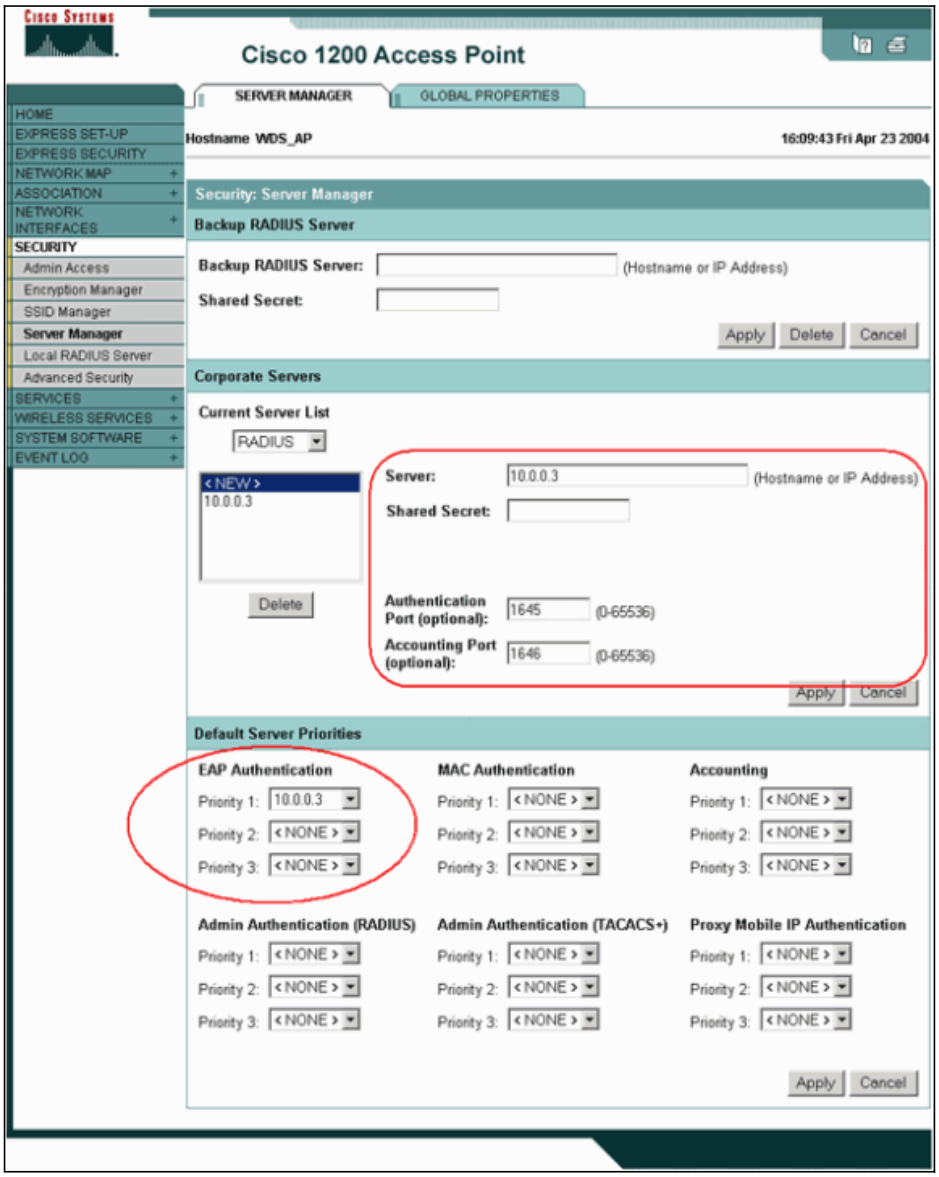
Задайте AP как WDS

Первый шаг - задать точку доступа как WDS. Точка доступа WDS - единственная точка, которая сообщается с сервером аутентификации.

Для задания точки доступа WDS необходимо выполнить следующие шаги:

1. Выберите **Security > Server Manager**, закладку точки доступа WDS Server Manager:

    1. Внесите IP-адрес сервера аутентификации в поле Server.
    2. Укажите общий секретный ключ и порты.
    3. В соответствующем типе проверки подлинности, установите IP адресу этого сервера поле приоритета 1.



Или подайте следующие команды из командной строки:

```
WDS_AP#configure terminal
Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
WDS_AP(config)#aaa group server radius rad_eap

WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
WDS_AP(config-sg-radius)#exit
```

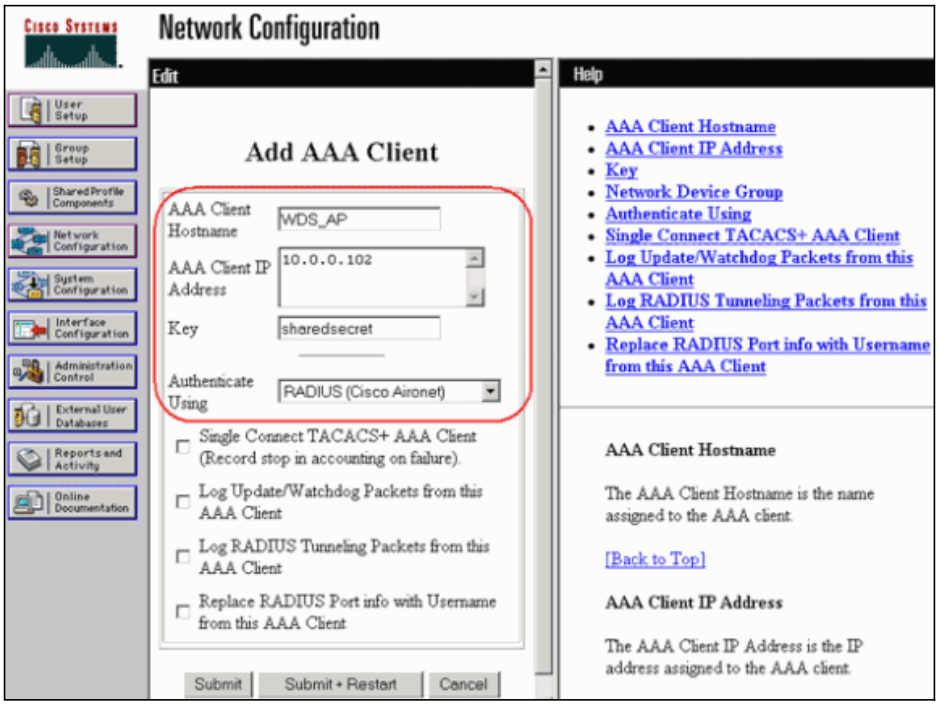
```
WDS_AP(config)#aaa new-model

WDS_AP(config)#aaa authentication login eap_methods group rad_eap


WDS_AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102


!--- Эта команда отображается в двух строках из-за ограничения по длине.


WDS_AP(config)#end

WDS_AP#write memory
```

2. Настройте точку доступа WDS на сервере аутентификации как клиент аутентификации, авторизации и учета (AAA). Выполните следующие шаги:

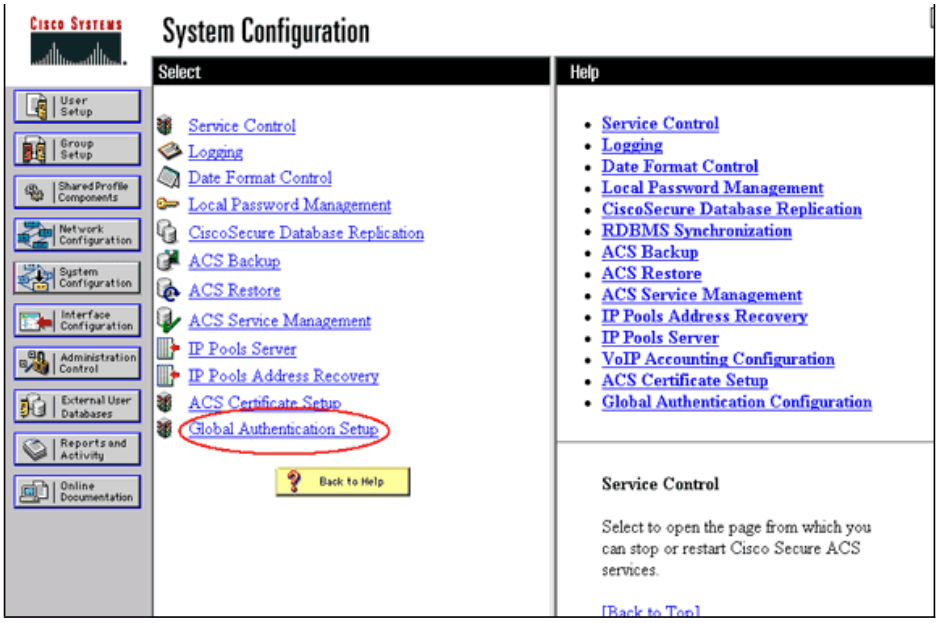
    1. В сервере управления доступом Cisco (ACS) это происходит на странице Настройка сети, где вы определяете следующие параметры для точки доступа WDS:

        - Имя
        - IP-адрес
        - Общий секрет
        - Метод аутентификации
            - RADIUS Cisco Aironet
            - RADIUS Internet Engineering Task Force [IETF]

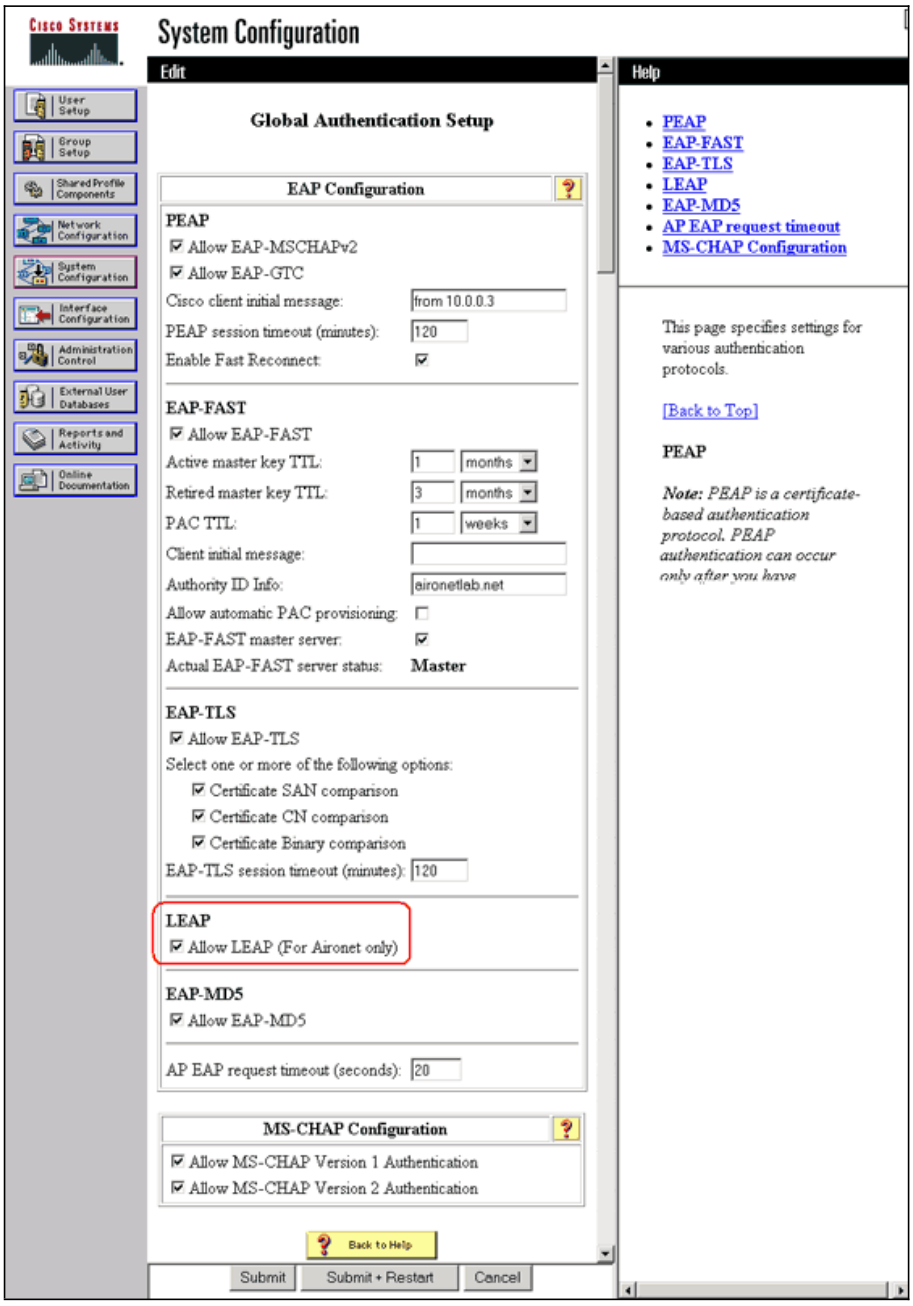
    Для получения информации о серверах не-ACS аутентификации обратитесь к документации производителя.



2. Кроме этого, в ACS Cisco Secure необходимо убедиться, что вы настраиваете ACS для выполнения аутентификации LEAP на странице Настройка системы - Настройка глобальной аутентификации. Сначала выберите **Настройка системы**, затем **Настройка глобальной аутентификации**.



3. Прокрутите страницу до описания настройки LEAP. При установке данного флажка ACS выполняет проверку подлинности LEAP.



3. Выберите **Security > WDS** в точке доступа WDS и перейдите в область WDS закладки **General Set-Up**. Выполните данные действия:

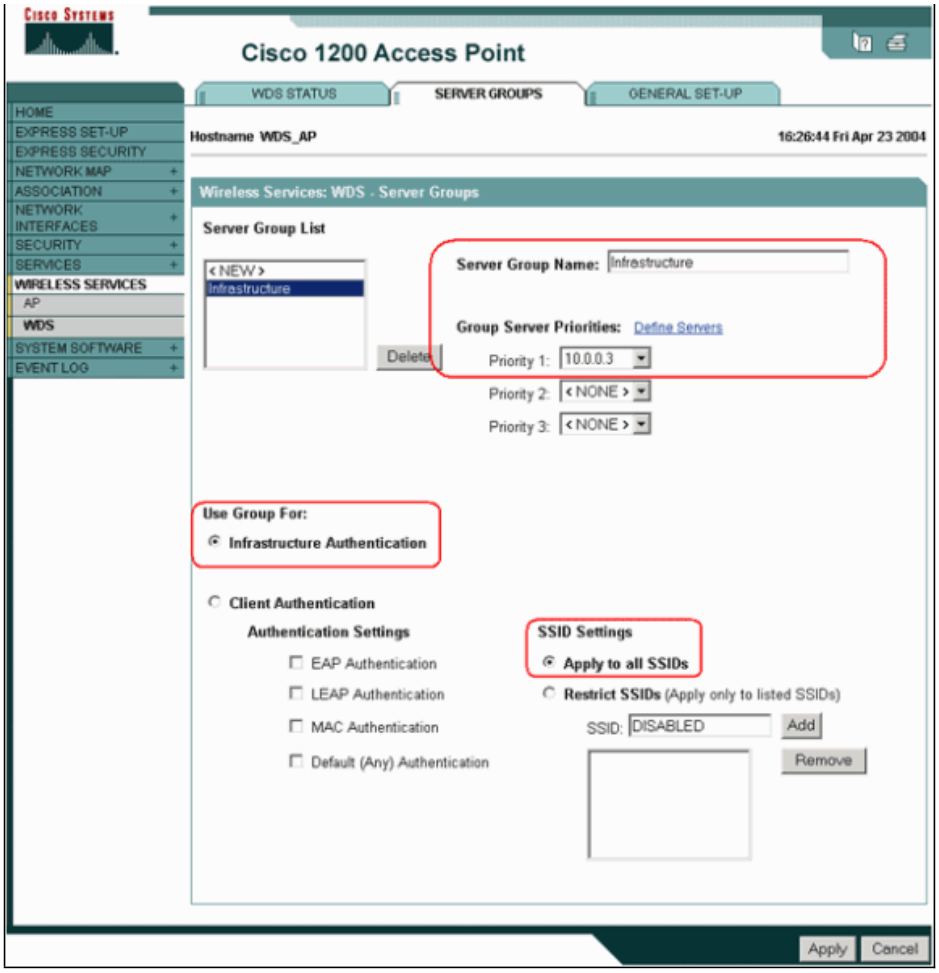
1. Проверьте **Use this AP as Wireless Domain Services**.
2. В поле Wireless Domain Services Priority задайте значение около **254**, которое является первым значением.

Или подайте следующие команды из командной строки:

```
WDS_AP#configure terminal
Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
WDS_AP(config)#wlccp wds priority 254 interface BVI1
WDS_AP(config)#end
WDS_AP#write memory
```

4. Выберите **Wireless Services > WDS** и перейдите к закладке **Server Groups** :

1. Определите имя группы серверов, проверяющих подлинность других точек доступа, как инфраструктурную группу.
2. Установите приоритет 1 для ранее настроенного сервера аутентификации.
3. Установите флажок **Use Group For: Infrastructure Authentication** .
4. Примените эти настройки к соответствующему идентификатору набора служб (SSID).



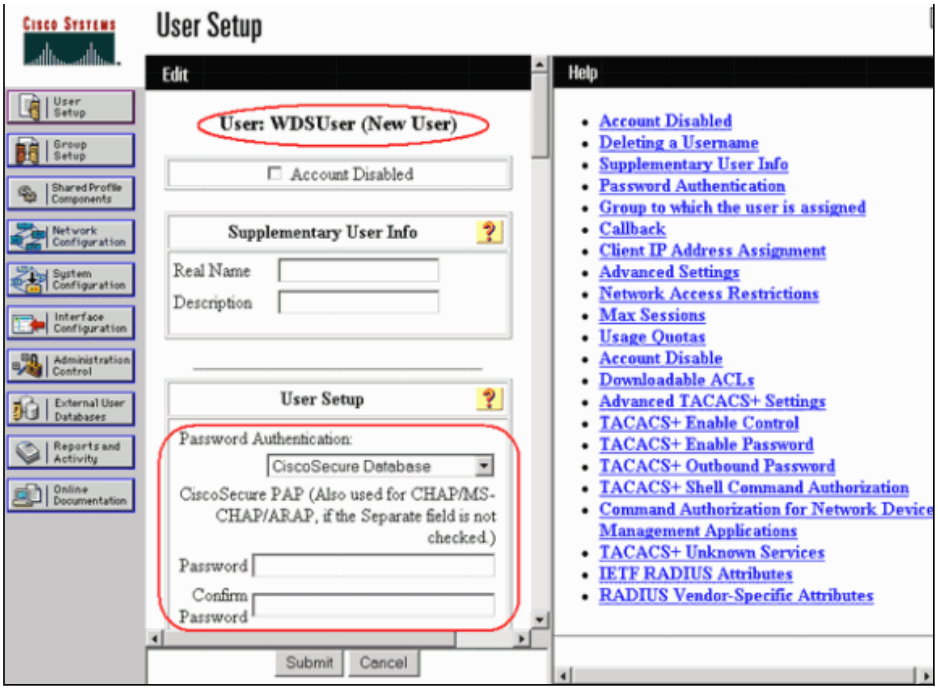
Или подайте следующие команды из командной строки:

```
WDS_AP#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.

WDS_AP(config)#wlccp authentication-server infrastructure
method_Infrastructure


WDS_AP(config)#aaa group server radius Infrastructure


WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645
acct-port 1646

WDS_AP(config-sg-radius)#exit

WDS_AP(config)#aaa authentication login method_Infrastructure
group Infrastructure


WDS_AP(config)#end

WDS_AP#write memory


!--- Некоторые команды отображаются в двух строках и более из-за ограничения
!--- по длине. Убедитесь в том, что вы вводите эти команды одной строкой.
```

5. Настройте имя пользователя и пароль WDS как у пользователя сервера аутентификации.

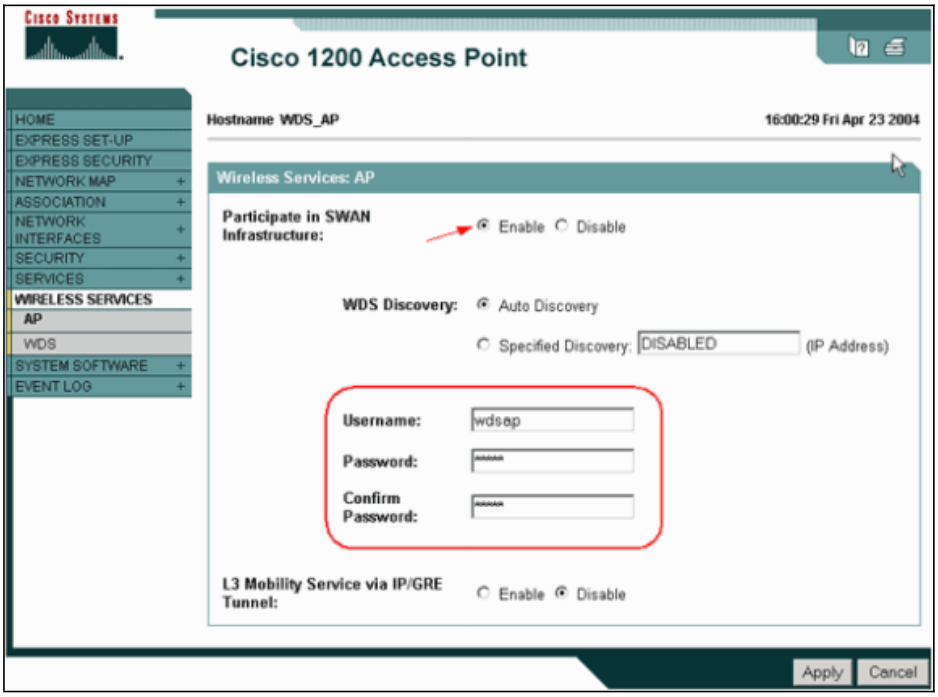
   В ACS Cisco Secure это происходит на странице User Setup, где вы определяете имя пользователя и пароль WDS. Для получения информации о серверах не-ACS аутентификации обратитесь к документации производителя.

   Примечание: Не включайте пользователя WDS в группу, обладающую большими правами и обязанностями, — WDS требует ограниченной аутентификации.



6. Выберите **Wireless Services > AP**, затем нажмите **Enable** для выбора параметра Wireless Services. Введите имя пользователя и пароль WDS .

   Нужно определить имя пользователя WDS и пароль на сервере проверки подлинности для всех устройств, предназначенных стать элементами WDS.



   Или подайте следующие команды из командной строки:

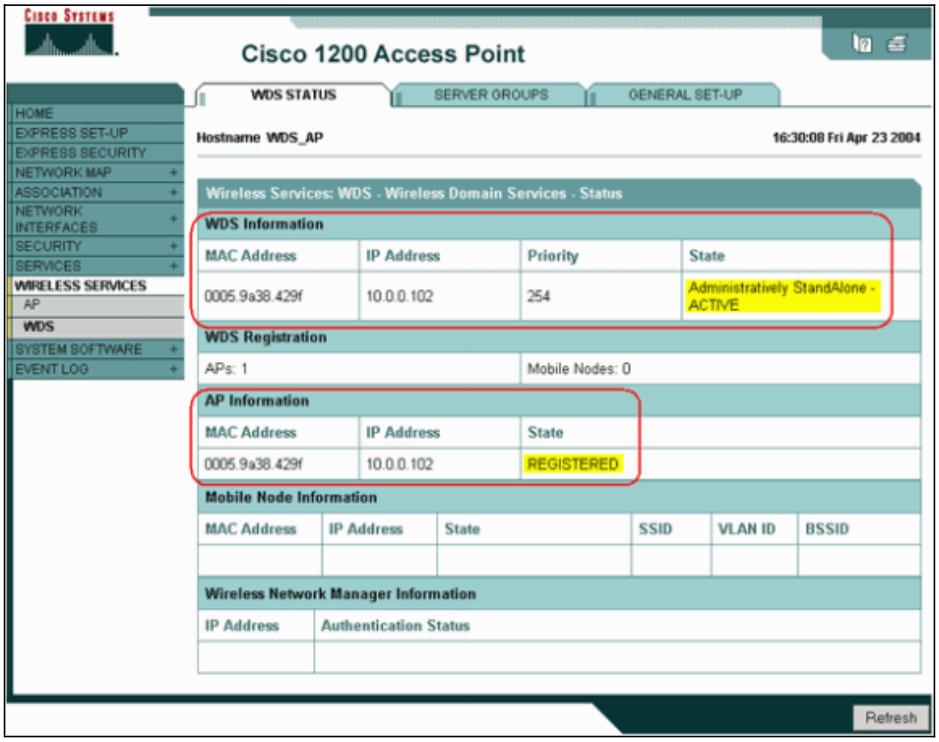
```
WDS_AP#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.

WDS_AP(config)#wlccp ap username wdsap password wdsap

WDS_AP(config)#end

WDS_AP#write memory
```

7. Выберите **Wireless Services > WDS**. В закладке WDS Status необходимо проверить, появляется ли точка доступа WDS в области сведений WDS в состоянии ACTIVE. Эта точка доступа также должна появиться в области сведений AP в состоянии REGISTERED.

   1. Если точка доступа не находится ни в одном из состояний (REGISTERED или ACTIVE), проверьте сервер аутентификации

на наличие ошибок или неудачных попыток аутентификации.

2. Когда точка доступа будет зарегистрирована должным образом, добавьте клиента точки доступа для использования служб WDS.



Или подайте следующие команды из командной строки:

```
WDS_AP#show wlccp wds ap

   MAC-ADDR        IP-ADDR           STATE          LIFETIME
0005.9a38.429f     10.0.0.102       REGISTERED       261

WDS_AP#show wlccp ap

WDS = 0005.9a38.429f, 10.0.0.102
state = wlccp_ap_st_registered
IN Authenticator = 10.0.0.102
MN Authenticator = 10.0.0.102

WDS_AP#
```

Примечание: Вы не можете протестировать подключение клиента, т.к. условия для аутентификации клиента еще не созданы.

Задайте WLSM как WDS

Следующий шаг - задать WLSM как WDS. WDS - единственное устройство, которое сообщается с сервером аутентификации.

Примечание: Введите эту команду в командную строку WLSM (а не Supervisor Engine 720) `enable`. Для доступа к командной строке WLSM выполните следующие команды в командной строке Supervisor Engine 720 `enable` :

```
c6506#session slot x proc 1

!--- В этой команде "x" - это номер слота, где находится WLSM.

The default escape character is Ctrl-^, then x.
Вы можете также ввести "exit" в удаленной строке для окончания сеанса.
Trying 127.0.0.51 ... Open


User Access Verification
```

```
Username: <username>
Password:  <password>

wlan>enable
Password: <enable password>
wlan#
```

Примечание: Для устранения неполадок и облегчения работы с WLSM настройте удаленный доступ Telnet к WLSM. Обратитесь к разделу Настройка удаленного доступа Telnet.

Для задания WLSM как WDS:

1. Из интерфейса CLI WLSM введите следующие команды и установите соединение с сервером аутентификации.

```
wlan#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
wlan(config)#aaa new-model
wlan(config)#aaa authentication login leap-devices group radius
wlan(config)#aaa authentication login default enable
wlan(config)#radius-server host ip_address_of_authentication_server
auth-port 1645 acct-port 1646

!--- Эта команда должна быть написана одной строкой..

wlan(config)#radius-server key shared_secret_with_server

wlan(config)#end
wlan#write memory
```

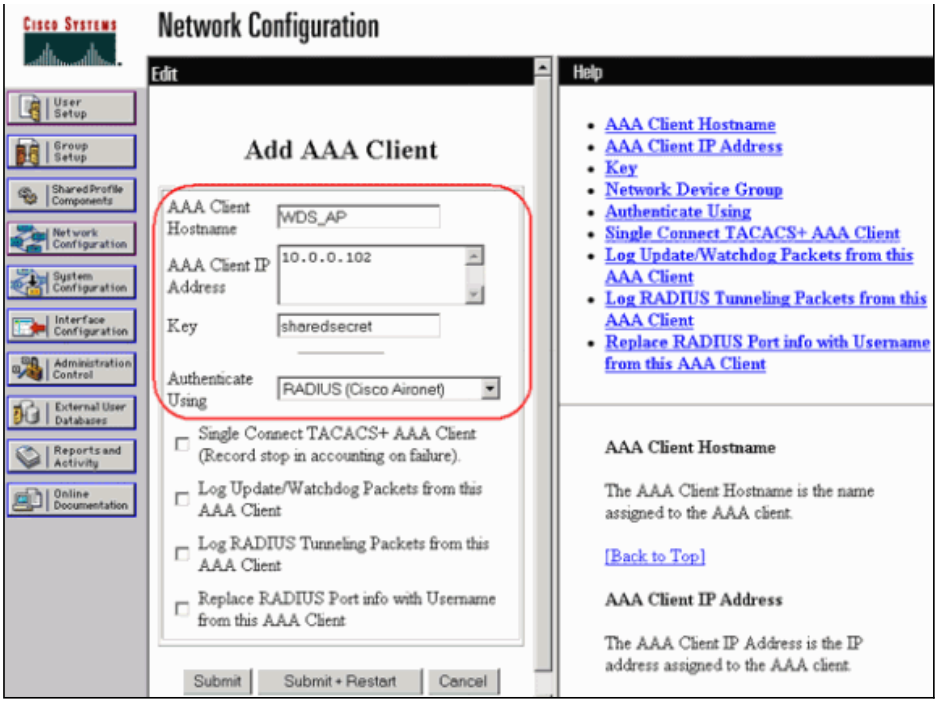
   Примечание: В WLSM не используется управление приоритетом. Если в сети содержатся несколько модулей WLSM, WLSM использует настройку избыточности для определения первичного модуля.

2. Настройте WLSM на сервере аутентификации как клиент аутентификации, авторизации и учета (AAA).

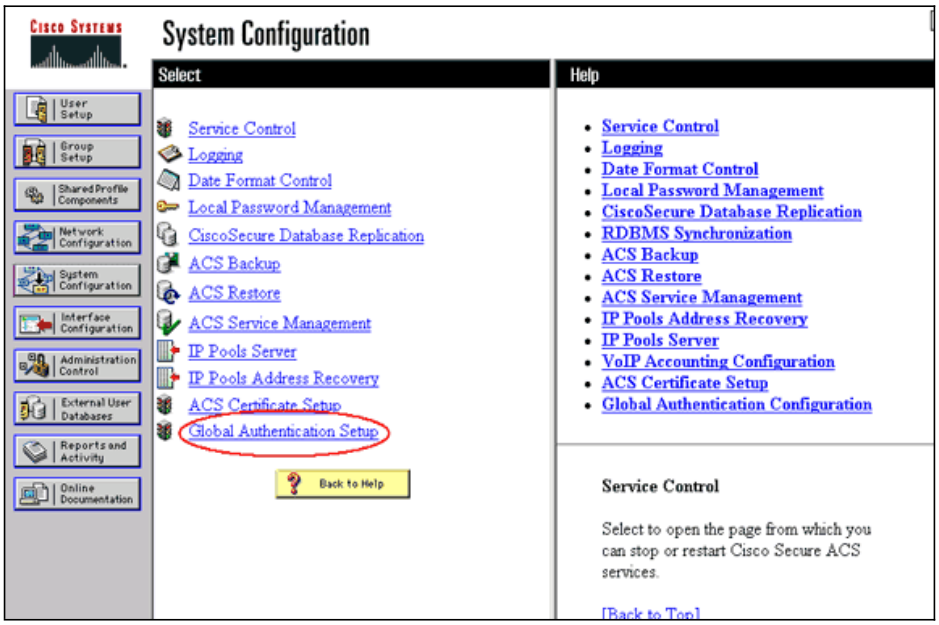
   В сервере управления доступом Cisco (ACS) это происходит на странице Настройка сети, где вы определяете следующие параметры для WLSM :

   - Имя
   - IP-адрес
   - Общий секрет
   - Метод аутентификации
     - RADIUS Cisco Aironet
     - Протокол RADIUS, разработанный Инженерной группа по развитию Интернета [IETF]

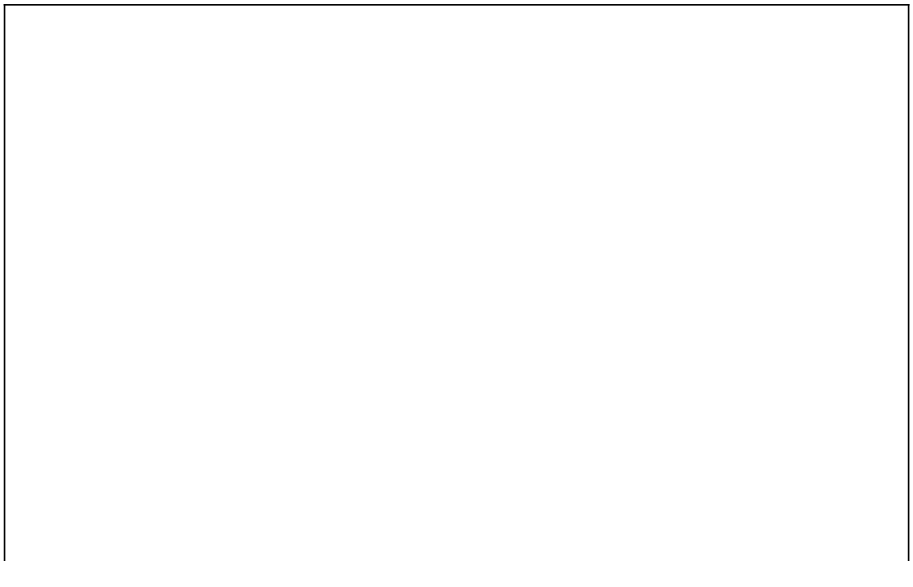
   Для получения информации о серверах не-ACS аутентификации обратитесь к документации производителя.

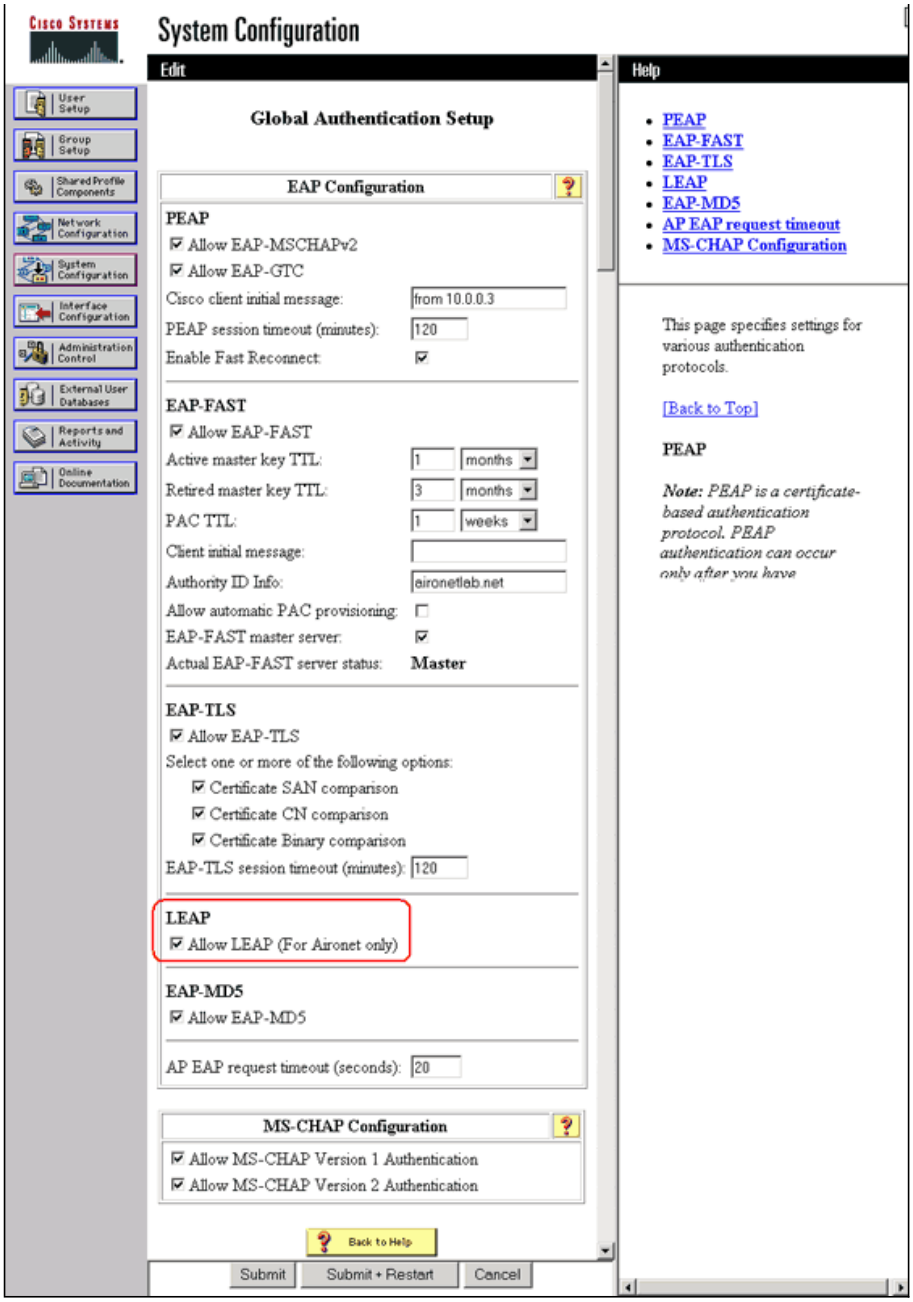


1. Кроме этого, в ACS Cisco Secure необходимо настроить ACS для выполнения аутентификации LEAP на странице Настройка системы - Настройка глобальной аутентификации. Сначала выберите **Настройка системы**, затем **Настройка глобальной аутентификации**.



2. Прокрутите страницу до описания настройки LEAP. При установке данного флажка ACS выполняет проверку подлинности LEAP.





3. Определите на WLSM способ аутентификации других AP (группа серверов инфраструктуры.)

```
wlan#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
wlan(config)#wlccp authentication-server infrastructure leap-devices

wlan(config)#end
wlan#write memory
```

4. На WLSM определите метод аутентификации клиентских устройств (группы клиент-сервер) и типы EAP, используемые этими клиентами.

```
wlan#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
wlan(config)#wlccp authentication-server client any leap-devices

wlan(config)#end
wlan#write memory
```

Примечание: Этот шаг освобождает от необходимости процесса Определения метода аутентификации клиента.

5. Определите уникальную VLAN между Supervisor Engine 720 и WLSM, чтобы позволить WLSM сообщаться с внешними объектами, такими как точки доступа и серверы аутентификации. Эта VLAN не используется в другом месте и для других целей в

сети. Создайте VLAN сначала на Supervisor Engine 720, затем выполните следующие команды:

- Для Supervisor Engine 720:

```
c6506#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
c6506(config)#wlan module slot_number allowed-vlan vlan_number

c6506(config)#vlan vlan_number

c6506(config)#interface vlan vlan_number

c6506(config-if)#ip address ip_address subnet_mask

c6506(config-if)#no shut
c6506(config)#end
c6506#write memory
```

- Для WLSM:

```
wlan#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
wlan(config)#wlan vlan vlan_number

wlan(config)#ipaddr ip_address subnet_mask

wlan(config)#gateway ip_address_of_vlan_interface_on_Sup720_created_above

wlan(config)#ip route 0.0.0.0 0.0.0.0


!--- Обычно этот адрес совпадает с инструкцией шлюза.

wlan(config)#admin
wlan(config)#end
wlan#write memory
```

6. Для проверки функций WLSM используются следующие команды:

- Для WLSM:

```
wlan#show wlccp wds mobility

LCP link status: up
HSRP state: Not Applicable
Total # of registered AP: 0
Total # of registered MN: 0

Tunnel Bindings:
Network ID    Tunnel IP         MTU     FLAGS
==========  ===============  =========  =====
 <vlan>       <ip address>        1476  T

Flags: T=Trusted, B=IP Broadcast enabled, N=Nonexistent
wlan#
```

- Для Supervisor Engine 720:

```
c6506#show mobility status
WLAN Module is located in Slot: 5 (HSRP State: Active)
LCP Communication status      : up
Number of Wireless Tunnels    : 0
Number of Access Points       : 0
Number of Access Points       : 0
```

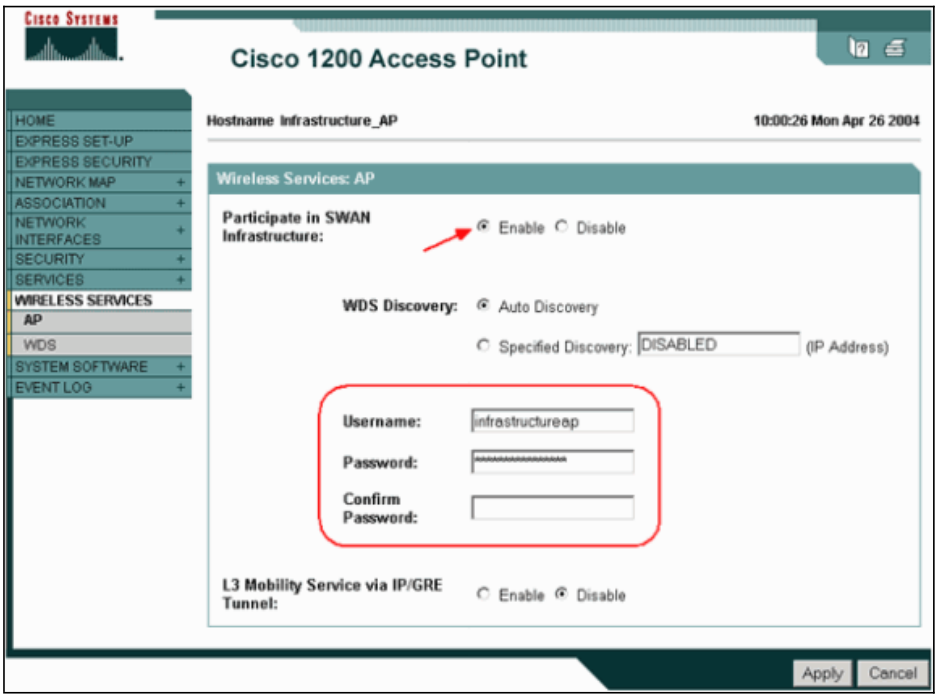
Задайте AP как инфраструктуру

Далее, необходимо обозначить по крайней мере одну инфраструктурную точку доступа и привязать эту точку доступа к WDS. Клиенты устанавливают соединение с инфраструктурными точками доступа. Инфраструктурные точки доступа требуют точку доступа WDS или WLSM для проверки их подлинности.

Выполните следующие шаги, чтобы добавить инфраструктурную точку доступа, использующую услуги WDS:

1. Выберите **Wireless Services > AP**. На инфраструктурной точке доступа выберите **Enable** для определения параметра Wireless Services. Затем введите имя пользователя и пароль WDS .

   Необходимо определить имя пользователя WDS и его пароль на сервере проверки подлинности для всех устройств, которые будут являться членами WDS.



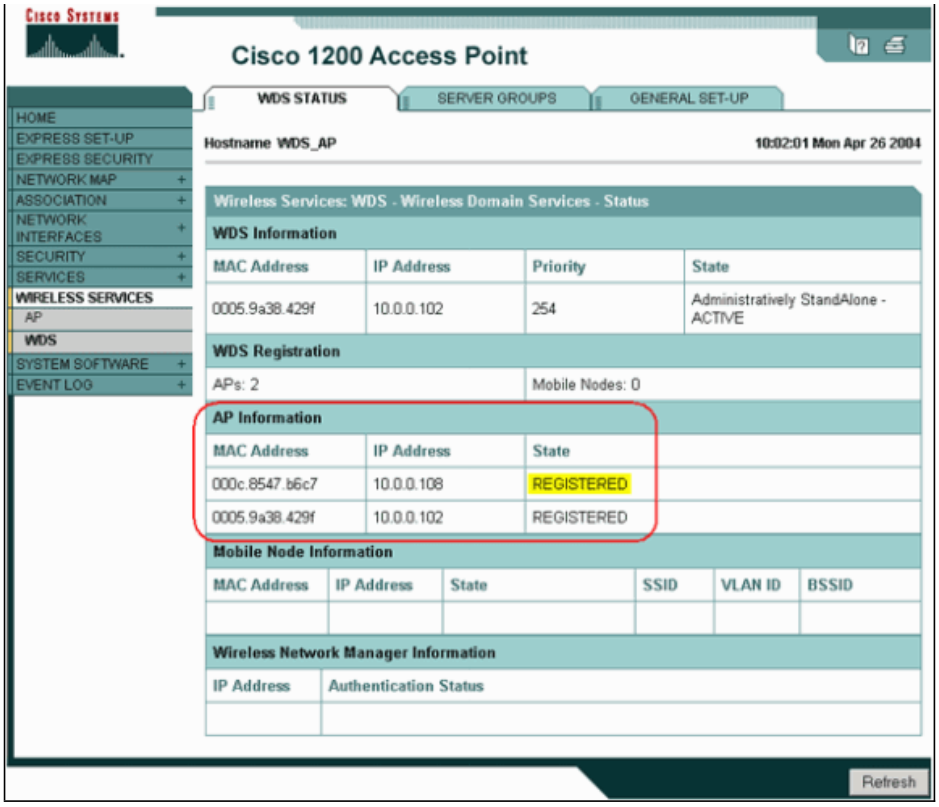
   Или подайте следующие команды из командной строки:

```
WDS_AP#configure terminal

Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.

Infrastructure_AP(config)#wlccp ap username infrastructureap password infrastructureap

Infrastructure_AP(config)#end

Infrastructure_AP#write memory
```

2. Выберите **Wireless Services > WDS**. В закладке WDS Status необходимо проверить, появляется ли точка доступа WDS в области сведений WDS в состоянии ACTIVE, и в области сведений AP в состоянии REGISTERED.

   1. Если точка доступа не находится ни в одном из состояний (REGISTERED и/или ACTIVE), проверьте сервер аутентификации на наличие ошибок или неудачных попыток аутентификации.

   2. Как только точка доступа получит статус ACITVE (активно) и/или REGISTERED (зарегистрировано), добавьте в раздел WDS метод аутентификации клиента.



Или подайте следующую команду из командной строки:

```
WDS_AP#show wlccp wds ap

   MAC-ADDR        IP-ADDR          STATE          LIFETIME
000c.8547.b6c7     10.0.0.108       REGISTERED       194
0005.9a38.429f     10.0.0.102       REGISTERED       76
```

Или выполните следующую команду из WLSM:

```
wlan#show wlccp wds ap
   MAC-ADDR        IP-ADDR          STATE          LIFETIME
000c.8547.b6c7     10.0.0.108       REGISTERED       194
0005.9a38.429f     10.0.0.102       REGISTERED       76
wlan#
```

Затем выполните следующую команду на инфраструктурной точке доступа:

```
Infrastructure_AP#show wlccp ap

WDS = 0005.9a38.429f, 10.0.0.102
state = wlccp_ap_st_registered
IN Authenticator = 10.0.0.102
MN Authenticator = 10.0.0.102

Infrastructure_AP#
```

Примечание: Вы не можете протестировать подключение клиента, т.к. условия для аутентификации клиента еще не созданы.

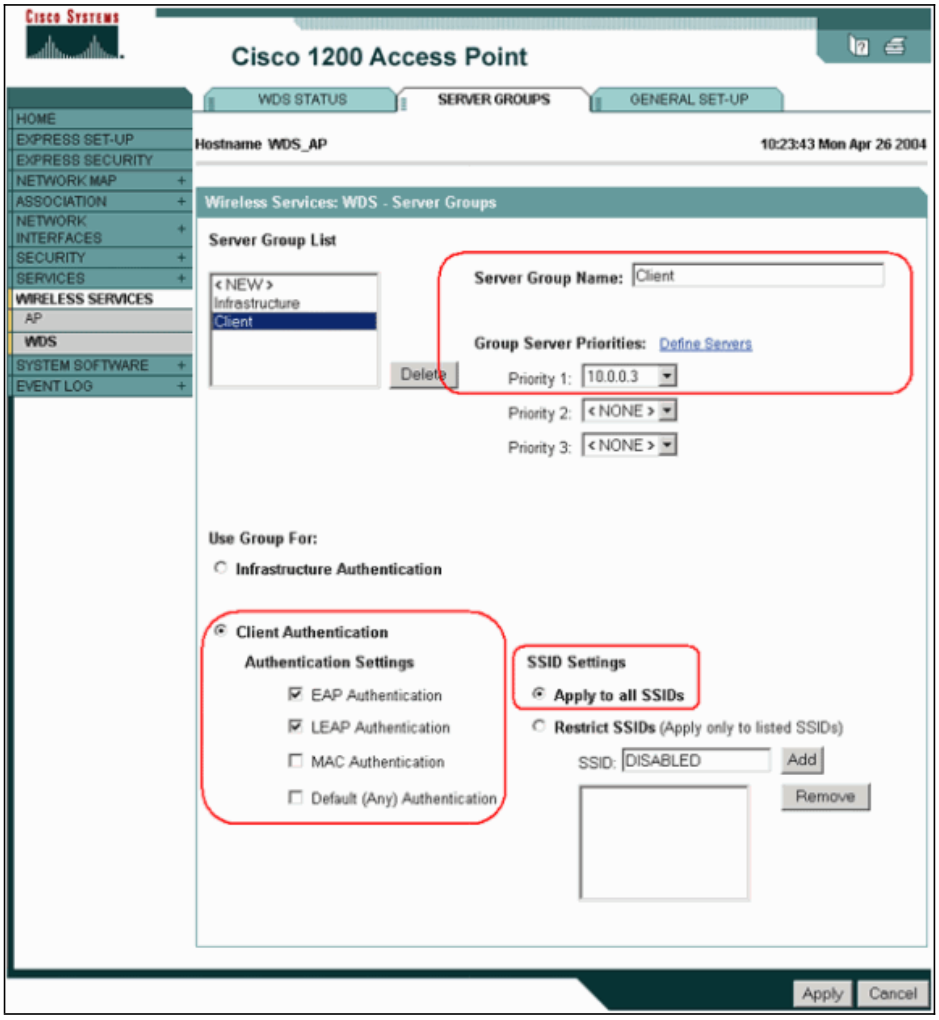
Определите метод аутентификации клиента

Наконец, определите метод аутентификации клиента.

Выполните следующие шаги, чтобы добавить добавить метод проверки подлинности клиента:

1. Выберите **Wireless Services > WDS**. Выполните следующие шаги на закладке Server Groups точки доступа WDS:

    1. Определите группу сервера, которая проверяет подлинность клиента (Client group).
    2. Установите приоритет 1 для ранее настроенного сервера аутентификации.
    3. Установите подходящий тип аутентификации (LEAP, EAP, MAC и т.д.).
    4. Примените эти настройки к соответствующим SSID.



Или подайте следующие команды из командной строки:

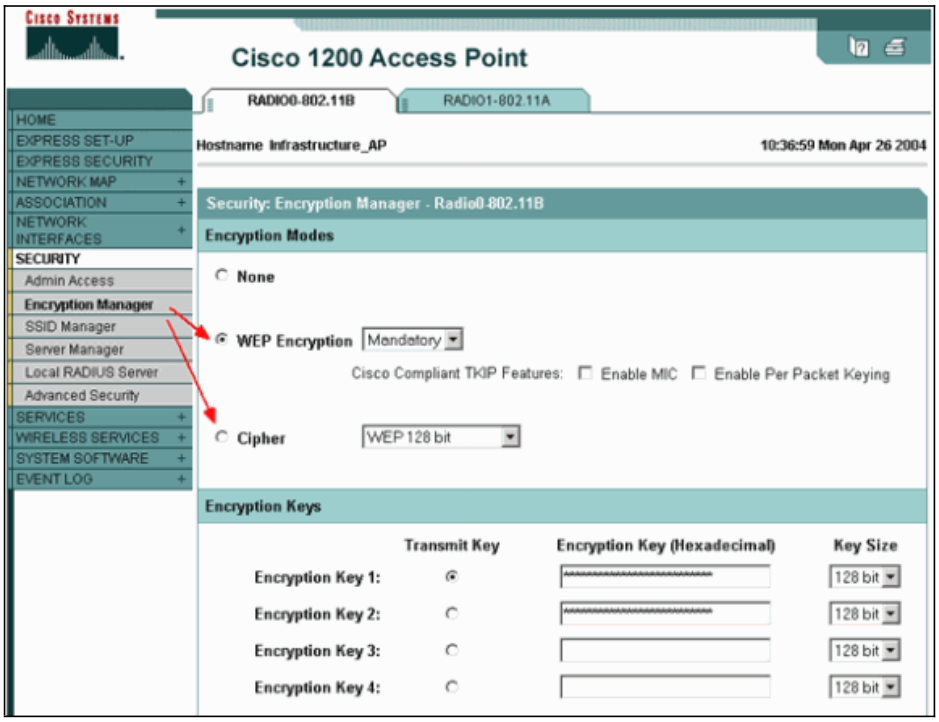
```
WDS_AP#configure terminal
Введите команды настройки, каждую в отдельной строке.  В конце введите CNTL/Z.
WDS_AP(config)#wlccp authentication-server client eap method_Client
WDS_AP(config)#wlccp authentication-server client leap method_Client
WDS_AP(config)#aaa group server radius Client
WDS_AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
WDS_AP(config-sg-radius)#exit
WDS_AP(config)#aaa authentication login method_Client group Client
WDS_AP(config)#end
WDS_AP#write memory
```

Примечание: Например, точка доступа WDS является выделенной и не поддерживает подключение клиента.

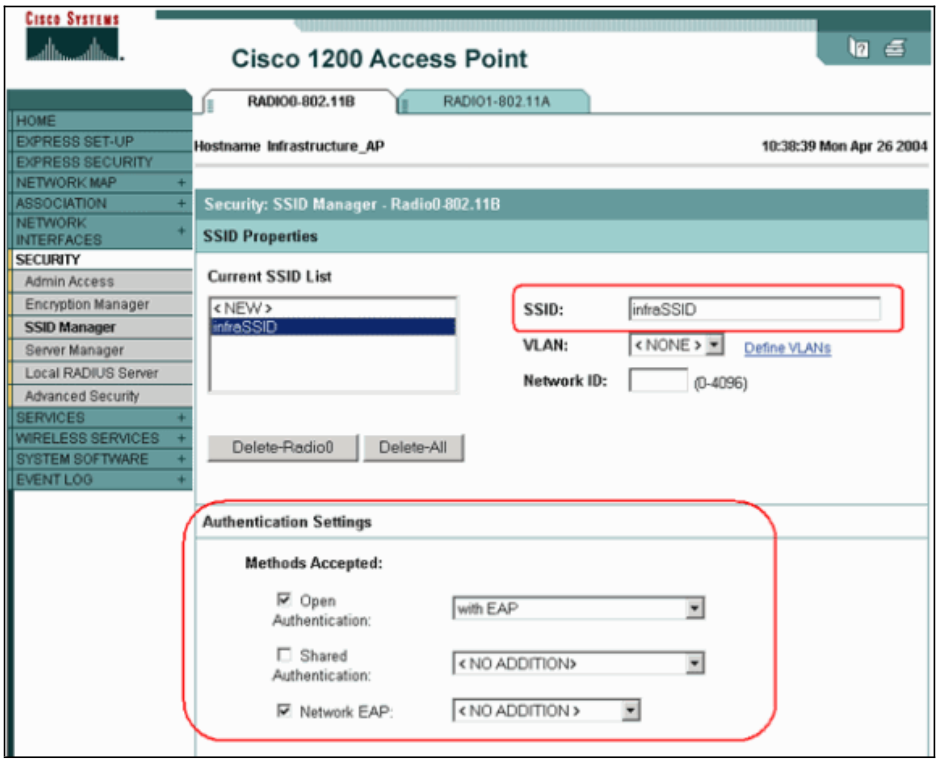
Примечание: Не стоит настраивать инфраструктурные точки доступа для групп серверов, т.к. эти точки доступа направляют все запросы на WDS для обработки.

2. Для инфраструктурной точки (или точек) доступа:

    1. Выберите **Security > Encryption Manager**, затем **WEP Encryption** или **Cipher** в зависимости от используемого протокола аутентификации.

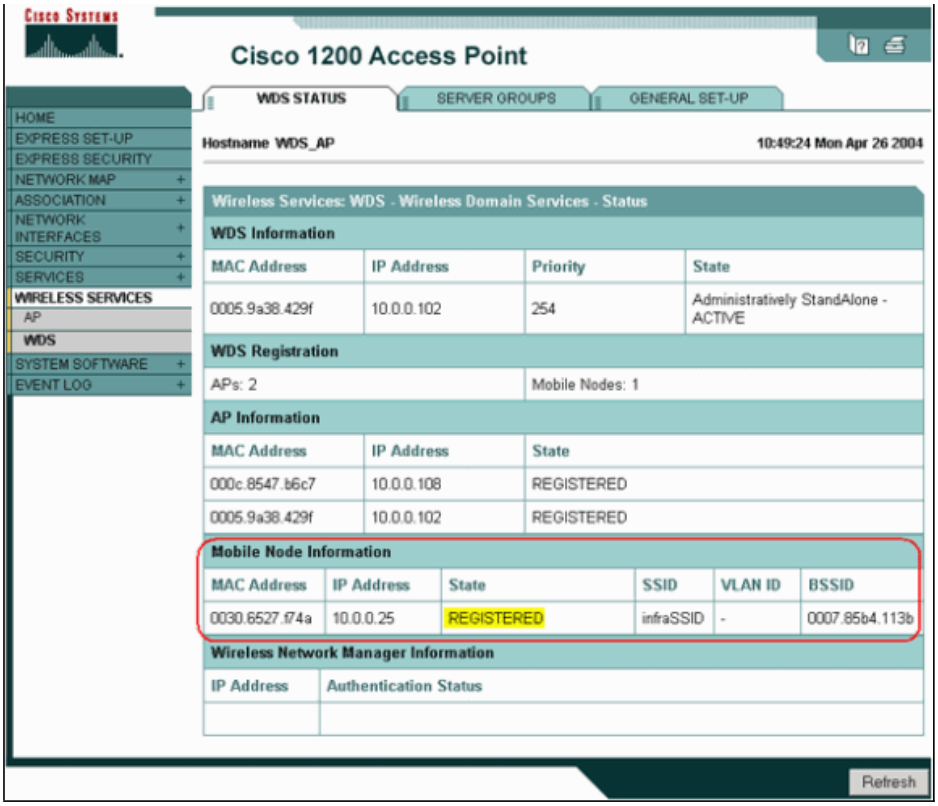


    2. Выберите **Security > SSID Manager**, затем выберите методы проверки подлинности, соответствующие используемому протоколу аутентификации.



3. Теперь можно успешно протестировать, проходят ли клиенты аутентификацию для точек доступа к инфраструктуре. Точка доступа WDS в закладке WDS Status (**Wireless Services > WDS**) показывает, что клиент появляется в пространстве сведений о мобильных узлах и имеет статус REGISTERED.

    Если клиент не появляется, проверьте сервер аутентификации на наличие ошибок или неудачных попыток аутентификации клиентами.



Или подайте следующие команды из командной строки:

```
WDS_AP#show wlccp wds

     MAC: 0005.9a38.429f, IP-ADDR: 10.0.0.102     , Priority: 254
     Interface BVI1, State: Administratively StandAlone - ACTIVE
     AP Count: 2  , MN Count: 1

WDS_AP#show wlccp wds mn

   MAC-ADDR       IP-ADDR          Cur-AP            STATE
0030.6527.f74a  10.0.0.25       000c.8547.b6c7      REGISTERED

WDS_AP#
```

Примечание: Если вы хотите исправить аутентификацию, убедитесь, что вы исправляете ее на точке доступа WDS, т.к. точка доступа WDS является устройством, сообщающимся с серером аутентификации.

Проверка

В настоящий момент для этой настройки отсутствует процедура проверки.

Устранение неполадок

В данном разделе описывается процесс устранения неполадок настройки. Далее приведен список наиболее распространенных вопросов о команде WDS для пояснения значения этих команд:

- **Вопрос: Какие настройки рекомендуется установить на точке доступа WDS для следующих параметров?**
  - **radius-server timeout**
  - **radius-server deadtime**
  - **Temporal Key Integrity Protocol (TKIP) message integrity check (MIC) Failure Holdoff Time**
  - **Client Holdoff Time**

- **Интервал повторной проверки подлинности EAP или MAC**
- **EAP Client Timeout (необязательно)**

Ответ: Предлагается сохранить настройки по умолчанию и менять их только при возникновении проблемы со временем.

Рекомендуемые настройки для точки доступа WDS:

- Отключить **radius-server timeout**. Это время (в секундах), которое точка доступа ждет ответа на запрос RADIUS перед повторной отправкой запроса. Значение по умолчанию равно пяти секундам.
- Отключить **radius-server deadtime**. RADIUS игнорируется дополнительными запросами в течение промежутка времени (в минутах), пока все серверы не буду помечены как заблокированные.
- Значение TKIP MIC Failure Holdoff Time по умолчанию равно 60 секундам. При включении времени задержки вы можете вводить этот интервал в секундах. Если точка доступа обнаружит 2 ошибки MIC в течение 60 секунд, она блокирует всех клиентов TKIP на этом интерфейсе на период времени, равный заданному значению времени задержки.
- Client Holdoff Time по умолчанию должно быть отключено. При включении задержки, введите количество секунд, которое точка доступа должна ждать с момента обнаружения ошибки аутентификации до обработки следующего запроса аутентификации.
- Интервал повторной проверки подлинности EAP или MAC по умолчанию отключен. При включении повторной проверки подлинности вы можете задать интервал или принять это значение от сервера аутентификации. Если вы хотите самостоятельно задать интервал, введите интервал времени (в секундах), которое точка доступа будет ожидать до инициации повторной проверки уже аутентифицированного клиента.
- EAP Client Timeout (необязательно) равно по умолчанию 120 секундам. Введите промежуток вермени, в течение которого точка доступа должна ожидать ответ на запрос аутентификации от беспроводных клиентов.

- **Вопрос: Вопрос о времени задержки TKIP: я читал(а), что оно должно быть равно 100 мсек, а не 60 сек. Я предполагаю, что оно устанавливается равным одной секунде из обозревателя, т.к. это самое маленькое значение, которое можно выбрать. Так ли это?**

  Ответ: Нет специальных рекомендаций для установления значения равным 100 мсек; это используется лишь в случае сообщения об ошибке, когда единственный способ ее устранения - увеличить это время. Минимальное значение - 1 секунда.

- **Вопрос: Помогают ли как-нибудь следующие две команды аутентификации клиента и нужны ли они на WDS или инфраструктурной точке доступа?**

  - **radius-server attribute 6 on-for-login-auth**
  - **radius-server attribute 6 support-multiple**

  Ответ: Эти команды не помогают процессу аутентификации, и они не нужны на WDS или точке доступа.

- **Вопрос: Я полагаю, что на инфраструктурной точке доступа не нужны настройки диспетчера сервера (Server Manager) и глобальных свойств (Global Properties), т.к. точка доступа получает информацию от WDS. Так ли это? Нужны ли какие-либо из нижеперечисленных команд для инфраструктурной точки доступа?**

  - **radius-server attribute 6 on-for-login-auth**
  - **radius-server attribute 6 support-multiple**
  - **radius-server timeout**
  - **radius-server deadtime**

  Ответ: Для инфраструктурных точек доступа не нужны ни Server Manager, ни Global Properties. WDS выполняет эти функции, поэтому нет необходимости в следующих настройках:

  - **radius-server attribute 6 on-for-login-auth**
  - **radius-server attribute 6 support-multiple**
  - **radius-server timeout**

- **radius-server deadtime**

Настройка **radius-server attribute 32 include-in-access-req format %h** необходима и устанавливается по умолчанию.

Команды поиска и устранения неисправностей

Интерпретатор выходных данных (только для зарегистрированных пользователей) (OIT) поддерживает определенные команды **show**. Используйте OIT для просмотра анализа выходных данных команды **show** .

Примечание: Обратитесь к разделу Важные сведения о командах отладки перед использованием команд **debug** .

- **debug dot11 aaa authenticator all**—показывает различные согласования клиента, возникающие во время процесса 802.1x или EAP соединения и аутентификации клиента. Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. Эта команда заметила отладочную команду **debug dot11 aaa dot1x all** в этом и более поздних выпусках ПО.
- **debug aaa authentication**—показывает процесс аутентификации с точки зрения AAA.
- **debug wlccp ap**—показывает согласования WLCCP, участвующие в соединении точки доступа и WDS.
- **debug wlccp packet**—показывает подробную информацию обо всех согласованиях WLCCP.
- **debug wlccp leap-client**—показывает детали соединения инфраструктурного устройства с WDS.

Дополнительная информация

- **Настройка WDS, быстрого и безопасного роуминга и радиоуправления**
- **Примечания по настройке модуля служб беспроводных сетей LAN серии Catalyst 6500 Cisco**
- **Протокол развертывания модуля служб беспроводных сетей LAN серии Catalyst 6500 (WLSM)**
- **Настройка пакетов Cipher Suites и WEP**
- **Настройка типов аутентификации**
- **Страницы поддержки беспроводных сетей LAN**
- **Техническая поддержка и документация - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92150/WDS.shtml