Настройка беспроводных доменных служб

Содержание

Введение

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 (WLSE), получив возможность использовать его функции.

Предварительные условия

Требования

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

- Имейте доскональное знание беспроводных локальных сетей и вопросов их безопасности.

- Знания современных методов обеспечения безопасности расширенного протокола аутентификации (EAP).

Используемые компоненты

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

- AP с программным обеспечением Cisco IOS
- Программное обеспечение Cisco IOS версии 12.3 (2) JA2 или позже
- Сервисный модуль беспроводной локальной сети серии Catalyst 6500

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. 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 интерфейса командной строки (CLI). При работе в действующей сети перед применением команды необходимо изучить все возможные последствия ее выполнения.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Беспроводные доменные сервисы

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:

- Быстро безопасный роуминг
- Взаимодействие WLSE
- Радиоуправление

Необходимо установить отношения между AP, которые участвуют в WDS и WLSM, прежде чем будут работать любые другие основанные на WDS функции. 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:

- Смена ключа
- Роуминг
- Когда пользователь запускает устройство клиента

Любой основанный на RADIUS протокол Аутентификации eap может быть туннелирован через WDS, такой как они:

- Легковесный EAP (LEAP)
- Защищенный EAP (PEAP)
- Transport Layer Security EAP (EAP-TLS)
- ГИБКАЯ АУТЕНТИФИКАЦИЯ EAP через безопасный, туннелирующий (EAP-FAST)

Аутентификация с использованием MAC-адреса может также туннелировать или к внешнему серверу проверки подлинности или против списка, локального для AP WDS. WLSM не поддерживает аутентификацию MAC-адреса.

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.

AP, настроенный как устройство WDS, поддерживает до 60 участвующих AP. Маршрутизатор ISR (ISR), настроенный как устройства WDS, поддерживает до 100 участвующих AP. И оборудованный коммутатор WLSM поддерживает до 600 участвующих AP и до 240 групп мобильности. Одиночный AP поддерживает до 16 групп мобильности.

Примечание: Cisco рекомендует, чтобы AP инфраструктуры выполнили ту же версию IOS как устройство WDS. При использовании более старой версии IOS AP могли бы быть не в состоянии аутентифицироваться на устройстве WDS. Кроме этого, Cisco рекомендует использовать последнюю версию ПО IOS. Последнюю версию ПО IOS можно найти на странице Беспроводные устройства .

Роль устройства WDS

Устройство WDS выполняет несколько задач на вашей беспроводной локальной сети:

- Объявляет его возможность WDS и участвует в избрании лучшего устройства WDS для вашей беспроводной локальной сети. При настройке беспроводной локальной сети для WDS вы устанавливаете одно устройство как главного кандидата WDS и одно или более дополнительных устройств как резервные кандидаты WDS. Если основное устройство WDS уходит линия, одно из резервных устройств WDS занимает свое место.

- Аутентифицирует все AP в подсети и устанавливает безопасный канал связи с каждым из них.
- Собирает радио-данные от AP в подсети, объединяет данные, и вперед это к устройству WLSE в вашей сети.
- Законы как passthrough для всех устройств аутентифицированного клиента 802.1x связались к участвующим AP.
- Регистрирует все устройства клиента в подсети, которые используют динамическое манипулирование, устанавливает ключи сеанса для них и кэширует их учетные данные безопасности. Когда клиент перемещается к другому AP, устройство WDS вперед учетные данные безопасности клиента к новому AP.

Роль точек доступа Использование устройства WDS

AP на вашей беспроводной локальной сети взаимодействуют с устройством WDS в этих действиях:

- Обнаружьте и отследите текущее устройство WDS и релейные рекламные объявления WDS к беспроводной локальной сети.
- Аутентифицируйтесь с устройством WDS и установите безопасный канал связи к устройству WDS.
- Зарегистрируйте привязанные устройства клиента в устройстве WDS.
- Данные радио отчёта к устройству WDS.

!--- конфигурацию

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 инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

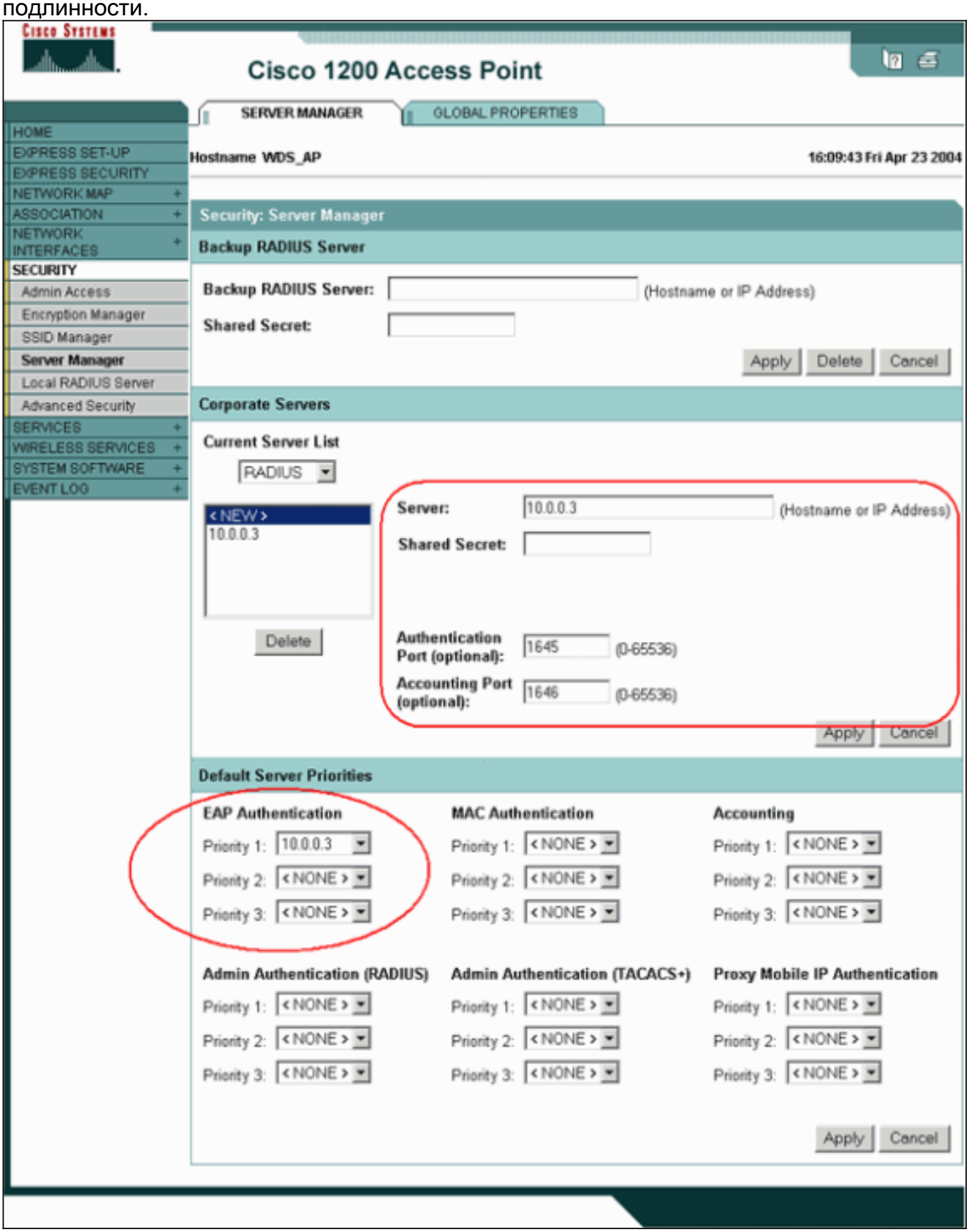
Задайте AP как WDS

Первый шаг должен определять AP как WDS. Точка доступа WDS - единственная точка, которая сообщается с сервером аутентификации.

Для задания точки доступа WDS необходимо выполнить следующие шаги:

1. Для настройки Сервера проверки подлинности на AP WDS выберите **Security> Server Manager**, чтобы перейти к вкладке Server Manager:Под Корпоративными серверами введите IP-адрес сервера проверки подлинности в поле Server.Укажите общий секретный ключ и порты.Под Приоритетами Сервера По умолчанию, набор поле Priority 1 к тому IP-адресу сервера под соответствующим типом проверки

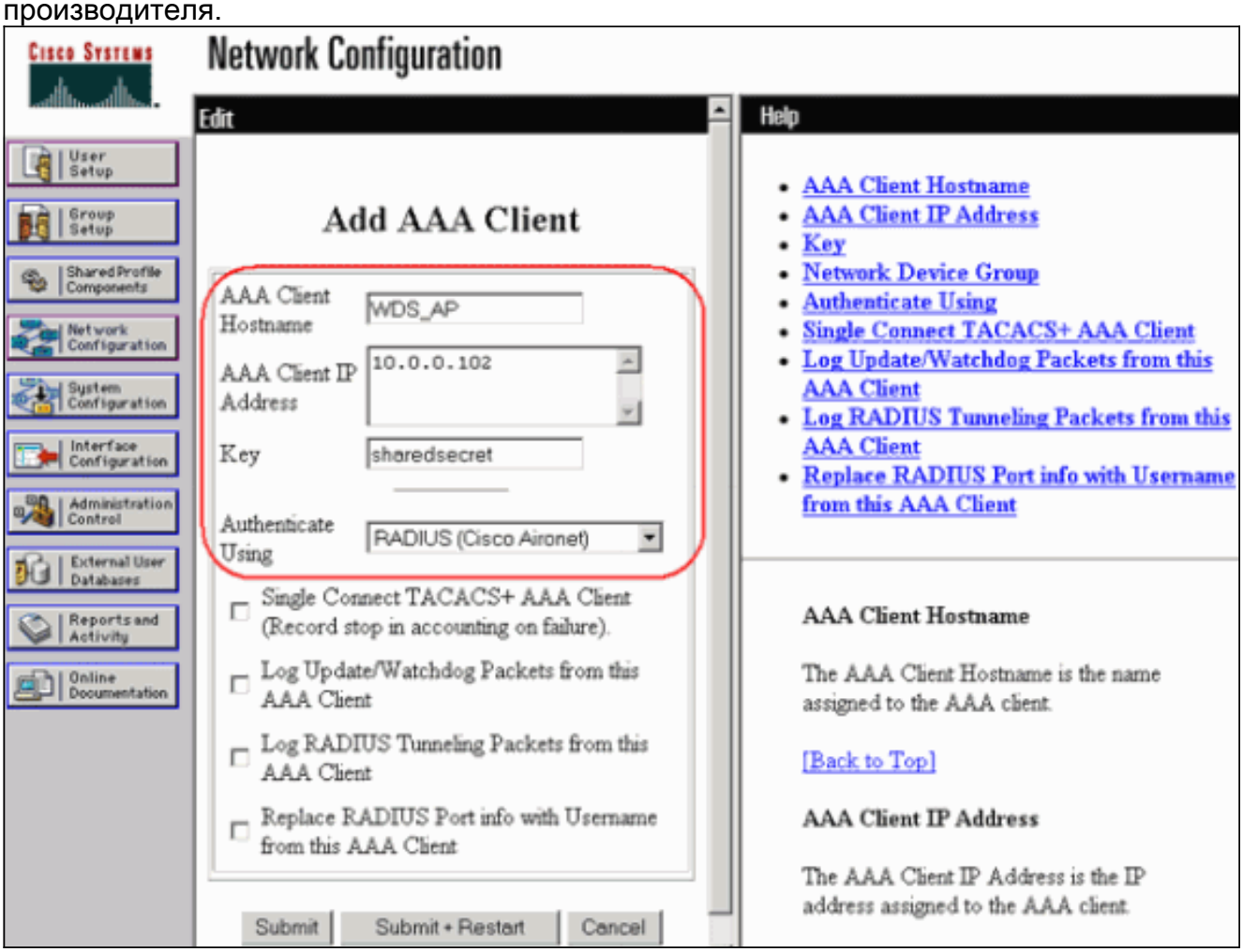
подлинности.



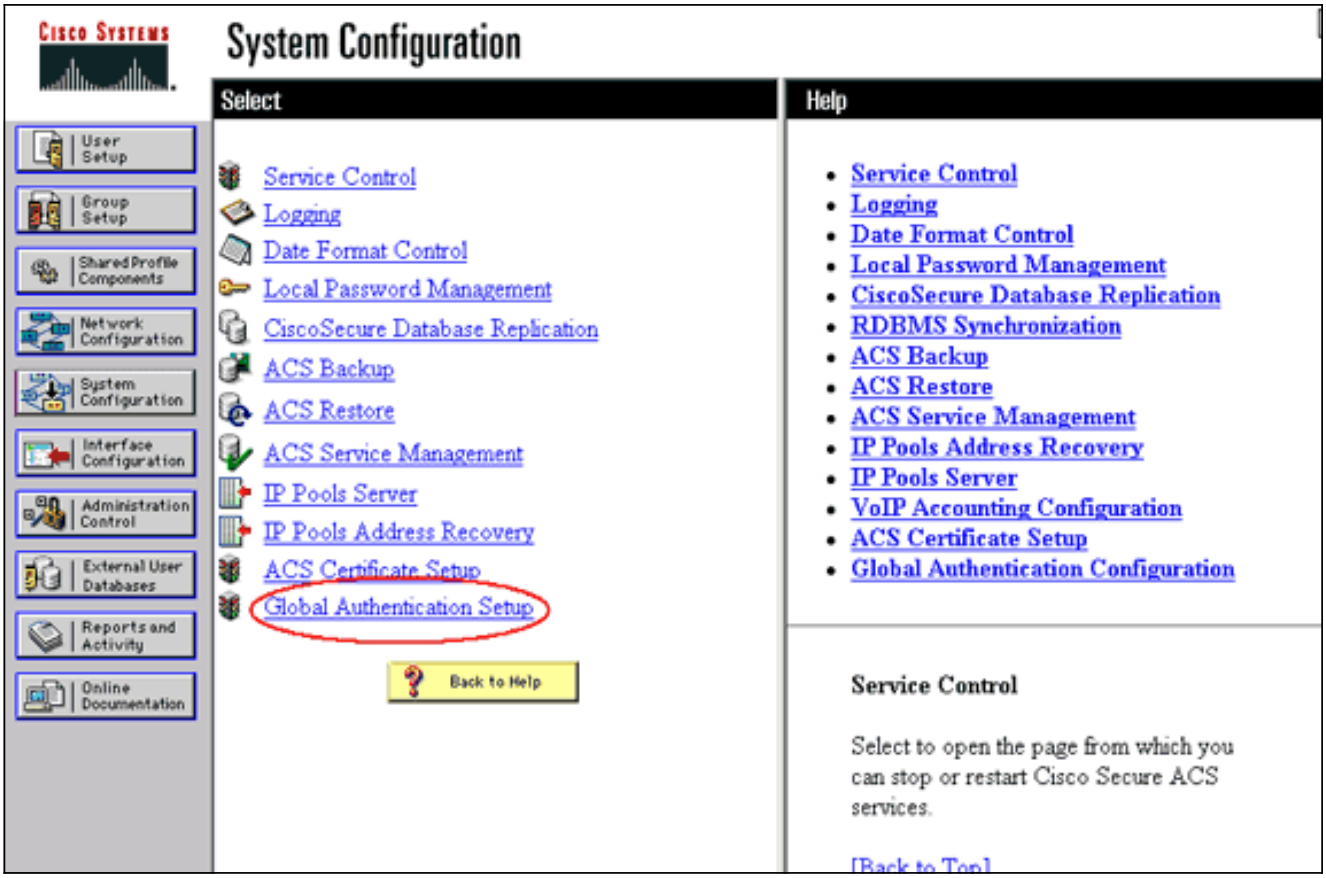
Или подайте следующие команды из командной строки:

2. Следующий шаг должен настроить AP WDS в сервере проверки подлинности как клиент аутентификации, авторизации и учета (AAA). Для этого необходимо добавить AP WDS как клиент AAA. Выполните следующие действия:**Примечание:** Этот документ использует сервер Cisco Secure ACS в качестве сервера проверки подлинности.В сервере управления доступом Cisco (ACS) это происходит на странице Настройка сети , где вы определяете следующие параметры для точки доступа WDS:NameIP-адресОбщий secretAuthentication methodRADIUS Cisco AironetПротокол RADIUS,

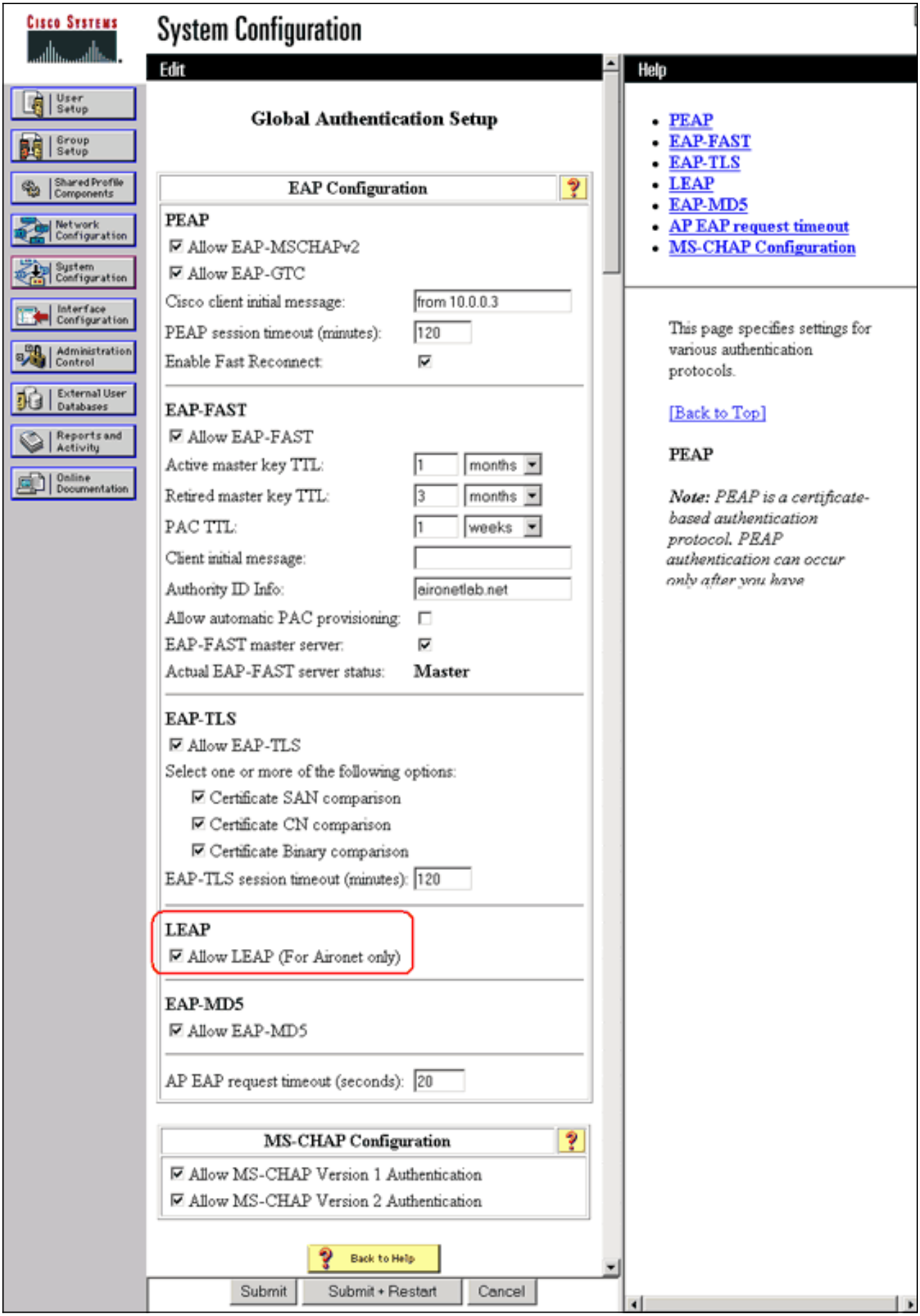
разработанный Инженерной группа по развитию Интернета [IETF]Щелкните **по Submit**.Для получения информации о серверах не-ACS аутентификации обратитесь к документации
производителя.



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.

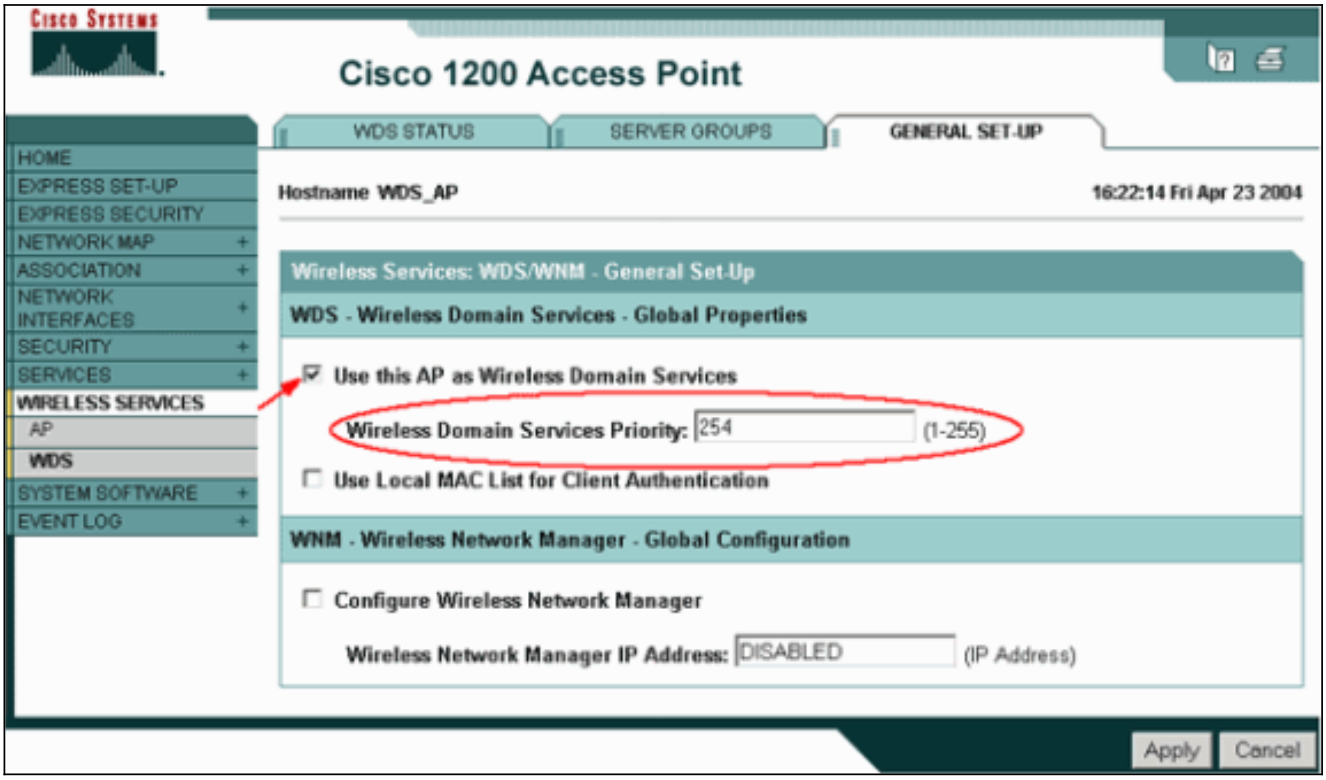


Прокрутите страницу до описания настройки LEAP. При установке данного флажка ACS выполняет проверку подлинности
LEAP.



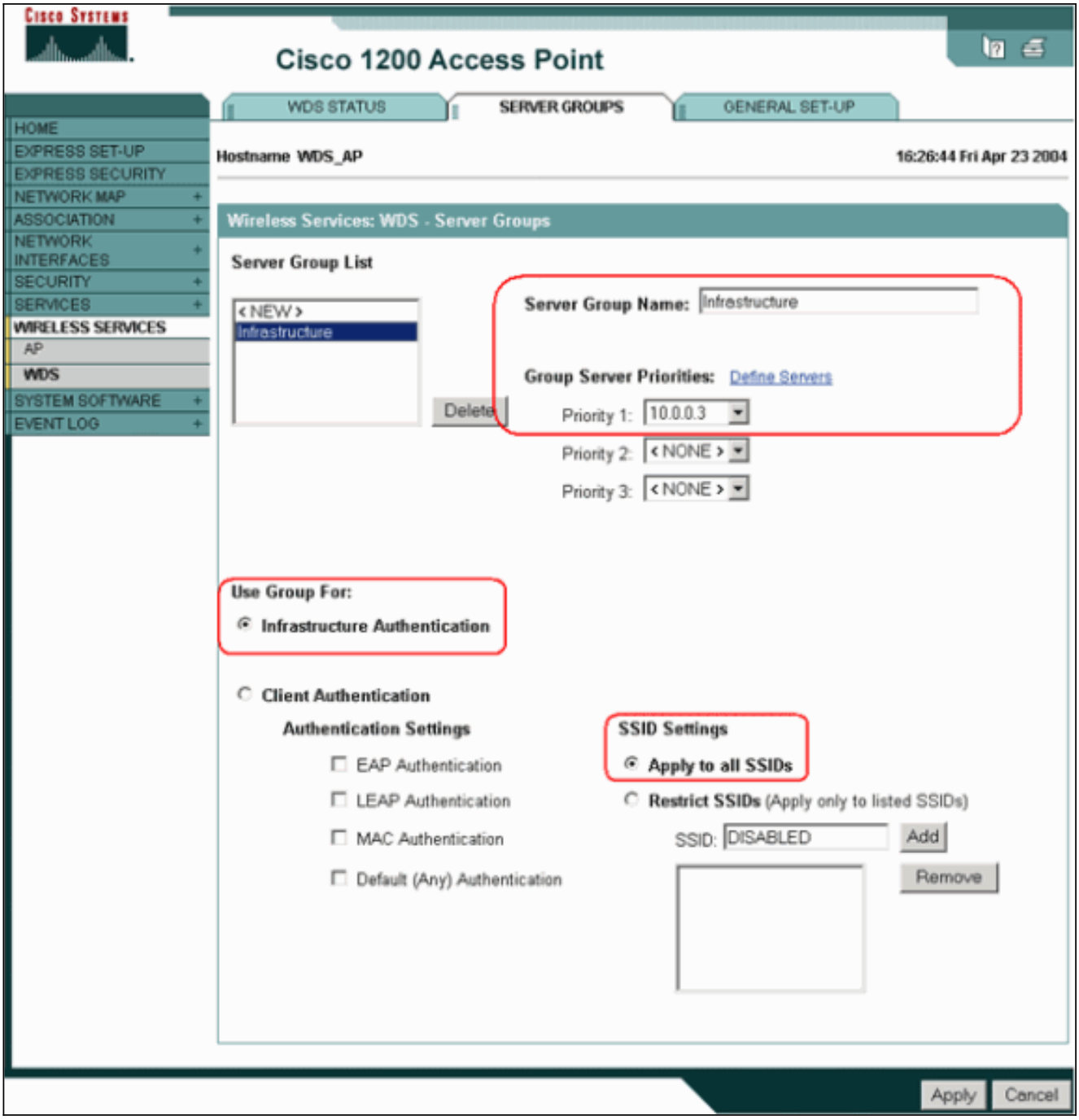
3. Для настройки параметров настройки WDS на AP WDS выберите **Wireless Services> WDS** на AP WDS и щелкните по вкладке **General Set-Up**. Выполните данные действия:Под Беспроводными доменными сервисами WDS - Глобальные свойства,

проверьте **Использование этот AP как Беспроводные доменные сервисы.В поле Wireless Domain Services Priority задайте значение около 254, которое является первым значением.** Можно настроить один или несколько AP или коммутаторы как кандидаты для обеспечения WDS. Устройство с наивысшим приоритетом предоставляет WDS.



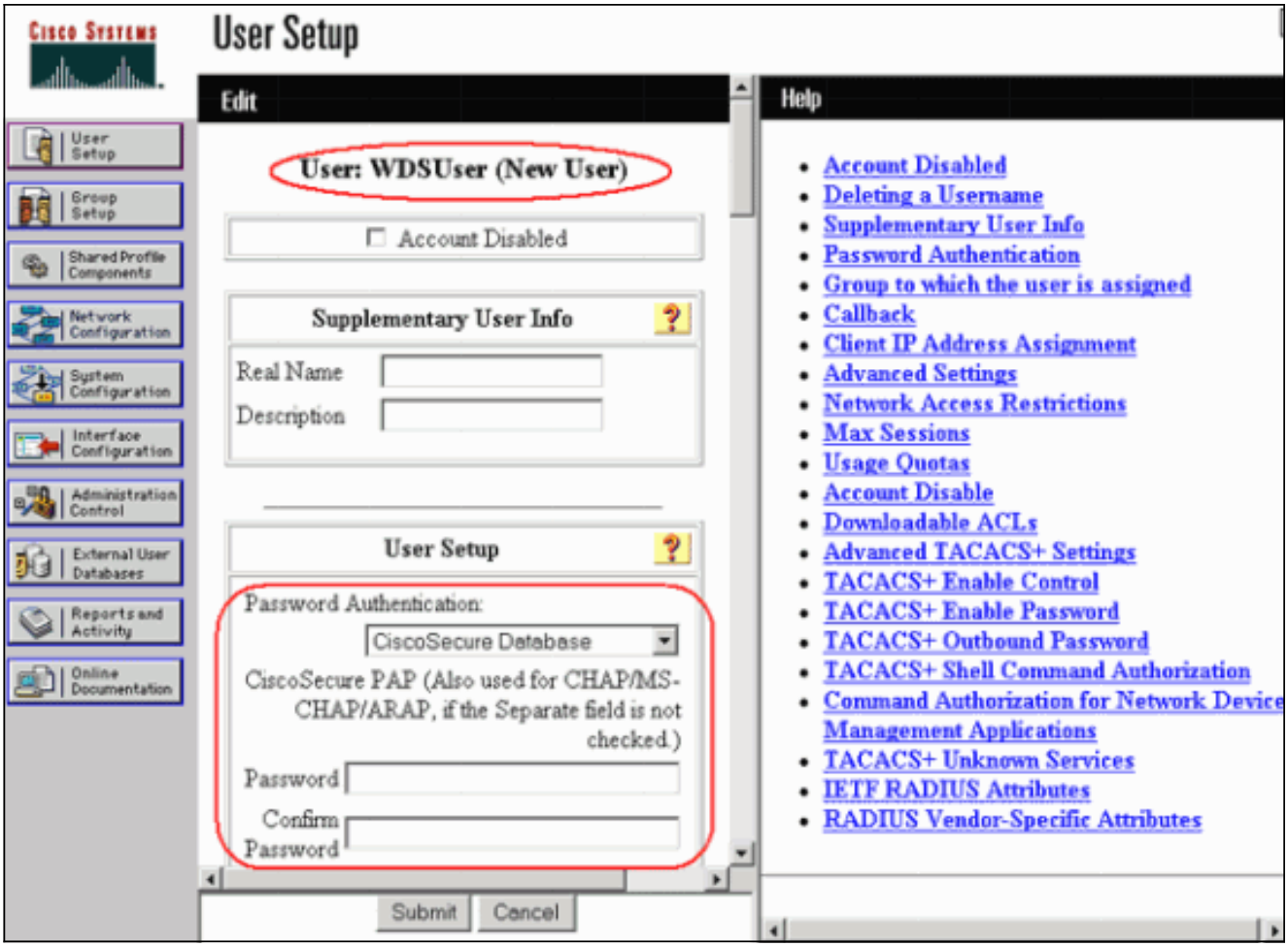
Или подайте следующие команды из командной строки:

4. Выберите **Wireless Services> WDS** и перейдите к вкладке **Server Groups**:Определите имя группы серверов, проверяющих подлинность других точек доступа, как инфраструктурную группу.Установите приоритет 1 для ранее настроенного сервера аутентификации.**Установите флажок Use Group For: Infrastructure Authentication .**Примените эти настройки к соответствующему идентификатору набора служб (SSID).



Или подайте следующие команды из командной строки:

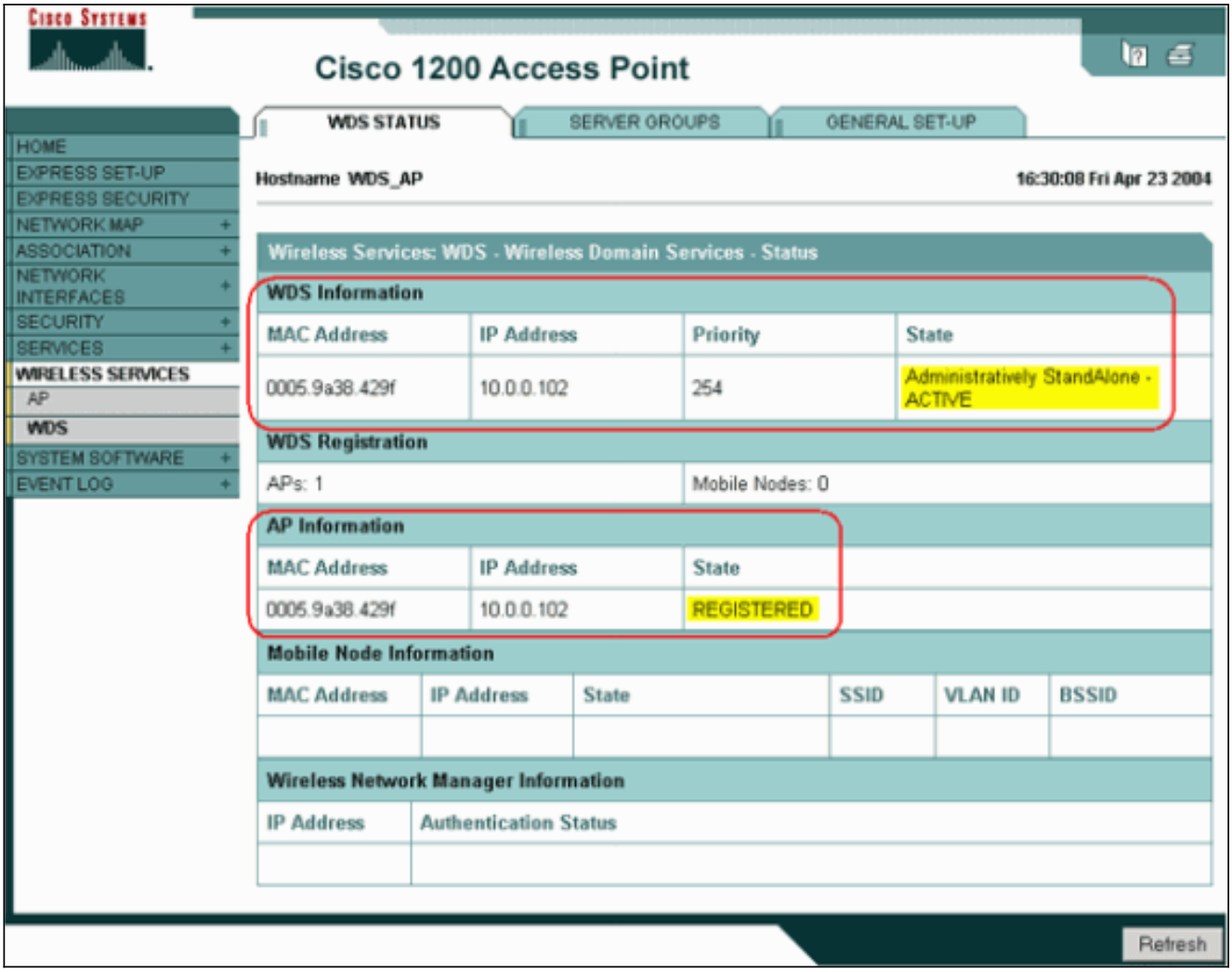
5. Настройте имя пользователя и пароль WDS как у пользователя сервера аутентификации.[В ACS Cisco Secure это происходит на странице User Setup , где вы определяете имя пользователя и пароль WDS.](#) Для получения информации о серверах не-ACS аутентификации обратитесь к документации производителя.**Примечание:** Не помещайте пользователя WDS в группу, которой назначают много прав и привилегий — WDS только требует ограниченной аутентификации.



6. Выберите **Wireless Services> AP** и нажмите **Enable** для Участвования в опции Инфраструктуры SWAN. Затем 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:

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.Если точка доступа не находится ни в одном из состояний (REGISTERED или ACTIVE), проверьте сервер аутентификации на наличие ошибок или неудачных попыток аутентификации.Когда точка доступа будет зарегистрирована должным образом, добавьте клиента точки доступа для использования служб WDS.



Или подайте следующие команды из командной строки:**Примечание:** Вы не можете ассоциации тестового клиента, потому что аутентификация клиента еще не имеет условий.

Задайте WLSM как WDS

Этот раздел объясняет, как настроить WLSM как WDS. WDS - единственное устройство, которое сообщается с сервером аутентификации.

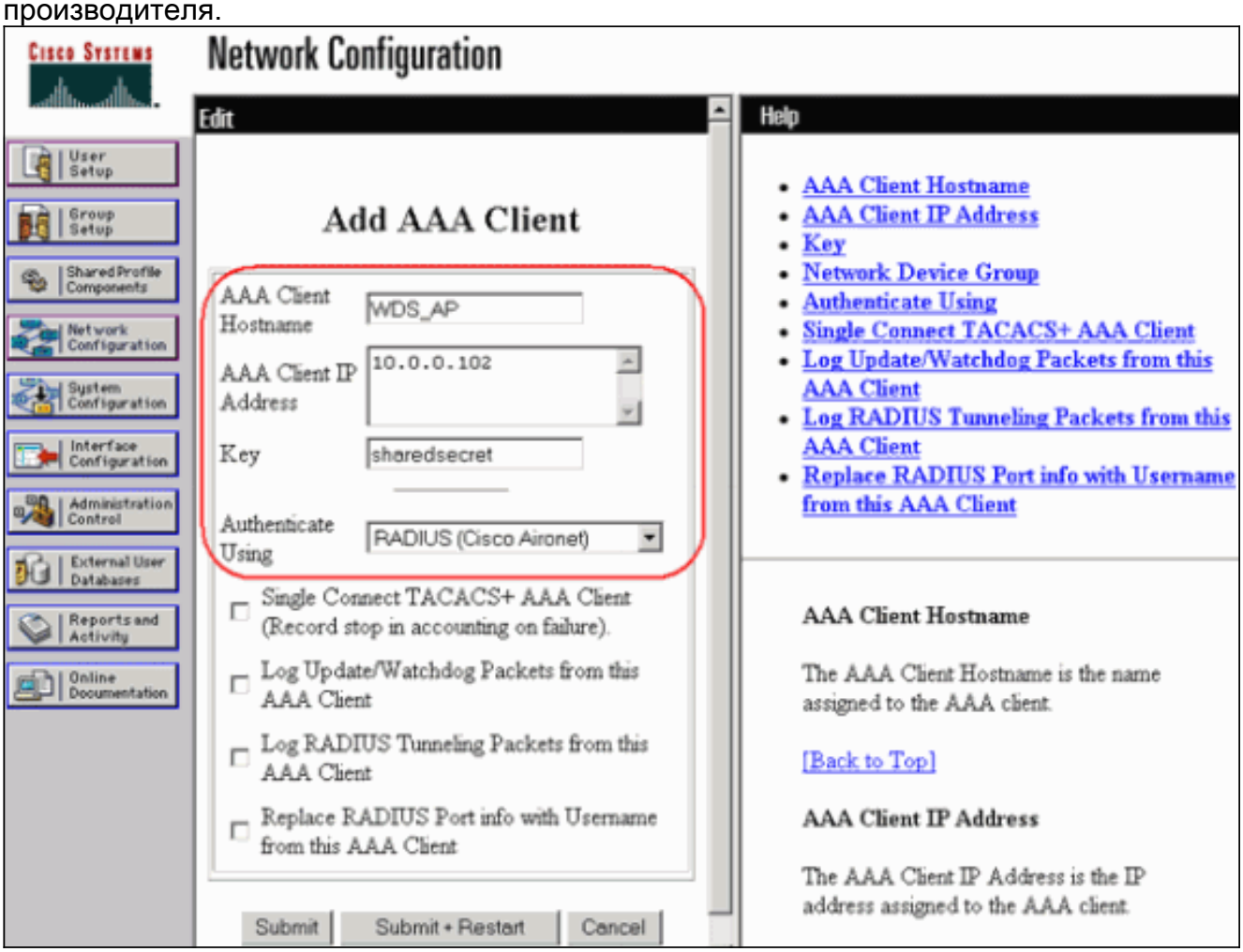
Примечание: Выполните эти команды в командной строке WLSM, не модуля управления Supervisor Engine 720. Для получения до командной строки WLSM выполните эти команды в командной строке в модуле управления Supervisor Engine 720:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

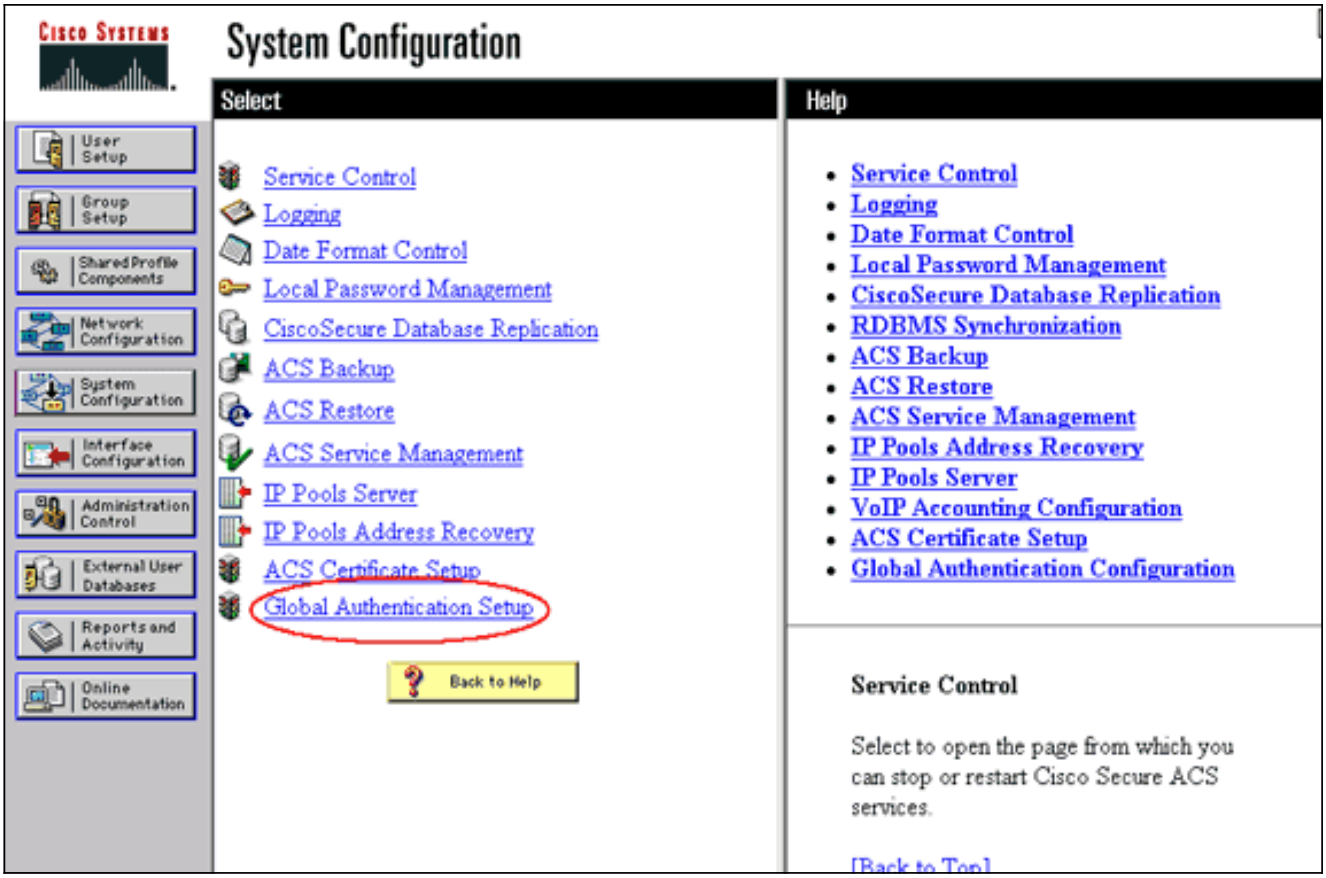
Примечание: Чтобы устранить неполадки и поддержать ваш WLSM более легко, настройте удаленный доступ Telnet к WLSM. См. в разделе "Настройка удаленного доступа Telnet".

Для задания WLSM как WDS:

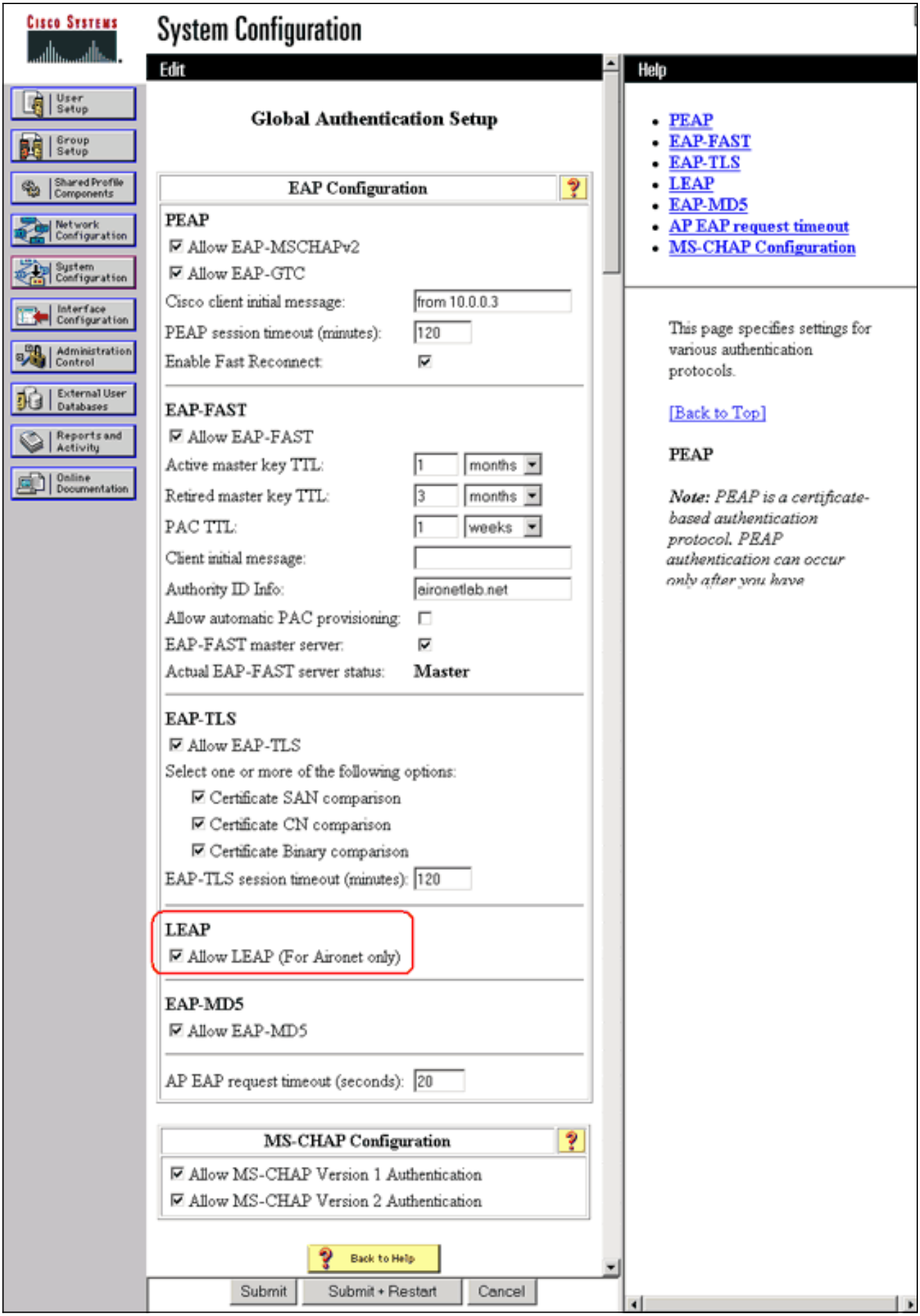
1. Из интерфейса CLI WLSM введите следующие команды и установите соединение с сервером аутентификации:**Примечание:** В WLSM не используется управление приоритетом. Если в сети содержатся несколько модулей WLSM, WLSM использует настройку избыточности для определения первичного модуля.
2. Настройте WLSM 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 :NameIP-адресОбщий secretAuthentication methodRADIUS Cisco AironetIETF RADIUSДля получения информации о серверах не-ACS аутентификации обратитесь к документации производителя.



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.**



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.).
4. На WLSM определите метод аутентификации клиентских устройств (группы клиент-

сервер) и типы EAP, используемые этими клиентами.**Примечание:** Этот шаг избавляет от необходимости Определить процесс 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:На WLSM:
6. Для проверки функций WLSM используются следующие команды:На WLSM:Для Supervisor Engine 720:

Определяйте AP как устройство, относящееся к инфраструктуре

Затем, необходимо определять по крайней мере один AP инфраструктуры и отнестись AP к WDS. Клиенты устанавливают соединение с инфраструктурными точками доступа. Инфраструктурные точки доступа требуют точку доступа WDS или WLSM для проверки их подлинности.

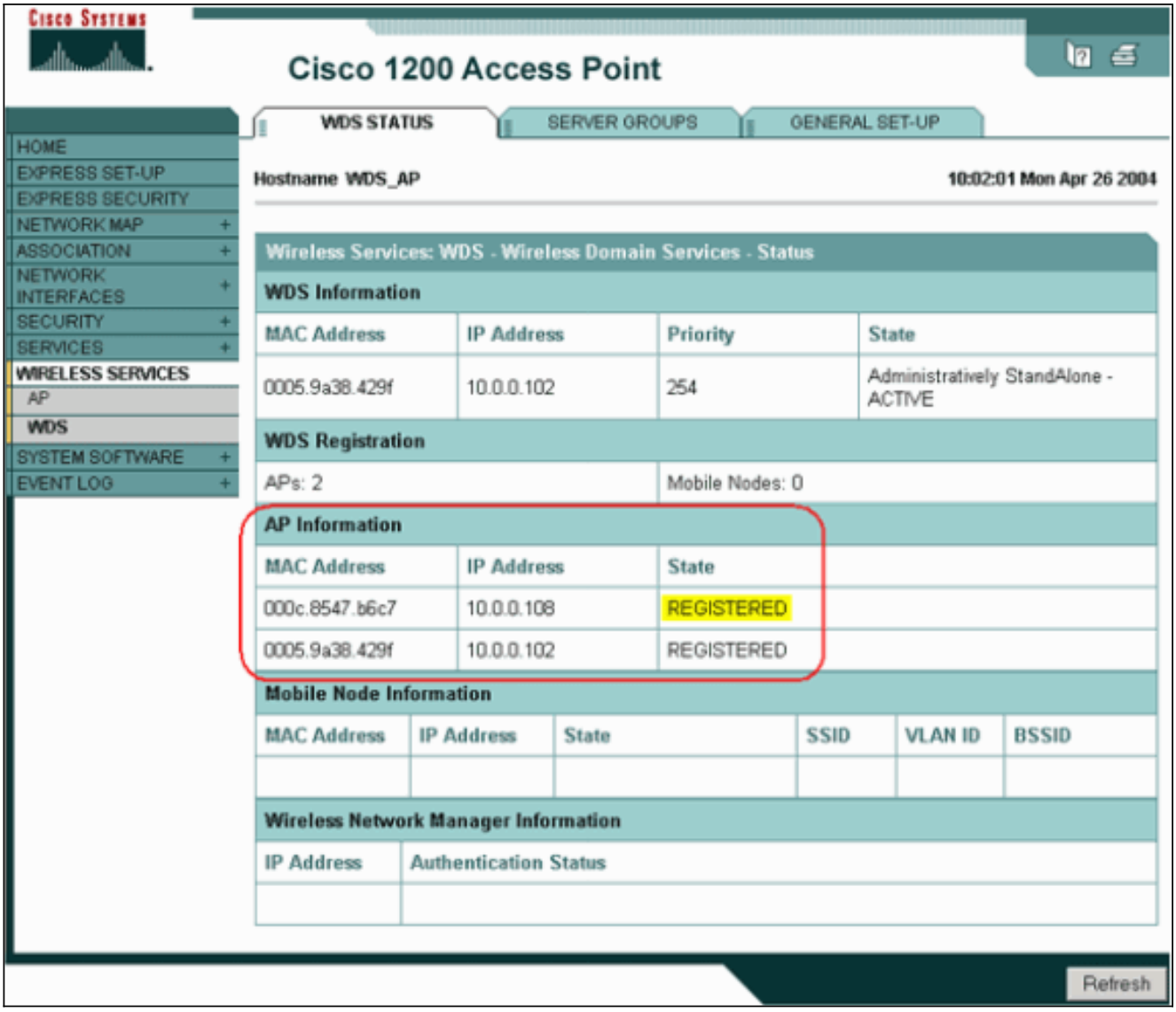
Выполните следующие шаги, чтобы добавить инфраструктурную точку доступа, использующую услуги WDS:

Примечание: Эта конфигурация применяется только к AP инфраструктуры а не AP 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:

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.Если точка доступа не находится ни в одном из состояний (REGISTERED и/или ACTIVE), проверьте сервер аутентификации на наличие ошибок или неудачных попыток аутентификации.Как только точка доступа получит статус ACITVE (активно) и/или REGISTERED (зарегистрировано), добавьте в раздел WDS метод аутентификации
клиента.



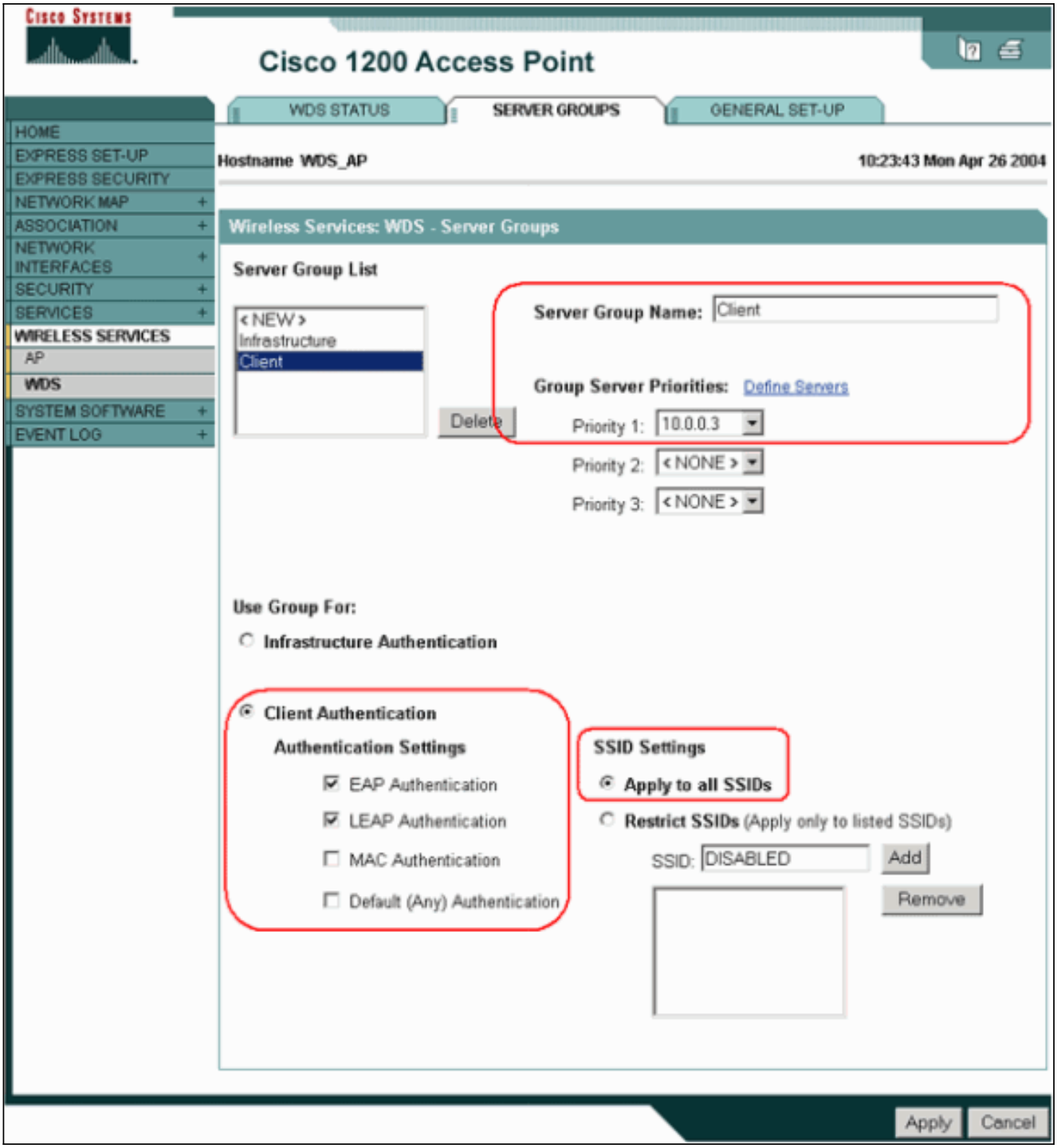
Или подайте следующую команду из командной строки:Также выполните эту команду от WLSM:Затем выполните следующую команду на инфраструктурной точке доступа:**Примечание:** Вы не можете ассоциации тестового клиента, потому что аутентификация клиента еще не имеет условий.

Определите метод аутентификации клиента

Наконец, определите метод аутентификации клиента.

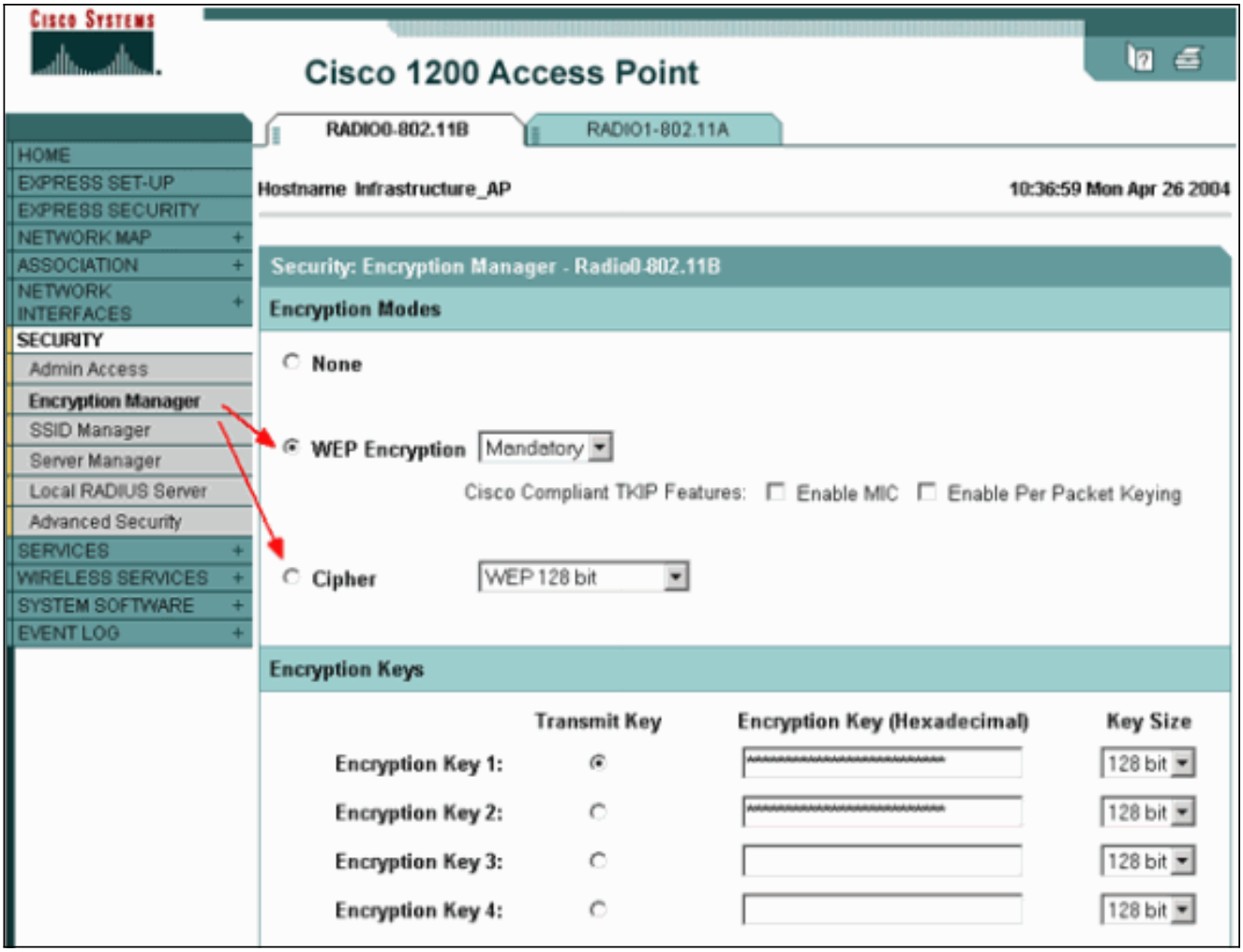
Выполните следующие шаги, чтобы добавить добавить метод проверки подлинности клиента:

1. Выберите **Wireless Services> WDS**. Выполните следующие шаги на закладке Server Groups точки доступа WDS:Определите группу сервера, которая проверяет подлинность клиента (Client group).Установите приоритет 1 для ранее настроенного сервера аутентификации.Установите подходящий тип аутентификации (LEAP, EAP, MAC и т.д.).Примените эти настройки к соответствующим SSID.

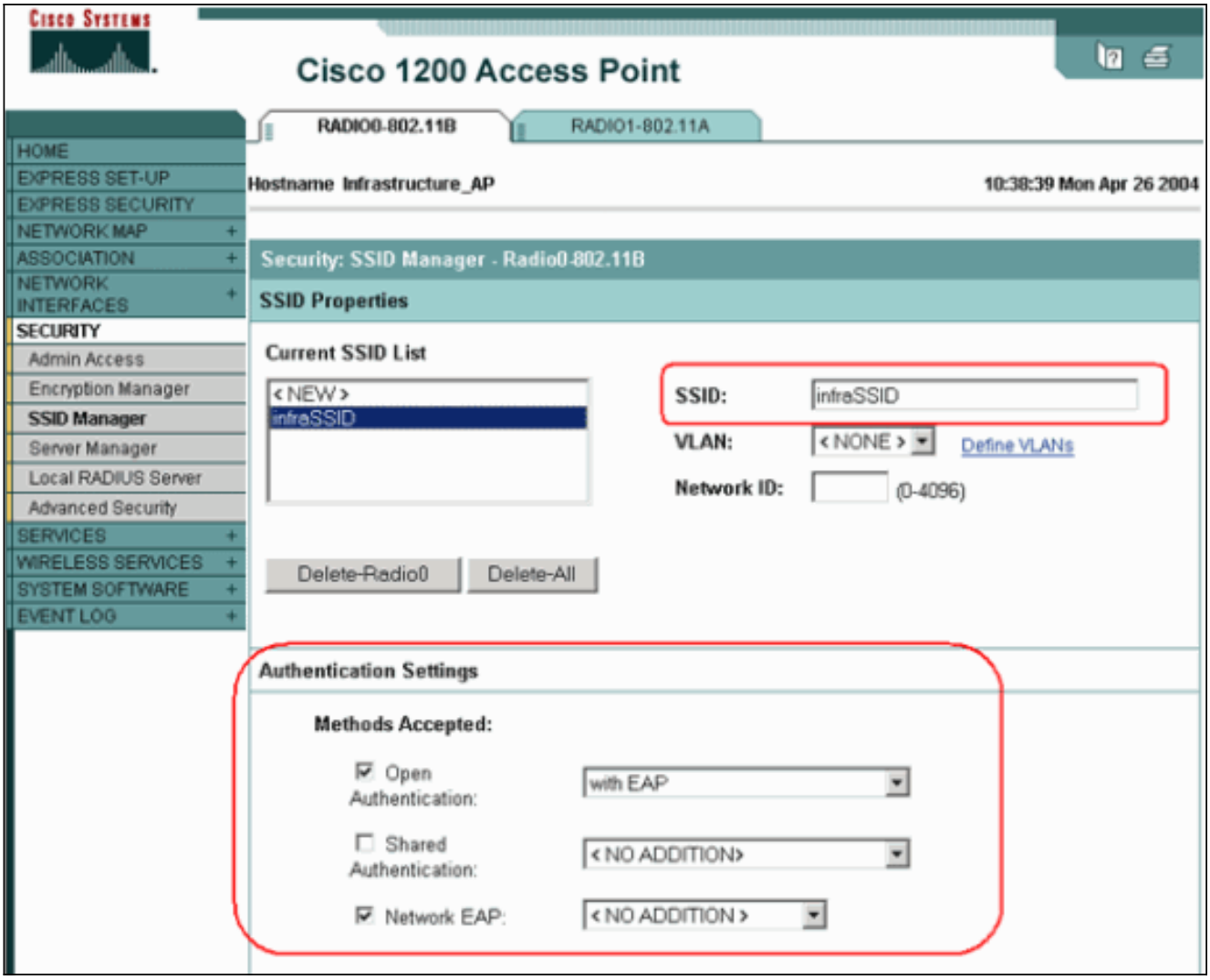


Или подайте следующие команды из командной строки:**Примечание:** AP WDS в качестве примера выделен и не принимает связывания клиента.**Примечание:** Не настраивайте на AP инфраструктуры для групп серверов, потому что AP инфраструктуры передают любые запросы к WDS, который будет обработан.

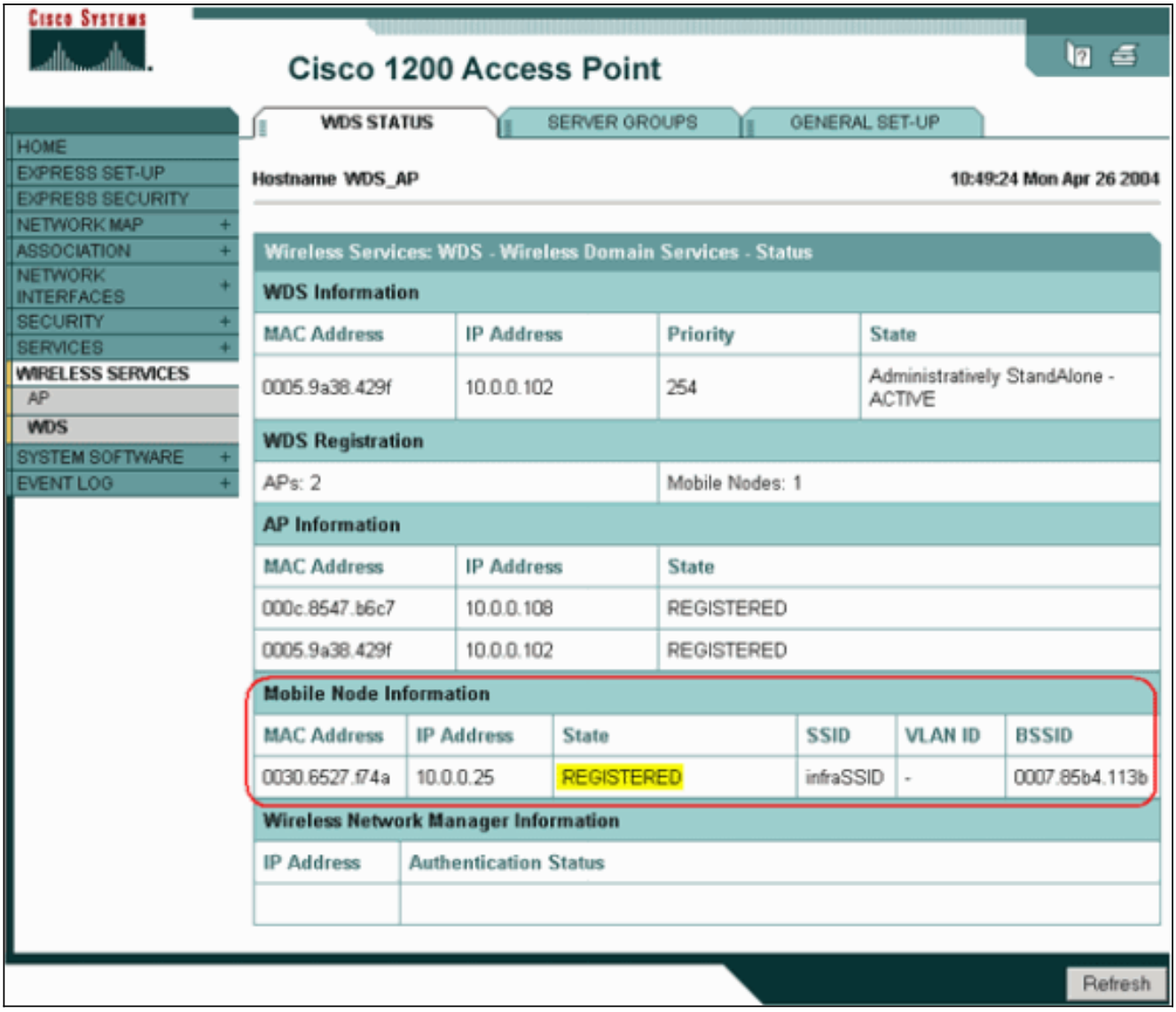
2. Для инфраструктурной точки (или точек) доступа:Под элементом меню **Security> Encryption Manager** нажмите **WEP Encryption** или **Cipher**, как требуется протоколом аутентификации, который вы используете.



Под элементом меню **Security> SSID Manager** выберите методы аутентификации как требуется протоколом аутентификации, который вы используете.



3. Теперь можно успешно протестировать, проходят ли клиенты аутентификацию для точек доступа к инфраструктуре. AP WDS во вкладке WDS Status (под элементом меню **Wireless Services> WDS**) указывает, что клиент появляется в Информационной области Мобильного узла и имеет ЗАРЕГИСТРИРОВАННОЕ Состояние.Если клиент не появляется, проверьте сервер аутентификации на наличие ошибок или неудачных попыток аутентификации
клиентами.



Или подайте следующие команды из командной строки:**Примечание:** Если вы нуждаетесь к debug authentication, гарантируете, что отлаживаете на AP WDS, потому что AP WDS является устройством, которое связывается с сервером проверки подлинности.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

- **Вопрос: На AP WDS, каковы рекомендуемые настройки для этих элементов?radius-server timeoutradius-server deadtimeВремя Рассинхронизации Сбоя Message Integrity Check (MIC) Протокола TKIPВремя удержания клиентаEAP или интервал переаутентификации MAC(Дополнительный) таймаут клиента EAPОтвет:** 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 браузера, 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: эти две команды помогают аутентификации клиента в каком-либо случае, и они необходимы на AP инфраструктуры или WDS?radius-server attribute 6 on-for-login-authмножественный поддержкой radius-server attribute 6Ответ:** 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. какая-либо из этих определенных команд необходима для AP инфраструктуры?radius-server attribute 6 on-for-login-authмножественный поддержкой radius-server attribute 6radius-server timeoutradius-server deadtimeОтвет:** 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-authмножественный поддержкой radius-server attribute 6radius-server timeoutradius-server deadtimeRadius-server attribute 32 include-in-access-req форматирует** значение **%h**, остается по умолчанию и требуется.

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.
- AP, настроенный как устройство WDS, не функционирует как ожидалось, и конфигурация WDS не работает.**Примечание:** Вы не можете настроить AP/мост Cisco Aironet 1300 года как ведущее устройство 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.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

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

- **средство проверки подлинности debug dot11 aaa все** — Показывают различные согласования, что клиент проходит как клиент, связывается и аутентифицируется посредством процесса EAP или 802.1x. Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. **Эта команда заметила отладочную команду dot11 aaa dot1x all в этой и последующих версиях.**
- **debug aaa authentication** — Показывает процесс проверки подлинности с точки зрения AAA общего назначения.
- **debug wlccp ap** — Показывает согласования WLCCP, включенные, поскольку AP присоединяется к WDS.
- **debug wlccp packet** — Показывает подробные сведения о согласованиях WLCCP.
- **отладьте wlccp клиента скачка** — Показывает подробные данные, поскольку устройство, относящееся к инфраструктуре присоединяется к WDS.

Дополнительные сведения

- Настройке сервиса WDS, быстрого безопасного роуминга и радиоуправления
- Примечание к конфигурации сервисного модуля беспроводной локальной сети серии Catalyst 6500

- Настройка пакетов Cipher Suites и WEP
- Настройка типов аутентификации
- Страницы поддержки беспроводных сетей LAN
- Cisco Systems – техническая поддержка и документация