Пример настройки сервера AP беспроводных служб доменов в качестве сервера AAA

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Настройте AP WDS
Настройте AP инфраструктуры
Настройте метод аутентификации клиента
Проверка
Устранение неполадок
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для настройки Точки доступа (AP) к:

- Предоставьте беспроводные доменные сервисы (WDS).
- Выполните роль аутентификации, авторизации и учета (AAA).

Можно использовать этот вид настройки, когда у вас нет внешнего сервера RADIUS для аутентификации AP инфраструктуры и устройств клиента, которые участвуют в WDS.

Предварительные условия

Требования

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

- Базовые знания о WDS
- Методы безопасности Протокола EAP знания текущего

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- AP Cisco Aironet серии 1200, которые выполняют релиз 12.3 программного обеспечения Cisco IOS (7) JA1

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

WDS является частью Технологии управления беспроводными локальными сетями Cisco SWAN (SWAN). WDS является набором функций ПО Cisco IOS, которые улучшают Беспроводную локальную сеть (WLAN) мобильность клиента и упрощают развертывание WLAN и управление.

WDS является ядром для многих функций такой как Быстро Безопасный Роуминг, Мобильность уровня 3 и радио-управление.

См. WDS Настройки, Быстро Безопасный Роуминг, Радио-менеджмент и Wireless Intrusion Detection Services для получения дополнительной информации об этих функциях.

Одна из основных целей WDS должна кэшировать учетные данные пользователя на первой аутентификации клиента сервером проверки подлинности. На последующих попытках WDS аутентифицирует клиента на основе кэшируемой информации. Для выполнения этого:

- Один из AP должен быть настроен как AP WDS.
- Другие AP должны быть настроены как AP инфраструктуры, которые связываются с AP WDS.
- AP WDS должен установить отношение с сервером проверки подлинности путем аутентификации на нем с именем пользователя и паролем WDS.

Когда эти устройства аутентифицируются впервые, этот сервер проверки подлинности проверяет учетные данные AP инфраструктуры и клиентов. Сервер проверки подлинности может или быть внешним сервером RADIUS или локальным сервером RADIUS на AP WDS.

WDS и AP инфраструктуры связываются по протоколу групповой адресации, названному Протоколом управления контекста беспроводной локальной сети (WLCCP). Эти многоадресные сообщения не могут маршрутизироваться. Поэтому WDS и привязанные AP инфраструктуры должны быть в той же подсети IP и на одинаковом сегменте локальной сети.

Этот документ объясняет, как использовать функцию локального сервера RADIUS на AP WDS для выполнения проверки учетных данных.

Настройка

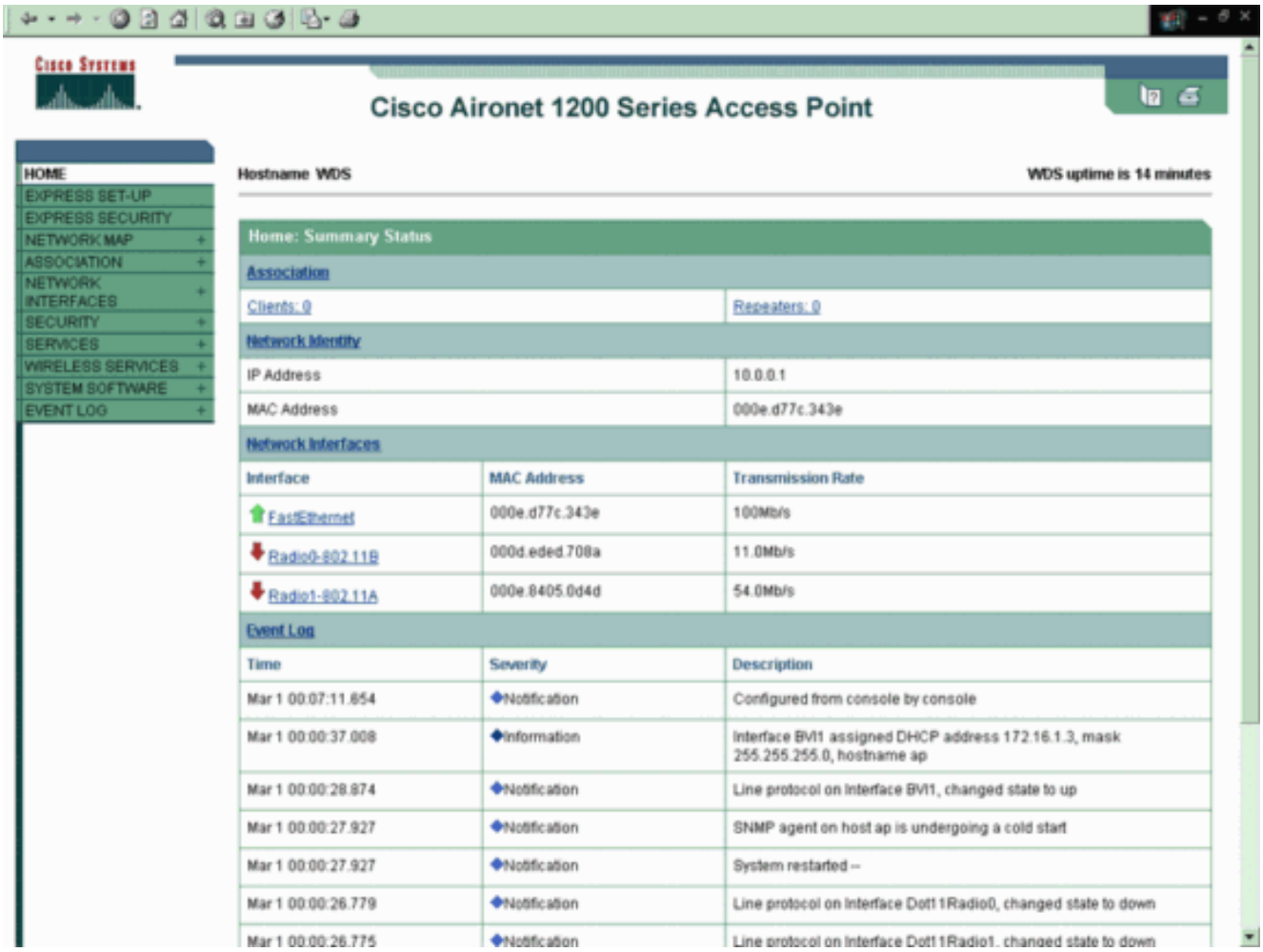
Настройте AP WDS

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

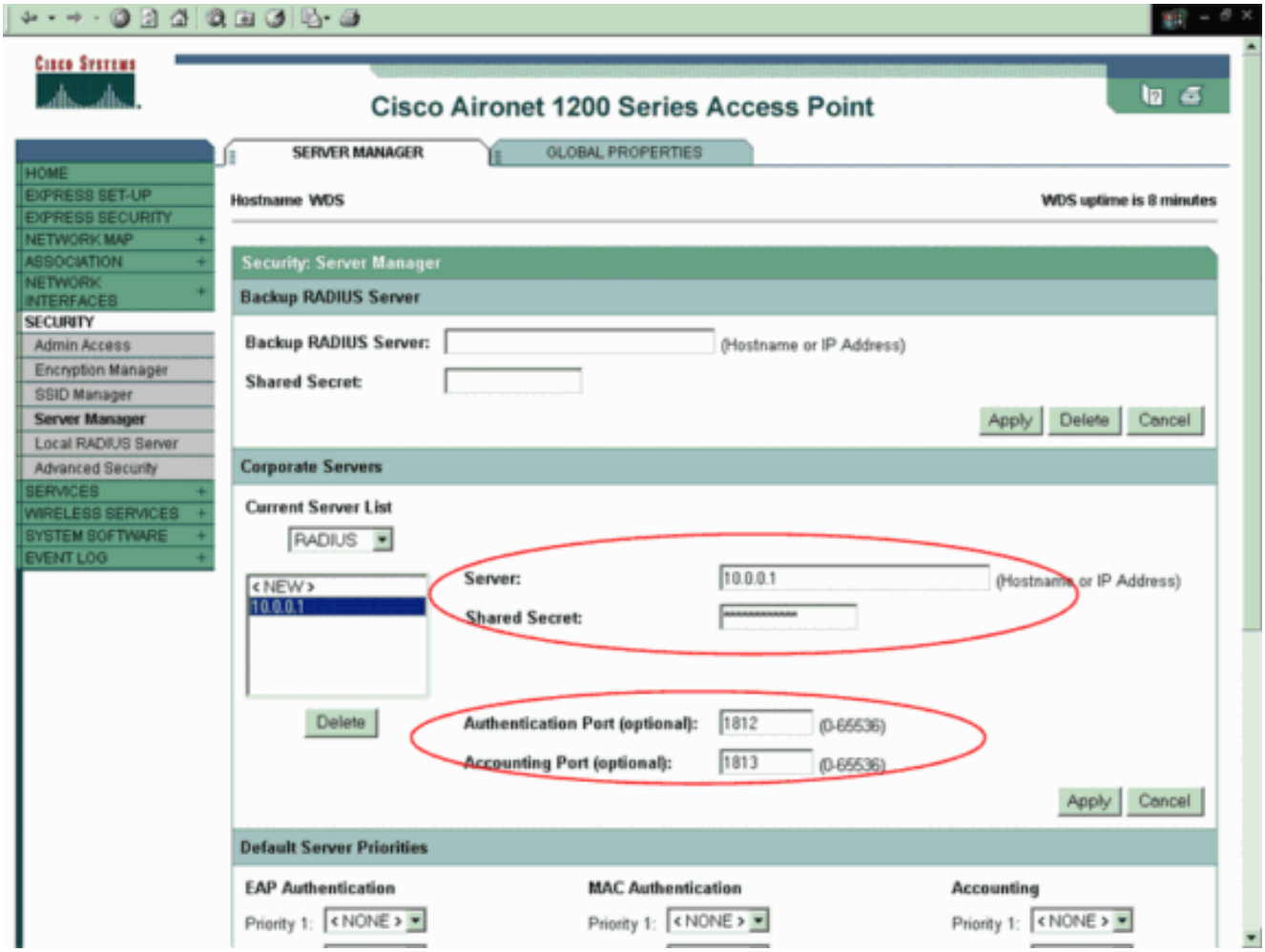
Для настройки AP для служения в качестве AP WDS с функциональностью AAA-сервера, необходимо сначала активировать опцию локального сервера RADIUS на AP.

Выполните следующие действия:

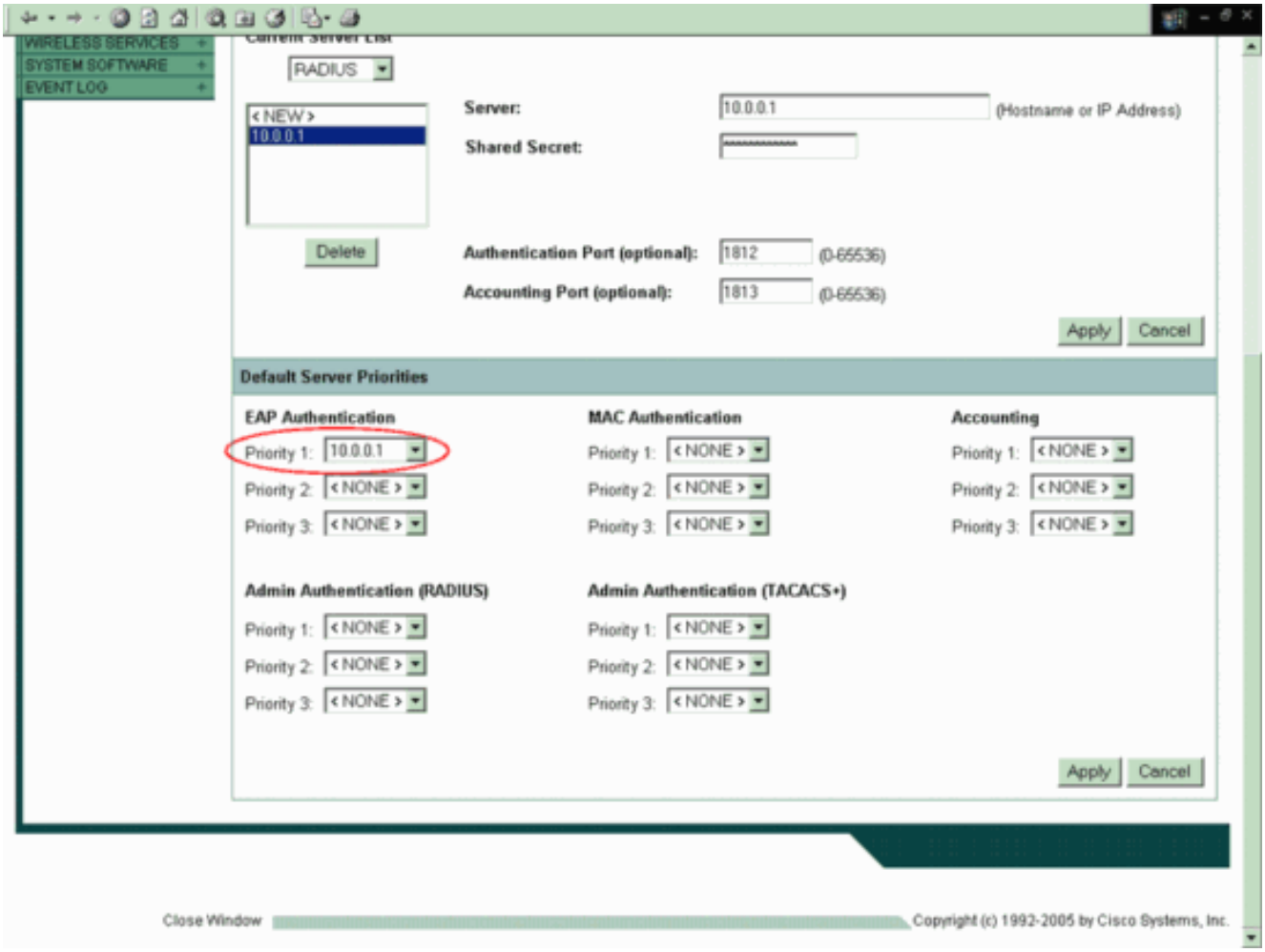
1. Войдите к AP через GUI.Откроется страница Summary Status.



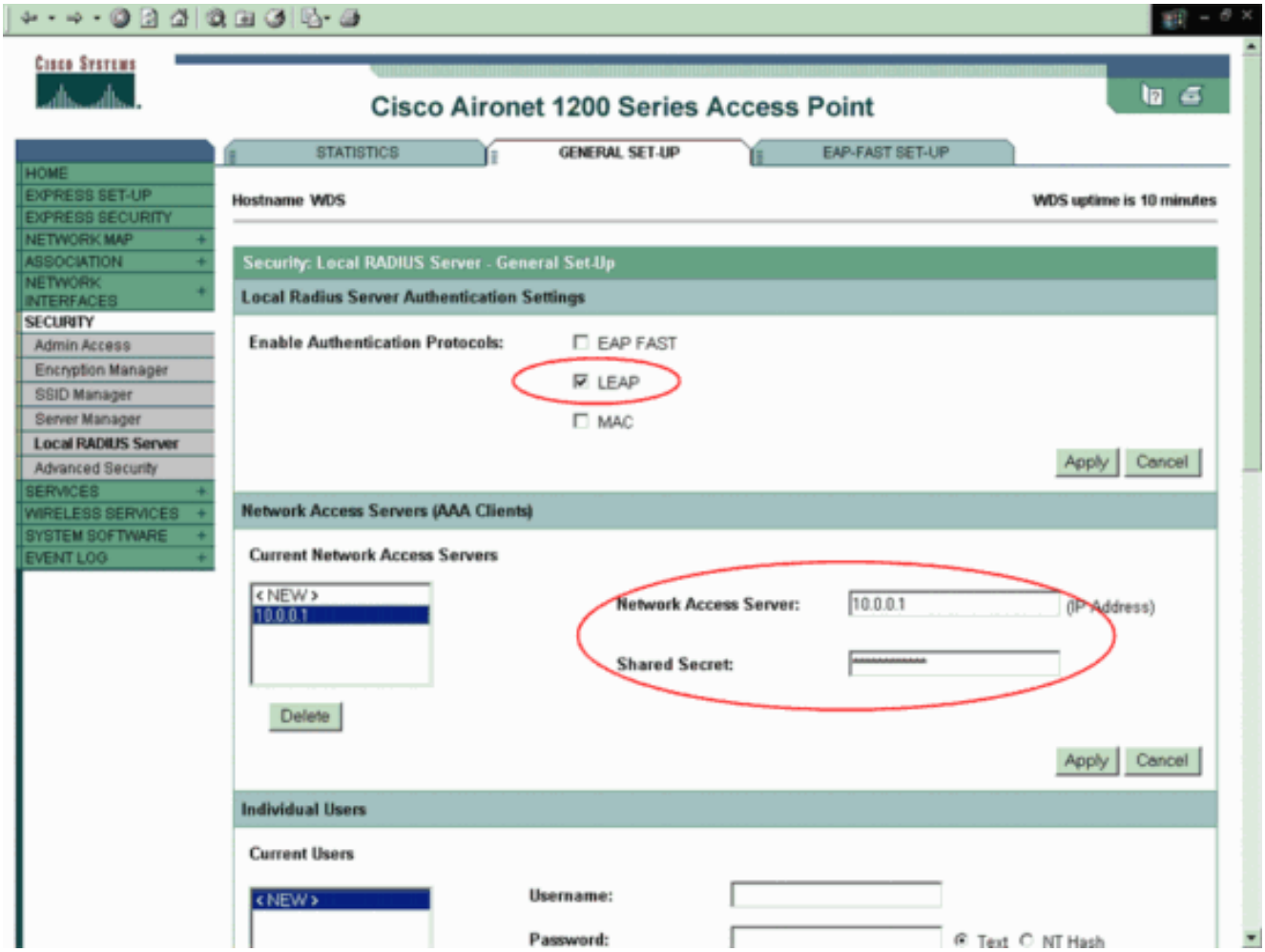
2. Выберите **Security> Server Manager** из левого бокового меню на AP.
3. Введите IP-адрес и общий секретный ключ AP, который действует как сервер RADIUS под Корпоративными серверами.В этом случае введите IP-адрес AP WDS, так как AP WDS переходит к действию как к серверу RADIUS. Пример использует IP-адрес 10.0.0.1. Так как это - локальный сервер RADIUS, необходимо использовать 1812 и 1813 в качестве Аутентификации и Портов учета как показано в примере.
4. **Щелкните "Применить".**



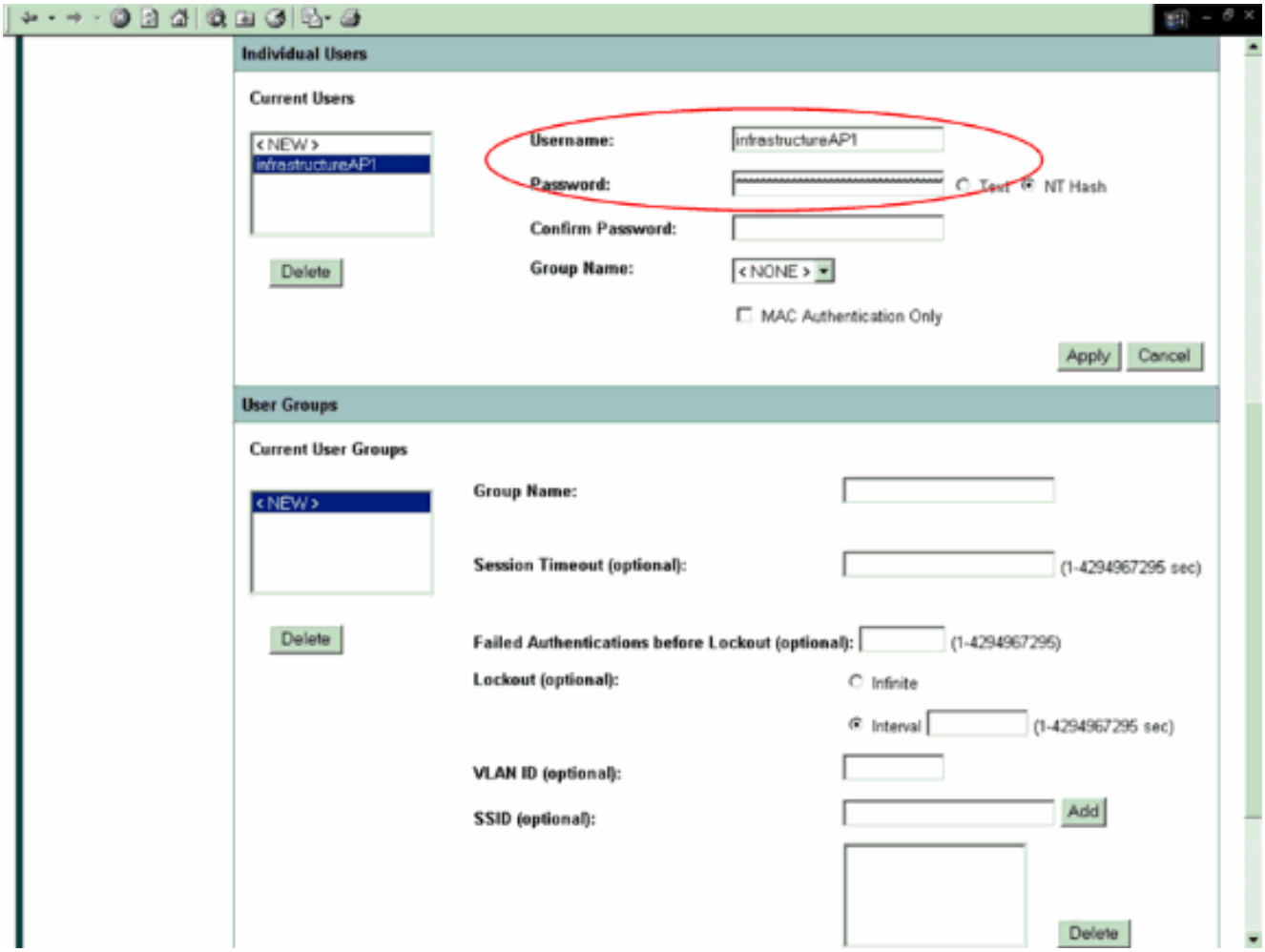
5. Выберите WDS APs IP address как **Приоритет 1** под Приоритетами Сервера По умолчанию для Аутентификации eap.**Щелкните "Применить".**Это позволяет локальному серверу RADIUS быть предпочтительным вариантом для аутентификации AP инфраструктуры и
клиентов.



6. Выберите **Security> Local Radius server из левого бокового меню**.Нажмите **General Set-up** для настройки параметров локального сервера RADIUS.Выберите **LEAP** при Локальных Параметрах настройки аутентификации сервера RADIUS и нажмите **Apply**.Введите IP-адрес AP WDS и общего секретного пароля под Серверами доступа к сети. Данный пример использует общий секретный пароль в качестве **test123**.**Щелкните "Применить".**



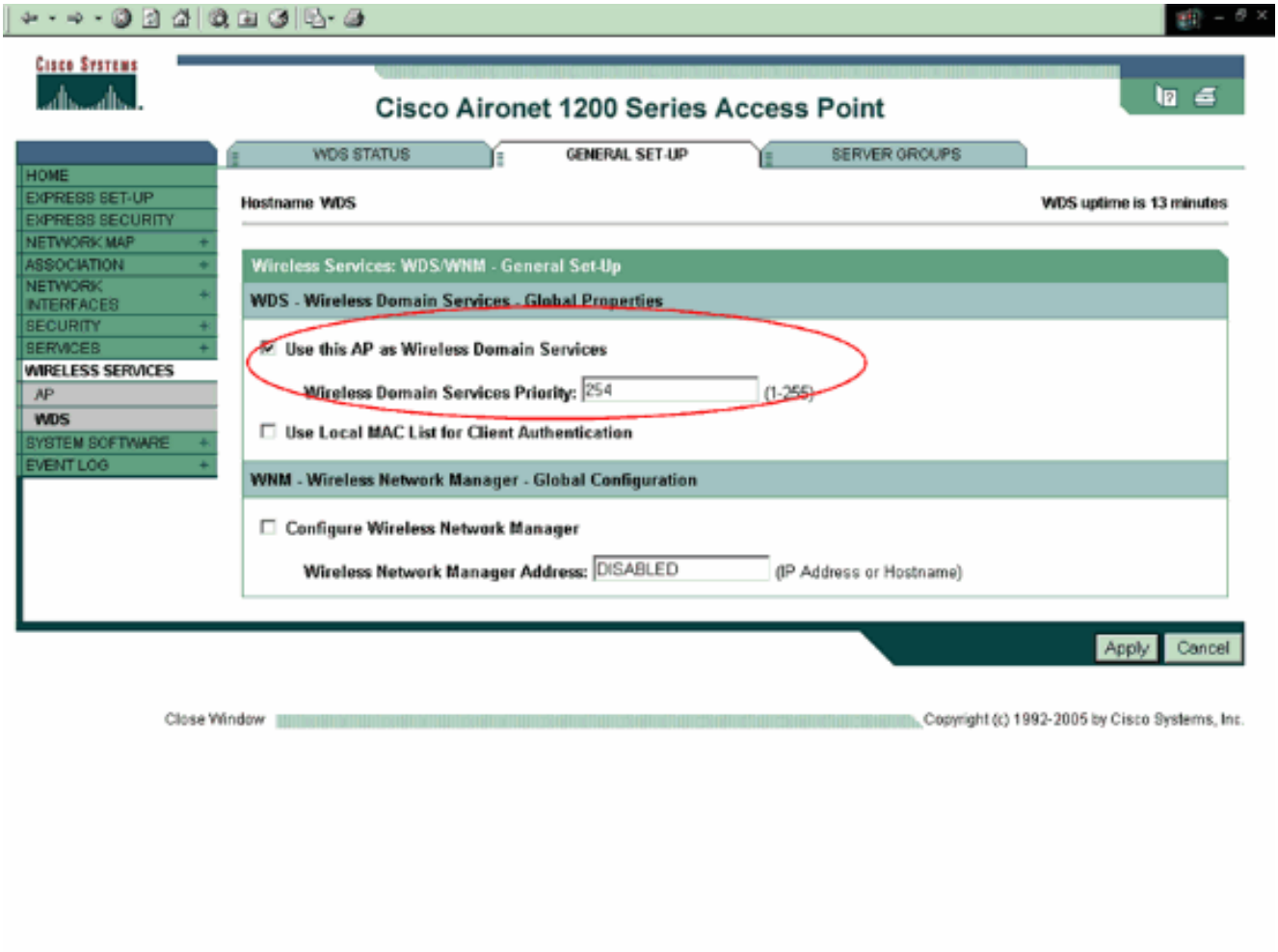
7. Введите имя пользователя и пароль всех AP инфраструктуры и клиентов, которые связываются с AP WDS при Отдельных пользователях.**Щелкните "Применить".**Данный пример включает имя пользователя и пароль AP инфраструктуры, который вы настраиваете для регистрации в AP WDS. Данный пример использует имя пользователя в качестве **infrastructureAP1** и пароль как **Cisco**. То же имя пользователя и пароль должны быть настроены на точке доступа инфраструктуры.



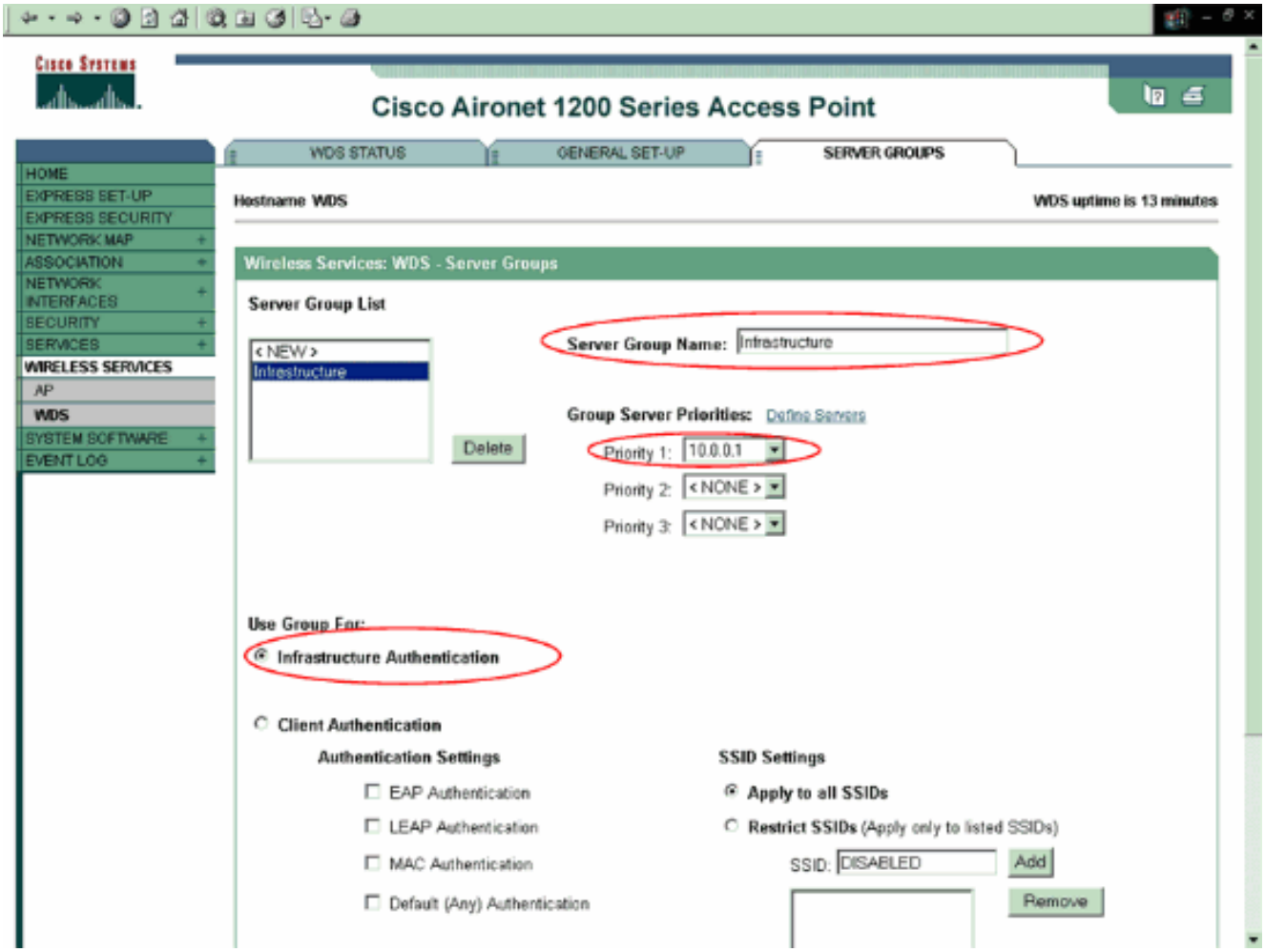
После настройки функции локального сервера RADIUS на AP необходимо включить функциональность WDS на AP.

Выполните следующие действия:

1. Выберите **Wireless Services> WDS** из левого бокового меню на AP.
2. Нажмите **General Set-up**.



3. Проверьте **Использование этот AP как Беспроводные доменные сервисы** на Общей Странице настройки.Войдите **254** в Приоритетном поле Беспроводных доменных сервисов. **Щелкните "Применить".**
4. Включите аутентификацию инфраструктуры.Нажмите **Server Groups** на странице WDS.Введите имя в поле Server Group Name для аутентификации AP инфраструктуры. Данный пример использует Имя серверной группы в качестве **Инфраструктуры**.Выберите IP-адрес локального сервера RADIUS от выпадающего списка Приоритетов Сервера Группы.AP WDS использует этот сервер для аутентификации AP инфраструктуры.Выберите **Infrastructure Authentication** под Use Group для.**Щелкните "Применить".**



AP WDS теперь действует как AAA-сервер. Настройте один из AP инфраструктуры для регистрации себя в AP WDS.

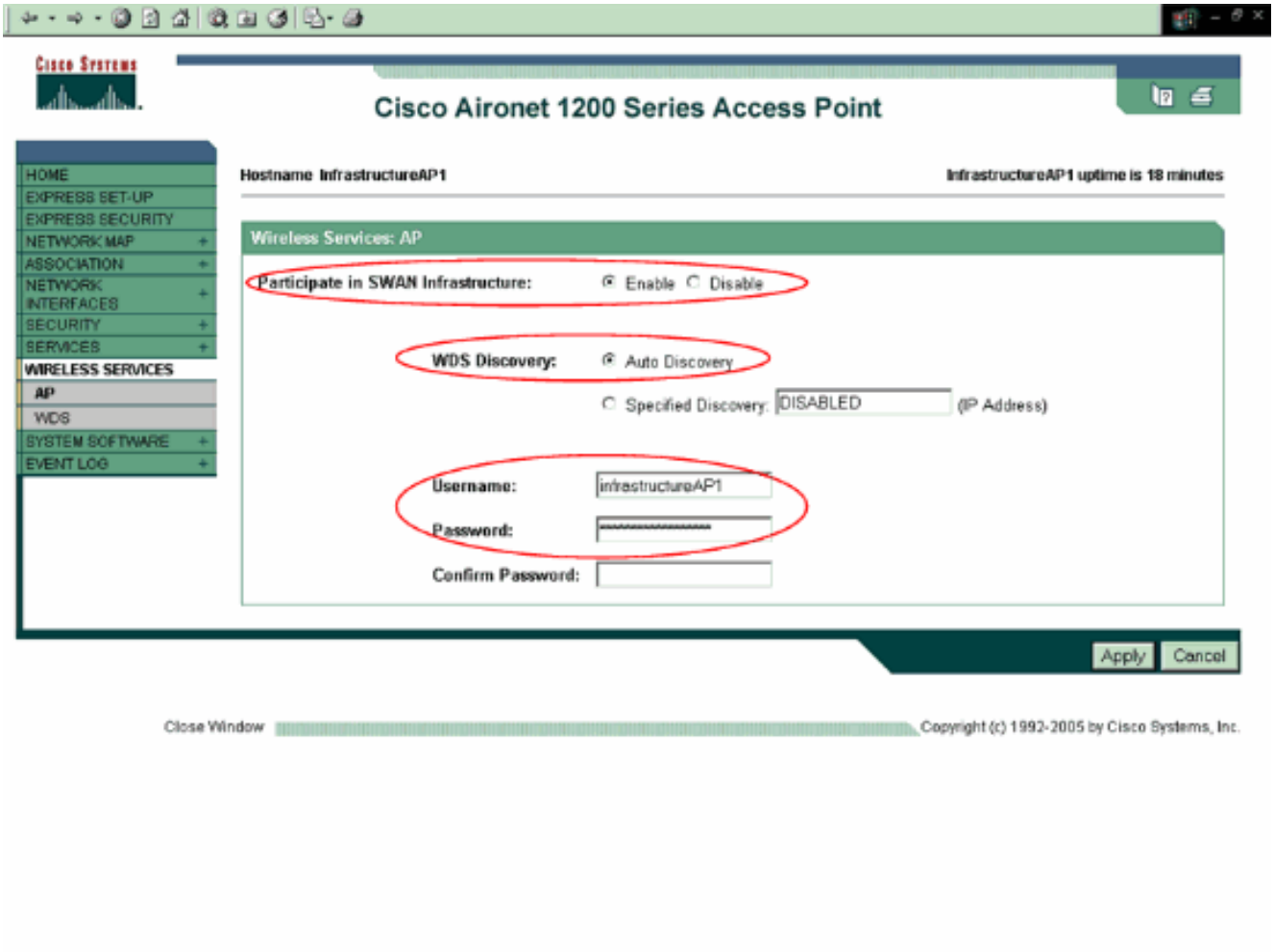
Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Настройте AP инфраструктуры

Этот раздел объясняет конфигурацию, требуемую на AP инфраструктуры зарегистрировать себя в AP WDS. Клиенты устанавливают соединение с инфраструктурными точками доступа. AP инфраструктуры запрашивают AP WDS выполнить аутентификацию для них.

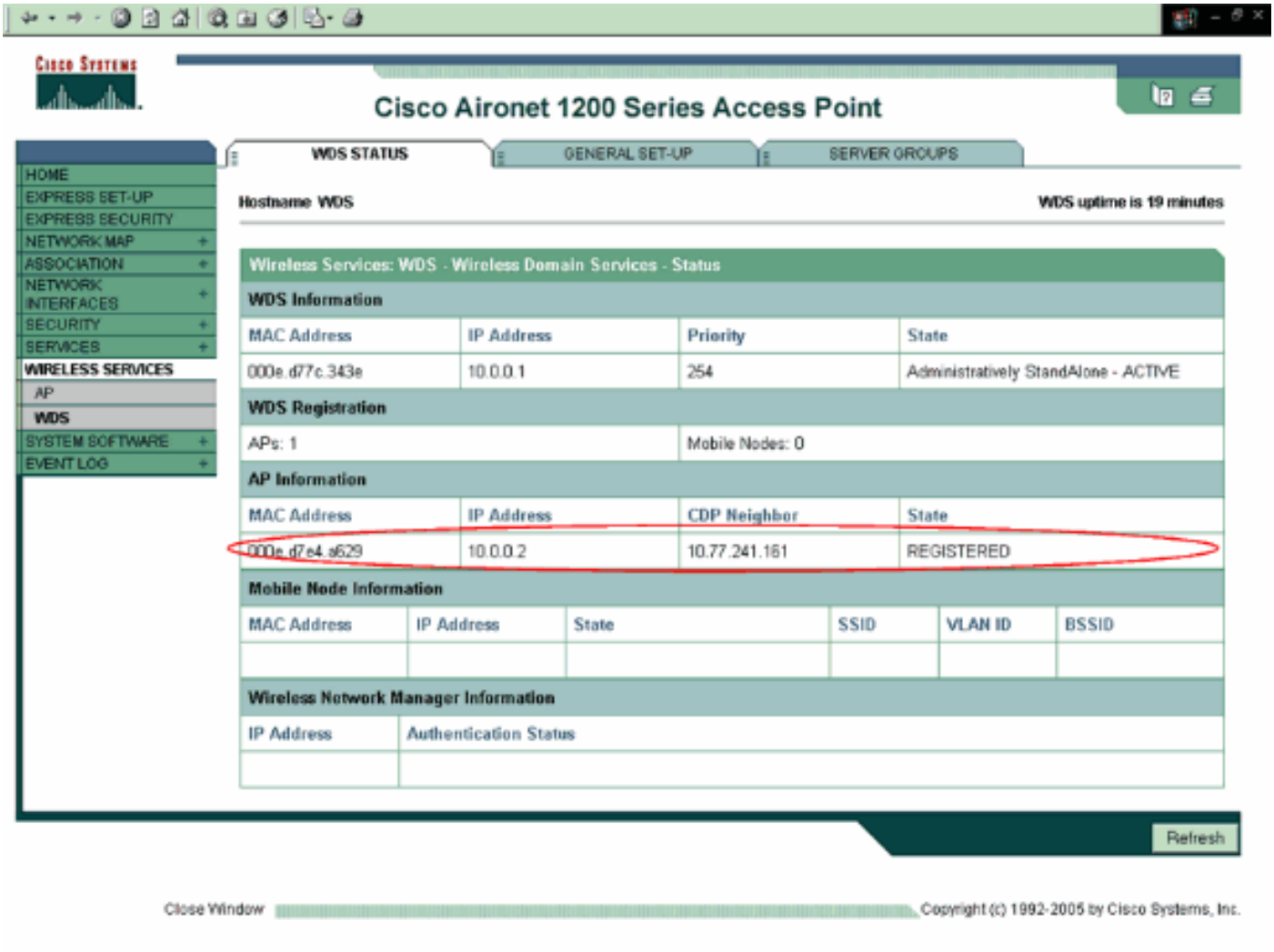
Выполните эти шаги для добавления AP инфраструктуры, который использует сервисы WDS:

1. Выберите **Wireless Services> AP** из левого бокового меню.
2. Выберите **Enable** под, участвуют в инфраструктуре SWAN.
3. Выберите **Auto Discovery** под обнаружением WDS.



4. Введите имя пользователя и пароль WDS в соответствующие поля.**Щелкните "Применить".**Имя пользователя и пароль должно существовать на локальном сервере RADIUS. Необходимо определить имя пользователя WDS и его пароль на сервере проверки подлинности для всех устройств, которые будут являться членами WDS.

AP инфраструктуры появляется в Информационной области AP с Состоянием, как ЗАРЕГИСТРИРОВАНО, как только вы настраиваете AP WDS и AP инфраструктуры на AP WDS, вкладке WDS Status. Это находится под элементом меню Wireless Services> WDS.



Неправильные настройки аутентификации или на AP WDS или на AP инфраструктуры могут заставить AP не появляться как АКТИВНЫЕ и/или ЗАРЕГИСТРИРОВАННЫЕ. Проверьте статистику Сервера проверки подлинности для любых ошибок или неудачных попыток аутентификации. Выберите **Security> Local Radius Server>** статистика **Statistics for Authentication server**.

Можно также использовать **команду show wlccp wds ap** от CLI на AP WDS для проверки конфигурации. На успешной регистрации с AP WDS выходные данные после того, как успешная регистрация с AP WDS похожа на данный пример:

```
WDS#show wlccp wds ap MAC-ADDR IP-ADDR STATE LIFETIME CDP-NEIGHBOR 000e.d7e4.a629 10.0.0.2
REGISTERED 97 10.77.241.161
```

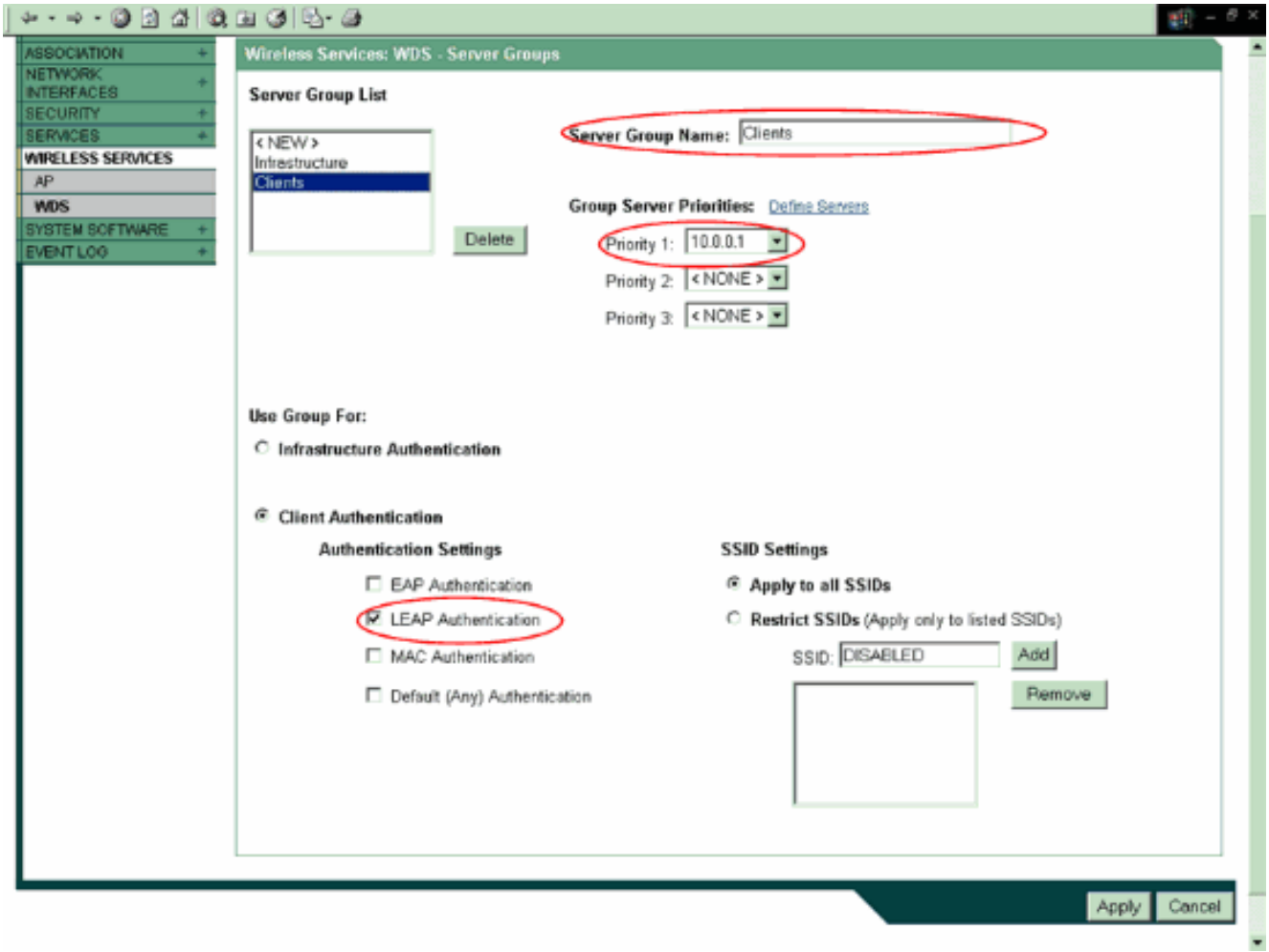
Настройте метод аутентификации клиента

Добавьте метод аутентификации клиента для WDS.

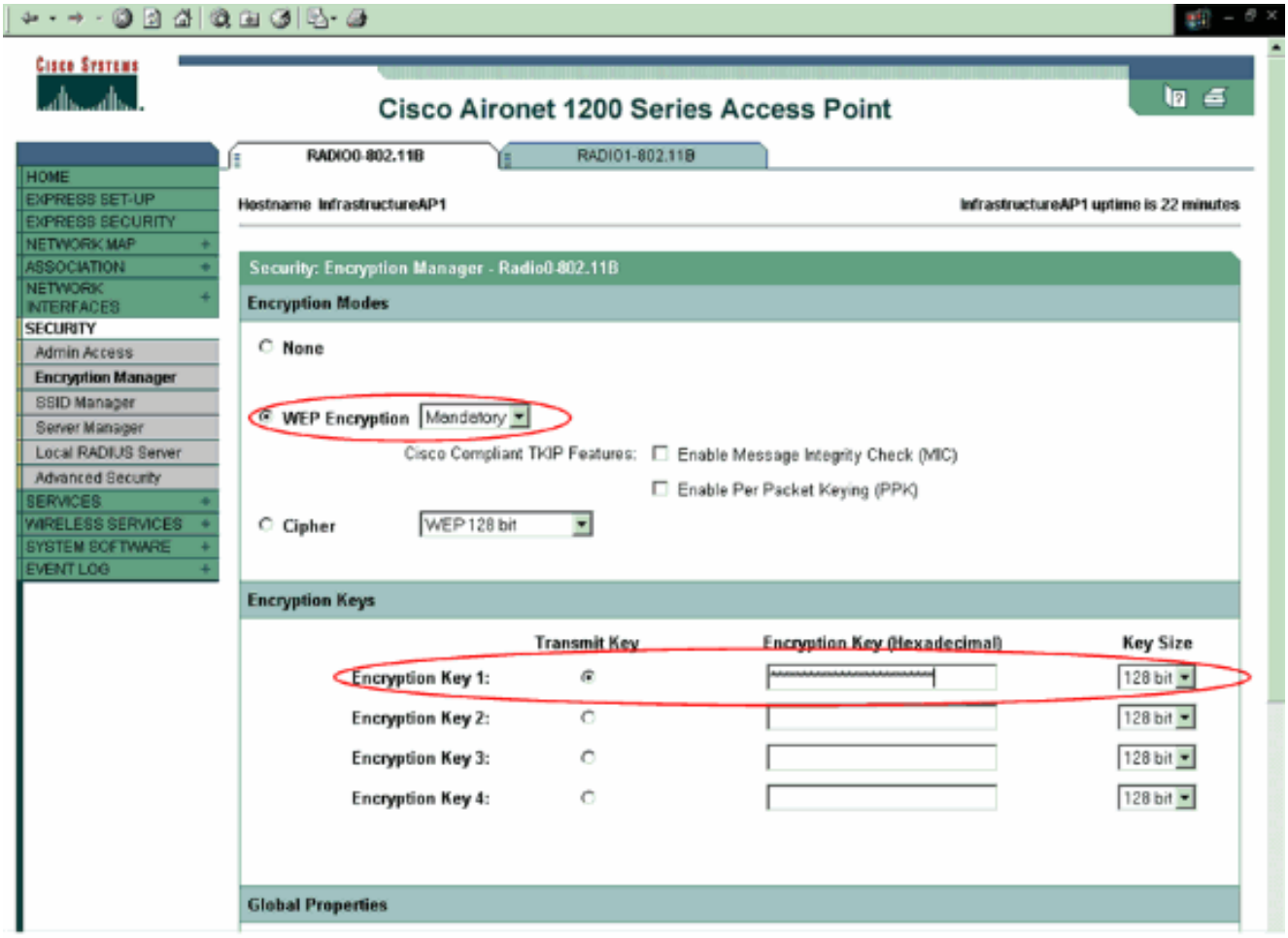
Выполните следующие действия:

1. Выберите **Wireless Services> WDS> Server Groups** на AP WDS.Определите группу сервера, которая проверяет подлинность клиента (Client group).Это должно отличаться от ранее группа настроенного сервера для аутентификации инфраструктуры. Данный пример использует Имя серверной группы в качестве **Клиентов**.Приоритет набора 1 к локальному серверу RADIUS.Выберите тип аутентификации (LEAP, EAP, MAC, и т.д) для использования для аутентификации клиента.В данном примере используется

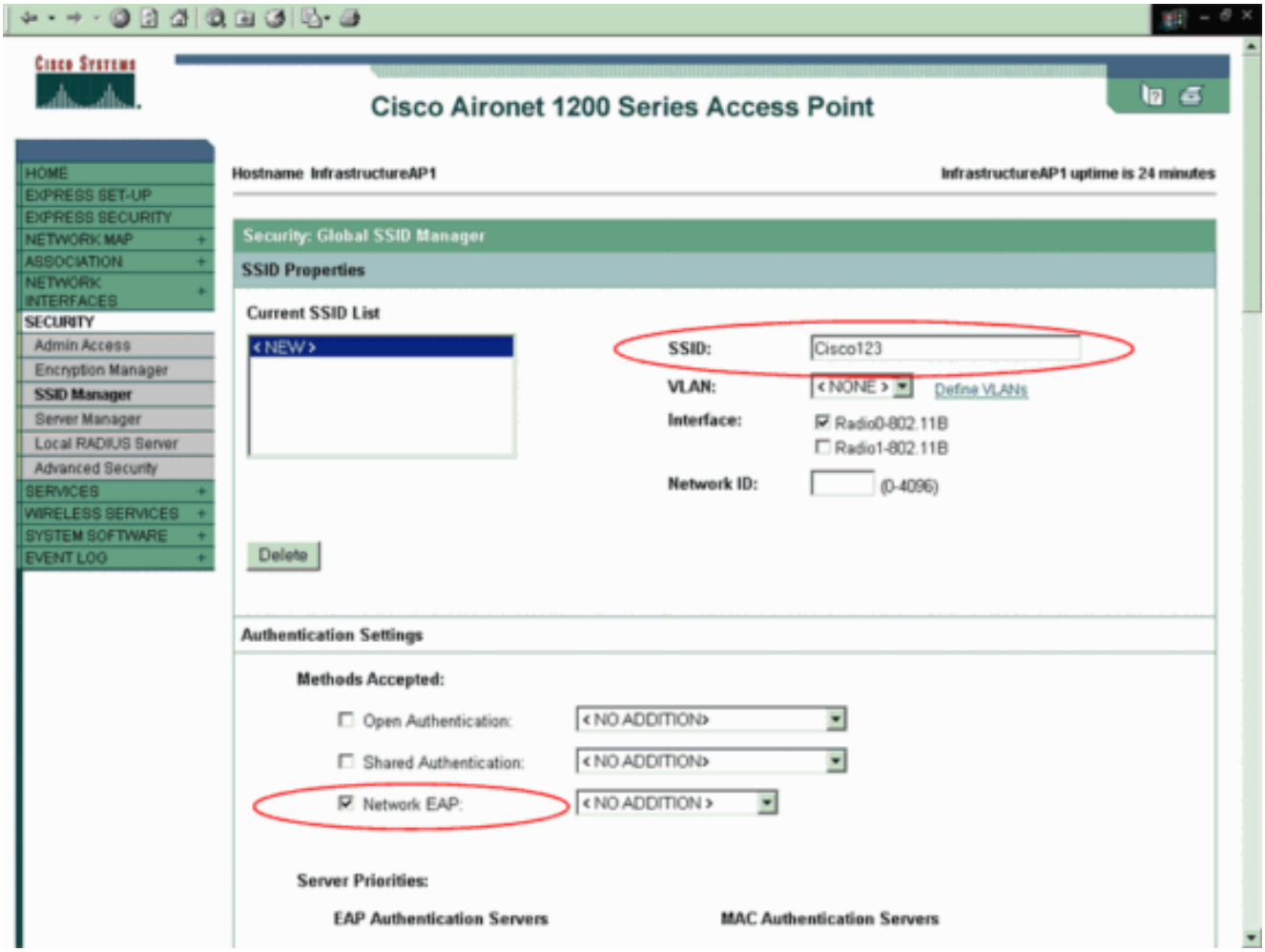
аутентификация LEAP.Примените эти настройки к соответствующим SSID.



2. Выполните эти шаги на AP инфраструктуры:Выберите **Security> Encryption Manager** и нажмите **WEP Encryption** и выберите **Mandatory** из раскрывающегося меню. Под Ключами шифрования введите 128-разрядный Ключ шифрования WEP. Данный пример использует ключ шифрования в качестве **1234567890abcdef1234567890**.



Выберите **Security> SSID Manager** и создайте новый SSID.Данный пример использует SSID в качестве **Cisco123**. Затем, выберите метод аутентификации.Выберите **Network EAP** на AP
инфраструктуры.



Тест, который клиенты аутентифицируют успешно и партнер с AP инфраструктуры. Клиент передает его учетные данные AP инфраструктуры, когда он подходит впервые. AP инфраструктуры тогда вперед то же к AP WDS, который проверяет учетные данные.

Примечание: Этот документ не объясняет, как настроить клиентский адаптер. См. клиентские адаптеры беспроводной локальной сети Cisco Aironet для получения информации о том, как настроить клиентский адаптер.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- **show wlccp wds mn** - Использование эта команда от CLI на AP WDS для проверки успешной аутентификации клиента и ассоциации с AP WDS.

```
WDS#show wlccp wds mn MAC-ADDR IP-ADDR Curr-AP STATE 0040.96a5.b5d4 10.0.0.15 000e.d7e4.a629
REGISTERED
```

Следующие команды отладки также полезны.

- **debug wlccp ap {млн | wds-обнаружение | состояние}** - Использование эта команда для превращения демонстрирующимся из сообщений отладки отнесся к устройствам клиента **(млн)**, **процесс обнаружения WDS** и проверка подлинности точки доступа к точке доступа WDS **(состояние)**.
- **debug wlccp packet** - Используйте эту команду для превращения демонстрирующимися из пакетов к и от точки доступа WDS.
- **debug radius local-server** - Активирует показ сообщений об ошибках, отнесенных к

отказавшим аутентификациям клиента к локальному аутентификатору

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Настройка беспроводных доменных служб
- Cisco Aironet Client Adapter
- Часто задаваемые вопросы о беспроводных доменных службах
- Примеры конфигурации WLAN и технические примечания
- Примеры конфигурации и технические примечания Cisco Aironet серии 1200
- Cisco Systems – техническая поддержка и документация