Разрешение работы защищенного шелла (SSH) на точке доступа (AP)

Содержание

Введение

В этом документе поясняется настройка точки доступа (AP) для включения доступа по протоколу SSH.

Предварительные условия

Требования

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

- Знание того, как настроить AP Cisco Aironet
- Базовые знания о SSH и отнесенных понятиях безопасности

Используемые компоненты

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

- AP aironet серии 1200, который выполняет релиз 12.3 программного обеспечения Cisco IOS (8) JEB

- ПК или портативный ПК с утилитой Клиента SSH

Примечание: Этот документ использует утилиту Клиента SSH для проверки конфигурации. Можно использовать любую стороннюю служебную программу клиента для регистрации к AP с использованием SSH.

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.

Доступ к интерфейсу командной строки (CLI) на AP Aironet

Можно использовать любой из этих методов для доступа к интерфейсу командной строки (CLI) на AP Aironet:

- Консольный порт
- Telnet
- SSH

Если AP имеет консольный порт, и у вас есть физический доступ к AP, можно использовать консольный порт, чтобы войти к AP и изменить конфигурацию при необходимости. Для получения информации о том, как использовать консольный порт для регистрации к AP, обратитесь к *Соединению с точками доступа серии 1200 Локально* раздел Настройки документа точка доступа впервые.

Если можно только обратиться к AP через Ethernet, используйте или Протокол Telnet или протокол SSH для регистрации к AP.

Протокол Telnet использует порт 23 для связи. Telnet передает и получает данные в открытом тексте. Поскольку передача данных происходит в открытом тексте, хакер может легко поставить под угрозу пароли и обратиться к AP. RFC 854 определяет Telnet и расширяет Telnet с помощью опций на многие другие RFC.

SSH является приложением и протоколом, который предоставляет безопасную замену r-программным-средствам Беркли. SSH является протоколом, который предоставляет безопасное, удаленное соединение Уровню 2 или прибору слоя 3. Существует две версии SSH: Версия SSH 1 и версия SSH 2. Это поддержки релиза ПО обе версии SSH. Если вы не задаете номер версии, настройки по умолчанию AP к версии 2.

Когда устройство аутентифицируется, SSH предоставляет больше безопасности для удаленных соединений, чем Telnet путем обеспечения строгого шифрования. Это шифрование является преимуществом перед сеансом Telnet, на котором связь происходит в открытом тексте. Для получения дополнительной информации о SSH обратитесь к часто задаваемым вопросам Secure Shell (SSH). Функция SSH имеет сервер SSH и интегрированного клиента SSH. Поддержки клиентов эти методы аутентификации пользователей:

- RADIUS (для получения дополнительной информации, обратитесь к Доступу точки доступа Управления с разделом RADIUS),
- Локальная проверка подлинности и авторизация (для получения дополнительной информации, обратитесь к Настройке точку доступа для раздела Локальной проверки подлинности и Авторизации),

Для получения дополнительной информации о SSH, обратитесь к Части 5, *"Другие Характеристики безопасности"* в *Руководстве по конфигурации Безопасности Cisco IOS для релиза 12.3.*

Примечание: Функция SSH в этом выпуске ПО не поддерживает IP-безопасность (IPSec).

Можно настроить AP для SSH с использованием или CLI или GUI. Этот документ объясняет оба способа конфигурации.

Настройка

Конфигурация интерфейса командой строки CLI

В этом разделе вам предоставляют информацию по настройке функций, описанную в этом документе с использованием CLI.

Пошаговые инструкции

Для включения основанного на SSH доступа на AP сначала необходимо настроить AP как сервер SSH. Выполните эти действия для настройки сервера SSH на AP от CLI:

1. Настройте имя хоста и доменное имя для AP.`AP#configure terminal !--- Enter global configuration mode on the AP. AP<config>#hostname Test !--- This example uses "Test" as the AP host name. Test<config>#ip domain name abc.com !--- This command configures the AP with the domain name "abc.com".`
2. Генерируйте Rivest, Shamir и Adelman (RSA) ключ для вашего AP.Генерация ключа RSA включает SSH на AP. Выполните эту команду в режиме глобальной конфигурации:`Test<config>#crypto key generate rsa rsa_key_size !--- This generates an RSA key and enables the SSH server.` **Примечание:** Рекомендуемый минимальный размер ключа RSA 1024.
3. Настройте проверку подлинности пользователя на AP.На AP можно настроить проверку подлинности пользователя для использования или локального списка или внешней проверки подлинности, авторизации, и бухгалтерский (AAA) сервер. Данный пример использует локально генерируемый список для аутентификации пользователей:`Test<config>#aaa new-model !--- Enable AAA authentication. Test<config>#aaa authentication login default local none !--- Use the local database in order to authenticate users. Test<config>#username Test password Test123 !--- Configure a user with the name "Test". Test<config>#username ABC password xyz123 !--- Configure a second user with the name "ABC".` Эта конфигурация настраивает AP для выполнения основанной на пользователе аутентификации с использованием локальной базы данных, которая настроена на AP. Пример настраивает двух пользователей в локальной базе данных, "Тесте" и "ABC".
4. Настройте параметры SSH.`Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]} !--- Configure the SSH control variables on the AP.` **Примечание:** Вы

можете задать таймаут в секундах, но не превышаете 120 секунд. По умолчанию равняется 120. Эта установка применяется к этапу согласования SSH. Вы можете также задать количество опознавательных повторных попыток, но не превышаете пять опознавательных повторных попыток. По умолчанию равняется трем.

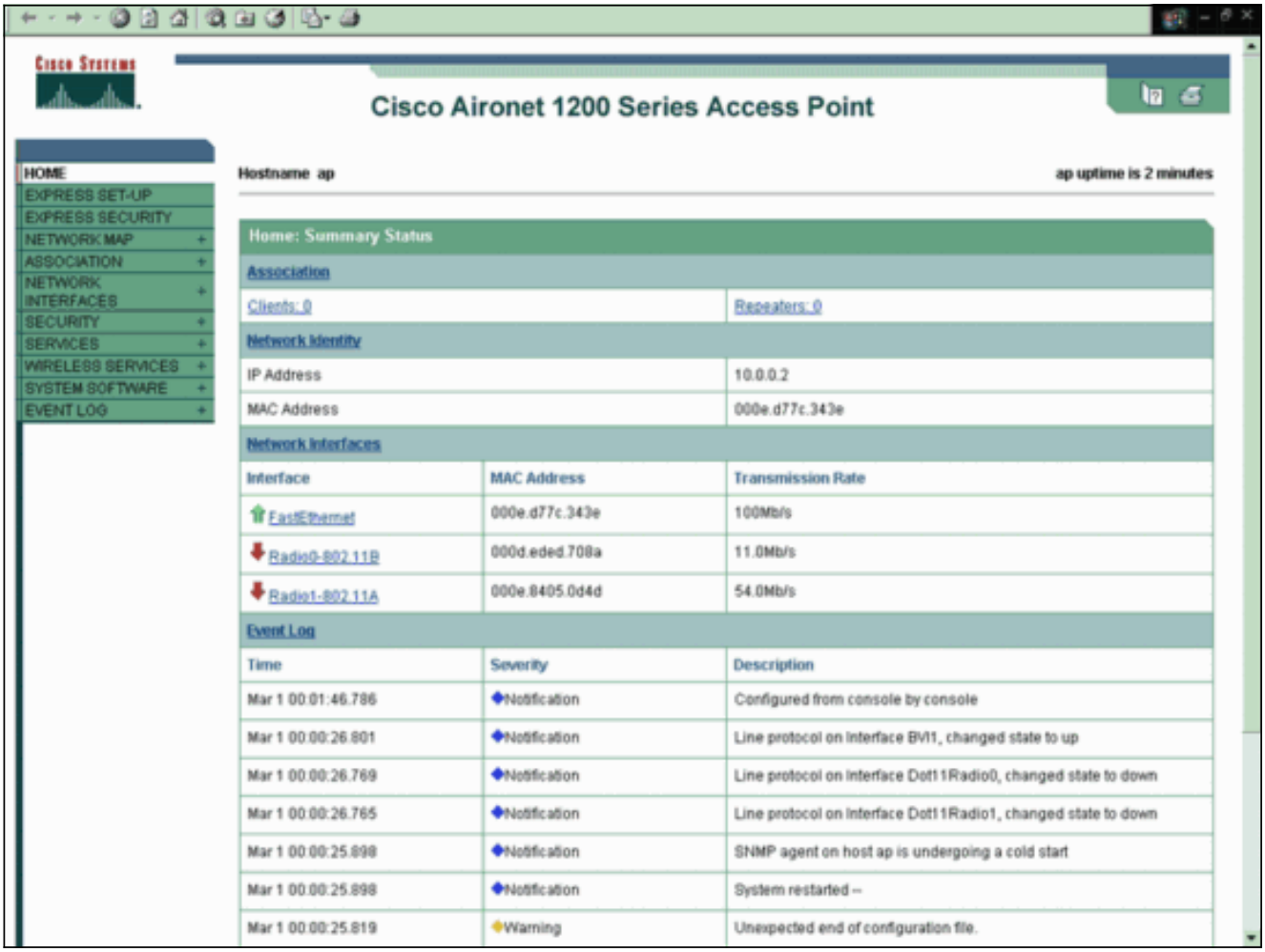
Конфигурация графического интерфейса пользователя (GUI)

Можно также использовать GUI для включения основанного на SSH доступа на AP.

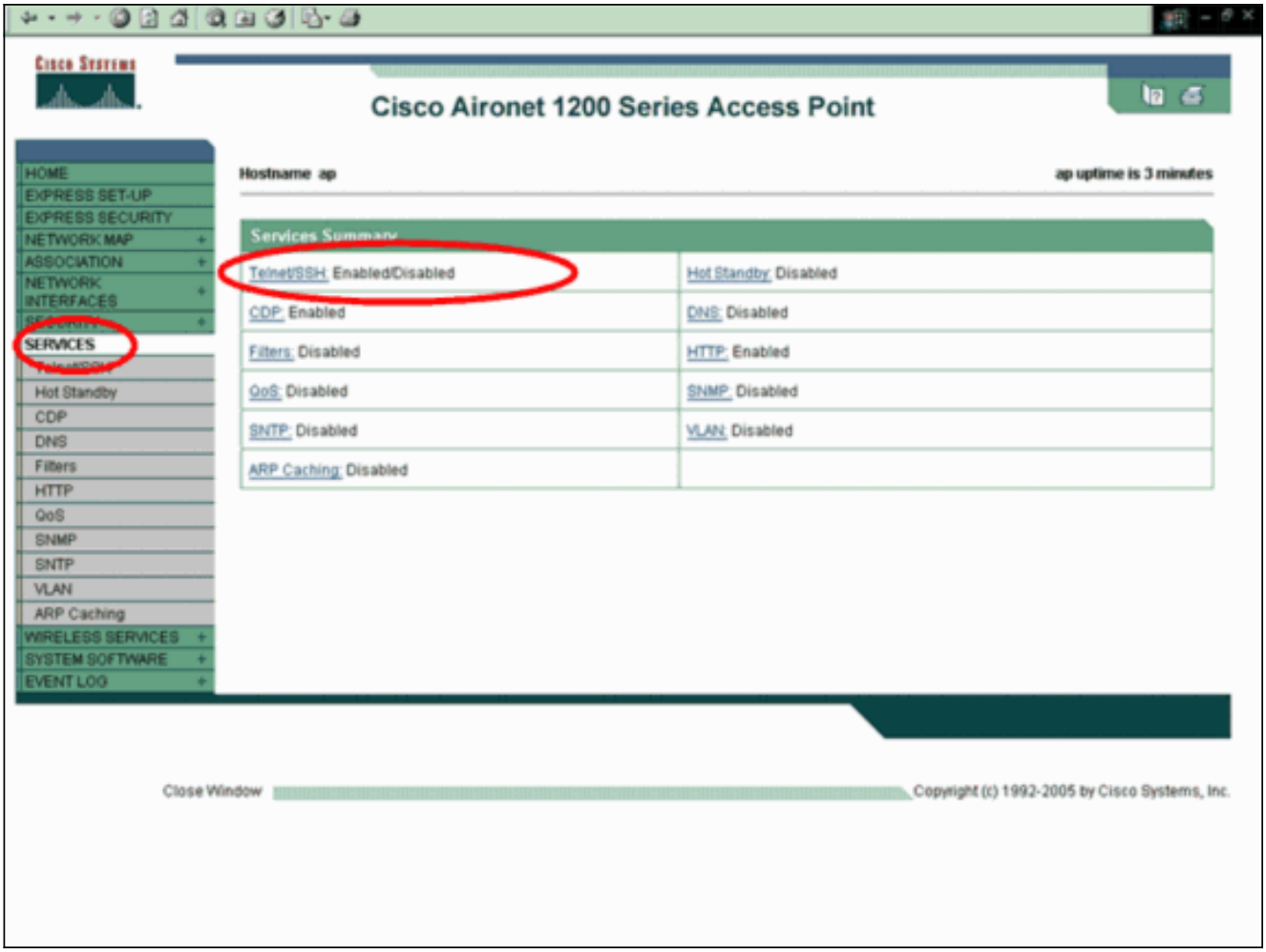
Пошаговые инструкции

Выполните следующие действия:

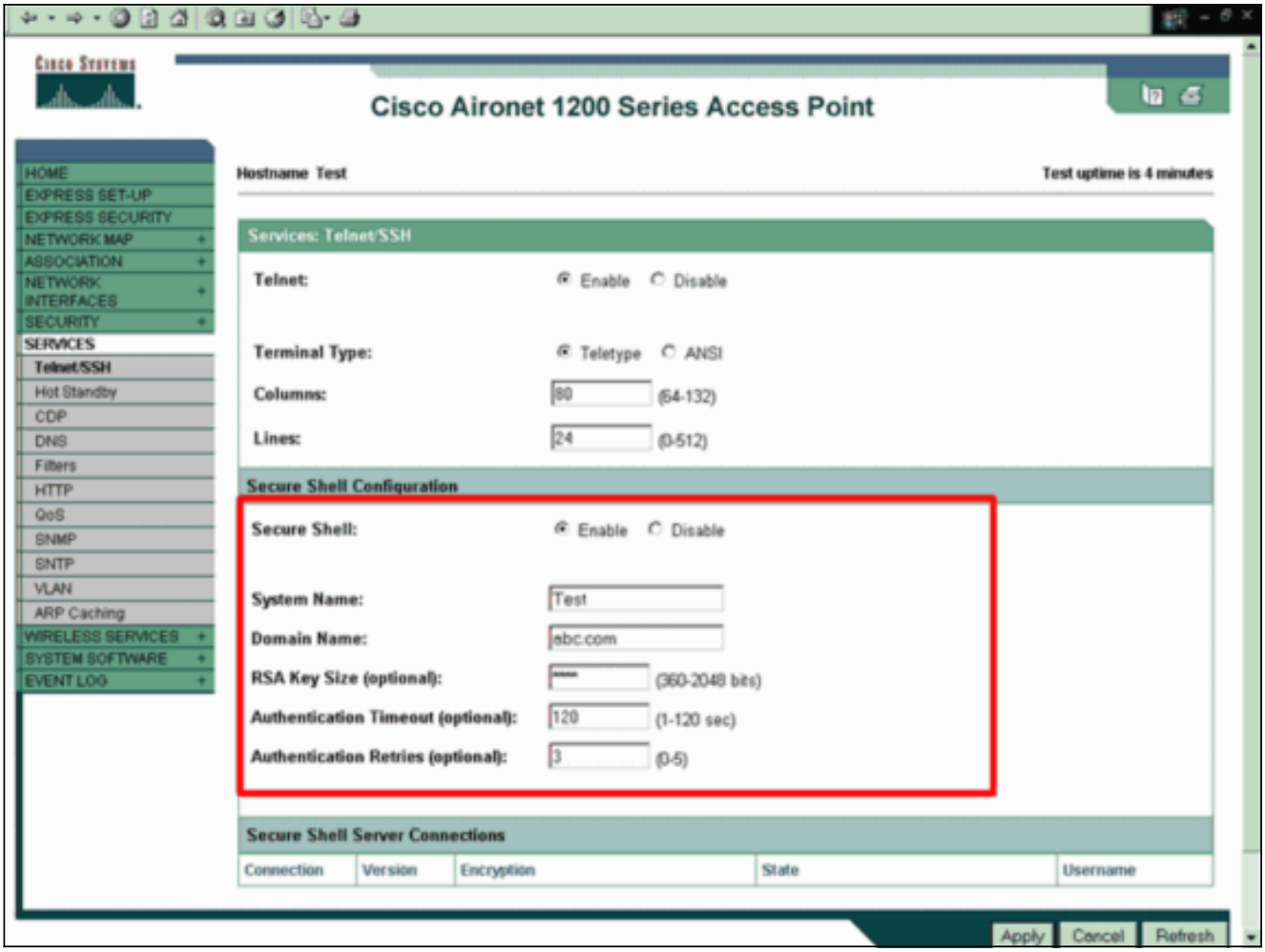
1. Войдите к AP через браузер.Показы окна Summary Status.



2. Нажмите **Services** в меню слева.Показы Окна со сводной информацией Сервисов.



3. Нажмите **Telnet/SSH**, чтобы включить и настроить параметры Telnet/SSH.Сервисы: показы окна Telnet/SSH. Прокрутите вниз к Области конфигурации Secure Shell. Нажмите **Enable beside Secure Shell** и введите параметры SSH как показано в примере:Данный пример использует эти параметры:Имя системы: ТестИмя домена: a B C. comРазмер ключа RSA: 1024Время ожидания при аутентификации: 120Число попыток аутентификации:
   3



4. Нажмите **Apply** для сохранения изменений.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

- **show ip ssh** — Проверяет, включен ли SSH на AP и позволяет вам проверить версию SSH, который работает на AP. Приведенные данные являются

```
Test#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

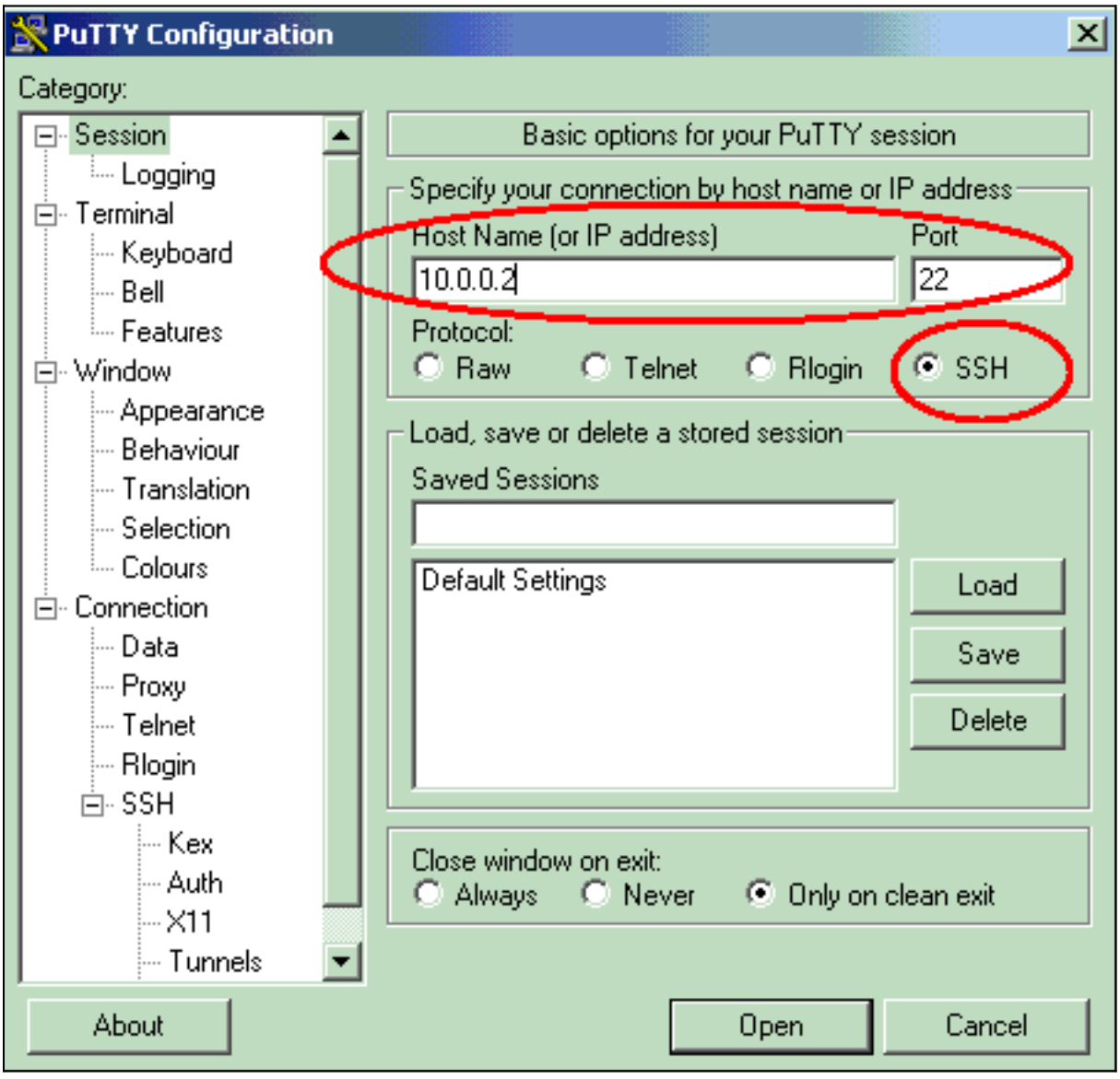
примером:

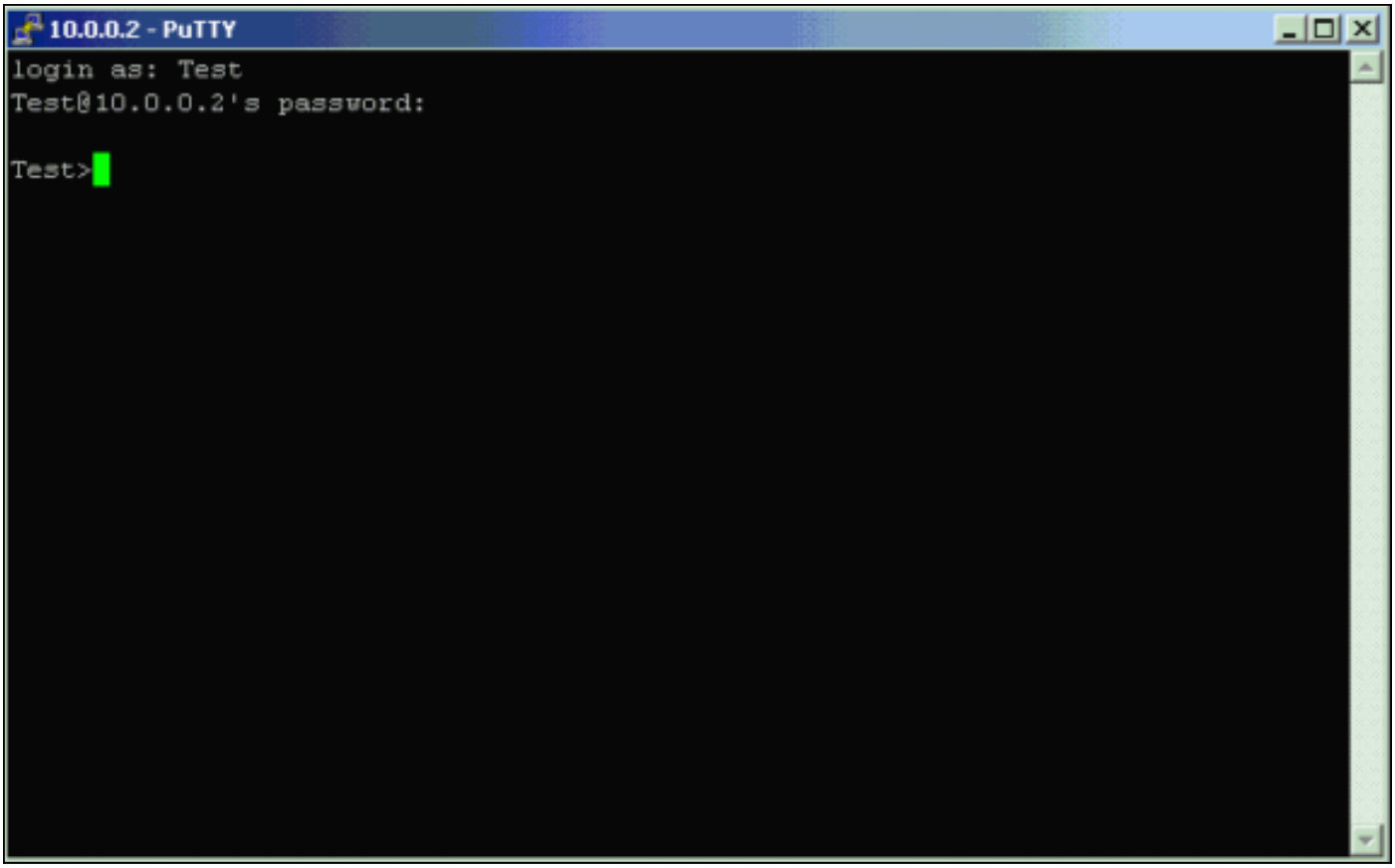
- **show ssh** — Позволяет вам просмотреть статус своих соединений сервера SSH. Приведенные данные являются

```
Test#show ssh
Connection Version Mode Encryption  Hmac          State          Username
0          2.0     IN   aes256-cbc  hmac-sha1     Session started  ABC
0          2.0     OUT  aes256-cbc  hmac-sha1     Session started  ABC
```

примером:

Теперь, инициируйте соединение через ПК, который выполняет стороннее программное обеспечение SSH, и затем предпримите попытку войти к AP. Эта проверка использует IP-адрес AP, 10.0.0.2. Поскольку вы настроили Тест имени пользователя, используйте это название для доступа к AP через SSH:





Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Если ваши команды конфигурации SSH отклонены как запрещенные команды, вы успешно не генерировали Открытые и секретные ключи криптосистемы RSA для своего AP. См. раздел *Советов по устранению проблем* документа Configuring Secure Shell для списка возможных причин для этой проблемы.

Отключите SSH

Для отключения SSH на AP необходимо удалить пару RSA, которая генерируется на AP. Для удаления пары RSA выполните **команду crypto key zeroize rsa** в режиме глобальной конфигурации. При удалении Открытых и секретных ключей криптосистемы RSA вы автоматически отключаете сервер SSH. Приведенные данные являются примером:

```
Test(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Дополнительные сведения

- Configuring Secure Shell

- Настройка точка доступа впервые
- Страница технической поддержки Secure Shell (SSH)
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация