アクセス ポイント（AP）でのセキュア シェル（SSH）の有効化

目次

はじめに

このドキュメントでは、セキュア シェル（SSH）ベース アクセスをイネーブルにするためにアクセス ポイント（AP）を設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco Aironet AP の設定方法に関する知識
- SSH および関連するセキュリティの概念に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS(R) ソフトウェア リリース 12.3(8)JEB が稼働する Aironet 1200 シリーズ AP
- SSH クライアント ユーティリティをインストールした PC またはラップトップ

注: このドキュメントでは、設定を検証するために、SSH クライアント ユーティリティを使用します。 SSH を使用して AP に口グインするために任意のサードパーティ クライアント ユーティ

リティを使用できます。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Aironet AP でのコマンドライン インターフェイス（CLI）へのアクセス

Aironet AP でコマンドライン インターフェイス（CLI）にアクセスするには、次のいずれかの方法を使用できます。

- コンソール ポート
- Telnet
- SSH

AP にコンソール ポートがあり、AP に物理的にアクセスできる場合、コンソール ポートを使用して AP にログインでき、必要に応じて設定を変更できます。 コンソール ポートを使用して AP にログインする方法については、『アクセス ポイントの最初の設定』の「*1200 シリーズのアクセス ポイントへのローカル接続*」セクションを参照してください。

イーサネットを介してのみ AP にアクセスできる場合、AP にログインするには、Telnet プロトコルまたは SSH プロトコルを使用します。

Telnet プロトコルでは通信用にポート 23 が使用されます。 Telnet はクリア テキストでデータを送受信します。 データ通信はクリア テキストで実行されるため、ハッカーは簡単にパスワードを改ざんでき、AP にアクセスできます。 RFC 854 では Telnet が規定されており、他の多数の RFC によって Telnet が拡張されています。

SSH は Berkley の r ツールに代わる安全性の高いプロトコルおよびアプリケーションです。 SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。 SSH には 2 つのバージョンがあります。 SSH バージョン 1 と SSH バージョン 2 です。 このソフトウェア リリースでは、どちらの SSH バージョンもサポートしています。 バージョン番号を指定しない場合、AP はデフォルトのバージョン 2 になります。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。 この暗号化は、通信がクリア テキストで実行される Telnet セッションと比べて長所になります。 SSH の詳細については、セキュア シェル（SSH）に関する FAQ を参照してください。 SSH 機能では SSH サーバと SSH 統合クライアントを使用します。 クライアントは次のユーザ認証方式をサポートしています。

- RADIUS（詳細については、「RADIUS を使用したアクセス ポイントのアクセス制御」セクションを参照）。
- ローカル認証および許可（詳細については、「ローカル認証と許可に対するアクセス ポイントの設定」セクションを参照）

SSH の詳細については、『*Cisco IOS セキュリティ設定ガイド、リリース 12.3*』のパート 5「そ

の他のセキュリティ機能」を参照してください。

注: このソフトウェア リリースの SSH 機能は IP セキュリティ（IPSec）をサポートしていません。

CLI または GUI を使用して SSH 用に AP を設定できます。 このドキュメントでは、両方の設定方法を説明します。

設定

CLI 設定

この項では、このドキュメントで説明する機能を、CLI を使用して設定するための情報を提供します。

手順説明

AP で SSH ベースのアクセスを可能にするには、まず、SSH サーバとして AP を設定する必要があります。 CLI から、AP 上の SSH サーバを設定するには、次の手順を実行します。

1. AP のホスト名とドメイン名を設定します。
   ```
   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. AP の Rivest, Shamir, and Adelman（RSA）のキーを生成します。RSA キーを生成することにより、AP 上で SSH がイネーブルになります。 グローバル コンフィギュレーション モードで次のコマンドを発行します。
   ```
   Test<config>#crypto key generate rsa rsa_key_size
   !--- This generates an RSA key and enables the SSH server.
   ```
   注: 推奨される RSA のキーの最小サイズは 1024 です。
3. AP 上にユーザ認証を設定します。AP では、ローカル リストまたは外部認証、許可、アカウンティング（AAA）サーバを使用するようにユーザ認証を設定できます。 この例では、ローカルで生成されたリストを使用してユーザを認証します。
   ```
   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".
   ```
   この設定では、AP 上に設定されたローカル データベースを使用してユーザ ベースの認証を行うように AP を設定します。 この例では、ローカル データベースに 2 人のユーザ、「Test」と「ABC」を設定します。
4. SSH パラメータを設定します。
   ```
   Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]}
   !--- Configure the SSH control variables on the AP.
   ```
   注: 120 秒以内のタイムアウトを秒数で指定できます。 デフォルトは 120 です。 この設定は、SSH ネゴシエーション フェーズに適用されます。 認証の再試行回数（5 回以内）も指定できます。 デフォルトは 3 です。

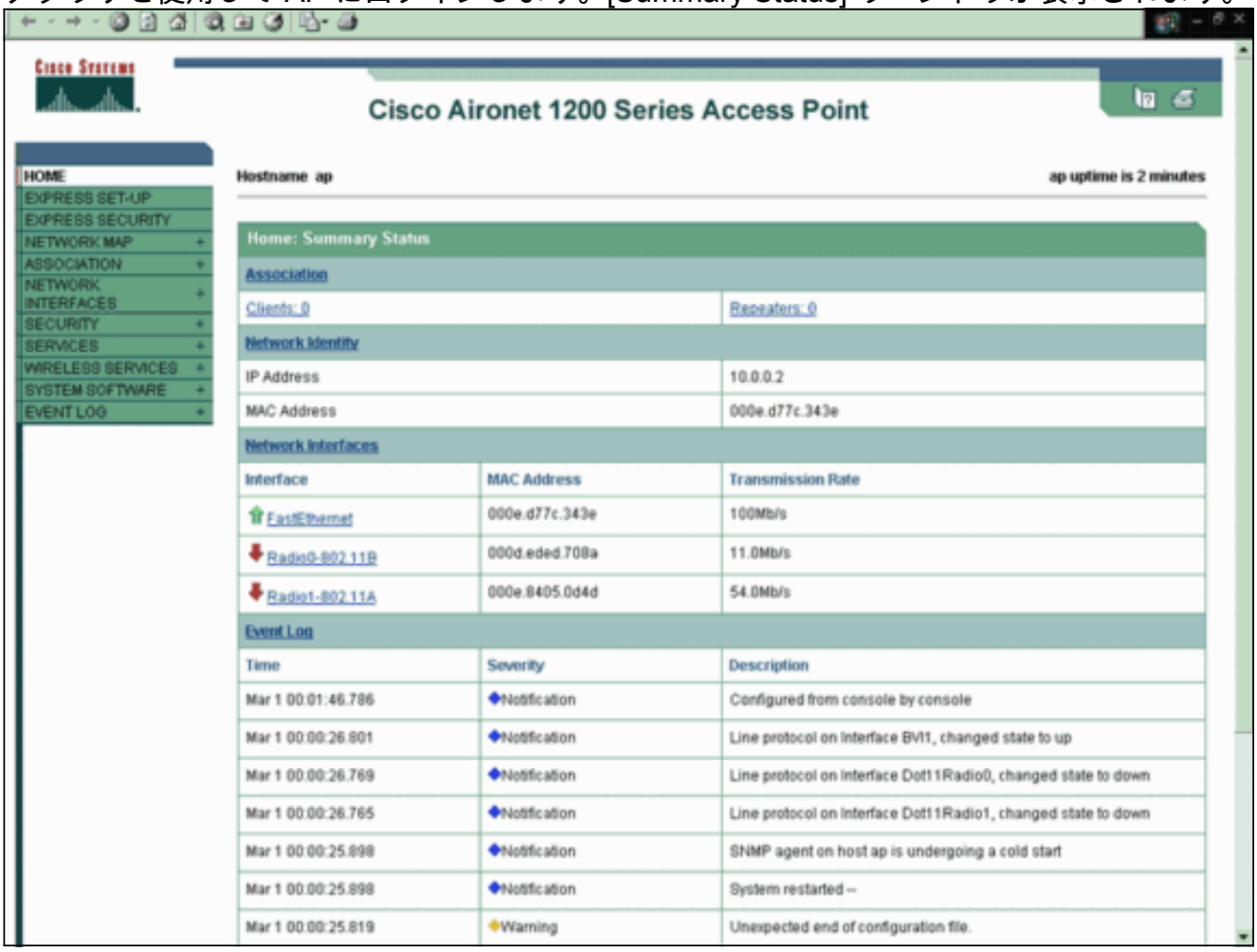
GUI 設定

AP 上で SSH ベースのアクセスをイネーブルにするために GUI を使用することもできます。

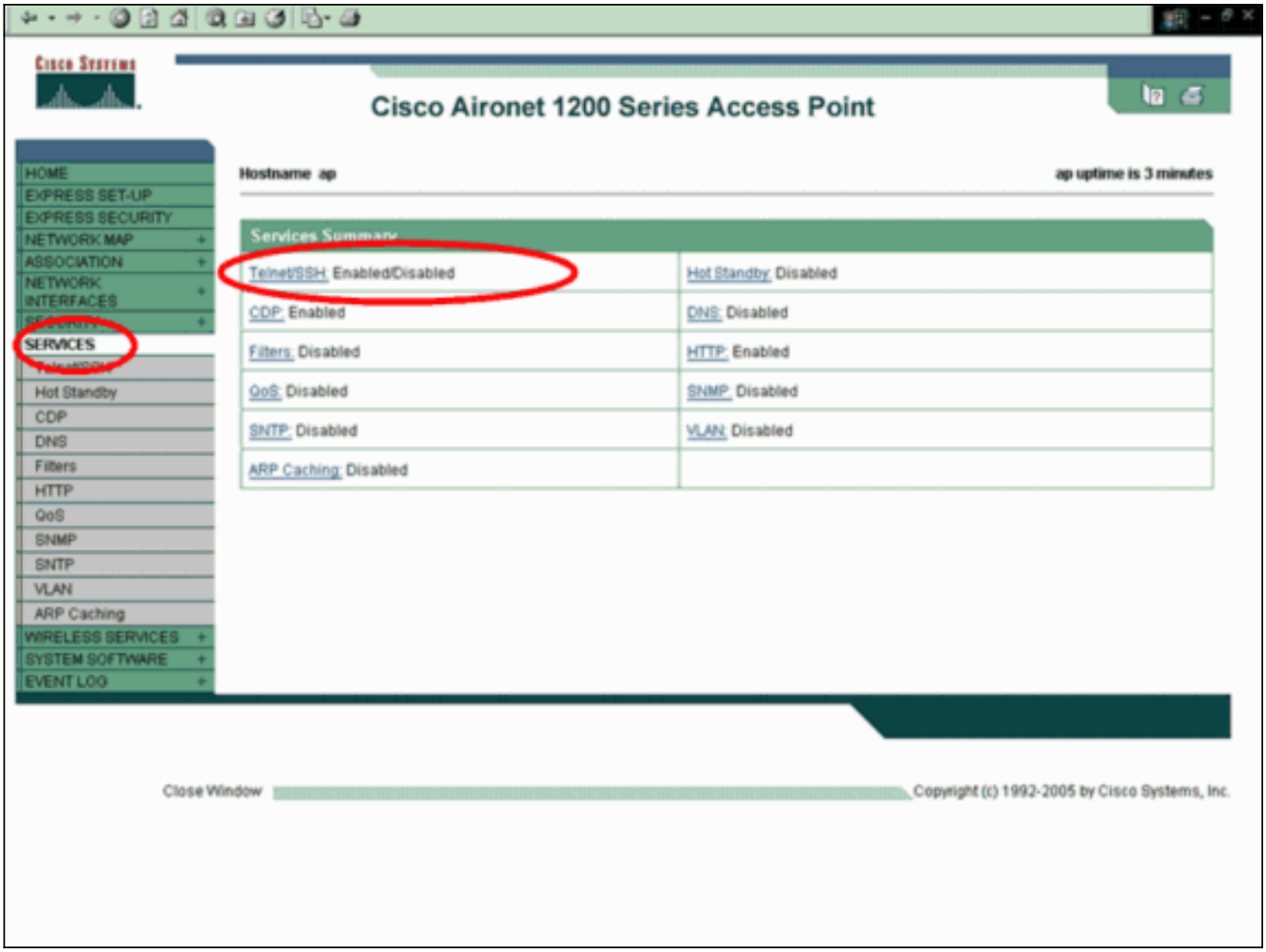
手順説明

次の手順を実行します。

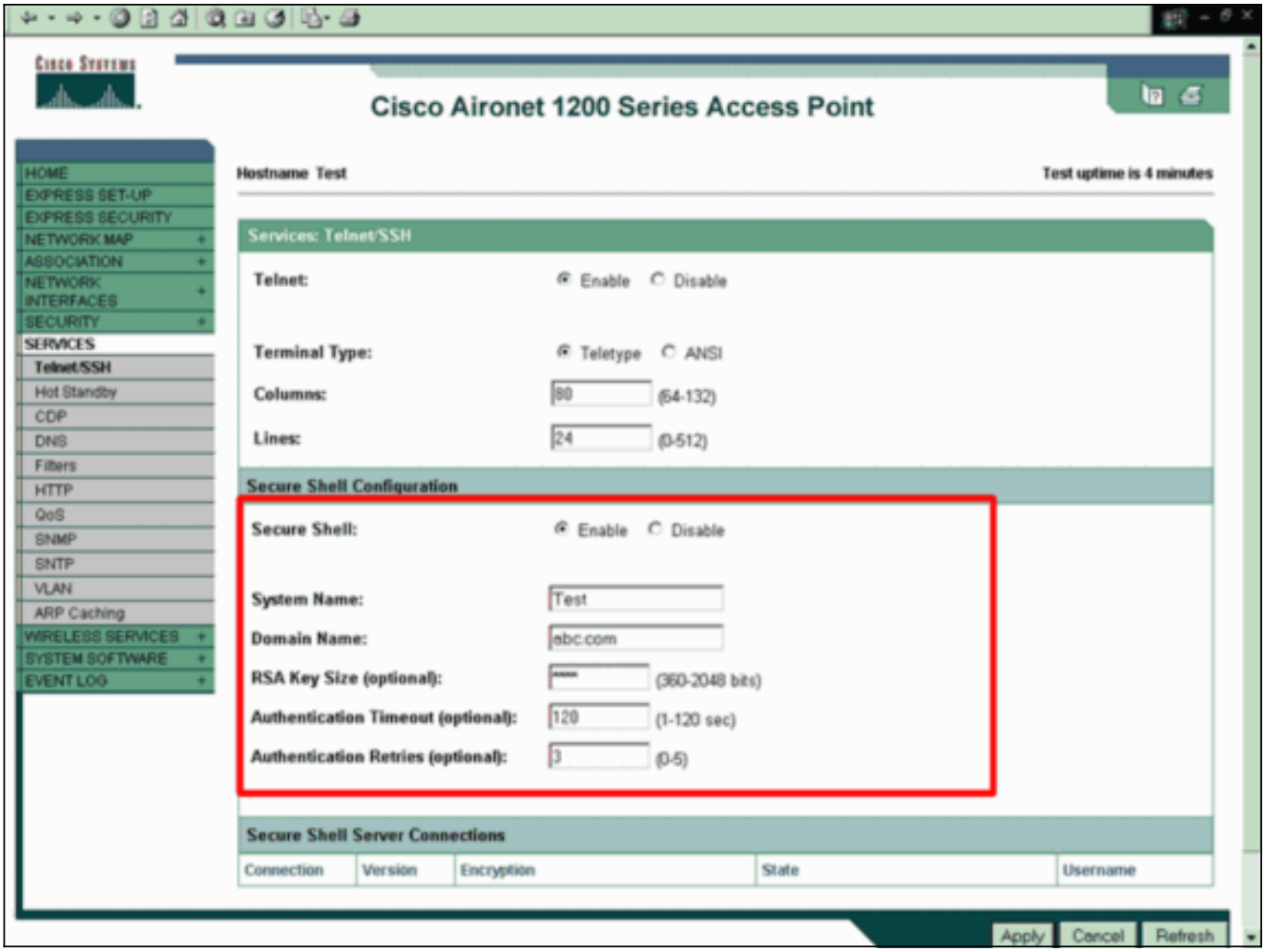
1. ブラウザを使用して AP にログインします。[Summary Status] ウィンドウが表示されます。



2. 左側のメニューで [Services] をクリックします。[Services Summary] ウィンドウが表示されます。



3. Telnet/SSH パラメータをイネーブルにして設定するには、[Telnet/SSH] をクリックします。[Services: Telnet/SSH] ウィンドウが表示されます。 [Secure Shell Configuration] 領域までスクロールします。 Secure Shell のそばの [Enable] をクリックし、次の例に示すように SSH パラメータを入力します。この例では、次のパラメータを使用します。[System Name]： テスト[Domain Name]： abc.com[RSA Key Size]： 1024[Authentication Timeout]： 120[Authentication Retries]：
   3



4. [Apply] をクリックして変更を保存します。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show ip ssh** - SSH が AP でイネーブルかどうかを検証し、AP で実行されている SSH のバージョンを確認できます。 次に出力例を示します。

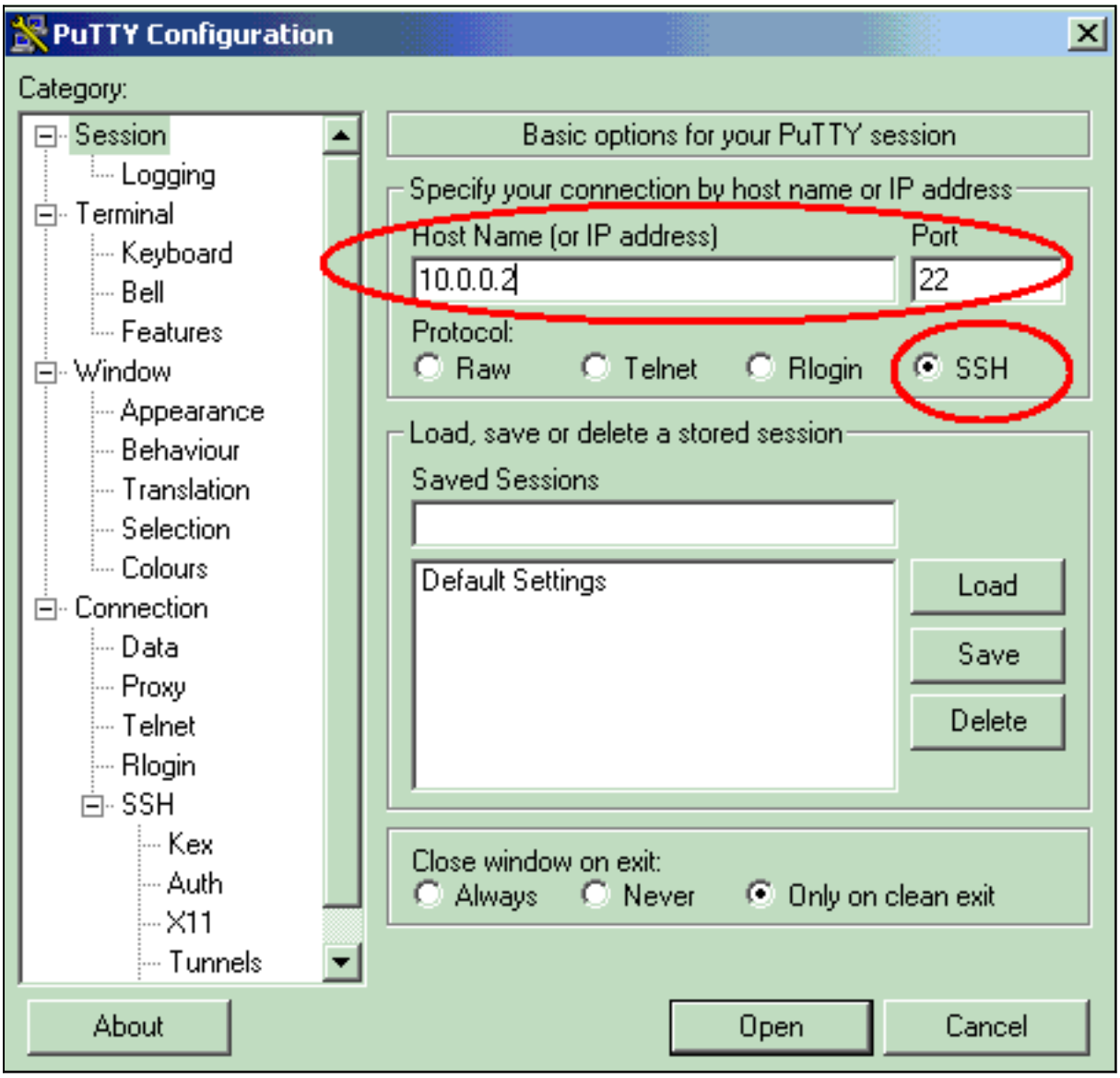
```
Test#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

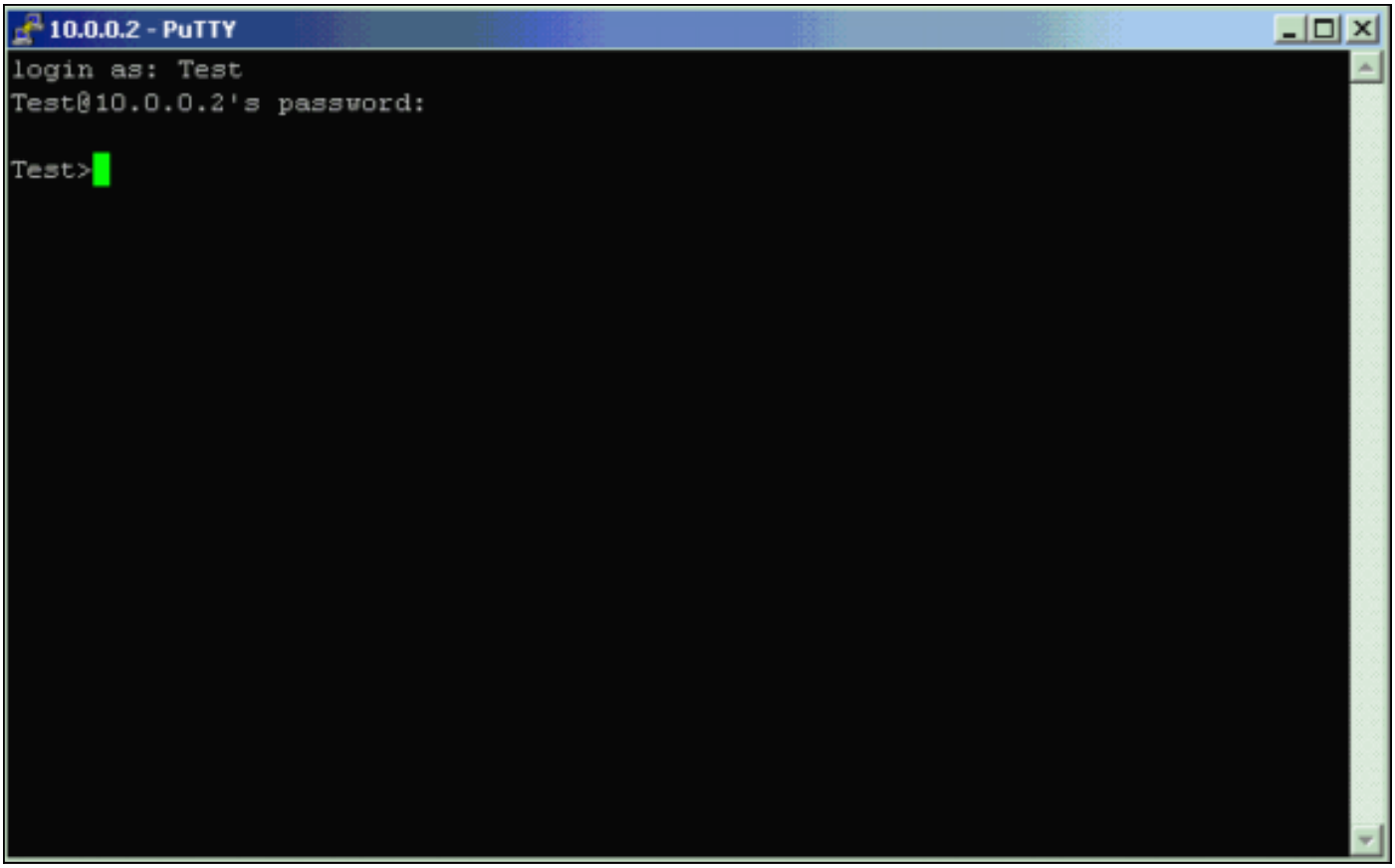
- **show ssh** - SSH サーバの接続のステータスを表示できます。 次に出力例を示します。

```
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
```

ここで、サードパーティの SSH ソフトウェアを実行する PC を介して接続を開始し、AP への口

グインを試行します。 この検証では、AP の IP アドレス、10.0.0.2 を使用します。 ユーザ名 Test を設定したため、SSH を使用して AP にアクセスするには、この名前を使用してください。





トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

SSH コンフィギュレーション コマンドが正規のコマンドとして拒否される場合、AP の RSA キー ペアを正常に生成していません。 この問題の考えられる理由のリストについては、『セキュア シェルの設定』の「トラブルシューティングのヒント」セクションを参照してください。

SSH のディセーブル化

AP 上の SSH をディセーブルにするには、AP で生成された RSA ペアを削除する必要があります。 RSA ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize rsa** コマンドを発行します。 RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。 次に出力例を示します。

```
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
```

関連情報

- セキュア シェルの設定
- アクセス ポイントの最初の設定

- セキュア シェル (SSH) に関するサポート ページ
- ワイヤレスに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems