在访问接入点(AP)的Secure Shell (SSH)启动

目录

简介

本文解释如何配置接入点(AP)为了启用安全壳SSH -基于访问。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 知识如何配置Cisco Aironet AP
- SSH和相关安全概念基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Aironet 1200运行Cisco IOS软件版本12.3(8)JEB的系列AP
- PC或笔记本电脑用SSH客户端工具

注意： 本文使用SSH客户端工具为了验证配置。您能使用所有第三方客户端工具为了登陆到与使用的AP SSH。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

访问在Aironet AP的命令行界面(CLI)

您能使用这些方法中的任一个为了访问在Aironet AP的命令行界面(CLI) ：

- 控制台端口
- Telnet
- SSH

如果AP有一个控制台端口，并且访问物理访问AP，您能使用控制台端口为了登陆到AP和如果需要，更改配置。关于如何使用控制台端口的信息为了登陆到AP，参考*连接到本地1200系列接入点第一次配置接入点的*区分本文。

如果能通过以太网只访问AP，请使用Telnet协议或SSH协议为了登陆到AP。

Telnet协议使用端口23通信。Telnet传送并且接收在明文的数据。由于数据通信在明文发生，黑客能容易地减弱密码和访问AP。RFC 854 定义了Telnet并且由许多其他RFC延伸与选项的Telnet。

SSH是提供一安全替代给Berkley R工具的应用程序和协议。SSH是提供一安全的对Layer2的协议，远程连接或第3层设备。有SSH两个版本：SSH版本1和SSH版本2。此软件版本支持两个SSH版本。如果不指定版本号， AP默认为版本2。

SSH为远程连接比Telnet提供更多安全通过提供强加密，当设备验证时。此加密是一个优点超过远程登录会话，通信在明文发生。关于SSH的更多信息，参考安全壳SSH FAQ。SSH功能有一个SSH服务器和一个SSH集成客户端。客户端支持这些用户认证方法：

- RADIUS欲知更多信息， (参考与RADIUS部分的控制访问点访问)
- 本地认证和授权欲知更多信息， (参考配置本地认证和授权部分的接入点)

关于SSH的更多信息，参考第5部分， *“其他安全功能”在版本12.3的Cisco IOS安全配置指南。*

注意： 在此软件版本的SSH功能不支持IP安全。

您能配置SSH的AP与使用CLI或GUI。本文解释配置两个方法。

配置

CLI 配置

在此部分，您提交以信息配置在与使用的本文描述的功能CLI。

逐步指导

为了启用在AP的基于SSH的访问，您必须首先配置AP作为SSH服务器。遵从这些步骤为了配置在AP的一个SSH服务器从CLI ：

1. 配置一个主机名和域名AP的。
   ```
   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. 生成您的AP的一Rivest、沙米尔和Adelman (RSA)密钥。RSA密钥的生成启用在AP的SSH。发出此in命令全局配置模式：

```
Test<config>#crypto key generate rsa rsa_key_size
!--- This generates an RSA key and enables the SSH server.
```

注意： 推荐的最低的RSA密钥大小是1024。

3. 配置在AP的用户认证。在AP，您能配置用户认证使用当地资料目录或外部验证、授权和核算(AAA)服务器。此示例使用一本地生成的列表为了验证用户：

```
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".
```

此配置配置AP进行基于用户的身份验证与在AP配置的使用本地数据库。示例配置本地数据库的两个用户，“测验”和“ABC”。

4. 配置SSH参数。

```
Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]}
!--- Configure the SSH control variables on the AP.
```

注意： 您能指定Timeout in seconds，但是不超出120秒。默认是120。此设置运用对SSH协商阶段。您能也指定验证重试次数数量，但是不超出五验证重试次数。默认是三。

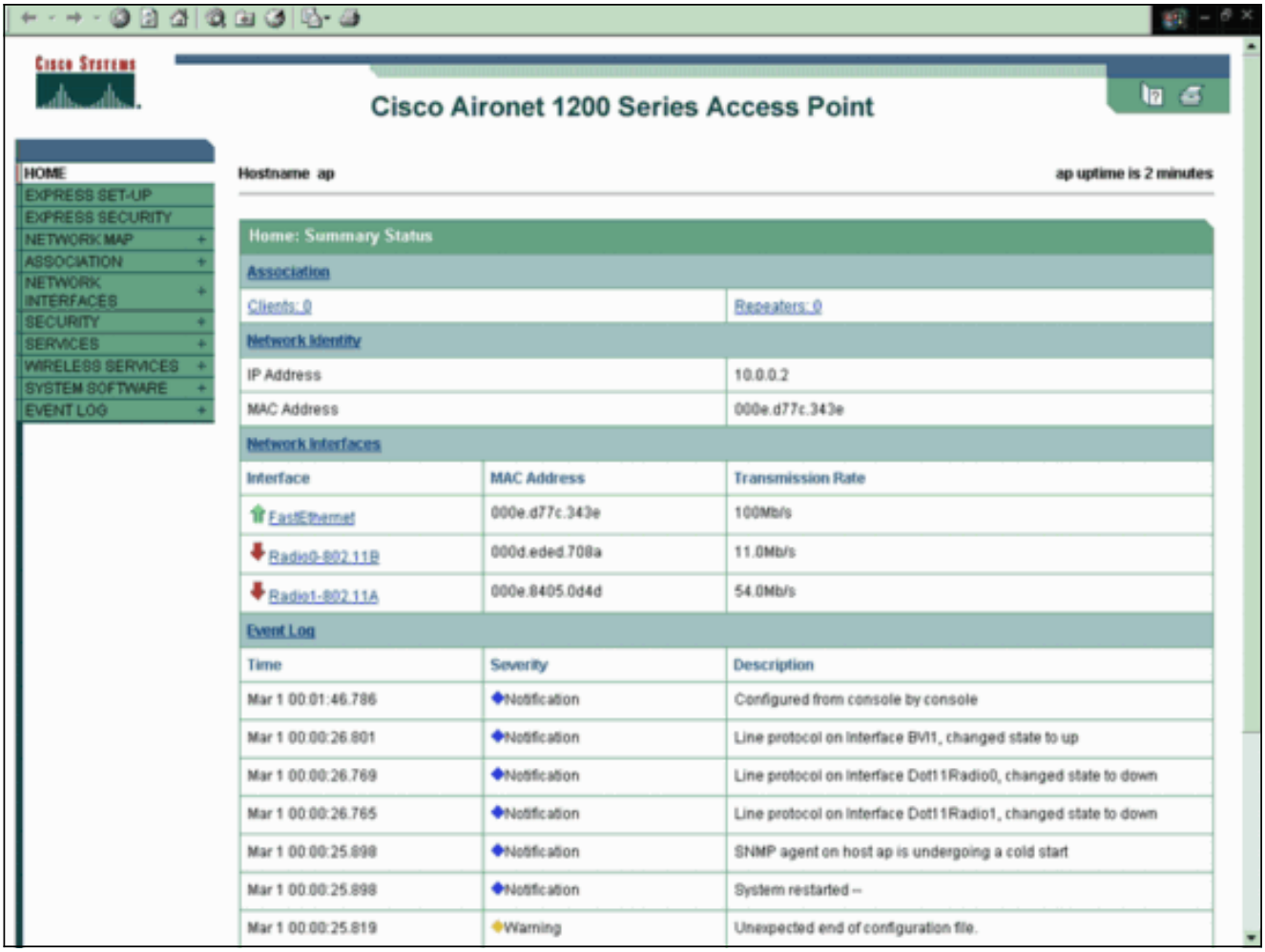
GUI 配置

您能也使用GUI为了启用在AP的基于SSH的访问。

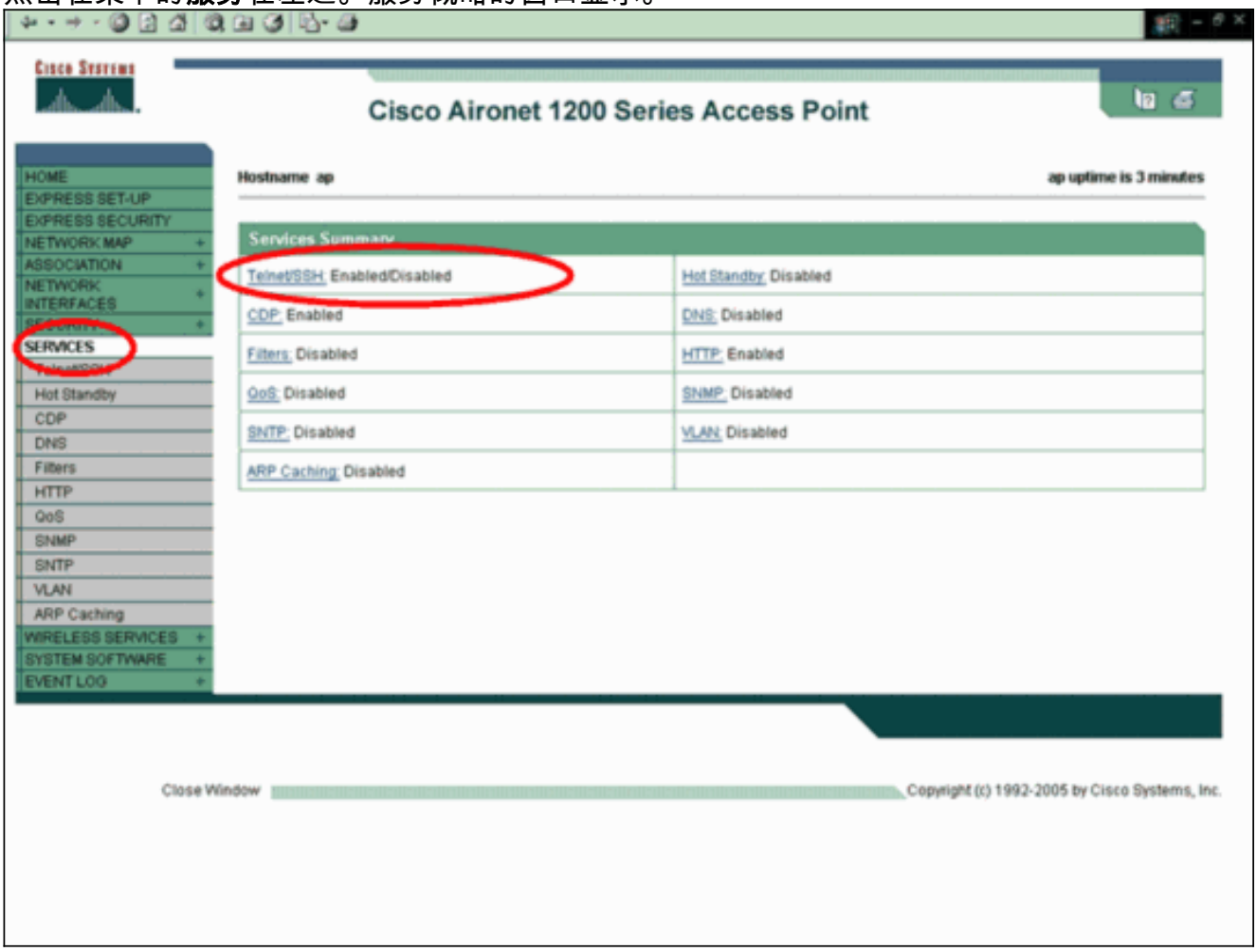
逐步指导

完成这些步骤：

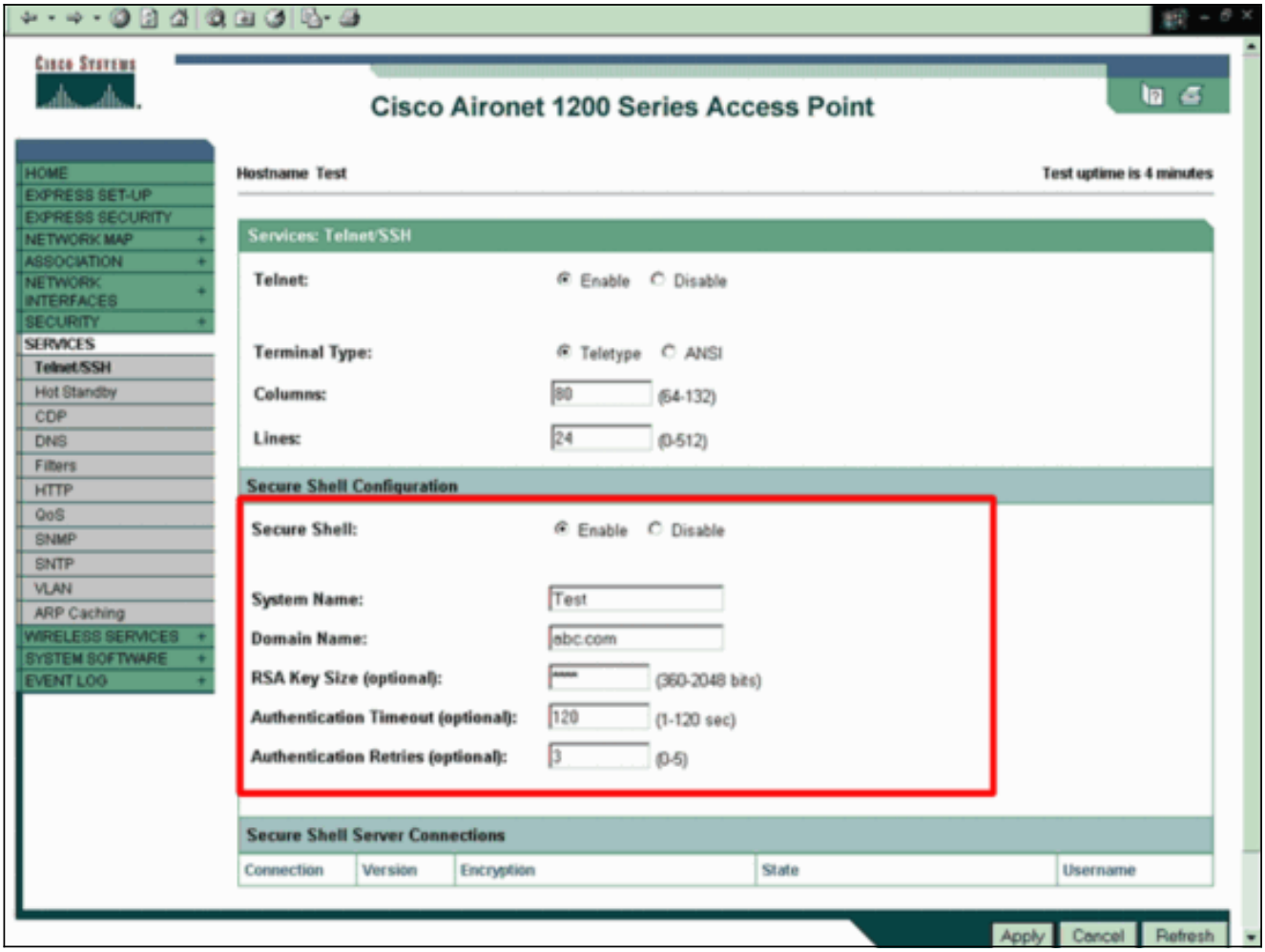
1. 登陆对AP通过浏览器。汇总状态窗口显示。



2. 点击在菜单的**服务**在左边。服务概略的窗口显示。



3. 点击**Telnet/SSH**为了启动并设定Telnet/SSH参数。服务：Telnet/SSH窗口显示。移下来到Secure Shell配置地区。点击在Secure Shell旁边的**Enable (event)**，并且输入SSH参数，此示例显示：此示例使用这些参数：系统名称：测验域名：abc.comRSA密钥大小：1024Authentication timeout:120身份认证重试：3



4. 单击 **Apply** 以保存更改。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ip ssh** —验证，如果SSH在AP启用并且使您检查在AP运行SSH的版本。此输出提供一个

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

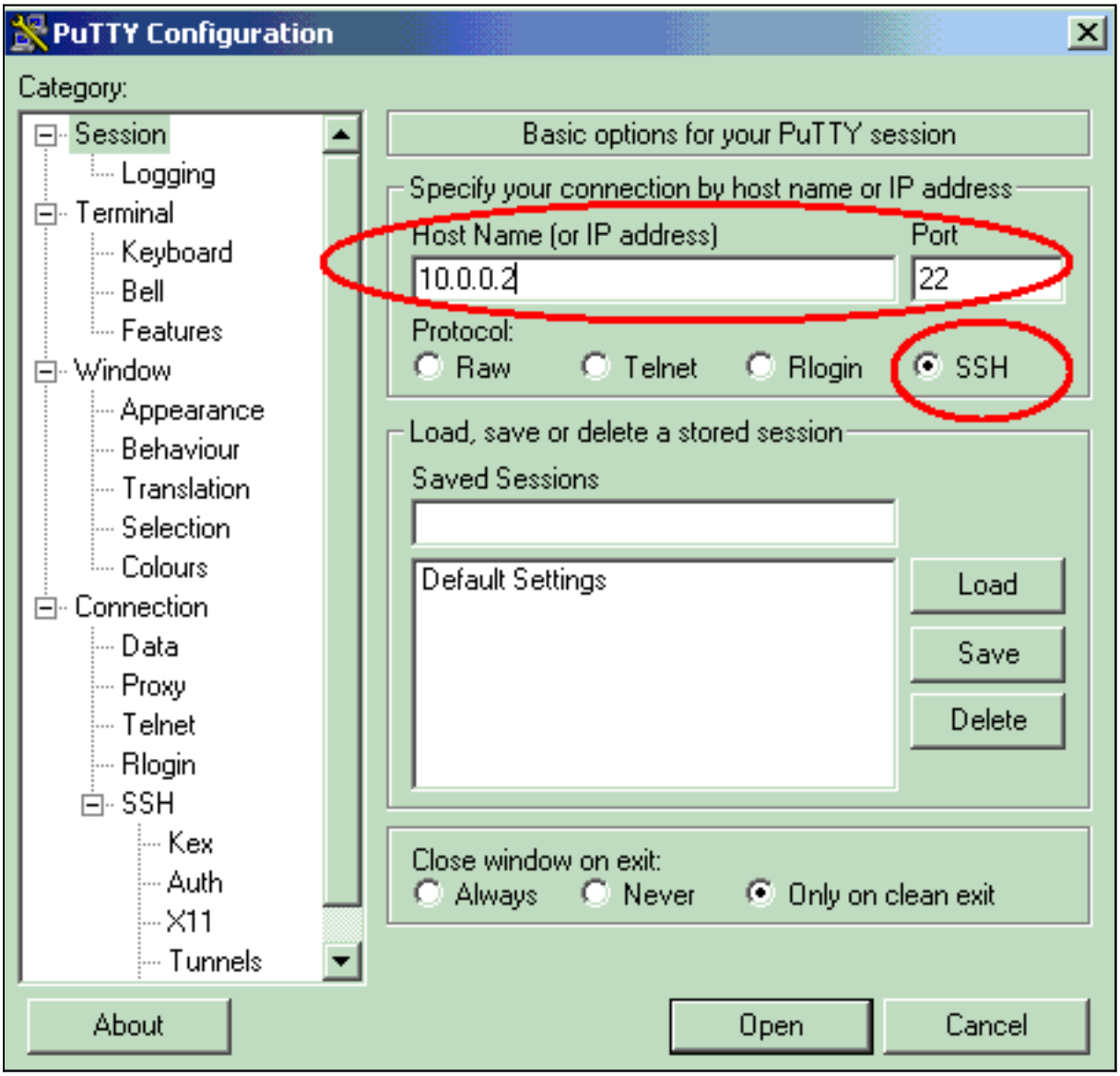
示例：

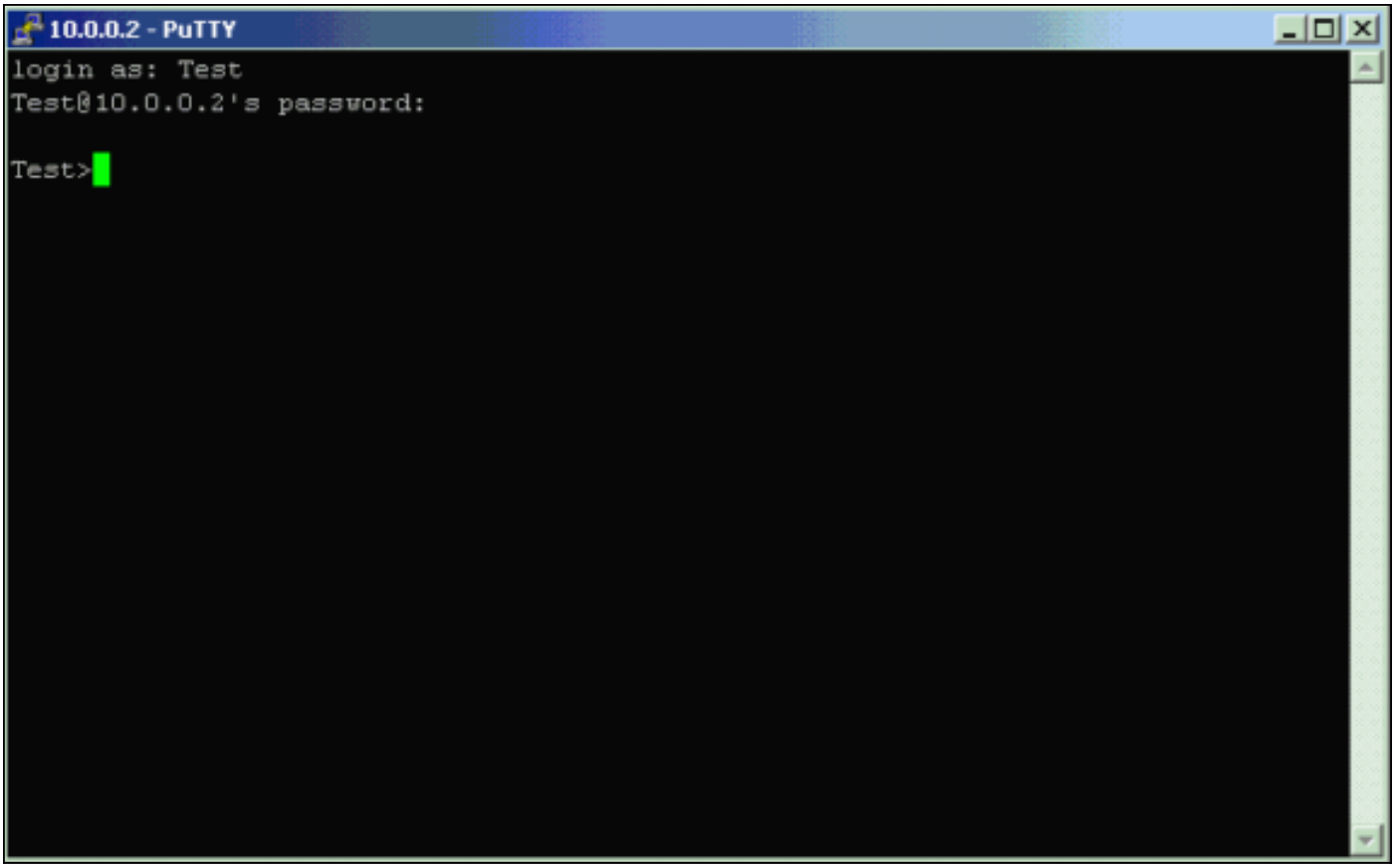
- **show SSH** —使您查看您的SSH服务器连接状况。此输出提供一个示例

```
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
```

:

现在，请通过运行第三方SSH软件的PC首次连接然后做出尝试登陆到AP。此验证使用AP IP地址，10.0.0.2。由于您配置用户名测验，请使用此命名为了通过SSH访问AP ：





故障排除

使用本部分可排除配置故障。

如果您的SSH配置命令拒绝作为非法指令，您未顺利地生成您的AP的一个RSA密钥对。参考配置可能的来源列表的本文的*故障排除提示*部分Secure Shell此问题的。

禁用SSH

为了禁用在AP的SSH，您必须删除在AP生成的RSA对。为了删除RSA对，请发出**crypto key zeroize rsa命令**在全局配置模式。当您删除RSA密钥对时，您自动地禁用SSH服务器。此输出提供一个示例：

```
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
```

相关信息

- **配置Secure Shell**
- **第一次配置接入点**
- **安全壳SSH支持页面**
- **无线支持页**

- 技术支持和文档 - Cisco Systems