Habilitação do Shell Seguro (ssh) em um Access Point (AP)

Índice

Introdução

Este documento explica como configurar um ponto de acesso (AP) para ativar o acesso baseado em Secure Shell (SSH).

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar o Cisco Aironet AP
- Conhecimento básico do SSH e de conceitos relacionados da Segurança

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 1200 Series AP de Aironet que executa o Software Release 12.3(8)JEB de Cisco IOS®
- PC ou portátil com utilidade do cliente SSH

Note: Este documento usa a utilidade do cliente SSH a fim verificar a configuração. Você pode usar todo o utilitário de cliente da terceira a fim entrar ao AP com o uso do SSH.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Alcançando o comando line interface(cli) em Aironet AP

Você pode usar qualquens um métodos a fim alcançar o comando line interface(cli) em Aironet AP:

- A porta de Console
- Telnet
- SSH

Se o AP tem uma porta de Console e você tem o acesso físico ao AP, você pode usar a porta de Console a fim entrar ao AP e mudar caso necessário a configuração. Para obter informações sobre de como usar a porta de Console a fim entrar ao AP, refira a *conexão ao 1200 Series que os Access point localmente* secionam do documento que configura o Access point pela primeira vez.

Se você pode somente alcançar o AP com os Ethernet, use o protocolo telnet ou o protocolo SSH a fim entrar ao AP.

O protocolo telnet usa a porta 23 para uma comunicação. O telnet transmite e recebe dados no texto claro. Porque a comunicação de dados acontece no texto claro, um hacker pode facilmente comprometer as senhas e alcançar o AP. O RFC 854 define o telnet e estende o telnet com opções por muitos outros RFC.

O SSH é um aplicativo e um protocolo que forneça uma substituição segura às r-ferramentas de Berkley. O SSH é um protocolo que forneça um seguro, conexão remota a uma camada 2 ou um dispositivo da camada 3. Há duas versões do SSH: Versão de SSH 1 e versão de SSH 2. Este suportes para o software release ambas as versões de SSH. Se você não especifica o número de versão, o AP opta a versão 2.

O SSH fornece mais Segurança para conexões remotas do que o telnet fornecendo a criptografia forte quando um dispositivo é autenticado. Esta criptografia é uma vantagem sobre uma sessão de Telnet, em que a comunicação acontece no texto claro. Para obter mais informações sobre do SSH, refira o Shell Seguro (ssh) FAQ. A característica SSH tem um servidor de SSH e um cliente integrado SSH. Os suportes ao cliente estes métodos de autenticação de usuário:

- RAIO (para mais informação, refira o acesso de controlo do Access point com seção do RAIO)
- Autenticação local e autorização (para mais informação, refira configurar o Access point para a seção da autenticação local e da autorização)

Para obter mais informações sobre do SSH, refira a parte 5, *"outros recursos de segurança" no manual de configuração do Cisco IOS Security para a Versão 12.3.*

Note: A característica SSH neste software release não apoia a Segurança IP (IPsec).

Você pode configurar AP para o SSH com o uso do CLI ou do GUI. Este documento explica ambos os métodos de configuração.

Configurar

Configuração de CLI

Nesta seção, você é presentado com a informação para configurar as características descritas neste documento com o uso do CLI.

Instruções passo a passo

A fim permitir SSH-baseou o acesso no AP, você primeiramente deve configurar o AP como um servidor de SSH. Siga estas etapas a fim configurar um servidor de SSH no AP do CLI:

1. Configurar um nome de host e um Domain Name para o 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. Gerencia uma chave de Rivest, de Shamir, e de Adelman (RSA) para seu AP.A geração de uma chave RSA permite o SSH no AP. Emita este comando no modo de configuração global:
   ```
   Test<config>#crypto key generate rsa rsa_key_size
   !--- This generates an RSA key and enables the SSH server.
   ```
   Note: O tamanho chave mínimo recomendado RSA é 1024.
3. Configurar a autenticação de usuário no AP.No AP, você pode configurar a autenticação de usuário para usar a lista local ou uma autenticação externa, uma autorização, e um server da contabilidade (AAA). Este exemplo usa uma lista localmente gerada a fim autenticar os usuários:
   ```
   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".
   ```
   Esta configuração configura o AP para executar a autenticação USER-baseada com o uso de um base de dados local que seja configurado no AP. O exemplo configura dois usuários no base de dados local, “teste” e “ABC”.
4. Configurar os parâmetros SSH.
   ```
   Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]}
   !--- Configure the SSH control variables on the AP.
   ```
   Note: Você pode especificar o intervalo nos segundos, mas não excede 120 segundos. O padrão é 120. Este ajuste aplica-se à fase de negociação SSH. Você pode igualmente especificar o número de novas tentativas da autenticação, mas não excede cinco novas tentativas da autenticação. O padrão é três.

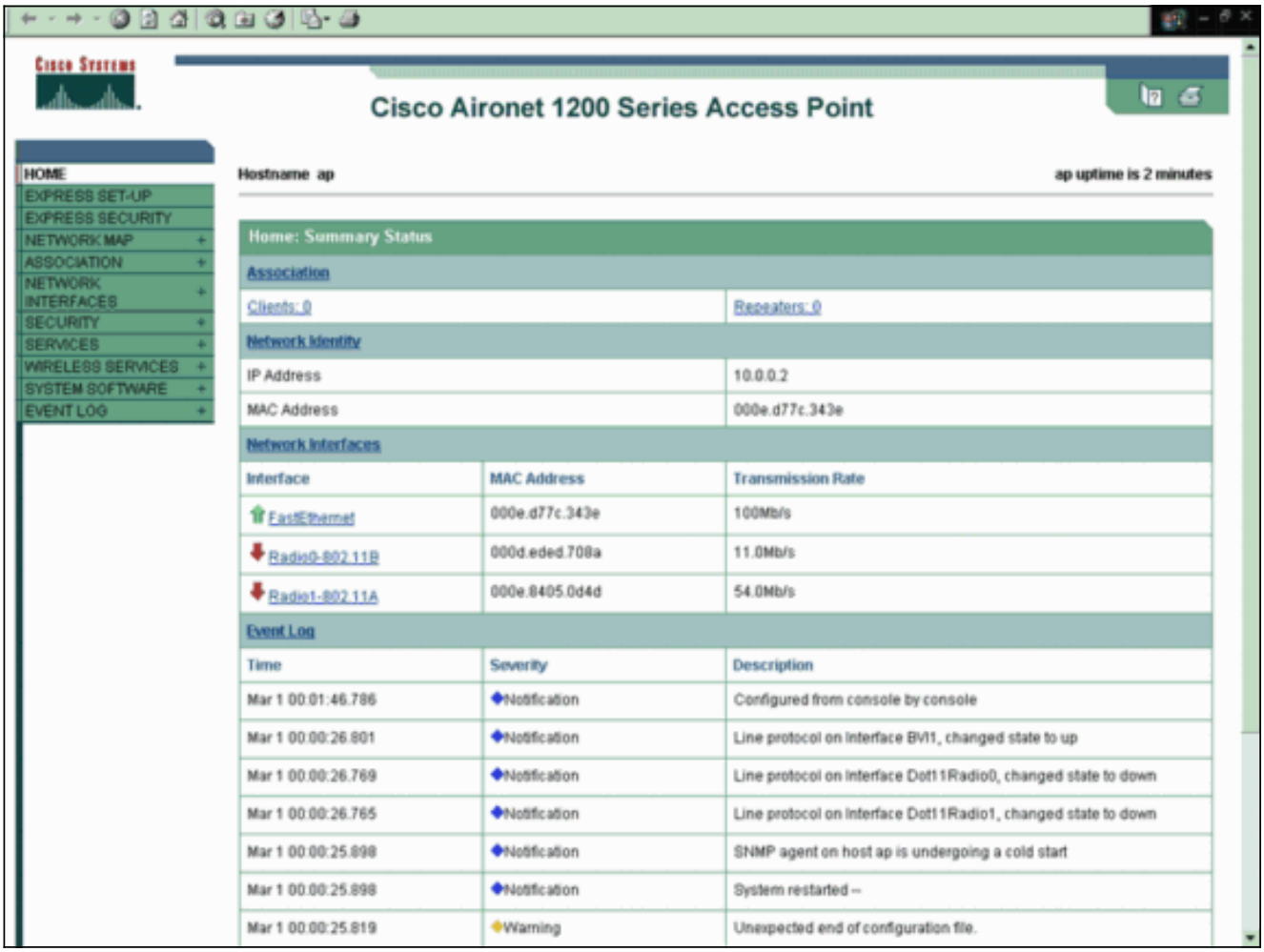
Configuração de GUI

Você pode igualmente usar o GUI a fim permitir o acesso SSH-baseado no AP.

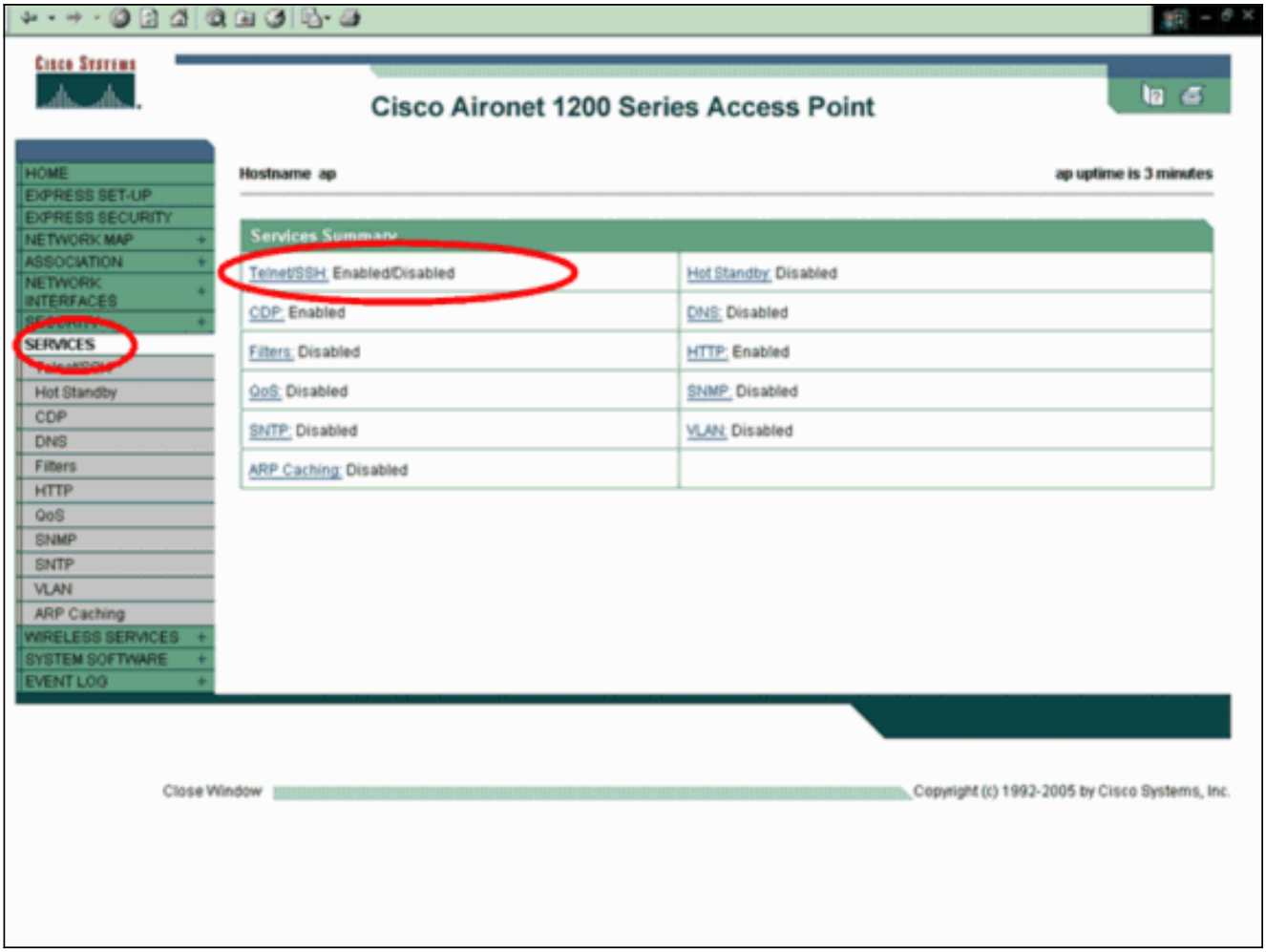
Instruções passo a passo

Conclua estes passos:

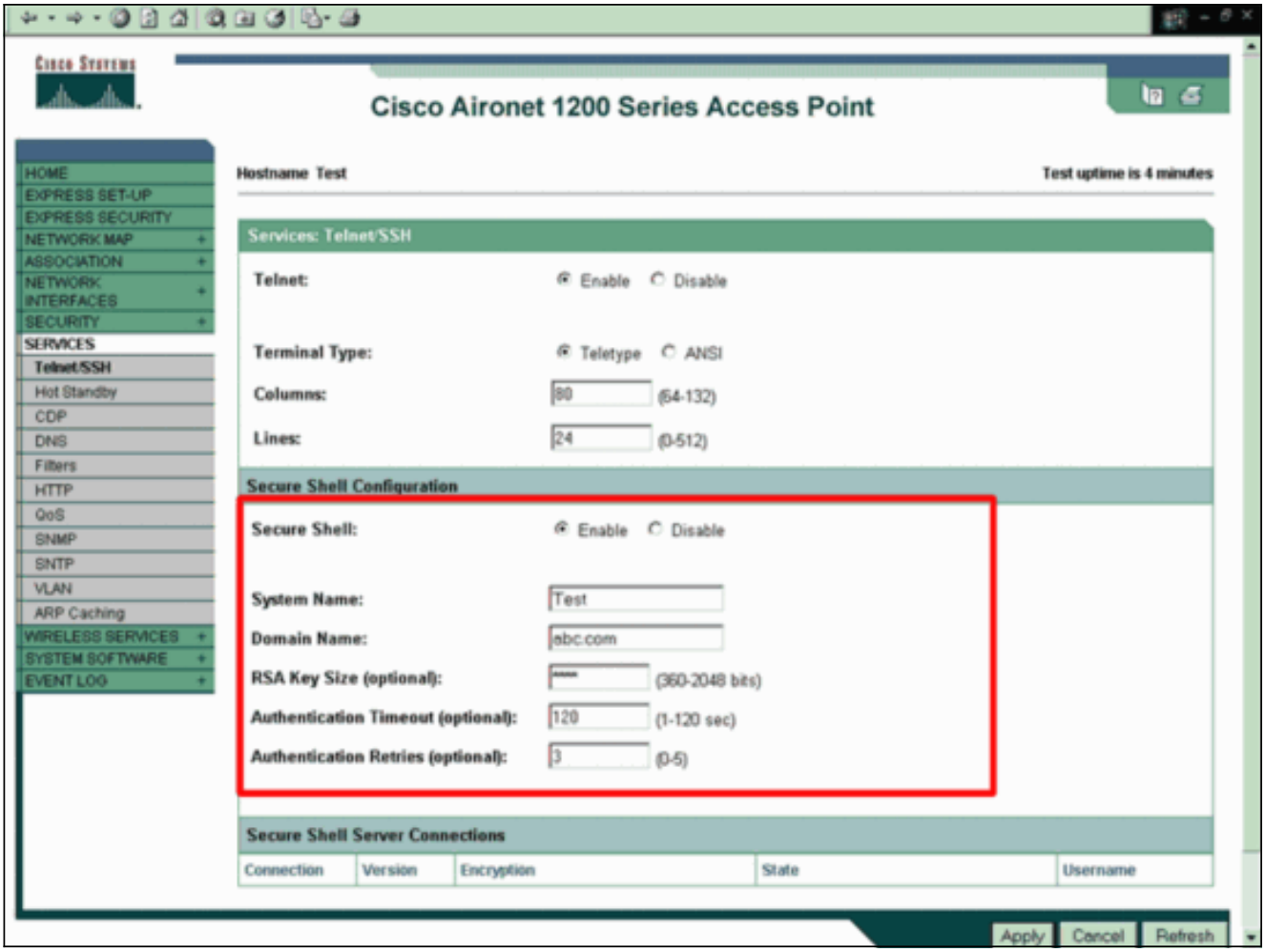
1. Entre ao AP através do navegador.Os indicadores do indicador do status sumário.



2. **Serviços do** clique no menu à esquerda.Os indicadores da janela de sumário dos serviços.



3. Clique o **telnet/SSH** a fim permitir e configurar os parâmetros do telnet/SSH.Os serviços: Indicadores do indicador do telnet/SSH. Enrole para baixo a área de configuração do Secure Shell. O clique **permite** ao lado do Secure Shell, e incorpora os parâmetros SSH enquanto este exemplo mostra:Este exemplo usa estes parâmetros:Nome de sistema: TesteDomain Name: abc.comTamanho chave RSA: 1024Intervalo da autenticação: 120Retries da autenticação:
   3



4. Clique em **Apply** para salvar as alterações.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o ssh IP** — Verifica se o SSH é permitido no AP e permite-o de verificar a versão do SSH que executa no AP. Esta saída fornece um

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

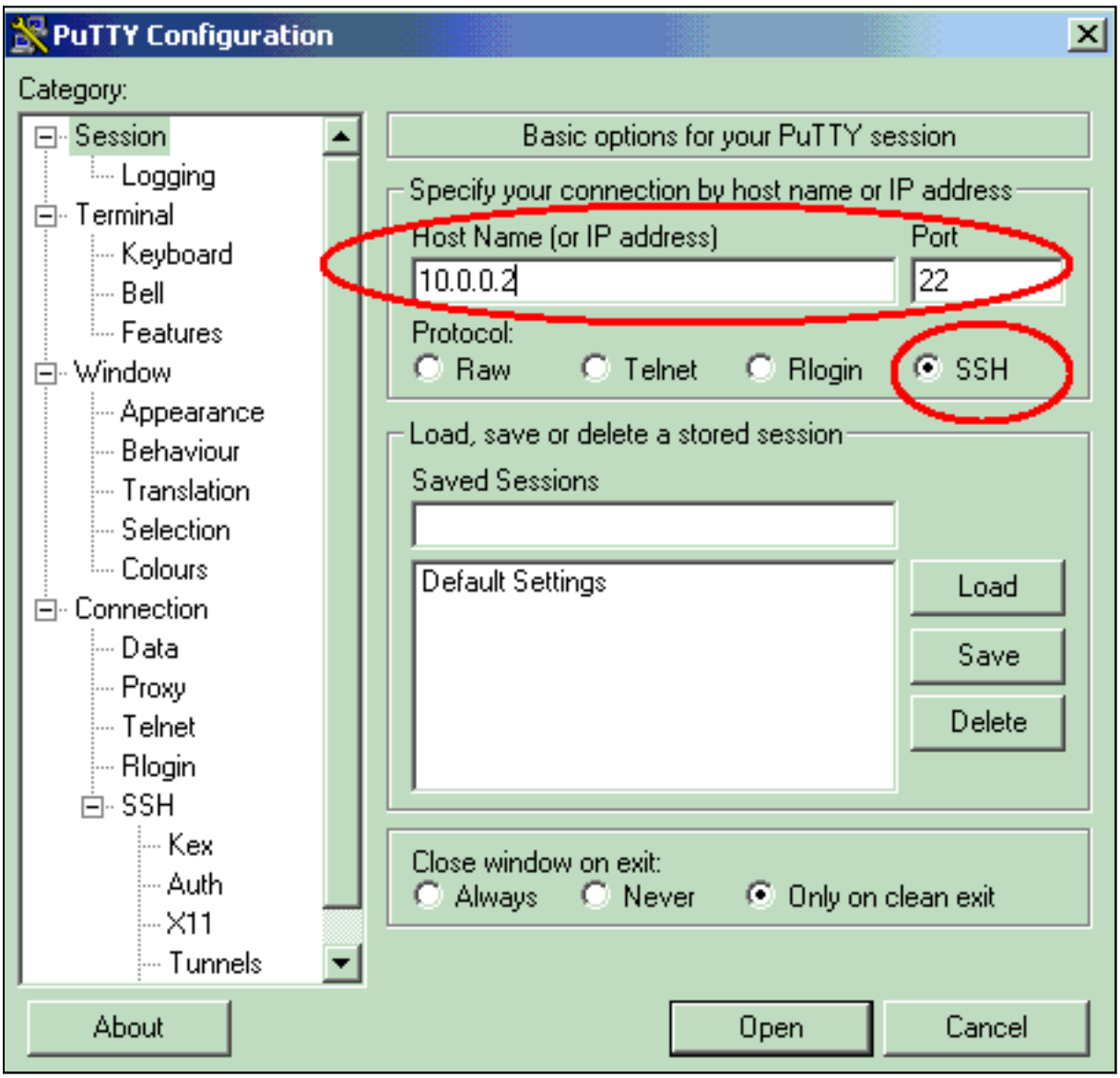
exemplo:

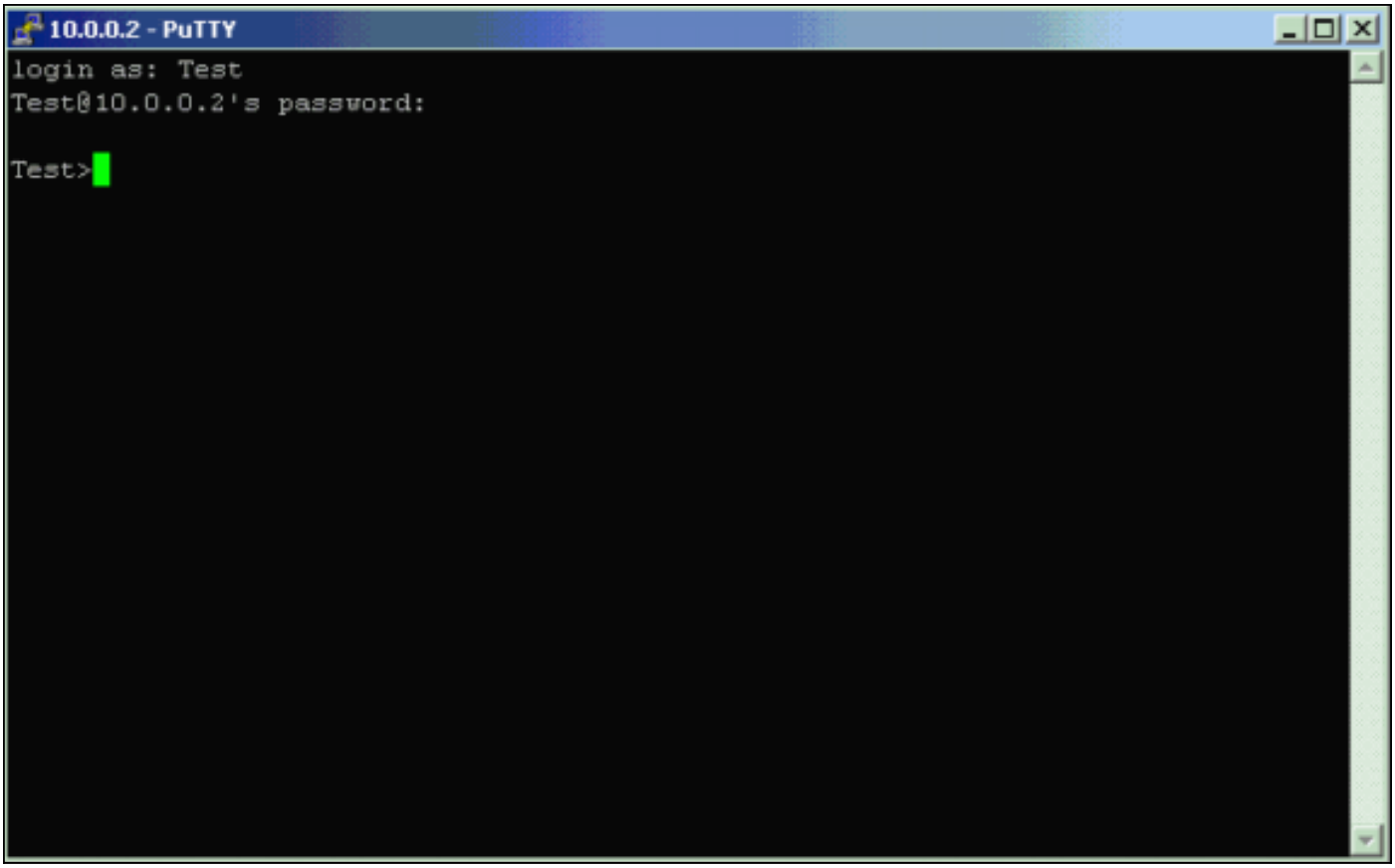
- **ssh da mostra** — Permite-o de ver o estado de suas conexões do servidor de SSH. Esta saída fornece um

```
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
```

exemplo:

Agora, inicie uma conexão com um PC que execute o software SSH da terceira e faça então uma tentativa de entrar ao AP. Esta verificação usa o endereço IP de Um ou Mais Servidores Cisco ICM NT AP, 10.0.0.2. Porque você configurou o teste do nome de usuário, use este nome a fim alcançar o AP com o SSH:





Troubleshooting

Use esta seção para resolver problemas de configuração.

Se seus comandos de configuração SSH são rejeitados como comandos ilegais, você não gerou com sucesso um par de chaves RSA para seu AP. Refira a seção dos *dicas de Troubleshooting do* Configuring Secure Shell do documento para uma lista de razões possíveis para este problema.

Desabilite o SSH

A fim desabilitar o SSH em um AP, você deve suprimir do par RSA que é gerado no AP. A fim suprimir dos pares RSA, emita o **comando crypto key zeroize rsa no** modo de configuração global. Quando você suprime do par de chaves RSA, você desabilita automaticamente o servidor de SSH. Esta saída fornece um exemplo:

```
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
```

Informações Relacionadas

- Configuring Secure Shell

- Configurando o Access point pela primeira vez
- Página de suporte do Shell Seguro (ssh)
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems