## Management Access for the SRX 210 Services Gateway

Telnet allows you to connect to the SRX 210 services gateway and access the Command Line Interface (CLI) to execute commands from a remote system. Telnet connections are not encrypted and therefore can be intercepted.

**NOTE:** Telnet access to the root user is prohibited. You must use more secure methods, such as SSH, to log in as root.

SSH provides the following features:

- Allows you to connect to the device and access the CLI to execute commands from a remote system
- Encrypts traffic so that it cannot be intercepted (unlike Telnet)
- Can be configured so that connections are authenticated by a digital certificate
- Uses public–private key technology for both connection and authentication

The SSH client software must be installed on the machine where the client application runs. If the SSH private key is encrypted (for greater security), the SSH client must be able to access the passphrase used to decrypt the key.

For information about obtaining SSH software, see http://www.ssh.com and http://www.openssh.com.

If you are using a JUNOScript server to configure and monitor devices, you can activate cleartext access on the device to allow unencrypted text to be sent directly over a TCP (Transmission Control Protocol) connection without using any additional protocol (such as SSH, SSL, or Telnet). For more information about the JUNOScript application programming interface (API), see the *JUNOScript API Guide*.

**NOTE:** Information sent in cleartext is not encrypted and therefore can be intercepted.

If the device is operating in a Common Criteria environment, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

**Related Topics**

- SRX 210 Services Gateway Basic Connectivity Overview
- Loopback Address for the SRX 210 Services Gateway
- Built-In Ethernet Port for the SRX 210 Services Gateway