

Chapter 2

Configuring JUNOS Software

To configure the JUNOS software, you must specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as some system hardware properties. After you have created a candidate configuration, you commit the configuration to be evaluated and activated by the JUNOS software.

This chapter discusses the following topics:

- Configuring the Software from External Devices on page 7
- Methods for Configuring JUNOS Software on page 8
- Configuring a Router for the First Time on page 10
- Managing Available Disk Space on page 17
- Using Software Monitoring Tools on page 18
- Router Security on page 19

Configuring the Software from External Devices

You can configure the router from a system console connected to the routing platform's console port or by using Telnet to access the router remotely. The router provides three ports on the craft interface for connecting external management devices to the Routing Engine and the JUNOS software:

- Console port—Connects a system console using an RS-232 serial cable.
- Auxiliary port—Connects a laptop or modem using an RS-232 serial cable.
- Ethernet management port—Connects the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for remote management through a PC or other client device. The Ethernet port is 10/100 megabits-per-second (Mbps) autosensing and requires an RJ-45 connector.

Methods for Configuring JUNOS Software

You can use any of the methods shown in Table 6 to configure JUNOS system software:

Table 6: Methods for Configuring JUNOS Software

| Method | Description |
|--|---|
| Command-line interface (CLI) | Create the configuration for the router using the CLI. You can enter commands from a single command line, and scroll through recently executed commands. |
| ASCII file | Load an ASCII file containing a router configuration that you created earlier, either on this system or on another system. You can then activate and run the configuration file, or you can edit it using the CLI and then activate it. |
| J-Web graphical user interface (GUI) | Use the J-Web graphical user interface (GUI) to configure the router. J-Web allows you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser. The J-Web GUI is preinstalled on J-series Services Routers and is an optional software package that can be installed on M-series and T-series routers. |
| JUNOScript application programming interface (API) | Use JUNOScript Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use the JUNOScript API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The JUNOScript API is customized for JUNOS software and operations in the API are equivalent to JUNOS CLI. |
| NETCONF application programming interface (API) | Use NETCONF Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use NETCONF API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The NETCONF API includes features that accommodate the configuration data models of multiple vendors. |
| Configuration commit scripts | Create scripts that run at commit time to enforce custom configuration rules. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT). |

This section contains complete descriptions of each method you can use to configure JUNOS system software:

- The JUNOS Command-Line Interface (CLI) on page 9
- The J-Web Package on page 9
- JUNOScript API Software on page 9
- NETCONF API Software on page 10
- Configuration Commit Scripts on page 10

The JUNOS Command-Line Interface (CLI)

The JUNOS CLI is a straightforward command interface. You use Emacs-style keyboard sequences to move around on a command line and scroll through a buffer that contains recently executed commands. You type commands on a single line, and the commands are executed when you press the **Enter** key. The CLI also provides command help and command completion. For more information about the CLI, see the *JUNOS CLI User Guide* and *JUNOS System Basics and Services Command Reference*.

The J-Web Package

As an alternative to entering CLI commands, JUNOS supports a J-Web graphical user interface (GUI). The J-Web user interface allows you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

The J-Web user interface is preinstalled on J-series Services Routers. It is provided as an optional, licensed software package (**jweb** package) on M-series and T-series routing platforms. The **jweb** package is not included in **jinstall** and **jbundle** software bundles. It must be installed separately. To install the package on M-series and T-series routing platforms, follow the procedure described in “Upgrading Individual Software Packages” on page 31.

J-Web supports weak (56-bit) encryption by default. This enables international customers to install J-Web and use HTTPS connections for J-Web access. Domestic customers can also install the **jcrypto** strong encryption package. This package automatically overrides the weak encryption. For more information about the J-Web GUI, see the *J-Web Interface User Guide*.



NOTE: Because the J-Web package is bundled separately from other packages, it is possible to have a version mismatch between J-Web and other JUNOS software packages you have installed.

To check for a version mismatch, use the **show system alarms** CLI command. If the version number does not match exactly, a system alarm appears. For example, if you install the 7.4R1.2 **jroute** package and the 7.4R1.1 **jweb** package, an alarm is activated. For more information on the **show system alarms** command, see the *JUNOS System Basics and Services Command Reference*.

JUNOScript API Software

The JUNOScript API is an Extensible Markup Language (XML) application that client applications use to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. This API is customized for JUNOS software, and operations in the API are equivalent to JUNOS CLI configuration mode commands. The JUNOScript API includes a set of Perl modules that enable client applications to communicate with a JUNOScript server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and JUNOScript API software, see the *JUNOScript API Guide*.

NETCONF API Software

The NETCONF API is an Extensible Markup Language (XML) application that client applications can use to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. This API is customized for JUNOS software, and includes features that accommodate the configuration data models of multiple vendors. The NETCONF API includes a set of Perl modules that enable client applications to communicate with a NETCONF server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and NETCONF API software, see the *NETCONF API Guide*.

Configuration Commit Scripts

You can create and use scripts that run at commit time to enforce custom configuration rules. If a configuration breaks the custom rules, the script can generate actions that the JUNOS software performs. These actions include:

- Generating custom error messages
- Generating custom warning messages
- Generating custom system log messages
- Making changes to the configuration

Configuration commit scripts also enable you to create macros, which expand simplified custom aliases for frequently used configuration statements into standard JUNOS configuration statements. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT). For more information, see the *JUNOS Configuration and Diagnostic Automation Guide*.

Configuring a Router for the First Time

On most JUNOS routing platforms, the JUNOS software is installed on the flash disk and on the hard disk. When you first turn on a routing platform, it runs the version of the JUNOS software installed on the flash. The copy of JUNOS software on the hard disk is a backup. Another backup copy of the JUNOS software is available on removable media, such as a PC Card or a compact flash card. Be sure to put the backup JUNOS software (on removable media) in a safe place.

When you turn on a routing platform the first time, the JUNOS software automatically boots and starts. You must enter basic configuration information so that the routing platform is on the network and you can log in to it over the network.

To configure the routing platform initially, you must connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default. Remote management access to the routing platform and all management access protocols, including Telnet, FTP, and SSH, are disabled by default.

When you first connect to the routing platform console, you must log in as the user **root**. At first, the root account requires no password. You see that you are the user **root** because the routing platform command prompt shows the username **root@#**.

You must start the JUNOS software command-line interface (CLI) using the command **cli**. The command prompt **root@>** indicates that you are the user **root** and that you are in the JUNOS software operational mode. Enter the JUNOS software configuration mode by typing the command **configure**. The command prompt **root@#** indicates that you are in the JUNOS software configuration mode.

When you first configure a routing platform, you must configure the following basic properties:

- Routing platform hostname
- Domain name
- IP address of the routing platform Ethernet management interface—**fxp0**
- IP address of a backup router
- The IP address of one or more DNS name servers on your network
- Password for the root account

To configure the software for the first time, follow these steps:

1. Connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default.
2. Power on the routing platform and wait for it to boot.

The JUNOS software boots automatically. The boot process is complete when you see the **login:** prompt on the console.

3. Log in as the user **root**.

Initially, the **root** user account requires no password. You can see that you are the **root** user because the prompt on the routing platform shows the username **root@#**.

4. Start the JUNOS software command-line interface (CLI):

```
root@# cli
root@>
```

5. Enter JUNOS software configuration mode:

```
cli> configure
[edit]
root@#
```

6. Configure the name of the routing platform (the routing platform hostname). We do not recommend spaces in the routing platform name. However, if the name does include spaces, enclose the entire name in quotation marks (" ").

```
[edit]
root@# set system host-name host-name
```

7. Configure the routing platform's domain name:

```
[edit]
root@# set system domain-name domain-name
```

8. Configure the IP address and prefix length for the router management Ethernet interface, `fxp0`. `fxp0` is an Ethernet management interface that provides a separate out-of-band management network for the router.

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

9. Configure the IP address of a backup or default routing platform. This device is called the backup router because it is used only while the routing protocol process is not running. Choose a router that is directly connected to the local routing platform by way of the management interface. The routing platform uses this backup router only when it is booting and only or when the JUNOS routing software (the routing protocol process, `rpd`) is not running.

For routing platforms with two Routing Engines, the backup Routing Engine, **RE1**, uses the backup router as a default gateway after the routing platform boots. This enables you to access the backup Routing Engine. (**RE0** is the default master Routing Engine.)

```
[edit]
root@# set system backup-router address
```

10. Configure the IP address of a DNS server. The routing platform uses the DNS name server to translate hostnames into IP addresses.

```
[edit]
root@# set system name-server address
```

11. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string. For more information about passwords, see "Specifying Plain-Text Passwords" on page 21.

Choose one of the following:

- a. To enter a clear-text password, use the following command:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

- b. To enter a password that is already encrypted, use the following command:

```
[edit]
root@# set system root-authentication encrypted-password
      encrypted-password
```

- c. To enter an SSH public key, use the following command:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

12. Optionally, display the configuration statements:

```
[edit]
root@ show
system {
  host-name host-name;
  domain-name domain.name;
  backup-router address;
  root-authentication {
    (encrypted-password "password" | public-key);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
  name-server {
    address;
  }
}
interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address address;
      }
    }
  }
}
}
```

13. Commit the configuration, which activates the configuration on the routing platform:

```
[edit]
root@# commit
```

After committing the configuration, you see the newly configured host name appear after the username in the prompt—for example, `user@host#`.

JUNOS software defaults are now set on the routing platform.

If you want to configure additional JUNOS software properties at this time, remain in the CLI configuration mode and add the necessary configuration statements. For more information about how to configure additional properties, see “Configuring Software Properties” on page 17 and the *JUNOS System Basics Configuration Guide*. You will need to commit your configuration changes to activate them on the routing platform.

14. Exit from the CLI configuration mode.

```
[edit]
root@host-name# exit
root@host-name>
```

15. Back up the configuration on the hard drive.

After you have installed the software on the routing platform, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the **request system snapshot** command to back up the new software to the `/altconfig` file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot device will be out of sync with the configuration on the primary boot device.

The **request system snapshot** command causes the root file system to be backed up to `/altroot`, and `/config` to be backed up to `/altconfig`. The root and `/config` file systems are on the routing platform's flash disk, and the `/altroot` and `/altconfig` file systems are on the routing platform's hard disk.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

Configuring a Router with Dual Routing Engines for the First Time

If a routing platform has dual Routing Engines, you must initially configure each routing platform independently. The sequence is irrelevant.

Configure the hostnames and addresses of the two Routing Engines using configuration groups in the `[edit groups]` hierarchy level. Use the reserved configuration group `re0` for the Routing Engine in slot 0 and `re1` for the Routing Engine in slot 1 to define properties specific to the individual Routing Engines. Configuring `re0` and `re1` groups lets both Routing Engines use the same configuration file.

Use the `apply-groups` statement to reproduce the configuration group information in the main part of the configuration.

The `commit synchronize` command commits the same configuration on both Routing Engines. The command makes the active or applied configuration the same for both Routing Engines with the exception of the groups, `re0` being applied to only `RE0` and `re1` being applied only to `RE1`. If you don't synchronize the configurations between two Routing Engines and one of them fails, the routing platform may end up in a very dysfunctional state since the backup Routing Engine may have a different configuration.

To initially configure a routing platform with dual Routing Engines, follow these steps in “Configure the First Routing Engine” on page 15 and “Configure the Second Routing Engine” on page 16.

Configure the First Routing Engine

1. Go to “Configuring a Router for the First Time” on page 10 and follow Steps 1 to 12 to initially configure the backup Routing Engine.
2. Instead of Step 6 and Step 8 in “Configuring a Router for the First Time” on page 10, configure a hostname for each Routing Engine and an IP address for each fxp0 management Ethernet interface as follows.

```
[edit]
root@# edit groups
[edit groups]
root@# set re0 system host-name router1
root@# set re0 interfaces fxp0 unit 0 family inet address 10.10.10.1/24
root@# set re0 system host-name router2
root@# set re1 interfaces fxp0 unit 0 family inet address 10.10.10.2/24
```

3. Set the loopback interface address for each Routing Engine.

```
[edit groups]
root@# set re0 interfaces lo0 unit 0 family inet address 2.2.2.1/32
root@# set re1 interfaces lo0 unit 0 family inet address 2.2.2.2/32
```

4. Configure the `apply-groups` statement to reproduce the configuration group information to the main part of the configuration.

```
[edit groups]
root@# top
[edit]
root@# set apply-groups [re0 re1]
```

5. Configure Routing Engine redundancy.

```
[edit]
root@# set chassis redundancy routing-engine 0 master
root@# set chassis redundancy routing-engine 1 backup
root@# set chassis redundancy routing-engine graceful-switchover enable
```

6. Save the configuration change on both Routing Engines

```
[edit]
user@host> commit
root@#
```

- After you have installed the new software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software on both master and backup Routing Engines.

```
{master}
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the routing platform's flash disk, and the `/altroot` and `/altconfig` file systems are on the routing platform's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software because the running copy, and backup copy of the software are identical.

Configure the Second Routing Engine

- Connect to the second Routing Engine and repeat the steps in “Configure the First Routing Engine” on page 15 to configure the second Routing Engine.

JUNOS Software Default Settings That Protect the Router

The following JUNOS default software settings protect against common router security weaknesses:

- The JUNOS software does not forward directed broadcast messages. Directed broadcast services send ping requests from a spoofed source address to a broadcast address and can be used to attack other Internet users. For example, if broadcast ping messages were allowed on the `200.0.0.0/24` network, a single ping request could result in up to 254 responses to the supposed source of the ping. The source would actually become the victim of a denial-of-service (DoS) attack.
- Only console access to the router is enabled by default. Remote management access to the router and all management access protocols, including Telnet, FTP, and SSH (Secure Shell), are disabled by default.
- The JUNOS software does not support the SNMP set capability for editing configuration data. While the software supports the SNMP set capability for monitoring and troubleshooting the network, this support exposes no known security issues. (You can configure the software to disable this SNMP set capability.)
- The JUNOS software ignores martian addresses that contain the following prefixes: `0.0.0.0/8`, `127.0.0.0/8`, `128.0.0.0/16`, `191.255.0.0/16`, `192.0.0.0/24`, `223.255.55.0/24`, and `240.0.0.0/4`. Martian addresses are reserved host or network addresses about which all routing information should be ignored.

Configuring Software Properties

After completing the initial minimal configuration, you can configure software properties. If you configure the software interactively using the CLI, you enter software configuration statements to create a candidate configuration that contains a hierarchy of statements. At any hierarchy level, you generally can enter statements in any order. While you are configuring the software, you can display all or portions of the candidate configuration, and you can insert or delete statements. Any changes you make affect only the candidate configuration, not the active configuration that is running on the router. For information about using the CLI and committing the current configuration, see the *JUNOS CLI User Guide*.

The configuration hierarchy logically groups related functions, which results in configuration statements that have a regular, consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy. For more information about the JUNOS hierarchy, see the *JUNOS Hierarchy and RFC Reference*.

At each level of the hierarchy, you can display a list of the statements available at that level, along with short descriptions of the statements' functions. To have the CLI complete the statement name if it is unambiguous or to provide a list of possible completions, you can type a partial statement name followed by a space or tab.

More than one user can edit a router's configuration simultaneously. All changes made by all users are visible to everyone editing the configuration. For more information, see the *JUNOS CLI User Guide*.

Activating a Configuration

To have a candidate configuration take effect, you commit the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

The CLI always maintains a copy of previously committed versions of the software configuration. If you need to return to a previous configuration, you can do this from within the CLI. For more information, see the *JUNOS CLI User Guide*.

Managing Available Disk Space

A software installation or upgrade may fail if your router has a shortage of disk space. If a disk space error occurs, use one or more of the following options to complete the installation:

- Use the `request system storage cleanup` command to delete unnecessary files and increase storage space on the router.
- Specify the `unlink` option when you use the `request system software add` command to install the JUNOS software:
 - On the J-series platform, the `unlink` option removes the software package at the earliest opportunity to create enough disk space for the installation to finish.

- On the M-series and T-series platforms, the `unlink` option removes the software package after a successful upgrade.
- Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. The download program provides intelligent disk space management to enable installation.



NOTE: If you are upgrading the J-series router from a remote location, the installation program automatically checks for enough disk space for the process to finish.

For more information on the `request system storage cleanup` command and the `request system software add` command, see the *JUNOS System Basics and Services Command Reference*.

Using Software Monitoring Tools

The primary method of monitoring and troubleshooting the software, routing protocols, network connectivity, and the router hardware is to enter commands from the CLI. The CLI enables you to display information in the routing tables and routing protocol-specific data, and to check network connectivity using `ping` and `traceroute` commands.

The J-Web graphical user interface (GUI) is a Web-based alternative to using CLI commands to monitor, troubleshoot, and manage the router. For more information about J-Web, see “The J-Web Package” on page 9.

The JUNOS software includes SNMP software, which allows you to manage routers. The SNMP software consists of an SNMP master agent and a MIB II agent, and supports MIB II SNMP version 1 traps and version 2 notifications, SNMP version 1 `Get` and `GetNext` requests, and version 2 `GetBulk` requests. For more information, see the *JUNOS Network Management Configuration Guide*.

The software also supports tracing and logging operations so that you can track events that occur in the router—both normal router operations and error conditions—and track the packets that are generated by or pass through the router. Logging operations use a `syslog`-like mechanism to record system-wide, high-level operations, such as interfaces going up or down and users logging in to or out of the router. Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions.

Router Security

Router security consists of three major elements: physical security of the router, operating system security, and security that can be effected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console. The inherent security of the JUNOS operating system also plays an important role in router security. The JUNOS software is extremely stable and robust. The JUNOS software also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

This section discusses some JUNOS software features available to improve router security:

- Router Access on page 19
- User Authentication on page 20
- Specifying Plain-Text Passwords on page 21
- Routing Protocol Security Features on page 22
- Firewall Filters on page 22
- Auditing for Security on page 22

Router Access

When you first install the JUNOS software, all remote access to the router is disabled, thereby ensuring that remote access is possible only if deliberately enabled by an authorized user. You can establish remote communication with a router in one of the following ways:

- Out-of-band management—Allows connection to the router through an interface dedicated to router management. Juniper Networks routing platforms support out-of-band management with a dedicated management Ethernet interface (`fxp0`), as well as EIA-232 console and auxiliary ports. The management Ethernet interface connects directly to the Routing Engine. No transit traffic is allowed through this interface, providing complete separation of customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the router.
- Inband management—Allows connection to the routers using the same interfaces through which customer traffic flows. While this approach is simple and requires no dedicated management resources, it has some disadvantages:
 - Management flows and transit traffic flows are mixed together. Any attack traffic that is mixed with the normal traffic can affect the communication with the router.
 - The links between router components might not be totally trustworthy, leading to the possibility of wiretapping and replay attacks.

For management access to the router, the standard ways to communicate with the router from a remote console are with Telnet and SSH. SSH provides secure encrypted communications and is therefore useful for inband router management. Telnet provides unencrypted, and therefore less secure, access to the router. For more information about router access, see the *JUNOS System Basics Configuration Guide*.

User Authentication

On a router, you can create local user login accounts to control who can log into the router and the access privileges they have. A password, either an SSH key or a Message Digest 5 (MD5) password, is associated with each login account. To define access privileges, you create login classes into which you group users with similar jobs or job functions. You use these classes to explicitly define what commands their users are and are not allowed to issue while logged in to the router.

The management of multiple routers by many different personnel can create a user account management problem. One solution is to use a central authentication service to simplify account management, creating and deleting user accounts only on a single, central server. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks (attacks in which someone uses a captured password to pose as a router administrator).

The JUNOS software supports two protocols for central authentication of users on multiple routers:

- Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).
- RADIUS, a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS. For more information about configuring user access, see the *JUNOS System Basics Configuration Guide*.

The JUNOS software also supports the following authentication methods:

- Internet Protocol Security (IPSec). IPSec architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). For more information about IPSec, see the *JUNOS Services Interfaces Configuration Guide*.
- MD5 authentication of MSDP peering sessions. This authentication provides protection against spoofed packets being introduced into a peering session. For more information about SNMPv3, see the *JUNOS Multicast Protocols Configuration Guide*.
- SNMPv3 authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules. For more information about SNMPv3, see the *JUNOS Network Management Configuration Guide*.

Specifying Plain-Text Passwords

The JUNOS software has special requirements when you create plain-text passwords on a routing platform. The default requirements for plain-text passwords are as follows:

- The password must be between 6 and 128 characters long
- You can include uppercase letters, lowercase letters, numbers, punctuation marks, and any of the following special characters:

! @ # \$ % ^ & * , + = < > : ;

Control characters are not recommended.

- The password must contain at least one change of case or character class.

You can change the requirements for plain-text passwords. For more information, see the *JUNOS System Basics Configuration Guide*.

You can include the `plain-text-password` statement at the following hierarchy levels.

- [edit system diag-port-authentication]
- [edit system pic-console-authentication]
- [edit system root-authentication]
- [edit system login user *username* authentication]

Table 7 lists error messages that appear when you enter an invalid plain-text password.

Table 7: Plain-Text Password Error Messages

| Error message | Problem with password |
|---|---|
| The minimum password length is <i>number</i> . (<i>number</i> is the default length configured.) | Too few characters; for example, abC. |
| Require additional changes of case, numbers or punctuation | Does not include the required changes of case, numbers or special characters; for example, abcdefg. |
| Passwords are not equal; aborting | Does not match the original password. |

For more information about how to create plain-text passwords, see the *JUNOS System Basics Configuration Guide*.

Routing Protocol Security Features

The main task of a router is to forward user traffic toward its intended destination based on the information in the router's routing and forwarding tables. You can configure routing policies that define the flows of routing information through the network, controlling which routes the routing protocols place in the routing tables and which routes they advertise from the tables. You can also use routing policies to change specific route characteristics, change the BGP route flap-damping values, perform per-packet load balancing, and enable class of service (CoS).

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which can degrade the functionality of the router. To prevent such attacks, you must ensure that routers form routing protocol peering or neighboring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The JUNOS BGP, IS-IS, OSPF, RIP, and RSVP protocols support HMAC-MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

The JUNOS software supports the IPSec security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. The JUNOS software also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

Firewall Filters

Firewall filters allow you to control packets transiting the router to a network destination and packets destined for and sent by the router. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and the Routing Engine. Firewall filters provide a means of protecting your router from excessive traffic. Firewall filters that control local packets can also protect your router from external aggressions, such as DoS attacks.

To protect the Routing Engine, you can configure a firewall filter only on the router's loopback interface. Adding or modifying filters for each interface on the router is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine. For more information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

Auditing for Security

The JUNOS software logs significant events that occur on the router and within the network. Although logging itself does not increase security, you can use the system logs to monitor the effectiveness of your security policies and router configurations. You can also use the logs when reacting to a continued and deliberate attack as a means of identifying the source address, router, or port of the attacker's traffic. You can configure the logging of different levels of events, from only critical events to all events, including informational events. You can then inspect the contents of the system log files either in real time or later.

Debugging and troubleshooting are much easier when the timestamps in the system log files of all routers are synchronized, because events that span the network might be correlated with synchronous entries in multiple logs. The JUNOS software supports the Network Time Protocol (NTP), which you can enable on the router to synchronize the system clocks of routers and other networking equipment. By default, NTP operates in an unauthenticated mode. You can configure various types of authentication, including an HMAC-MD5 scheme. For more information about system logging, see the *JUNOS System Basics Configuration Guide* and the *JUNOS System Log Messages Reference*.

