

Chapter 18

System Management Overview

The JUNOS software provides a variety of parameters that allow you to configure system management functions, including the router's hostname, address, and domain name; the addresses of Domain Name System (DNS) servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; and properties of the router's auxiliary and console ports.

This chapter discusses the following topics, which provide background information related to configuring system management:

- Specifying IP Addresses, Network Masks, and Prefixes on page 356
- Specifying Filenames and URLs on page 356
- Directories on the Router on page 357
- Tracing and Logging Operations on page 358
- Configuring Protocol Authentication on page 360
- Configuring User Authentication on page 360

Specifying IP Addresses, Network Masks, and Prefixes

Many statements in the JUNOS software configuration include an option to specify an IP address or route prefix. In this manual, this option is represented in one of the following ways:

- *network/prefix-length*—Network portion of the IP address, followed by a slash and the destination prefix length (previously called the subnet mask). For example, `10.0.0.1/8`.
- *network*—IP address. For example, `10.0.0.2`.
- *destination-prefix/prefix-length*—Route prefix, followed by a slash and the destination prefix length. For example, `192.168.1.10/32`.

You enter all IP addresses in classless mode. You can enter the IP address with or without a prefix length, in standard dotted notation (for example, `1.2.3.4`), or hexadecimal notation as a 32-bit number in network-byte order (for example, `0x01020304`). If you omit any octets, they are assumed to be zero. Specify the prefix length as a decimal number in the range from 1 through 32.

Specifying Filenames and URLs

In some command-line interface (CLI) commands and configuration statements—including `file copy`, `file archive`, `load`, `save`, `set system login user username authentication load-key-file`, and `request system software add`—you can include a filename. On a routing matrix, you can include chassis information; for example, `lcc0`, `lcc0-re0`, or `lcc0-re1`, as part of the file name. A routing matrix is a multichassis architecture composed of one TX Matrix platform, to which you can connect from one to four T640 routing nodes. For more information about the routing matrix, see “TX Matrix Platform and T640 Routing Node Configuration Guidelines” on page 812 and the *TX Matrix Platform Hardware Guide*.

You can specify a filename or URL in one of the following ways:

- *filename*—File in the user’s current directory on the local flash drive. You can use wildcards to specify multiple source files or a single destination file. Wildcards are not supported in Hypertext Transfer Protocol (HTTP) or FTP. For more information about how to use wildcards, see “Using Wildcards” on page 600.



NOTE: Wildcards are supported only by the `file` (`compare` | `copy` | `delete` | `list` | `rename` | `show`) commands. When you issue the `file show` command with a wildcard, it must resolve to one filename.

- *path/filename*—File on the local flash disk.
- */var/filename* or */var/path/filename*—File on the local hard disk. You can also specify a file on a local Routing Engine for a specific T640 routing node on a routing matrix:

```
user@host> file delete lcc0-re0:/var/tmp/junk
```

- *a:filename* or *a:path/filename*—File on the local drive. The default path is / (the root-level directory). The removable media can be in MS-DOS or UNIX (UFS) format.
- *hostname:/path/filename*, *hostname:filename*, *hostname:path/filename*, or *scp://hostname/path/filename*—File on an scp/ssh client. This form is not available in the worldwide version of the JUNOS software. The default path is the user's home directory on the remote system. You can also specify *hostname* as *username@hostname*.
- *ftp://hostname/path/filename*—File on an FTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. The default path is the user's home directory. To specify an absolute path, the path must start with %2F; for example, *ftp://hostname/%2Fpath/filename*. To have the system prompt you for the password, specify **prompt** in place of the password. If a password is required, and you do not specify the password or **prompt**, an error message is displayed:

```
user@host> file copy ftp://username@ftp.hostname.net//filename
file copy ftp.hostname.net: Not logged in.
user@host> file copy ftp://username:prompt@ftp.hostname.net//filename
Password for username@ftp.hostname.net:
```

- *http://hostname/path/filename*—File on an HTTP server. You can also specify *hostname* as *username@hostname* or *username:password@hostname*. If a password is required and you omit it, you are prompted for it.
- *re0:/path/filename* or *re1:/path/filename*—File on a local Routing Engine. You can also specify a file on a local Routing Engine for a specific T640 routing node on a routing matrix:

```
user@host> show log 1cc0-re1:chassisd
```

Directories on the Router

JUNOS software files are stored in the following directories on the router:

- */altconfig*—When you back up the currently running and active file system partitions on the router to standby partitions using the **request system snapshot** command, the */config* directory is backed up to */altconfig*. Normally, the */config* directory is on the flash drive and */altconfig* is on the hard disk.
- */altroot*—When you back up the currently running and active file system partitions on the router to standby partitions using the **request system snapshot** command, the root file system (/) is backed up to */altroot*. Normally, the root directory is on the flash drive and */altroot* is on the hard disk.

- `/config`—This directory is located on the primary boot device, that is, on the drive from which the router booted (generally the flash drive, device `wd0`). This directory contains the current operational router configuration and the last three committed configurations, in the files `juniper.conf`, `juniper.conf.1`, `juniper.conf.2`, and `juniper.conf.3`, respectively.
- `/var`—This directory is always located on the hard disk (device `wd2`). It contains the following subdirectories:
 - `/var/home`—Contains users' home directories, which are created when you create user access accounts. For users using SSH authentication, their `.ssh` file, which contains their SSH key, is placed in their home directory. When a user saves or loads a configuration file, that file is loaded from their home directory unless the user specifies a full pathname.
 - `/var/db/config`—Up to six additional previous versions of committed configurations, which are stored in the files `juniper.conf.4` through `juniper.conf.9`.
 - `/var/log`—Contains system log and tracing files.
 - `/var/tmp`—Contains core files. The software saves the current core file (0) and the four previous core files, which are numbered from 1 through 4 (from newest to oldest).

Each router ships with removable media (device `wfd0`) that contains a backup copy of the JUNOS software.

Tracing and Logging Operations

Tracing and logging operations allow you to track events that occur in the router—both normal router operations and error conditions—and to track the packets that are generated by or passed through the router. The results of tracing and logging operations are placed in files in the `/var/log` directory on the router.

Logging operations use a system logging mechanism similar to the UNIX `syslogd` utility to record systemwide, high-level operations, such as interfaces going up or down and users logging in to or out of the router. You configure these operations by using the `syslog` statement at the `[edit system]` hierarchy level, as described in “Configuring System Log Messages” on page 421, and by using the `options` statement at the `[edit routing-options]` hierarchy level, as described in the *JUNOS Routing Protocols Configuration Guide*.

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. You configure tracing operations using the `traceoptions` statement. You can define tracing operations in different portions of the router configuration:

- Global tracing operations—Define tracing for all routing protocols. You define these tracing operations at the `[edit routing-options]` hierarchy level of the configuration. For more information, see the *JUNOS Routing Protocols Configuration Guide*.
- Protocol-specific tracing operations—Define tracing for a specific routing protocol. You define these tracing operations in the `[edit protocol]` hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global `traceoptions` statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.
- Tracing operations within individual routing protocol entities—Some protocols allow you to define more granular tracing operations. For example, in Border Gateway Protocol (BGP), you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.
- Interface tracing operations—Define tracing for individual router interfaces and for the interface process itself. You define these tracing operations at the `[edit interfaces]` hierarchy level of the configuration as described in the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

Configuring Protocol Authentication

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- Simple authentication (IS-IS, OSPF, and RIP)—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you *not* use this authentication method.
- MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (“ ”).

JUNOS-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If JUNOS-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

Configuring User Authentication

The JUNOS software supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router, and the server runs on a remote network system.

You can configure the router to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the JUNOS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.