



---

Junos<sup>®</sup> OS

## Getting Started Guide for Routing Devices

Release  
15.1



---

Modified: 2016-11-08

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Junos<sup>®</sup> OS Getting Started Guide for Routing Devices*

15.1

Copyright © 2016, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Supported Platforms . . . . .	ix
	Using the Examples in This Manual . . . . .	ix
	Merging a Full Example . . . . .	x
	Merging a Snippet . . . . .	x
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiii
	Opening a Case with JTAC . . . . .	xiv
<b>Chapter 1</b>	<b>Accessing a Junos OS Device . . . . .</b>	<b>15</b>
	Understanding the Console Port . . . . .	15
	Accessing a Junos OS Device the First Time . . . . .	16
<b>Chapter 2</b>	<b>Configuring the Root Password . . . . .</b>	<b>19</b>
	Understanding the Root Password . . . . .	19
	Protecting Network Security by Configuring the Root Password . . . . .	20
	Recovering the Root Password . . . . .	22
<b>Chapter 3</b>	<b>Configuring the Hostname . . . . .</b>	<b>25</b>
	Understanding Hostnames . . . . .	25
	Configuring the Hostname of a Router or Switch by Using a Configuration Group . . . . .	26
<b>Chapter 4</b>	<b>Configuring DNS . . . . .</b>	<b>29</b>
	DNS Overview . . . . .	29
	DNS Components . . . . .	29
	DNS Server Caching . . . . .	29
	Reaching a Domain Name System Server . . . . .	30
	Example: Configuring the TTL Value for DNS Server Caching . . . . .	32
	Example: Configuring the Unique Identity of a Router for Making it Accessible on the Network . . . . .	33
<b>Chapter 5</b>	<b>Configuring Management and Loopback Interfaces . . . . .</b>	<b>37</b>
	Understanding Management Ethernet Interfaces . . . . .	37
	Configuring a Management Interface on a Dedicated Management Port . . . . .	39
	Understanding the Loopback Interface . . . . .	40
	Configuring a Loopback Interface . . . . .	41

<b>Chapter 6</b>	<b>Configuring User Accounts . . . . .</b>	<b>43</b>
	Understanding User Accounts . . . . .	43
	Configuring Junos OS User Accounts by Using a Configuration Group . . . . .	44
	Enabling Remote Access . . . . .	47
<b>Chapter 7</b>	<b>Configuring Backup Routers . . . . .</b>	<b>49</b>
	Understanding Backup Routers . . . . .	49
	Configuring a Backup Router . . . . .	50
	Configuring a Backup Router Running IPv4 . . . . .	51
	Configuring a Backup Router Running IPv6 . . . . .	52
<b>Chapter 8</b>	<b>Index . . . . .</b>	<b>55</b>
	Index . . . . .	57

# List of Figures

<b>Chapter 1</b>	<b>Accessing a Junos OS Device . . . . .</b>	<b>15</b>
	Figure 1: Connecting to the Console Port on a Junos OS Device . . . . .	16
<b>Chapter 7</b>	<b>Configuring Backup Routers . . . . .</b>	<b>49</b>
	Figure 2: Backup Router Sample Topology . . . . .	51



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>ix</b>
	Table 1: Notice Icons . . . . .	xi
	Table 2: Text and Syntax Conventions . . . . .	xii
<b>Chapter 4</b>	<b>Configuring DNS . . . . .</b>	<b>29</b>
	Table 3: Values to Use in Example . . . . .	34



# About the Documentation

- [Documentation and Release Notes on page ix](#)
- [Supported Platforms on page ix](#)
- [Using the Examples in This Manual on page ix](#)
- [Documentation Conventions on page xi](#)
- [Documentation Feedback on page xiii](#)
- [Requesting Technical Support on page xiii](#)

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- [ACX Series](#)
- [M Series](#)
- [MX Series](#)
- [T Series](#)
- [PTX Series](#)

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming

configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xsl;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:







```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

## Documentation Conventions

[Table 1 on page xi](#) defines notice icons used in this guide.

**Table 1: Notice Icons**

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

[Table 2 on page xii](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols <b>ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric metric&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(string1   string2   string3)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

---

## GUI Conventions

---

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
<b>&gt;</b> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes:  
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:  
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## CHAPTER 1

# Accessing a Junos OS Device

- [Understanding the Console Port on page 15](#)
- [Accessing a Junos OS Device the First Time on page 16](#)

### Understanding the Console Port

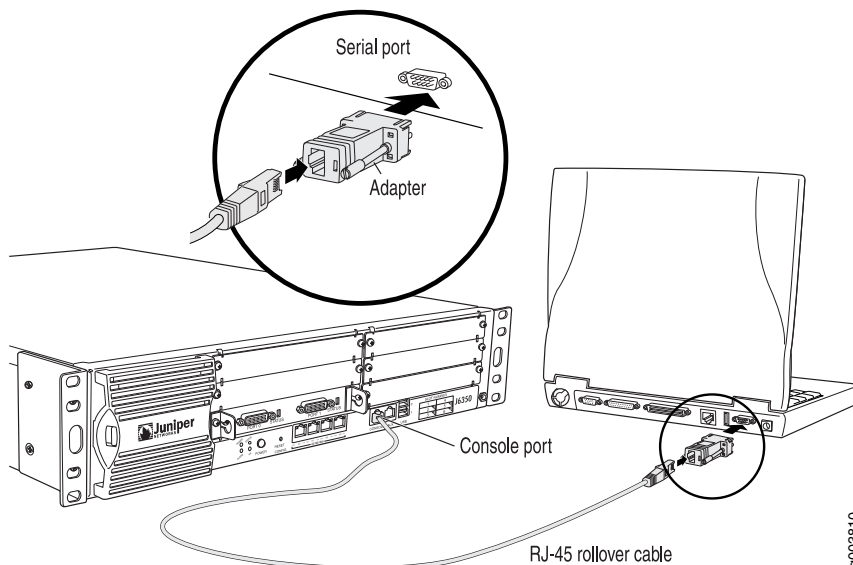
---

Console ports allow root access to the Junos operating system (Junos OS) devices through a terminal or laptop interface, regardless of the state of the Junos OS device, unless it is completely powered off. By connecting to the console port, you can access the root level of the Junos OS device without using the network to which the device might or might not be connected. This creates a secondary path to the Junos OS device without relying on the network.

Using the terminal interface provides a technician sitting in a Network Operations Center a long distance away the ability to restore a Junos OS device or perform an initialization configuration securely, using a modem, even if the primary network has failed. Without a connection to the console port, a technician would have to visit the site to perform repairs or initialization. A remote connection to the Junos OS device through a modem requires the cable and connector (provided in the device accessory box), plus a DB-9 male to DB-25 male (or similar) adapter for your modem, which you must purchase separately. For more information about connecting to the console port, see the administration guide for your particular router or switch.

To configure the device initially, you must connect a terminal or laptop computer to the device through the console port, as shown in [Figure 1 on page 16](#).

Figure 1: Connecting to the Console Port on a Junos OS Device



**Related  
Documentation**

- [Accessing a Junos OS Device the First Time on page 16](#)

## Accessing a Junos OS Device the First Time

When you power on a Junos OS device the first time, Junos OS automatically boots and starts.

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

To access a Junos OS device the first time:

1. Connect a terminal or laptop computer to the Junos OS device through the console port—a serial port on the front of the device.
2. Power on the device and wait for it to boot.

Junos OS 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 device shows the username **root@#**.

4. Start the Junos OS command-line interface (CLI).

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

5. Enter Junos OS configuration mode.

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

**Related  
Documentation**

- [Understanding the Root Password on page 19](#)
- [Protecting Network Security by Configuring the Root Password on page 20](#)
- [Recovering the Root Password on page 22](#)



## CHAPTER 2

# Configuring the Root Password

- [Understanding the Root Password on page 19](#)
- [Protecting Network Security by Configuring the Root Password on page 20](#)
- [Recovering the Root Password on page 22](#)

### Understanding the Root Password

---

The root user has complete privileges to operate and configure the Junos OS device, perform upgrades, and manage files in the file system. Initially, the root password is not defined on the Junos OS device. To ensure basic security, you must define the root password during initial configuration. If a root password is not defined, you cannot commit configuration settings on the device.



**NOTE:** If you use a plain text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it.

The root password must meet the following conditions:

- Be at least six characters long. Most character classes can be included in a password (alphabetic, numeric, and special characters), except control characters.
- Contain at least one change of case or character class.

#### Related Documentation

- [Protecting Network Security by Configuring the Root Password on page 20](#)

## Protecting Network Security by Configuring the Root Password

---

Configuring the root password on your Junos OS-enabled router helps prevent unauthorized users from making changes to your network. The root user (also referred to as superuser) has unrestricted access and full permissions within the system, so it is crucial to protect these functions by setting a strong password when setting up a new router.

After a new router is initially powered on, you log in as the user **root** with no password. Junos OS requires configuration of the root password before it accepts a commit operation. On a new device, the root password must always be a part of the configuration submitted with your initial commit.

To set the root password, you have a few options as shown in Step 1 of the following procedure.

- Enter a plain-text password that Junos OS encrypts.
- Enter a password that is already encrypted.
- Enter a secure shell (ssh) public key string.

The most secure options of these three are using an already encrypted password or an ssh public key string. Pre-encrypting your password or using a ssh public key string means the plain-text version of your password will never be transferred over the internet, protecting it from being intercepted by a man-in-the-middle attack.



**BEST PRACTICE:** Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group to strengthen security, as shown in Step 2 of this procedure. This step uses a group called **global** as an example.

To set the root password:

## 1. Use one of these methods to configure the root password:

- To enter a plain-text password that the system encrypts for you:

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

If you use a plain-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as **## SECRET-DATA** in the configuration.

- To enter a password that is already encrypted:



**CAUTION:** Do not use the `encrypted-password` option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

If you accidentally configure the `encrypted-password` option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to complete the root password recovery process.

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

- To enter an ssh public key string:

```
[edit groups global system]
root@# set root-authentication (ssh-dsa | ssh-eccdsa | ssh-rsa key)
```

## 2. (Optional) Strengthen security by only allowing root access from the console port.

```
[edit groups global system]
root@# set services ssh root-login deny
```

3. If you used a configuration group in Step 2, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

## 4. Commit the changes.

```
root@# commit
```

#### Related Documentation

- [Accessing a Junos OS Device the First Time on page 16](#)
- [Understanding User Accounts on page 43](#)
- [Recovering the Root Password on page 22](#)

## Recovering the Root Password

---

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.



**NOTE:** You need console access to recover the root password.



**Video:** [Recovering the Root Password](#)

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45-to-DB-9 serial port adapter supplied with the router.
4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.
5. Connect the other end of the Ethernet rollover cable to the console port on the router.
6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
9. Power on the router by pressing the power button on the front panel.

Verify that the POWER LED on the front panel turns green.

The terminal emulation screen on your management device displays the router's boot sequence.
10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

Depending on your device hardware, the bootstrap loader might proceed quite quickly at this step without pausing for input. Therefore, you might need to press the spacebar multiple times at the beginning of the boot sequence.

Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [kernel] in 9 seconds...

11. At the following prompt, type **boot -s** to start the system in single-user mode.

ok **boot -s**

12. At the following prompt, type **recovery** to start the root password recovery procedure.

Enter full pathname of shell or 'recovery' for root password recovery or RETURN  
for /bin/sh: **recovery**

13. Enter configuration mode in the CLI.

14. Set the root password.

When you configure a plain-text password, Junos OS encrypts the password for you.



**CAUTION:** Do not use the **encrypted-password** option unless the password is *already* encrypted, and you are entering the encrypted version of the password. If you commit the **encrypted-password** option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to repeat this password recovery process.

Optionally, instead of configuring the root password at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the root password.

For example:

```
user@host# set groups global system root-authentication plain-text-password
```

15. At the following prompt, enter the new root password, for example:

New password: **password**  
Retype new password:

16. At the second prompt, reenter the new root password.

17. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

18. After you have finished configuring the password, commit the configuration.

```
root@host# commit
commit complete
```

19. Exit configuration mode in the CLI.

20. Exit operational mode in the CLI.

21. At the prompt, type **y** to reboot the router.

Reboot the system? [y/n] **y**

**Related Documentation** • *Configuring the Root Password*

## CHAPTER 3

# Configuring the Hostname

- [Understanding Hostnames on page 25](#)
- [Configuring the Hostname of a Router or Switch by Using a Configuration Group on page 26](#)

## Understanding Hostnames

---

Almost all devices in your network have a hostname.

The hostname is the name that identifies the device on the network and is easier to remember than an IP address. When you first power on a Juniper Networks router, switch, or security device, the default hostname is *Amnesiac*. The *Amnesiac* prompt is indicative of a device that is booting from a factory-fresh Junos OS software load, which, by definition, does not have a hostname configured.

Administrators often follow conventions for naming devices. One such convention is to name the device based on its location, for example: *germany-berlin-R1*. The hostname should be unique within your network infrastructure, but there is no need for the local hostname to be globally unique.

A device's hostname usually has a corresponding entry in the domain name system (DNS) so that administrators can connect to the device using the hostname. The fully qualified domain name (FQDN), which is used in DNS, includes the hostname and the domain name. The hostname and the domain name labels are separated by periods or dots, as follows: *hostname.domain*. For example, if the hostname is *germany-berlin-R1* and the domain name is *emea*, the FQDN is *germany-berlin-R1.emea*. If the *emea* domain is registered and can be reached as *emea.net* on the Internet, the FQDN for the device is *germany-berlin-R1.emea.net*. The FQDN is globally unique.

In Junos OS, the hostname can contain any combination of alphabetic characters, numbers, dashes, and underscores. No other special characters are allowed.

Although Junos OS allows hostnames to contain up to 255 characters, keep in mind that the total length of the hostname as an FQDN cannot exceed 255 characters (including the delimiting dots), with each domain name label having a maximum length of 63 characters. In any case, an overly long hostname is difficult to type and to remember, so short and meaningful hostnames are a best practice.

- Related Documentation**
- [Configuring the Hostname of a Router or Switch by Using a Configuration Group on page 26](#)

## Configuring the Hostname of a Router or Switch by Using a Configuration Group

---

The hostname of a device is its identification. A router or switch must have its identity established to be accessible on the network to other devices. That is perhaps the most important reason to have a hostname, but a hostname has other purposes: Junos OS uses the configured hostname as part of the command prompt, to prepend log files and other accounting information, as well as in other places where knowing the device identity is useful. We recommend that the hostname be descriptive and memorable.

You can configure the hostname at the **[edit system]** hierarchy level, a procedure shown in [“Example: Configuring the Unique Identity of a Router for Making it Accessible on the Network” on page 33](#). Optionally, instead of configuring the hostname at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the hostname, especially if the device has dual Routing Engines. This procedure uses groups called **re0** and **re1** as an example.



**NOTE:** If you configure hostnames that are longer than the CLI screen width, regardless of the terminal screen width setting, the commit operation occurs successfully, starting with Junos OS release 13.2R3. Even if the terminal screen width is less than the hostname length, commit is successful. In Junos OS releases earlier than Release 13.2R3, if you configured such hostnames by using the `host-name hostname` statement at the **[edit system]** hierarchy level and the terminal screen width was less than the length of the hostname by using the `set cli screen-width` statement, a foreign file propagation (ffp) failure error message is displayed when you attempt to commit the configuration. In such a case, because of the ffp failure, the commit operation does not complete and you cannot recover the router unless you make the modification in the backend in the `juniper.conf.gz` file and commit the change from the shell prompt.

To set the hostname using a configuration group:

1. Include the **host-name** statement in the configuration at the **[edit groups *group-name* system]** hierarchy level.

The name value must be less than 256 characters.

```
[edit groups group-name system]
host-name hostname;
```

For example:

```
[edit groups re0 system]
root@# set host-name san-jose-router
```

```
[edit groups re1 system]
root@# set host-name san-jose-router1
```

2. If you used one or more configuration groups, apply the configuration groups, substituting the appropriate group names.

For example:

```
[edit]  
user@host# set apply-groups [re0 re1]
```

3. Commit the changes.

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

The hostname subsequently appears in the device CLI prompt.

```
san-jose-router@#
```

**Related Documentation**

- [Understanding Hostnames on page 25](#)



## CHAPTER 4

# Configuring DNS

- [DNS Overview on page 29](#)
- [Reaching a Domain Name System Server on page 30](#)
- [Example: Configuring the TTL Value for DNS Server Caching on page 32](#)
- [Example: Configuring the Unique Identity of a Router for Making it Accessible on the Network on page 33](#)

## DNS Overview

---

A Domain Name System (DNS) is a distributed hierarchical system that converts hostnames to IP addresses. The DNS is divided into sections called zones. Each zone has name servers that respond to the queries belonging to their zones.

This topic includes the following sections:

- [DNS Components on page 29](#)
- [DNS Server Caching on page 29](#)

## DNS Components

DNS includes three main components:

- **DNS resolver** — Resides on the client side of the DNS. When a user sends a hostname request, the resolver sends a DNS query request to the name servers to request the hostname's IP address.
- **Name servers** — Processes the DNS query requests received from the DNS resolver and returns the IP address to the resolver.
- **Resource records** — Data elements that define the basic structure and content of the DNS.

## DNS Server Caching

DNS name servers are responsible for providing the hostname IP address to users. The TTL field in the resource record defines the period for which DNS query results are cached. When the TTL value expires, the name server sends a fresh DNS query and updates the cache.

- Related Documentation**
- [Example: Configuring the TTL Value for DNS Server Caching on page 32](#)
  - [DNSSEC Overview](#)

---

## Reaching a Domain Name System Server

Domain name system (DNS) servers are used for resolving hostnames to IP addresses.

For redundancy, it is a best practice to configure access to multiple DNS servers. You can configure a maximum of three DNS servers. The approach is similar to the way Web browsers resolve the names of a Web site to its network address. Additionally, Junos OS enables you configure one or more domain names, which it uses to resolve hostnames that are not fully qualified (in other words, the domain name is missing). This is convenient because you can use a hostname in configuring and operating Junos OS without the need to reference the full domain name. After adding DNS server addresses and domain names to your Junos OS configuration, you can use DNS resolvable hostnames in your configuration and commands instead of IP addresses.

Optionally, instead of configuring the name server at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the name server. This procedure uses a group called **global** as an example.

Before you begin, configure your DNS servers with the hostname and an IP address for your Junos OS device. It does not matter which IP address you assign as the address of your Junos OS device in the DNS server, as long it is an address that reaches your device. Normally, you would use the management interface IP address, but you can choose the loopback interface IP address, or a network interface IP address, or even configure multiple addresses on the DNS server.

To configure the router or switch to resolve hostnames into addresses:

1. Reference the IP addresses of your DNS servers.

```
[edit groups group-name system]
name-server {
    address;
}
```

The following example shows how to reference two DNS servers:

```
[edit groups global system]
user@host# set name-server 192.168.1.253
user@host# set name-server 192.168.1.254

user@host# show
name server {
    192.168.1.253;
    192.168.1.254;
}
```

2. (Optional) Configure the name of the domain in which the device itself is located.

This is a good practice. Junos OS then uses this configured domain name as the default domain name to append to hostnames that are not fully qualified.

```
[edit system]
domain-name domain-name;
```

The following example shows how to configure the domain name:

```
[edit groups global system]
user@host# set domain-name company.net
```

```
user@host# show
domain-name company.net;
```

3. (Optional) Configure a list of domains to be searched.

If your device can reach several different domains, you can configure these as a list of domains to be searched. Junos OS then uses this list to set an order in which it appends domain names when searching for the IP address of a host.

```
[edit groups global system]
domain-search [ domain-list ];
```

The domain list can contain up to six domain names, with a total of up to 256 characters.

The following example shows how to configure two domains to be searched. This example configures Junos OS to search the company.net domain and then the domainone.net domain and then the domainonealternate.com domain when attempting to resolve unqualified hosts.

```
[edit groups global system]
domain-search [ company.net domainone.net domainonealternate.com ]
```

4. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

5. Commit the configuration.

```
user@host# commit
```

6. Verify the configuration.

If you have configured your DNS server with the hostname and an IP address for your Junos OS device, you can issue the following commands to confirm that DNS is working and reachable. You can either use the configured hostname to confirm resolution to the IP address or use the IP address of your device to confirm resolution to the configured hostname.

```
user@host> show host host-name
user@host> show host host-ip-address
```

For example:

```
user@host> show host san-jose-router1
san-jose-router1.company.net
san-jose-router1.company.net has address 192.168.187.1
user@host> show host 192.168.187.1
```

1.187.168.192.in-addr.arpa domain name pointer san-jose-router1.company.net.

**Related Documentation**

- [DNS Overview on page 29](#)

---

## Example: Configuring the TTL Value for DNS Server Caching

---

This example shows how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

- [Requirements on page 32](#)
- [Overview on page 32](#)
- [Configuration on page 32](#)
- [Verification on page 32](#)

### Requirements

No special configuration beyond device initialization is required before performing this task.

### Overview

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

### Configuration

#### Step-by-Step Procedure

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds.  
  
[edit]  
user@host# **set system services dns max-cache-ttl 86400**
2. Specify the maximum TTL value for negative cached responses, in seconds.  
  
[edit]  
user@host# **set system services dns max-ncache-ttl 86400**
3. If you are done configuring the device, commit the configuration.  
  
[edit]  
user@host# **commit**

### Verification

To verify the configuration is working properly, enter the **show system services** command.

**Related Documentation**

- [DNS Overview on page 29](#)

## Example: Configuring the Unique Identity of a Router for Making it Accessible on the Network

---

To use a router in a network, you must configure the router's identity. Configuring a router's identity makes the router accessible on the network and so that other users can log in to it. You can refer to any Internet-connected machine in either of two ways:

- By its IP address
- By its hostname

Once you have a hostname, you can find the IP address, you can use the Domain Name System (DNS) to resolve an IP address from a hostname, or you can manually map the hostname to a static IP address. Although using the DNS is an easier and more scalable way to resolve IP addresses from hostnames, you might not have a DNS entry for the router, or you might not want the computer to contact the DNS server to resolve a particular IP address (perhaps you use this particular IP address a lot, or you might be using it only for testing or development purposes and do not want to give it a DNS entry).

To configure a router's unique identity, you might need to include all or part of the following: the hostname of the router, its IP address, the domain name, two or three name servers, mapping of the hostname to the IP address.

- [Requirements on page 33](#)
- [Overview on page 33](#)
- [Configuration on page 34](#)
- [Verification on page 35](#)

### Requirements

No special configuration beyond device initialization is required before configuring this example.

### Overview

A hostname is the router's name. It is easier for most people to remember a hostname than an IP address. Junos OS uses the configured hostname as part of the command prompt, to prepend log files and other accounting information, as well as in other places where knowing the device identity is useful. You can use the hostname to telnet to a router.

The domain name is the string appended to hostnames that are not fully qualified. The domain name is the name of a network associated with an organization. For sites in the United States, domain names typically take the form of *org-name.org-type*.

The mapping of hostnames to IP addresses is handled through a service called the Domain Name System (DNS). A series of special DNS servers across the world known as name servers keep track of the hostname and IP address information for all the devices

on the Internet. Applications that need to determine an IP address from a hostname (or vice versa) contact the local name server to get this information. You can set a few name servers.

In case your hostname and IP address do not have a DNS entry in a name server, configure a static mapping.

In this example, the values given in [Table 3 on page 34](#) are used to configure each of these variables. You need to substitute data pertinent to your router and network for these values.

**Table 3: Values to Use in Example**

Name of Variable	Value Used in Example	Value You Substitute
domain-name <i>domain-name</i>	domain-name jtac.jnpr.net	
host-name <i>host-name</i>	host-name newton-re0	
inet <i>ip-address</i>	inet 172.22.147.39	
name-server <i>ip-address</i>	name-server 172.24.16.115 name-server 66.129.255.75	

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them in a text file, remove any line breaks, change the values used to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set system domain-name jtac.jnpr.net
set system host-name newton-re0
set system name-server 172.24.16.115
set system name-server 66.129.255.75
set system static-host-mapping newton-re0 inet 172.22.147.39
```

### Configuring the Router's Identity

### Step-by-Step Procedure

To configure the identity settings of a device:

1. Configure the domain name of your network.  
[edit]  
user@host# **set system domain-name jtac.jnpr.net**
2. Configure the hostname, using the **set system host-name** command.  
[edit]  
user@host# **set system host-name newton-re0**
3. Configure from one to three name servers.  
[edit]

```
user@host# set system name-server 172.24.16.115
user@host# set system name-server 66.129.255.75
```

4. Map from the hostname to the IP address, using the **set system static-host-mapping** command.

```
[edit]
user@host# set system static-host-mapping newton-re0 inet 172.22.147.39
```

---

## Results

To check the configuration, use the configuration mode **show system** command.

```
[edit]
user@host# show system
domain-name jtac.jnpr.net;
host-name newton-re0;
name-server {
  172.24.16.115;
  66.129.255.75;
}
static-host-mapping {
  newton-re0 {
    inet 172.22.147.39;
  }
}
```

When you have the correct configuration, enter **commit**.

## Verification

---

### Verifying the Hostname and IP Address of a Device

**Purpose** Verify the hostname and IP address of a device.

**Action** Issue the **show host *host-name*** operational command.

```
user@newton-re0> show host newton
newton.jtac.jnpr.net is an alias for newton-re0.jtac.jnpr.net.
newton-re0.jtac.jnpr.net has address 172.22.147.39
```

**Related Documentation**

- [Understanding Hostnames on page 25](#)
- [Reaching a Domain Name System Server on page 30](#)



## CHAPTER 5

# Configuring Management and Loopback Interfaces

- [Understanding Management Ethernet Interfaces on page 37](#)
- [Configuring a Management Interface on a Dedicated Management Port on page 39](#)
- [Understanding the Loopback Interface on page 40](#)
- [Configuring a Loopback Interface on page 41](#)

### Understanding Management Ethernet Interfaces

Management interfaces are the primary interfaces for accessing the device remotely. Typically, a management interface is not connected to the in-band network, but is connected instead to the device's internal network. Through a management interface you can access the device over the network using utilities such as **ssh** and **telnet** and configure the device from anywhere, regardless of its physical location. SNMP can use the management interface to gather statistics from the device.

A management interface lets authorized users and management systems connect to the device over the network. Some Juniper Networks devices have a dedicated management port on the front panel. For other types of platforms, you can configure a management interface on one of the network interfaces. This interface can be dedicated to management or shared with other traffic. Before users can access the management interface, you must configure it. Information required to set up the management interface includes its IP address and prefix. In many types of Junos OS devices (or recommended configurations), it is not possible to route traffic between the management interface and the other ports. Therefore, you should select an IP address in a separate (logical) network, with a separate prefix (netmask).

For devices with dedicated management ports, Junos OS automatically configures the router's management Ethernet interface, as either **em0** or **fxp0**. You can use the **show interfaces terse | match fxp0** or **show interfaces terse | match em0** command to display management interface information.

To use the management Ethernet interface as a management port, you must configure its logical port, **em0.0** or **fxp0.0**, with a valid IP address.

For some SRX Series Services Gateways, you can use any of the built-in Ethernet ports as a management interface. To use a built-in interface as a management Ethernet

interface, configure it with a valid IP address. To manually configure J-Web access, include the **interface *interface-name*** statement at the **[edit system services web-management http]** hierarchy level.

For PTX Series Packet Transport Routers, the Junos OS automatically creates the router's management Ethernet interface, **em0**. To use **em0** as an out-of-band management port, you must configure its logical port (for example, **em0.0**) with a valid IP address.

Internal Ethernet interfaces are automatically created to connect the Routing Engines to the Packet Forwarding Engines in the FPCs.

When you enter the **show interfaces** command on a PTX Series Packet Transport Router, the management Ethernet interface and internal Ethernet interfaces (and logical interfaces) are displayed:

```
user@host> show interfaces ?
...
em0
  em0.0
  ixgbe0
  ixgbe0.0
  ixgbe1
  ixgbe1.0
...
```



**NOTE:** *Routing Engine upgrade considerations*—When upgrading to a Routing Engine that supports em0 from a Routing Engine that supports fxp0, you must convert existing management Ethernet interface references in the router configuration files from fxp0, fxp1, or fxp2 interfaces to em0 interfaces. Whether you use an automated script or edit the configuration files manually, you must revise any command lines that reference the fxp0 management Ethernet interface by replacing “fxp0” with “em0.”

*Reusing scripts for standalone T1600 routers on T1600 routers in a routing matrix*—Automated scripts that you have developed for standalone T1600 routers (T1600 routers that are not in a routing matrix) might contain references to the fxp0 management Ethernet interface. Before reusing the scripts on T1600 routers in a routing matrix, edit the command lines that reference the fxp0 management Ethernet interface so that the commands reference the em0 management Ethernet interface instead.

*Restricted load-sharing next hops with fxp0*—On M Series Multiservices Edge Routers and T Series Core Routers running Junos OS later than Release 7.0R2.7 or Release 7.1R2.2, the fxp0 interface does not support load-sharing next hops. This restriction only affects fxp0 routes.

*CoS not supported on fxp0*—The fxp0 interface does not support class of service (CoS).

The Routing Engines in the PTX Series Packet Transport Routers do not support the management Ethernet interface fxp0, or the internal Ethernet interfaces fxp1 or fxp2.

---

**Related Documentation** • *Supported Routing Engines by Router*

## Configuring a Management Interface on a Dedicated Management Port

Management interfaces are the primary interfaces for accessing the device remotely. Typically, a management interface is not connected to the in-band network, but is connected instead to the device's internal network. Through a management interface you can access the device over the network using utilities such as **ssh** and **telnet** and configure the device from anywhere, regardless of its physical location. SNMP can use the management interface to gather statistics from the device.

Many types of Junos OS platforms include a dedicated management port on the front panel. For others, you can configure one of the Ethernet ports to act as the management interface. Platforms that use a network Ethernet interface for management include some SRX Series devices. A network interface can be configured as being dedicated to out-of-band management or as being shared by both management and network traffic.

Even if your device has a dedicated management port, you might prefer to configure a network interface to carry management traffic. For example, your organization might use this approach when cost does not justify a separate management infrastructure.

A dedicated management port supports out-of-band management access with complete physical separation from network traffic within your device. This approach limits access to your device, and thereby the potential for issues. Further, because it only carries management traffic, the management port is fully available to you for analyzing and reacting to issues if your device happens to be under attack.

Configuration of the dedicated management port requires assignment of the IP address that you want to use as the management interface. The interface name that you use depends on the type of device that you are setting up. Some devices use **me0**, some use **fxp0**, and some use **em0**.

To configure a dedicated management port:

1. Run the **show interfaces terse** command to determine the name of the dedicated management port on your device.

In this example, the device uses **fxp0** as its dedicated management port.

```
user@host> show interfaces terse | match me0
user@host> show interfaces terse | match em0
user@host> show interfaces terse | match fxp0
fxp0                up    up
```

2. Configure the IP address for this device's dedicated management port.

```
[edit interfaces fxp0 unit 0 family inet]
user@host# set address 192.168.187.1/25
```

Optionally, instead of configuring the dedicated management port at the **[edit interfaces]** hierarchy level, you can use configuration groups. This is a recommended best practice, especially if the device has dual Routing Engines.

```
[edit groups re0 interfaces fxp0 unit 0 family inet]
user@host# set address 192.168.187.1/25
```

```
[edit groups re1 interfaces fxp0 unit 0 family inet]
user@host# set address 192.168.187.2/25
```

```
[edit]
user@host# set apply-groups re0
user@host# set apply-groups re1
```

3. Commit the configuration.

```
user@host# commit
```

4. Confirm the configuration by making sure that the IP address is configured.

```
user@host> show interfaces terse | match fxp0
fxp0                up    up
fxp0.0              up    up    inet    192.168.187.1/25
```

If **telnet** or **ssh** access is enabled, log in to the device remotely, using the newly configured IP address.

- Related Documentation**
- [Understanding Management Ethernet Interfaces on page 37](#)
  - <http://www.juniper.net/us/en/local/pdf/implementation-guides/8010010-en.pdf>

---

## Understanding the Loopback Interface

The loopback address (**lo0**) has several uses, depending on the particular Junos feature being configured. It can perform the following functions:

- **Device identification**—The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes.

When you ping an individual interface address, the results do not always indicate the health of the device. For example, a subnet mismatch in the configuration of two endpoints on a point-to-point link makes the link appear to be inoperable. Pinging the interface to determine whether the device is online provides a misleading result. An interface might be unavailable because of a problem unrelated to the device's configuration or operation.

- **Routing information**—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as **ping mpls** require a loopback address to function correctly.
- **Packet filtering**—Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

The Internet Protocol (IP) specifies a loopback network with the (IPv4) address **127.0.0.0/8**. Most IP implementations support a loopback interface (**lo0**) to represent the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback

network is **127.0.0.1** for IPv4 and **::1** for IPv6. The standard domain name for the address is **localhost**.

The device also includes an internal loopback address (**lo0.16384**). The internal loopback address is a particular instance of the loopback address with the logical unit number 16384. Junos OS creates the loopback interface for the internal routing instance. This interface prevents any filter on **lo0.0** from disrupting internal traffic.

**Related  
Documentation**

- [Configuring a Loopback Interface on page 41](#)
- *Understanding Interfaces*
- *Understanding Management Interfaces for SRX Series and J Series Devices*
- *Understanding the Discard Interface*

---

## Configuring a Loopback Interface

The loopback interface supports many different network and operational functions and is an *always-up* interface. This means that the loopback interface ensures that the device is reachable, even if some of the physical interfaces are down or removed, or an IP address has changed. In most cases, you always define a loopback interface.

Junos OS follows the IP convention of identifying the loopback interface as lo0.

Junos OS requires that the loopback interface always be configured with a /32 network mask, thus avoiding any unnecessary allocation of address space.

If you are using routing instances, you can configure the loopback interface for the default routing instance or for a specific routing instance. The following procedure adds the loopback interface to the default routing instance.

Optionally, instead of configuring the loopback interface at the **[edit interfaces]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the loopback interface. This procedure uses a group called **global** as an example.

To configure a loopback interface:

1. Using the host IP address, assign it to the loopback interface.

Each host in your network deployment should have a unique loopback interface address. The address used here is only an example.

```
[edit groups global interfaces lo0 unit 0 family inet]
user@host# set address 192.26.0.110/32
```

2. (Optional) Set the preferred IP address.

You can configure as many addresses as you need on the lo0 interface, so it is good practice to designate one preferred IP address.

```
[edit groups global interfaces lo0 unit 0 family inet]
user@host# set address 192.26.0.110/32 preferred
```

3. (Optional) Configure additional addresses.

Only unit 0 is permitted as the master loopback interface. If you want to add more IP addresses to unit 0, you configure them in the normal way under unit 0, without the **preferred** option.

```
[edit groups global interfaces lo0 unit 0 family inet]
user@host# set address 192.168.1.1/32
user@host# set address 192.168.2.1/32
```

4. Configure the localhost address.

On the lo0.0 interface, it is useful to have the IP address 127.0.0.1 configured, as certain processes such as NTP and MPLS ping use this default host address. The 127.0.0.1/32 address is a Martian IP address (an address invalid for routing), so it is never advertised by the Juniper Networks device.

```
[edit groups global interfaces lo0 unit 0 family inet]
user@host# set address 127.0.0.1/32
```

5. (Optional) Configure an ISO address.

Depending on your network configuration, you might also need an ISO address for the IS-IS routing protocol.

```
[edit groups global interfaces lo0 unit 0 family iso]
user@host# address 49.0026.0000.0000.0110.00
```

6. If you used a configuration group, apply the configuration group, substituting **global** with the appropriate group name.

```
[edit]
user@host# set apply-groups global
```

7. Commit the configuration.

```
user@host# commit
```

**Related  
Documentation**

- [Understanding the Loopback Interface on page 40](#)

## CHAPTER 6

# Configuring User Accounts

- [Understanding User Accounts on page 43](#)
- [Configuring Junos OS User Accounts by Using a Configuration Group on page 44](#)
- [Enabling Remote Access on page 47](#)

### Understanding User Accounts

---

User accounts provide one way for users to access the device. Users can access the device without accounts if you configured RADIUS or TACACS+ servers. After you have created an account, the device creates a home directory for the user. An account for the user **root** is always present in the configuration. For each user account, you can define the following:

- **Username**—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username.
- **User's full name**—If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- **User identifier (UID)**—Numeric identifier that is associated with the user account name. The identifier range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- **User's access privilege**—You can create login classes with specific permission bits or use one of the predefined classes.
- **Authentication method or methods and passwords that the user can use to access the device**—You can use SSH or an MD5 password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. If you configure the plain-text-password option, you are prompted to enter and confirm the password.

#### Related Documentation

- [Understanding User Authentication Methods](#)
- [Example: Configuring a RADIUS Server for System Authentication](#)
- [Example: Configuring a TACACS+ Server for System Authentication](#)
- [Example: Configuring Authentication Order](#)

## Configuring Junos OS User Accounts by Using a Configuration Group

---

User accounts provide a way for users to access a router or switch. Junos OS requires that all users have a predefined user account before they can log in to the device. For each user account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

It is a common practice to use remote authentication servers to centrally store information about users. Even so, it is also a good practice to configure at least one nonroot user directly on each device, in case access to the remote authentication server is disrupted. This one nonroot user commonly has a generic name, such as **admin**.

Because user accounts are configured on multiple devices, they are commonly configured inside of a configuration group. As such, the examples shown here are in a configuration group called **global**. Using a configuration group for your user accounts is optional.

To create a user account:

1. Add a new user, using the user's assigned account login name.

```
[edit groups global]
user@host# edit system login user user username
```

2. (Optional) Configure a full descriptive name for the account.

If the full name includes spaces, enclose the entire name in quotation marks.

```
[edit groups global system login user user-name]
user@host# set full-name complete-name
```

For example:

```
user@host# show groups
global {
  system {
    login {
      user admin {
        full-name "general administrator";
      }
    }
  }
}
```

3. (Optional) Set the user identifier (UID) for the account.

As with UNIX systems, the UID enforces user permissions and file access. If you do not set the UID, Junos OS assigns one for you. The format of the UID is a number in the range of 100 to 64000.

```
[edit groups global system login user user-name]
user@host# set uid uid-value
```

For example:

```
user@host# show groups
global {
```

```

system {
  login {
    user admin {
      uid 9999;
    }
  }
}

```

4. Assign the user to a login class.

You can define your own login classes or assign one of the predefined Junos OS login classes.

The predefined login classes are as follows:

- super-user—all permissions
- operator—clear, network, reset, trace, and view permissions
- read-only—view permissions
- unauthorized—no permissions

```

[edit groups global system login user user-name]
user@host# set class class-name

```

For example:

```

user@host# show groups
global {
  system {
    login {
      user admin {
        class super-user;
      }
    }
  }
}

```

5. Use one of the following methods to configure the user password.

- To enter a clear-text password that the system encrypts for you, use the following command to set the user password:

```

[edit groups global system login user user-name]
user@host# set authentication plain-text-password password
New Password: type password here
Retype new password: retype password here

```

As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are therefore hidden and marked as ## SECRET-DATA in the configuration.

- To enter a password that is already encrypted, use the following command to set the user password:



**CAUTION:** Do not use the encrypted-password option unless the password is *already* encrypted, and you are entering the encrypted version of the password.

If you accidentally configure the encrypted-password option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as this user.

---

```
[edit groups global system login user user-name]  
user@host# set authentication encrypted-password "password"  
New Password: type password here  
Retype new password: retry password here
```

- To load previously generated public keys from a named file at a specified URL location, use the following command to set the user password:

```
[edit groups global system login user user-name]  
user@host# set authentication load-key-file URL filename
```

- To enter an ssh public string, use the following command to set the user password:

```
[edit groups global system login user user-name]  
user@host# set authentication (ssh-dsa | ssh-eccdsa | ssh-rsa) authorized-key
```

6. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]  
user@host# set apply-groups global
```

7. Commit the configuration.

```
user@host# commit
```

8. To verify the configuration, log out and log back in as the new user.

#### Related Documentation

- [Defining Junos OS Login Classes](#)
- [Example: Creating Login Classes with Specific Privileges](#)
- [Junos OS User Accounts Overview](#)
- [Limiting the Number of User Login Attempts for SSH and Telnet Sessions](#)
- [User Access and Authentication Feature Guide for Routing Devices](#)

## Enabling Remote Access

SSH, telnet, and FTP are widely used standards for remotely logging into network devices, and exchanging files between systems. Before authorized users can access your device, or your device can exchange data with other systems, you must configure one or more of these enabling services. They are all disabled by default in Junos OS.

SSH is a protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. SSH is telnet's successor and is the recommended method for remote access. SSH encrypts all traffic, including passwords, to effectively eliminate eavesdropping, connection hijacking, and other attacks. The SSH utility includes SCP (secure copy), a file transfer program that uses SSH and is the recommended method for secure file exchange.

Because both telnet and FTP are legacy applications that use clear text passwords (therefore creating a potential security vulnerability), we recommend that you use SSH (and SCP). If you do not intend to use FTP or telnet, you do not need to configure them on your device. However, do not forget to consider that some users might use FTP to store configuration templates, retrieve software, or other administrative tasks.

To set up remote access and file transfer services:

1. Enable SSH access.

```
[edit groups global]
user@host# set system services ssh
```

2. Enable telnet access.

```
[edit groups global]
user@host# set system services telnet
```

3. Enable FTP.

```
[edit groups global]
user@host# set system services ftp
```

4. At the top level of the configuration, apply the configuration group.

If you use a configuration group, you must apply it for it to take effect.

```
[edit]
user@host# set apply-groups global
```

5. Commit the configuration.

```
user@host# commit
```

### Related Documentation

- *Configuring SSH Service for Remote Access to the Router or Switch*
- *Configuring Telnet Service for Remote Access to a Router or Switch*
- *Configuring FTP Service for Remote Access to the Router or Switch*



## CHAPTER 7

# Configuring Backup Routers

- [Understanding Backup Routers on page 49](#)
- [Configuring a Backup Router on page 50](#)

### Understanding Backup Routers

---

If Junos OS is running on a routing device, you might want to specify a backup router. The purpose of the backup router is not to forward transit traffic. It is for local management of the routing device, by way of the out-of-band management interface (fxp0 or me0, for example). Traffic is not forwarded between the Packet Forwarding Engine and the management interface. You cannot route traffic between the management interface and the physical interfaces in the chassis.

The Junos OS process responsible for establishing routes is known as the routing protocol process (rpd). The backup router allows the routing device to install a route to a management network, before the routing protocol process is up and running. A backup router can be used during the initial boot process of Junos OS, before any routing protocols have converged. It allows the device to establish a Layer 3 connection quickly, thus keeping management unavailability to a minimum. In selecting a backup router, it is common practice to choose the default gateway of the management network that is directly connected to your routing device.

It is important to make sure that the specified backup router address is reachable and directly connected. The backup router address should be an address that is directly connected to the management interface.



**NOTE:** Router A can be the backup router for Router B, and Router B can be the backup router for Router A if the management interface of each router is connected to an interface on the other router, thus providing the necessary reachability.

When the routing protocol process starts, the backup route (the route created by the backup router) is removed, and any default, static, or protocol-learned routes are installed.

If the routing device has a backup Routing Engine (usually RE1), the backup router remains active, unless nonstop active routing is configured.

**Related Documentation** • [Configuring a Backup Router on page 50](#)

---

## Configuring a Backup Router

---

The backup router allows the routing device to install a route to the management network, before the routing protocol process (rpd) is up and running. This allows the device to establish a Layer 3 connection quickly, thus keeping management unavailability to a minimum.

When a routing device is booting, the routing protocol process is not running. Therefore, the router or switch has no routes. To ensure that the router or switch is reachable for management purposes while it boots or if the routing protocol process fails to start properly, configure a backup router, which is a router that is directly connected to the local router or switch (that is, on the same subnet) through its private management interface (for example, fxp0 or me0).

To achieve network reachability while loading, configuring, and recovering the router or switch, but without installing a default route in the forwarding table, include the **destination** option, specifying an address that is reachable through the backup router. Specify the address in the format **network/mask-length**.

Any destinations defined by the backup router are not visible in the routing table. They are only visible in the local forwarding table when the routing protocol process is not running. Therefore, a recommended best practice is to also include the destinations of the backup router configured as static routes with the **retain** option. The **retain** option is necessary to allow the static route to remain in the forwarding table when the routing protocol process stops running, because the routing table does not exist if the routing protocol process is not running.

On systems with dual redundant Routing Engines, the backup Routing Engine's reachability through the private management interface is based only on the functionality of the **backup-router** configuration. It is not based on whether the routing protocol process is running. The backup router adds the destination prefix upon bootup, whereas configuring a static route requires the routing protocol process to run first before installing the destination prefix. If the routing protocol process is allowed to run on the backup Routing Engine, then a destination can be added in the routing table and the forwarding table by configuring static route with the **retain** option.

Due to a system limitation, do not configure the destination address specified in the backup-router as 0.0.0.0/0 or ::/0. The mask has to be a nonzero value.

Active routes and more specific routes take precedence over destination prefixes defined with the **backup-router** statement.

If you have a backup router configuration in which multiple static routes point to a gateway from the management Ethernet interface, you must configure prefixes that are more specific than the static routes or include the **retain** option at the **[edit routing-options static route]** hierarchy level.

For example, if you configure the static route 172.16.0.0/12 from the management Ethernet interface for management purposes, you must specify the backup router configuration as follows:

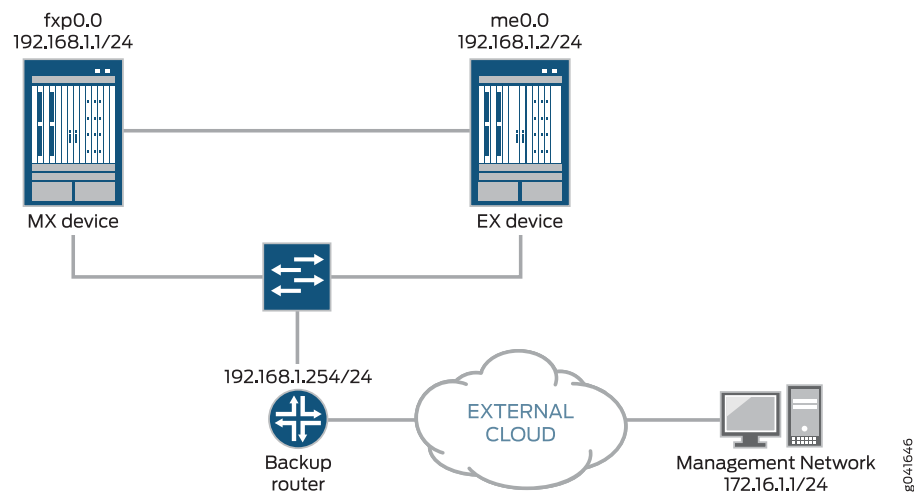
```
backup-router 172.29.201.62 destination [172.16.0.0/13 172.16.128.0/13]
```

## Configuring a Backup Router Running IPv4

In the example shown in [Figure 2 on page 51](#), the backup router is the default gateway of the management network.

As required, the backup router address is reachable and directly connected to the management interfaces on the two routing devices (fxp0 and me0).

**Figure 2: Backup Router Sample Topology**



Optionally, instead of configuring the backup router at the **[edit system]** hierarchy level, you can use a configuration group, as shown in this procedure. This is a recommended best practice for configuring the backup router, especially if the device has dual Routing Engines. This procedure uses groups called **re0** and **re1** as an example.

To configure a backup router running IPv4:

1. Include the **backup-router** statement at the **[edit system]** hierarchy level.

```
[edit groups group-name system]
backup-router address <destination destination-address>;
```

For example:

```
[edit groups re0 system]
backup-router 192.168.1.254 destination 172.16.1.0/24;

[edit groups re1 system]
backup-router 192.168.1.254 destination 172.16.1.0/24;
```

2. (Optional) Configure a static route to the management network.

Junos OS only uses the backup router during the boot sequence. If you want to configure a backup router for use after startup, you can set up a static route. The static route goes into effect when the routing protocol process is running.

```
routing-options {
  static {
    route 172.16.1.0/24 {
      next-hop 192.168.1.254;
      retain;
    }
  }
}
```

3. If you used one or more configuration groups, apply the configuration groups, substituting the appropriate group names.

For example:

```
[edit]
user@host# set apply-groups [re0 re1]
```

4. Commit the changes:

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

## Configuring a Backup Router Running IPv6

To configure a backup router running IPv6:

1. Include the **inet6-backup-router** statement at the **[edit system]** hierarchy level.

```
[edit groups group-name system]
inet6-backup-router address <destination destination-address>;
```

For example:

```
[edit groups re0 system]
inet6-backup-router 8:3::1 destination abcd::/48;

[edit groups re1 system]
inet6-backup-router 8:3::1 destination abcd::/48;
```

2. (Optional) Configure a static route to the management network.

Junos OS only uses the backup router during the boot sequence. If you want to configure a backup router for use after startup, you can set up a static route. The static route goes into effect when the routing protocol process is running.

```
routing-options {
  rib inet6.0 {
    static {
      route abcd::/48 {
        next-hop 8:3::1;
        retain;
      }
    }
  }
}
```

3. If you used one or more configuration groups, apply the configuration groups, substituting the appropriate group names.

For example:

```
[edit]
user@host# set apply-groups [re0 re1]
```

4. Commit the changes:

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

**Related  
Documentation**

- [Understanding Backup Routers on page 49](#)
- *Configuring Junos OS for the First Time on a Router or Switch with a Single Routing Engine*
- *Configuring Junos OS for the First Time on a Device with Dual Routing Engines*
- *Requirements for Routers with a Backup Router Configuration.*



## CHAPTER 8

# Index

- [Index on page 57](#)



# Index

## Symbols

#, comments in configuration statements.....	xii
( ), in syntax descriptions.....	xii
< >, in syntax descriptions.....	xii
[ ], in configuration statements.....	xii
{ }, in configuration statements.....	xii
(pipe), in syntax descriptions.....	xii

## A

addresses	
IP addresses.....	33
authentication	
methods.....	43
root password.....	20
user accounts.....	43
authentication statement	
usage guidelines.....	44

## B

backup routers.....	49, 50
backup-router statement	
usage guidelines.....	50
braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii

## C

cables	
console port, connecting.....	22
Ethernet rollover, connecting.....	22
class statement	
usage guidelines.....	44
comments, in configuration statements.....	xii
console port	
adapter.....	22
conventions	
text and syntax.....	xi
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

## D

DNS name servers.....	30
DNS server caching	
configuring TTL value.....	32
documentation	
comments on.....	xiii
domain names on routers.....	30
domain-name statement	
usage guidelines.....	30
domain-search statement	
usage guidelines.....	30
domains to be searched.....	30

## E

em0	
management interface.....	37
encrypted passwords.....	20
encrypted-password option.....	20
Ethernet rollover cable, connecting the router to a	
management device.....	22

## F

font conventions.....	xi
full-name statement	
usage guidelines.....	44
fxp0	
management interface.....	37

## H

host-name statement	
usage guidelines.....	26
hostname	
about.....	25

## I

inet6-backup-router statement	
usage guidelines.....	50
interfaces	
special interfaces.....	40
IP addresses	
router mapping.....	33

## L

laptop See management device	
lo0 interface functions.....	40
See also loopback interface	
lo0.16385, internal loopback address.....	40
load-key-file command	
usage guidelines.....	44

load-key-file statement	
usage guidelines.....	44
local password	
overview.....	43
login statement	
usage guidelines.....	44
loopback address, internal, lo0.16385.....	40
loopback interface	
functions.....	40

## M

management device	
recovering root password from.....	22
management interface	
em0.....	37
fxp0.....	37
manuals	
comments on.....	xiii

## N

name servers, DNS.....	30
name-server statement	
usage guidelines.....	30
names	
domain names on routers.....	30

## P

parentheses, in syntax descriptions.....	xii
password	
conditions.....	19
root.....	19, 20, 22
root recovery.....	22
root, setting .....	20
ssh public string.....	21, 46
PC See management device	
plain-text passwords	
root password.....	20
plain-text-password option.....	20

## R

RJ-45-to-DB-9 serial port adapter.....	22
rollover cable, connecting the console port.....	22
root password.....	19, 20
root password recovery.....	22
root-authentication statement	
usage guidelines.....	20
router names	
configuring.....	33
mapping to IP addresses.....	33

routers	
backup.....	49, 50
DNS name servers, configuring.....	30
domain names.....	30
domains to be searched.....	30
user accounts.....	44

## S

security	
user accounts.....	43
set system root-authentication command.....	21
set system root-authentication	
encrypted-password command.....	21
setting root password.....	20
special interfaces	
loopback interface.....	40
SSH key files.....	20
support, technical See technical support	
syntax conventions.....	xi
system management	
user accounts.....	43

## T

technical support	
contacting JTAC.....	xiii
troubleshooting	
root password recovery.....	22

## U

uid statement	
usage guidelines.....	44
user access	
user accounts.....	44
user accounts	
configuring.....	44
contents.....	43
user statement	
access	
usage guidelines.....	44
username	
description.....	43
users	
accounts See user accounts	
usernames.....	43