Extreme 9920 Software Deployment Guide, 21.1.0.0

Supporting Extreme 9920

9037101-00 Rev AA
June 2021

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

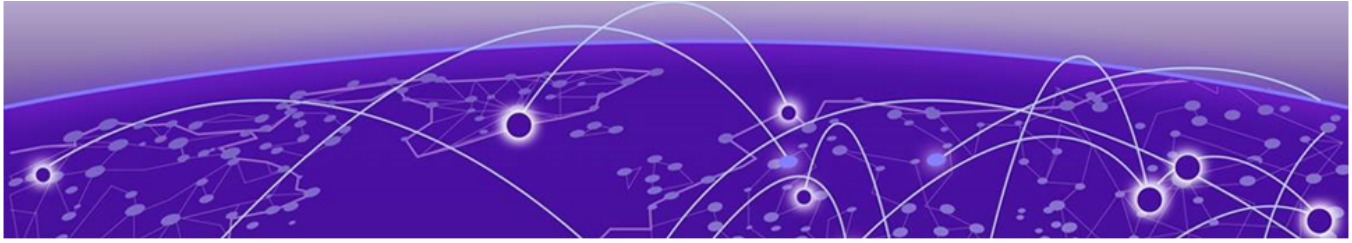


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

- Current Product Documentation
- Release Notes
- Hardware and software compatibility for Extreme Networks products
- Extreme Optics Compatibility
- Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

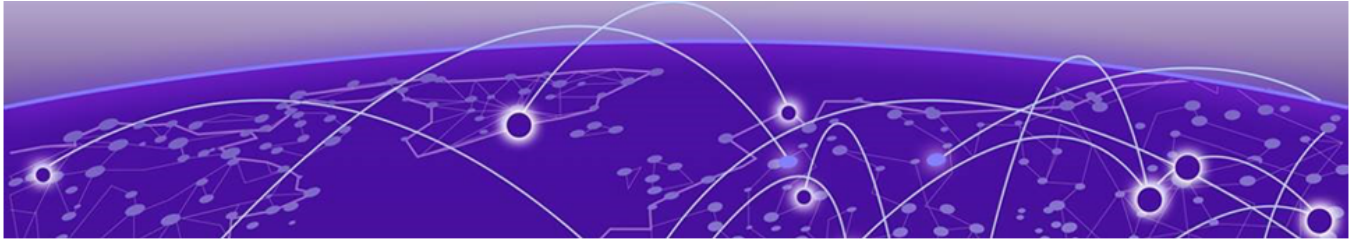
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



What's New in this Document

This document is new for the release of the Extreme 9920 software with the NPB application.

For more information about this release, see the *Extreme 9920 Software Release Notes, 21.1.0.0*.

Deployment Preparation

The Extreme 9920 device runs an operating system (TierraOS) that runs one or more applications. This version of the Extreme 9920 software has one application (NPB application).

NPB Application Overview

The NPB application provides functionality to process and prepare packets for visibility tools. This allows core networking devices to offload network monitoring.

When the Extreme 9920 running Extreme 9920 software is attached to optical taps between the core networking devices, a copy of the traffic is sent to the Extreme 9920 for filtering traffic of interest and formatting before being sent on to visibility tools.

The NPB application supports the following features:

- Aggregation: Aggregates traffic arriving from multiple ports and directs it to a single port or port-channel ("many to one").
- Replication: Replicates network traffic to multiple ports and port-channels ("one to many").
- Load balancing: Distributes network traffic among ports in a port-channel.
- ACL filtering: Directs network traffic based on Layer 2 to Layer 4 protocol headers.
- Route-map forwarding: Redirects packets based on Layer 2 to Layer 4 Protocol headers to the desired physical port or port-channel interfaces.
- Packet slicing: Truncates length of the packet to specified length.
- Tunnel origination: Encapsulates packets with IPv4 Generic Routing Encapsulation (GRE) headers.
- Tunnel termination: Tunnel termination classifies and decapsulates incoming IPv4 packets.
- Encapsulation-header stripping:
  - Removes tags that are not supported by visibility applications.
  - Supports 802.1BR, VN-Tag, VLAN, VXLAN, GTPU, GRE, and IPIP headers.

Supported Device Information

The Extreme 9920 software with the NPB application runs on Extreme 9920 devices.

Default CA certificate

A default CA certificate for TLS is provided to verify the certificate that the Extreme 9920 device issues. All gNMI requests to the device are over a secure channel. The Extreme 9920 uses the default HTTPS server certificate if you do not import an HTTPS server certificate.

Use the following CA certificate on the client to verify the certificate generated by the 9920.

```
-----BEGIN CERTIFICATE-----
MIIGPjCCBCagAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgbMxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTELMAkGA1UEBwwCU0oxGTAXBgNVBAoMEEV4dHJlbWUgTmV0
d29ya3MxHzAdBgNVBAsMFkV4dHJlbWUgTmV0d29ya3MgTkdOUEIxIjAgBgNVBAMM
GW5nbnBiLmV4dHJlbWVuZXR3b3Jrcy5jb20xKjAoBgkqhkiG9w0BCQEWG3N1cHBv
cnRAZXh0cmVtZW5ldHdvcmtzLmNvbTAeFw0yMDA3MDcyMTEzNDNaFw0zMDA3MDUy
MTEzNDNaMIGnMQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExGTAXBgNVBAoMEEV4
dHJlbWUgTmV0d29ya3MxJDAiBgNVBAsMG0V4dHJlbWUgTmV0d29ya3MgTmV4dEdl
bk5QQjEeMBwGA1UEAwwVTkdOUEIgSW50ZXJtZWRpYXRlIENBMSowKAYJKoZIhvcN
AQkBFhtzdXBwb3J0QGV4dHJlbWVuZXR3b3Jrcy5jb20wggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQC64lUkRcEvz+jWfm9V9+g/AgZFpDOKL5oR4c3IHdwM
vAA6Rt+Os+6wvOpLysDvzggeVh4L6BWULgFw5SyRhjKJbyz7PaMBg/id5XPqWntU
3MoPOdewdVozyZZf3MRDVqgw8f7nT4Ex55fSnfyYLOx5g2++rUUK3jpQo74vRI/W
SUZdOAvs9hkERcMJIm4DDcj86Z4HuYaB/iBBSqPDhRoErpaX36TOWY+2wCNomkK1
zzCO9PW3HhfZk+GWF10U/7ZkNOBMnd5nVIalf+VsSpaPzQxAJtIKS1xYqmoACW6s
S/myGEPuDqmYhilwSgP+lyRmpkGZEfPbwxZyrhxUAnwQ0+r8HUSvBRavK+utt+JQ
SeFiPPVeo6OoGgwRJ1t9KVid+Sp56+gwMj27Kf26cWYUJsjjHxyJgFFCforcn40M
Kox5idbZkQjdo7ciofK7Twz8U+ip/lyhbycUcz7cG7vimRvu+BpyJ29zL7It/PZX
U8fP3r0ssudasfwZGxl3AO58szhopE0m4eaIQzhotqwqXt6s8Vh/+qj6JMudMxa6
5HVeBVX6BEvLG8TwKaaQiJ4edwI/QY0WZ0wxfeDn05haSiyOhRkmA/F9cqv3h8qM
B5+IZ+nYNpjASyxc1QTtW9Xhn37vp61+7JddU9zxeSVkB43YGOK9Uq1+DXDawlzA
5wIDAQABo2YwZDAdBgNVHQ4EFgQU2Sn6JG7Jo3QzMRBsLHhQkVW8uzQwHwYDVR0j
BBgwFoAUuwS1PNyE3M192izM7zaoJm1vhTQwEgYDVR0TAQH/BAgwBgEB/wIBADAO
BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBAKRIQfsZiiIVZC3jCmBt
cwf3LRN2ESOy8bj4AV0LxgchjMtw/y/Dp7ST5FkUEIAya8HEmL1tjZhHFh0uNfBx
7UcRV2R7ZhGu08TujFbo9sVy2GHd+w1/L6VDauEjV6eUd4oI6kylcDK/OA3UoYwF
vbiiLlDYEFaP3/3MFaqk9osfmkxcmhu3qxOt3QxqevXPiXtXlNxT4w/LrQFXKMcJ
40zjFjgnNsdYlr92c2kwWDE/44xnOWEH7Ar2PuqvqHJi1GFv1lV/Ys+0wkqCyy/K
eAdde8d8ZWcXroSHzlGI34Tql2U9+bZjxNgU9Nc8VJGq+K9LBDTQqFfGg0n9qHYE
eCGGzw5eT+lJMSVompRPEHt44qCk5eKRmEWsMbgeD8d6cisPE4PffIynSV/evjsY
k9gaE0d86uhN5EuNQsqtLn5vsdWN8nBBP+umPLtHpppHATAGSWgW8WGgSLs8gBwS
IABCVCpV7oePXN0LCfzRTd2JwCmUpqxreGw3cuePDMNimOQvwnaAvLfNxFYSoRtp
wU8VGdAUQJxqkeS4xlkpKbOYGGHlntlskSP7VuygLn2ISa3v6xTRLlaTDcLuiu+K
vNGwM33rgKUiPtDFM9oK0CtiydM1TqfQZB3/B1a3RzqX2OmBvR6qB9M5jeNQXd+T
wa/daP9p2G6/lcNRE+AiCpul
-----END CERTIFICATE-----
```

Extreme 9920 Software

Extreme 9920 software consists of infrastructure/OS software and micro services. The infrastructure/OS software includes Linux kernel, root filesystem, and Kubernetes to control and manage micro services. Micro services are software components that provide various services and functionality.

The build script builds images for all modules and forms a ONIE compatible bin image during installation for both net-install and firmware update.

Extreme 9920 software image, `TierraOS-<release_no>-NPB.bin` is a binary file and contains all components except ONIE (bootloader). the application images can be downloaded from http://engartifacts1.extremenetworks.com:8089/artifactory/tierra-local-snapshots/build/.

You can download the Extreme 9920 software image from a remote server using any of the following methods:

- Prepared USB 3.0 device
- Remote NFS share
- HTTP
- FTP
- TFTP

Extreme 9920 Software Operating System

Extreme 9920 software Operating System (TierraOS) is built using the standard ONLPv2 procedure. Installation of Extreme 9920 software is done using Open Networking Install Environment (ONIE) standard.

ONIE is the combination of a boot loader and a small operating system for bare metal network devices that provides an environment for automated provisioning or recovery of the device. The Extreme 9920 device boots the software from the images stored on the hard disk of the device. ONIE also provides mechanisms to re-install or update the software if the normal software download process fails.

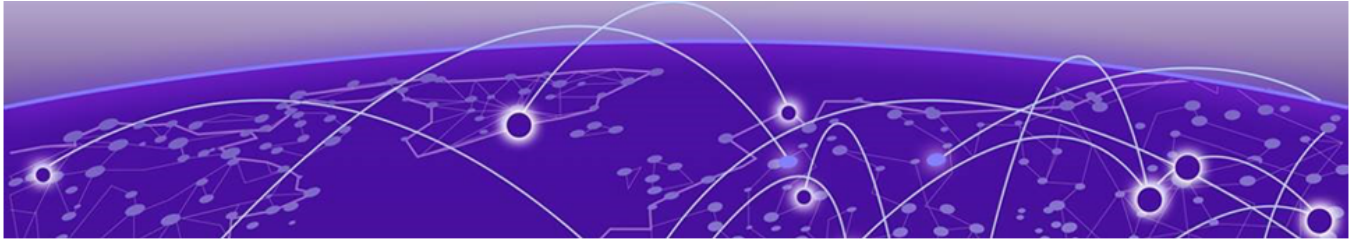
The process supported by the **`system firmware upgrade`** command is not affected by this feature. The Extreme 9920 software is not updated to the snapshot partition during the normal upgrade process.

ONL Linux 4.14 Kernel Design Components

ONL Linux 4.14 Kernel design provides boot loader ONIE (with EEPROM driver) and ONL (Super IO driver).

Table 4: ONL Linux 4.14 Kernel Design Components

Component	Linux Kernel Version	Description
Extreme Open Networking Install Environment (ONIE)	4.9.95	• Based on https://github.com/opencomputeproject/onie.git • `ONIE rootfs` contains binaries that are required to program `eeprom` and Network Operating System (NOS). • `eeprom address - 0x57` • `eeprom spec - <eeprom_spec_link>`.
Extreme Open Networking Linux (ONL)	4.14.59	• Based on https://github.com/opencomputeproject/OpenNetworkLinux/tree/ONLPv2. • The `ONL rootfs` is built and managed by the standard ONLPv2 compilation. • ONLPv2 is the base for building packages in TierraOS.



Installation and Upgrade

The topics in this section provide the information required to install and upgrade the Extreme 9920 software.

Install Extreme 9920 Software

Before You Begin

- Throughout the installation process, a serial console must be connected to the device.
- The out-of-band management Ethernet interface must be connected if you are using a remote NFS share, HTTP, FTP, or TFTP:
  - Availability of a DHCP server on the LAN for this Ethernet interface may allow you to skip the need to manually configure the ONIE to connect to one of the network-based methods of transferring the software.
  - If a DHCP server is not available, you need the default gateway, network mask, and an IP address that is not in use on the network to which the Ethernet interface is connected.

About This Task

Perform the following steps from the serial console.

Procedure

1. Access the ONIE Recovery Shell.
   a. Reboot the device using the CLI or power-cycle.
   b. When the BIOS splash screen is displayed, use the **Down Arrow** key to access the GRUB boot menu and stop the boot timer.
   c. Select **ONIE** from the first menu, and press the **Down Arrow** key to stop the boot timer.
   d. Select **ONIE: Rescue**, and press **Enter** when prompted.

      The ONIE shell opens.

   You can use ONIE for recovering or upgrading the device.

2. Perform one of the following:
   - If a DHCP server is running on the network, proceed to the next step.
   - If using remote server to download the firmware, go to step 5 on page 14.
3. Check connectivity to the server hosting the software.
   a. Ping the remote server to download the software.

   - USB 3.0 device
   - Remote NFS share
   - HTTP
   - FTP
   - TFTP

   a. If ping fails, run the following commands to gather information on the connection state.

   ```
   ip addr
   ip route show
   ifconfig
   ```

   If there are any errors, perform step 4 to resolve them. Else proceed to step 5 on page 14.
4. Configure static networking on eth0 for ONIE.
   a. Add the IP address to the eth0 interface.

   ```
   ONIE:/ #ip addr add <ip-addr/mask> dev eth0
   ```

   b. Configure the default gateway.

   ```
   ONIE:/ #ip route add default via <gateway-ip-addr> dev eth0
   ```
5. Download and install the Extreme 9920 software firmware using one of the following remote server methods:
   - Perform USB Disk-Based Recovery on page 14
   - Perform NFS-Based Recovery on page 15
   - Perform HTTP-Based Recovery on page 15
   - Perform FTP-Based Recovery on page 16
   - Perform TFTP-Based Recovery on page 16

   A checksum validation is done before installing the firmware.
6. Activate the firmware using `Activate gRPCs`.
7. Verify if the installation is successful using `Verify gRPCs`.

Perform USB Disk-Based Recovery

Procedure

1. From the serial console, download and decompress the software tarball.
2. Transfer the resulting directory to an inserted USB 3.0 device.
3. Eject or unmount the USB device and insert it into the correct port of the Extreme 9920 device.
4. Run the **`fdisk -l`** command. In the output, locate the device identifier of the inserted USB device.

   The USB device is generally the last device listed.

5. Run the **mkdir /media** and **mount /dev/<device-identifier> /media** commands.

   You may see a warning, but the disk should mount.
6. Change directory to the Network Packet Broker software that you want to install and start the installation using the `onie-nos-installer file: //`.
7. Select the binary file for the Extreme 9920.

   ```
   ONIE:/ #cd media/
   ONIE:/ media/ #ls ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

   The device reboots and loads the software.

Perform NFS-Based Recovery

Procedure

1. On a Linux device, configure a NFS share, download and decompress the software tarball, and move the resulting directory to the root of the NFS share.
2. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.

      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```

   b. Configure the default route.

      ```
      # route add default gw 10.139.69.1
      ```

   c. Verify network connectivity to the server.

      ```
      # ping 10.139.69.1
      ```
3. Run the **mkdir /media** and **mount :/<path-to-NFS-share>/ /media** commands.

   If an error results, troubleshoot the **mount** command. You may need more parameters or a more explicit path.
4. Change directory to the Network Packet Broker software that you want to install and start the installation using the `onie-nos-installer file: //`.
5. Select the binary file for the Extreme 9920.

   ```
   ONIE:/ #cd media/

   ONIE:/ media/ #ls ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

   The process takes approximately 15 to 20 minutes to complete. The device reboots and loads the software.

Perform HTTP-Based Recovery

Procedure

1. On a web server, download and decompress the software tarball and move the resulting directory to the root of the web server.
2. Modify the permissions of the directory to allow access for the web server daemon.
3. Verify that the software directory is accessible by using a web browser to access the directory.

4. On the Extreme 9920, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```
   c. Verify network connectivity to the server.
      ```
      # ping 10.139.69.1
      ```
5. Run the **onie-nos-install** command with the URL to the binary for the device.
   ```
   ONIE:/ #onie-nos-install http://<URL-to-binary>/
   ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

Perform FTP-Based Recovery

Procedure

1. On an FTP server, download and decompress the software tarball and move the resulting directory to the root of the FTP server.
2. Modify the permissions of the directory to allow access for the FTP server daemon. The FTP server must allow anonymous access.
3. Verify that the software directory is accessible by using an FTP client to access the directory.
4. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```
   c. Verify network connectivity to the server.
      ```
      # ping 10.139.69.1
      ```
5. Run the **onie-nos-install** command with the URL to the binary for the device.
   ```
   ONIE:/ #onie-nos-install http://<URL-to-binary>/
   ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
   ```

Perform TFTP-Based Recovery

Procedure

1. On a TFTP server, download and decompress the software tarball and move the resulting directory to the root of the TFTP server.
2. Modify the permissions of the directory to allow access for the TFTP server daemon.
3. On the Extreme 9920 device, configure and verify network connectivity to the server.
   a. Configure the network.
      ```
      # ifconfig eth1 10.139.69.108 netmask 255.255.254.0 up
      ```
   b. Configure the default route.
      ```
      # route add default gw 10.139.69.1
      ```

c. Verify network connectivity to the server.

```
# ping 10.139.69.1
```

TFTP may appear to be non-operational while transferring the file.

4. Run the **onie-nos-install** command with the URL to the binary for the device.

```
ONIE:/ #onie-nos-install http://<URL-to-binary>/
ONLPv2_ONIE_installer.bin.NGNPB_<version_date_build>_UTC
```

View Firmware Version Information

Procedure

1. View the primary and secondary firmware version information.

```
show firmware
```

2. View the last five firmware versions activated on the device.

```
show firmware history
```

3. View the firmware logging information.

```
show logging audit firmware
```

Upgrade Extreme 9920 Firmware

Extreme 9920 firmware contains primary and secondary images. When a new Extreme 9920 firmware is installed, the image in the secondary location is removed and the image in the primary location is moved to the secondary location. The new image is installed in the primary location.

Procedure

1. Update the Extreme 9920 firmware.

```
system firmware update [ [ scp | sftp [://username:password@host[:port]/filepath] ] |
[ htp | https [://[username:password@]host[:port]/filepath] ] ]
```

- If the firmware update is successful, the system is rebooted automatically to activate the new version.

  The reboot reason is updated to `RR_UPGRADE` to indicate firmware update or rollback. The reboot reason is notified through `chassis-0` property.

- After reboot, all micro services are expected to come up. If the micro services come up, `Firmware Rev` property in `chassis-0` component is published to `State DB` with the running firmware image.
- If any of the micro services fail to come up within the specified duration, an automatic rollback to the previous image is triggered.

2. (Optional) If the new firmware version is not required, rollback to the previous version.

```
system firmware rollback
```

Supported Microservice Upgrades

Extreme 9920 software supports the following microservice upgrades:

- agent-pbd-ms
- agent-sp-intf-ms
- agent-sp-nhop-ms
- agent-sp-sfcs-ms
- agent-sp-target-proxy-ms
- agent-svcplane-ms
- chassis-ms
- ifmgr-ms
- lacp-ms
- mgmt-security
- onboard-pcap-ms
- pktmgr-ms
- mgmt-snmp-agent

Upgrade Microservice

About This Task

Microservice images are `tar.gz` files. Each `tar.gz` file contains a `manifest.json` file with the service name and version number.

Before You Begin

- Micorservice upgrade must be performed in the maintenance window.
- Ensure that there is no change in the configuration during the upgrade procedure.

Procedure

1. Copy the microservice image to the device using SCP, SFTP, HTTP or HTTPS.
2. Update the required microservice.

```
system service update [ [ scp | sftp [://username:password@host[:port]/filepath] ] |
[ htp | https [://[username:password@]host[:port]/filepath] ] ]
```

3. Activate the new version.
   - All previous microservice images are saved at `flash://ms_images/<service-name>` `directories`.

     There is no limit to the number of files saved on the disk other than disk space. However, the files are removed if the the application firmware is upgraded.
   - The current service stops and the new service starts.
   - Service shutdown handler is invoked as part of the **`kubectl set image`** command.
   - The microservice handles graceful shutdown or recovery and sets the restart reason (`MSSR_UPGRADE`). When new version of the microservice comes up, it checks the restart reason and takes necessary steps to be operational again.

4. (Optional) If the new microservice version is not required, roll back to the previous running version.

```
system service rollback service-name
```

5. (Optional) Activate any of the previous versions of the microservice.

```
system service update flash://ms_images/<service-name> directories
```

After rollback, if any of the services do not come up, the `Status` property for `chassis-0` component is set to `Degraded` state.