



# Troubleshooting

---

- [Troubleshooting, on page 1](#)
- [Understanding Diagnostic Mode, on page 1](#)
- [Before Contacting Cisco or Your Reseller, on page 2](#)
- [show interfaces Troubleshooting Command, on page 2](#)
- [Software Upgrade Methods, on page 2](#)
- [Change the Configuration Register, on page 3](#)
- [Recovering a Lost Password, on page 6](#)

## Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a PC to the router via the console port. With a connected PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface by using Telnet. The Telnet option assumes that the interface is up and running.

## Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.

- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

## Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

## show interfaces Troubleshooting Command

Use the **show interfaces** command to display the status of all physical ports and logical interfaces on the router. describes messages in the command output.

The IR8340 supports the following interfaces:

- GigabitEthernet 0/0/0 and 0/0/1
- Cellular 0/4/0, Cellular 0/4/1, Cellular 0/5/0, and Cellular 0/5/1
- msata

## Software Upgrade Methods

Several methods are available for upgrading software on the Cisco IR1840H Routers, including:

- Copy the new software image to flash memory over the WAN interface when the existing Cisco IOS software image is in use.
- Copy the new software image over the console port while in ROM monitor mode.

- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To boot the image from the TFTP server, the TFTP server must be on the same network as the router.

## Change the Configuration Register

To change a configuration register, follow these steps:

### Procedure

- Step 1** Connect a PC to the CONSOLE port on the router.
- Step 2** At the privileged EXEC prompt (*router\_name #*), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

#### Example:

```
Router# show version
Cisco IOS XE Software, Version BLD_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91
Cisco IOS Software [Bengaluru], ir8340 Software (X86_64_LINUX_IOSD-UNIVERSALK9_IOT-M),
Experimental Version 17.7.20210827:033430
[S2C-build-v177_throttle-289-/nobackup/mcpre/BLD-BLD_V177_THROTTLE_LATEST_20210827_030512
154]
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 27-Aug-21 15:58 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: v0.33
```

```
Router uptime is 1 week, 1 day, 23 hours, 9 minutes
Uptime for this control processor is 1 week, 1 day, 23 hours, 10 minutes
System returned to ROM by Reload Command
System image file is
"flash:ir8340-universalk9.BLD_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91.SSA.bin"
Last reload reason: Reload Command
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Technology Package License Information:

```
-----
Technology Type Technology-package Technology-package
Current Next Reboot
-----
Smart License Perpetual network-advantage network-advantage
Smart License Subscription None None
```

The current crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

```
cisco IR8340-K9 (2RU) processor with 3717851K/6147K bytes of memory.
Processor board ID FDO2502JF0L
Router operating mode: Autonomous
1 Virtual Ethernet interface
14 Gigabit Ethernet interfaces
8 Serial interfaces
8 terminal lines
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7574982K bytes of flash memory at bootflash:.
33554432K bytes of mSATA at msata:.
929715K bytes of sdcard flash at sdcard:.
30031856K bytes of USB flash at usb0:.
```

Configuration register is 0x0

Router#

**Step 3** Record the setting of the configuration register.

**Step 4** To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register** *<value>* command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

## Configuring the Configuration Register for Autoboot



**Note** Altering the configuration register is only for advanced troubleshooting and should only be done with guidance from Cisco support.

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the **config-reg** 0x0 command.

- From the ROMMON prompt, use the **confreg 0x0** command.



**Note** Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

## Reset the Router

To reset the router, follow these steps:

### Procedure

- Step 1** If the break is disabled, turn off the router, wait for 5 seconds and turn the router back on. Within 60 seconds push the Reset button.

The terminal displays the Rommon prompt.

**Example:**

```
rommon 1>
```

- Step 2** Enter **confreg 0x2142** to ignore the running config.

**Example:**

```
rommon 2> confreg 0x142
```

- Step 3** Sync the configuration changes with the **sync** command.

**Example:**

```
rommon 3>sync
```

- Step 4** Reset the router to apply confreg. The router will reload with the reset.

**Example:**

```
rommon 4>reset
```

```
resetting...
```

- Step 5** Verify that the correct confreg 0x2142 was applied, and enter **n** when asked if you want to change the configuration.

**Example:**

```
rommon 1> confreg
Configuration Summary
(Virtual Configuration Register: 0x2142)
enabled are:
[ 0 ] console baud: 9600
boot:..... image specified by the boot system commands
do you wish to change the configuration? y/n [n]: n
```

- Step 6** Boot the image with the confreg 0x2142.

**Example:**

```
rommon 2> boot
flash:ir8340-universalk9.BLD_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91.SSA.bin
```

## Recovering a Lost Password

To recover a lost password, follow these steps. Refer to [Reset the Router, on page 5](#) for details.

1. Reset the router.
2. Change the confreg to 0x2142.
3. Boot the router with confreg 0x2142 from Rommon.
4. If you used the reset button, add the license:

```
Router#config term
Router#license smart reservation
```



**Note** Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

## Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

### Procedure

**Step 1** Enter the **configure terminal** command to enter global configuration mode:

**Example:**

```
Router# configure terminal
```

**Step 2** Enter the **configure register** command and the original configuration register value that you recorded.

**Example:**

```
Router(config)# config-reg
value
```

**Step 3** Enter **exit** to exit configuration mode:

**Example:**

```
Router(config)# exit
```

**Note** To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

**Step 4** Reboot the router, and enter the recovered password.

## Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>transport-map type console</b> <i>transport-map-name</i> <b>Example:</b> Router (config) # <b>transport-map type console consolehandler</b>	Creates and names a transport map for handling console connections, and enters transport map configuration mode.
<b>Step 4</b>	<b>connection wait [allow [interruptible]   none [disconnect]]</b> <b>Example:</b> Router (config-tmap) # <b>connection wait none</b>	Specifies how a console connection will be handled using this transport map. <ul style="list-style-type: none"> <li>• <b>allow interruptible</b>—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting.</li> </ul> <p><b>Note</b> Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> <ul style="list-style-type: none"> <li>• <b>none</b>—The console connection immediately enters diagnostic mode.</li> </ul>
<b>Step 5</b>	(Optional) <b>banner [diagnostic   wait]</b> <i>banner-message</i> <b>Example:</b> Router (config-tmap) # <b>banner diagnostic</b>	(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.

	Command or Action	Purpose
	<p><b>X</b> Enter TEXT message. End with the character 'X'. <b>--Welcome to Diagnostic Mode--</b> <b>X</b> Router(config-tmap)#</p>	<ul style="list-style-type: none"> <li>• <b>diagnostic</b>—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.</li> </ul> <p><b>Note</b> Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> <ul style="list-style-type: none"> <li>• <b>wait</b>—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.</li> <li>• <i>banner-message</i>—Banner message, which begins and ends with the same delimiting character.</li> </ul>
<b>Step 6</b>	<p><b>exit</b> <b>Example:</b>  Router(config-tmap)# <b>exit</b></p>	Exits transport map configuration mode to re-enter global configuration mode.
<b>Step 7</b>	<p><b>transport type console</b> <i>console-line-number</i> <b>input</b> <i>transport-map-name</i> <b>Example:</b>  Router(config)# <b>transport type console</b> <b>0 input consolehandler</b></p>	<p>Applies the settings defined in the transport map to the console interface.</p> <p>The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the <b>transport-map type console</b> command.</p>

### Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```



## Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

**show transport-map** [**all** | **name** *transport-map-name* | **type** [**console** ]]

This command can be used either in user EXEC mode or privileged EXEC mode.

### Example

The following example shows transport maps that are configured on the router: console port (*consolehandler*):

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type console
Transport Map:
Name: consolehandler

REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides

the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

### Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

## Using the factory reset Commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.




---

**Caution** Use of the factory reset command should not be done lightly. All customer configurations will be deleted and the platform will boot up as if new from the factory.

---




---

**Note** factory-reset all does not work if IOS-XE is running in controller mode. Please refer to SDWAN configuration information.

---

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
*Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.

***Return to ROMMON Prompt
```

### Boot Sequence after Factory Reset

Booting the image:

- The bootloader attempts to boot “golden.bin” from the bootflash: partition
- If no “golden.bin” is present, then boot the first image.

Loading the configuration:

- IOS looks for “golden.cfg” file on nvram: partition and applies it upon booting.
- If no “golden.cfg” is present on nvram: then IOS looks for “golden.cfg” file on bootflash: partition and applies it upon booting.
- If no “golden.cfg” is present on bootflash: then configurations are erased and Software Configuration dialog is used.

