

# Chapter 2

## Strategies for Monitoring and Troubleshooting the Router

This chapter describes the standard methods and most common tools used in troubleshooting the router. It discusses troubleshooting basics, including how, when, and why you use commands to monitor and troubleshoot the router and network. This chapter also includes a list of the commands most commonly used by Network Operation Centers (NOCs) for monitoring and troubleshooting.

This chapter discusses the following topics:

Basic Approaches to Troubleshooting on page 31

Tools for Troubleshooting on page 35

### Basic Approaches to Troubleshooting

This section discusses the following aspects of troubleshooting:

Troubleshooting Process on page 31

Identify the Symptoms on page 32

Isolate the Cause on page 32

Take Corrective Action on page 33

Evaluate the Solution on page 33

For a troubleshooting example, see “Example: Strategy for Isolating a Broken Network Connection” on page 34.

### ***Troubleshooting Process***

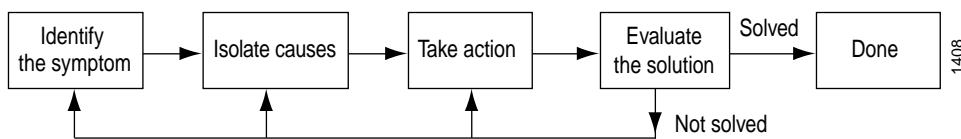
Troubleshooting can be simplified by following standard procedures, as illustrated by Figure 2. Standard troubleshooting procedures include the following steps:

1. Identify symptoms. A symptom can be defined as any undesired results or behavior. A problem or failure might exhibit one or more symptoms.
2. Isolate the cause of the symptom.
3. Take action to correct the problem.

4. Evaluate the system to see if the original problem is solved and to verify that new problems have not been introduced by the changes you made.
5. At this point, either you have solved the problem, or you must return to Steps 1, 2, or 3 and identify the symptoms more clearly, isolate additional possible causes, or take additional action to correct the problem.

During the troubleshooting process, you might isolate causes that require additional troubleshooting before you can continue with the standard process.

Figure 2: Troubleshooting Process



## Identify the Symptoms

Identifying symptoms requires careful observation. The best preparation for troubleshooting is knowing your network thoroughly before a problem occurs so that you have a baseline state from which to work. If you understand how the network functions under normal conditions, it is easier to distinguish between normal and abnormal activity.

Sometimes a problem is related to another condition that must be solved first. When identifying symptoms, record as many parameters as you can regarding the offending state. The more information you have, the easier it is to isolate the cause. If you find a set of symptoms, try to decide what they have in common. It is likely that they are related, and noticing as many symptoms as you can provides you with more information as you proceed.

It is also useful to record what changes have taken place since the system was last functioning correctly. Changes in activity are likely to be related to changes in configuration.

## Isolate the Cause

A particular symptom can be the result of one or more causes. Successful troubleshooting requires narrowing the focus to find each individual cause for unwanted behavior. While you might find a solution by just trying a variety of actions, you reach the desired solution more quickly if you systematically approach the problem.

There are several useful methods for isolating a problem:

**Retrace your steps**—Try to return to a state that existed before the problem appeared. When the network is in a known state, take small steps forward, watching carefully for the recurrence of symptoms.

**Divide the problem into its smallest unit**—Cut the problem in half and test each half. If only one half continues to have the problem, cut it in half again or compare it to the valid half to see how it is different. You might find the solution in the difference.

Identify which functions are working correctly—Do not waste time investigating functions that are not broken.

Keep careful records of changes and effects—Ask questions and document changes as you work on a system.

Notice how various symptoms might be related—If you are finding unexpected or undesired results in more than one area, try to discover what those areas have in common and what variables would affect them. You likely will find the source for the problem in the common areas.

Imagine what type of errors or failures could lead to the particular symptom— Test for the errors or failures to see if they are actually occurring.

Do not try to solve multiple unrelated problems simultaneously—If multiple symptoms occur that do not appear to be related, select one symptom or set of symptoms and focus on it. However, do not completely ignore the other symptoms, because you might discover that they are related after all.

Several useful tools exist for isolating the cause of a problem, including network analyzer traces, core dumps, serial line traces, stack dumps, and the output from various show commands in CLI. For information about the show commands, see the chapters in this manual that describe the JUNOS monitoring commands.

## ***Take Corrective Action***

The action required depends on the type of problem you have isolated. As you troubleshoot, keep in mind the following principles:

Document each step you take.

Use the various CLI show commands to verify which behaviors change with each action you take.

When you are considering several possible actions, you can choose to test the easiest first, thereby eliminating possibilities quickly, or you can choose the action that appears most likely to solve the problem, even if it is more time-consuming or difficult to perform.

## ***Evaluate the Solution***

Carefully test the solution to ensure that it does not introduce new symptoms. If new symptoms occur, start the troubleshooting process again, carefully documenting the changes you make in the process.

### **Example: Strategy for Isolating a Broken Network Connection**

To illustrate the troubleshooting process, we examine a problem that appears to include a broken network connection. By applying the strategy listed below and shown in Figure 3, you can usually isolate the failed node:

Identify symptom—Failure to reach remote host.

Isolate causes—Several possible causes are identified, including:

Local router is misconfigured.

Intermediate router is misconfigured.

Remote router is misconfigured.

No path to the remote router in the local routing table.

Take action—Appropriate actions are taken for each possible cause, including:

Check the local router's configuration and edit if appropriate.

Troubleshoot intermediate router.

Check the remote host configuration and edit if appropriate.

Troubleshoot routing protocols.

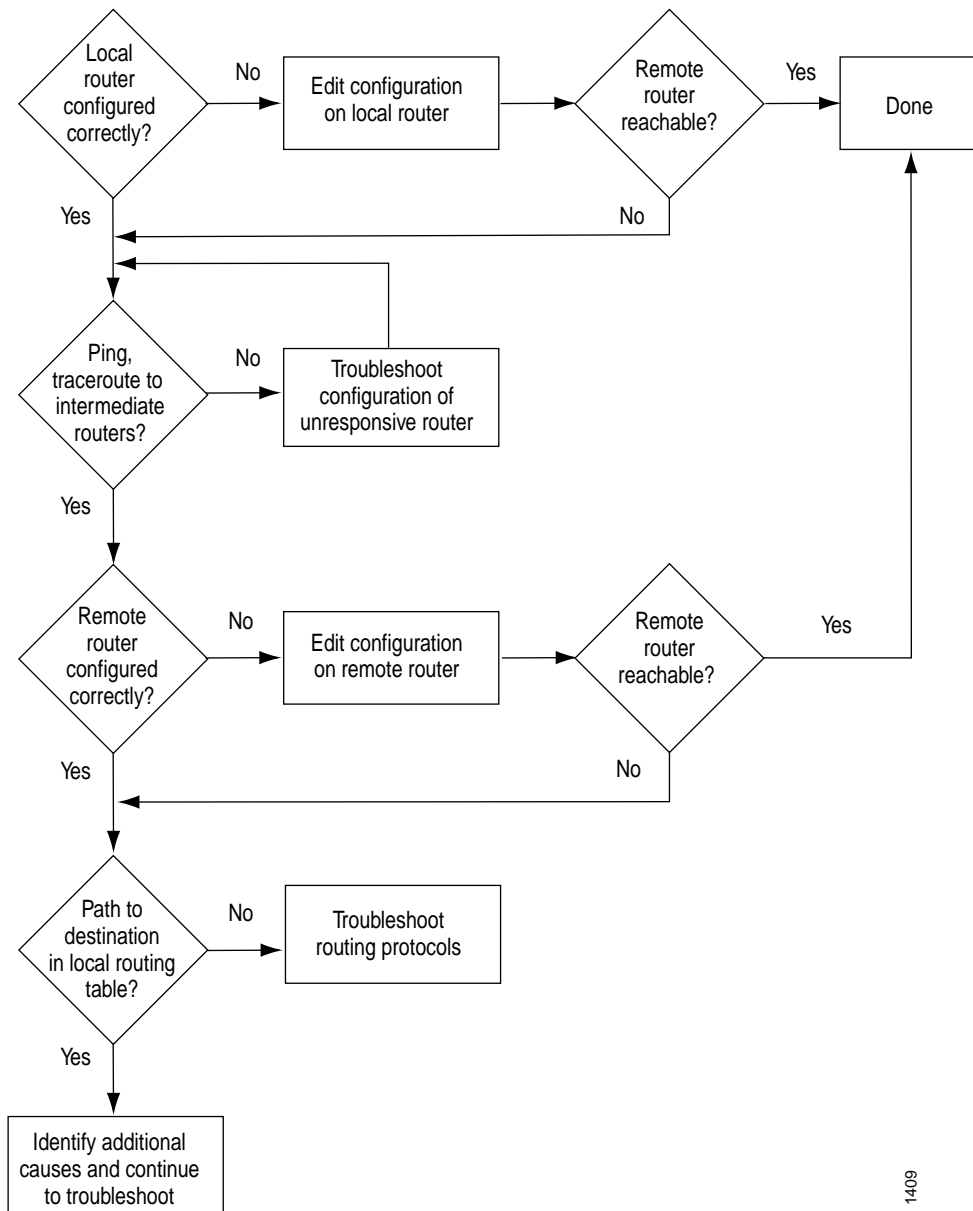
Identify additional possible causes.

Evaluate solution—If the problem is solved, you are done. If the problem remains or a new problem is identified, start the process over again.

You can address possible causes in any order. In Figure 3, we chose to work from the local router toward the remote router, but you might start at a different point, particularly if you had reason to believe the problem was related to a known issue, such as a recent change in configuration.

Often, troubleshooting one symptom will uncover other symptoms. Figure 3 shows two possible causes that might involve additional troubleshooting.

Figure 3: Example: Locating a Broken Network Connection



## Tools for Troubleshooting

You can use the following tools when troubleshooting your network:

Commonly Used Operational Mode Commands on page 36

Craft Interface on page 37

## Commonly Used Operational Mode Commands

Table 4 lists common operational mode commands that you can use to monitor and troubleshoot the router, network, and traffic.

Table 4: Commonly Used Operational Mode Commands

Task	Task or Information to Monitor	Command
Software Version	Versions of software running on the router.	show version on page 95
Log Files	Contents of the log files.	monitor on page 46
	Log files and their contents and recent user logins.	show log on page 60
Remote System Reachability	Host reachability and network connectivity.	ping on page 47
	Route to a network system.	traceroute on page 99
Configuration	Current running system configuration.	show configuration on page 58
Manipulate Files	List of files and directories on the router.	file list on page 45
	Contents of a file.	file show on page 46
Static Interface Information	Detailed information about interfaces.	show interfaces on page 126
	Summary information about interfaces.	show interfaces terse on page 288
Chassis	Chassis alarm status.	clear chassis craft-interface display on page 306
	Information currently on craft display.	show chassis craft-interface on page 313
	Router environment information.	show chassis environment on page 315
	Hardware inventory.	show chassis hardware on page 329
Routing Table Information	Information about the entries in the routing tables.	show route on page 350
Forwarding Table Information	Information about the entries in the kernel's forwarding table.	show route forwarding-table on page 367
IS-IS	Adjacent routers.	clear isis adjacency on page 392
OSPF	Adjacent routers.	show ospf neighbor on page 420
BGP	Entries in the BGP neighbor database.	clear bgp neighbor on page 428
MPLS	Status of interfaces on which MPLS is running.	show mpls interface on page 490
	Configured LSPs on this router, as well as all ingress, transit, and egress LSPs.	show mpls lsp on page 490
	Routes that form a label-switched path.	show route label-switched-path on page 373
RSVP	Status of interfaces on which RSVP is running.	show rsvp interface on page 505
	Currently active RSVP sessions.	show rsvp session on page 508
	RSVP packet and error counters.	show rsvp statistics on page 512
Information for Customer Support	System information to collect before contacting customer support.	request support information on page 50

## **Craft Interface**

You can use the craft interface to view and obtain status and troubleshooting information about the router. The craft interface is located on the front of the router and contains the following elements:

System LEDs—Report the status of the Routing Engine, the status of each Flexible PIC Concentrator (FPC), and general system alarm conditions.

System buttons—Used to reset clocks and stop alarms. Each FPC has a button that you press to take the FPC offline, allowing safe removal of the FPC.

LCD display (on some routers)—Displays current system status or alarm conditions.

Alarm relay contacts—Allow you to connect external alarm devices.

Routing Engine ports—Allow you to connect the following external management devices:

Console port—Used to connect a system console to the Routing Engine with an RS-232 serial cable.

Auxiliary port—Used to connect a laptop or modem to the Routing Engine with an RS-232 serial cable.

Ethernet management port—Used to connect the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management of the router system. The Ethernet port can be 10 or 100 Mbps and uses an autosensing RJ-45 connector.

