

Troubleshooting Tools

12.3.1

Software Troubleshooting Tools

As you know, networks are made up of software and hardware. Therefore, both software and hardware have their respective tools for troubleshooting. This topic discusses the troubleshooting tools available for both.

A wide variety of software and hardware tools are available to make troubleshooting easier. These tools may be used to gather and analyze symptoms of network problems. They often provide monitoring and reporting functions that can be used to establish the network baseline.

Click each button for a detailed description of common software troubleshooting tools.

Network Management System Tools

Network Management System Tools

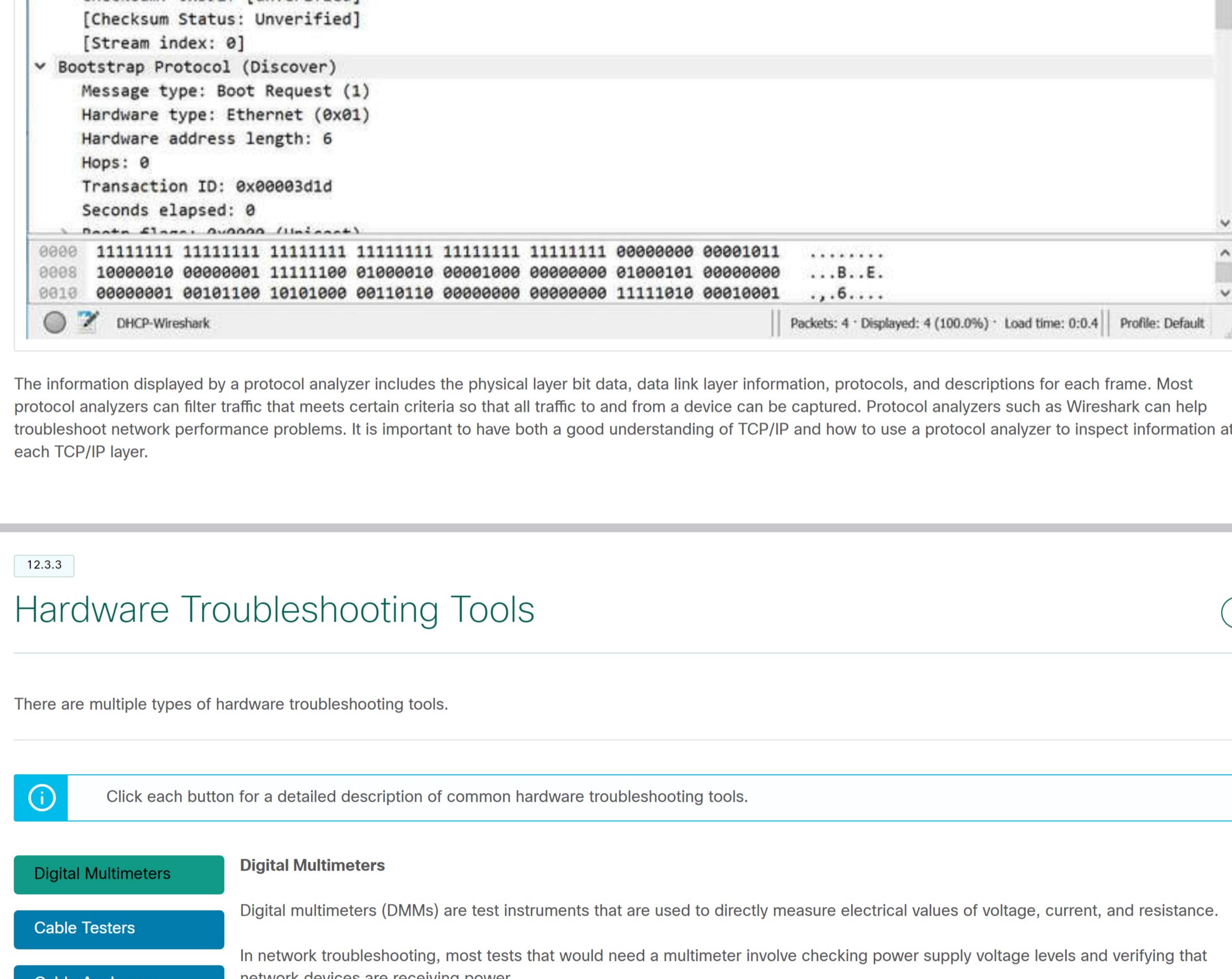
Network management system (NMS) tools include device-level monitoring, configuration, and fault-management tools. These tools can be used to investigate and correct network problems. Network monitoring software graphically displays a physical view of network devices, allowing network managers to monitor remote devices continuously and automatically. Device management software provides dynamic device status, statistics, and configuration information for key network devices. Search the Internet for "NMS Tools" for more information.



12.3.2

Protocol Analyzers

Protocol analyzers can investigate packet content while flowing through the network. A protocol analyzer decodes the various protocol layers in a recorded frame and presents this information in a relatively easy to use format. The figure shows a screen capture of the Wireshark protocol analyzer.



The information displayed by a protocol analyzer includes the physical layer bit data, data link layer information, protocols, and descriptions for each frame. Most protocol analyzers can filter traffic that meets certain criteria so that all traffic to and from a device can be captured. Protocol analyzers such as Wireshark can help troubleshoot network performance problems. It is important to have both a good understanding of TCP/IP and how to use a protocol analyzer to inspect information at each TCP/IP layer.

12.3.3

Hardware Troubleshooting Tools

There are multiple types of hardware troubleshooting tools.

Click each button for a detailed description of common hardware troubleshooting tools.

Digital Multimeters

Digital Multimeters

Digital multimeters (DMMs) are test instruments that are used to directly measure electrical values of voltage, current, and resistance.

In network troubleshooting, most tests that would need a multimeter involve checking power supply voltage levels and verifying that network devices are receiving power.

Cable Testers

Cable Testers

Cable testers are used to verify the integrity of network cables. They can check for continuity, identify the end of the cable, and detect faults such as short circuits or open wires.

Cable Analyzers

Cable Analyzers

Cable analyzers are used to verify the integrity of network cables. They can check for continuity, identify the end of the cable, and detect faults such as short circuits or open wires.

Portable Network Analyzers

Portable Network Analyzers

Portable network analyzers are handheld devices that can be used to troubleshoot network problems. They can capture and analyze network traffic to identify errors and determine the cause of a problem.

Cisco Prime NAM



12.3.4

Syslog Server as a Troubleshooting Tool

Syslog is a simple protocol used by an IP device known as a syslog client, to send text-based log messages to another IP device, the syslog server. Syslog is currently defined in RFC 5424.

Implementing a logging facility is an important part of network security and for network troubleshooting. Cisco devices can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Cisco devices can send log messages to several different facilities. Event messages can be sent to one or more of the following:

- Console** - Console logging is on by default. Messages log to the console and can be viewed when modifying or testing the router or switch using terminal emulation software while connected to the console port of the network device.
- Terminal Lines** - Enabled EXEC sessions can be configured to receive log messages on any terminal lines. Like console logging, this type of logging is not stored by the network device and, therefore, is only valuable to the user on that line.
- Buffered Logging** - Buffered logging is a little more useful as a troubleshooting tool because log messages are stored in memory for a time. However, log messages are cleared when the device is rebooted.
- SNMP Traps** - Certain thresholds can be preconfigured on routers and other devices. Router events, such as exceeding a threshold, can be processed by the router and forwarded as SNMP traps to an external SNMP network management station. SNMP traps are a viable security logging facility but require the configuration and maintenance of an SNMP system.
- Syslog** - Cisco routers and switches can be configured to forward log messages to an external syslog service. This service can reside on any number of servers or workstations, including Microsoft Windows and Linux-based systems. Syslog is the most popular message logging facility, because it provides long-term log storage capabilities and a central location for all router messages.

Cisco IOS log messages fall into one of eight levels, as shown in the table.

	Level	Keyword	Description	Definition
Highest Level	0	Emergencies	System is unusable	LOG_EMERG
	1	Alerts	Immediate action is needed	LOG_ALERT
	2	Critical	Critical conditions exist	LOG_CRIT
	3	Errors	Error conditions exist	LOG_ERR
Lowest Level	4	Warnings	Warning conditions exist	LOG_WARNING
	5	Notifications	Normal (but significant) condition	LOG_NOTICE
	6	Informational	Informational messages only	LOG_INFO
	7	Debugging	Debugging messages	LOG_DEBUG

The lower the level number, the higher the severity level. By default, all messages from level 0 to 7 are logged to the console. While the ability to view logs on a central syslog server is helpful in troubleshooting, sifting through a large amount of data can be an overwhelming task. The `logging trap level` command limits messages logged to the syslog server based on severity. The level is the name or number of the severity level. Only messages equal to or numerically lower than the specified level are logged.

In the command output, system messages from level 0 (emergencies) to 5 (notifications) are sent to the syslog server at 209.165.200.225.

```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
R1(config)#
```

12.3.5

Check Your Understanding – Troubleshooting Tools

Check your understanding of troubleshooting tools by choosing the BEST answer to the following questions.

1. Which of these is an on-line network device vendor resource that can be used as a source of information?

- Baseline tool
- Knowledge base
- Network Management System (NMS)
- Protocol analyzer

2. Which tool is useful to investigate packet content while flowing through the network?

- Baseline tool
- Knowledge base
- Network Management System (NMS)
- Protocol analyzer

3. Which hardware troubleshooting tool is a multifunctional handheld device used to test and certify copper and fiber cables for different services and standards?

- Cable Analyzer
- Cable Tester
- Digital Multimeters
- Network Analysis Module
- Portable Network Analyzers

4. Cisco IOS log messages fall into one of eight levels. Which syslog logging level is used to log the highest severity level?

- 0
- 1
- 4
- 6
- 7

Check

Show Me

Reset

12.2 Troubleshooting Process

12.4 Symptoms and Causes of Network Problems