Chapter 23: Device Management and Management Tools Troubleshooting

Instructor Materials

CCNP Enterprise: Advanced Routing

Chapter 23 Content

This chapter covers the following content:

- **Device Management Troubleshooting -** This section explains how to identify and troubleshoot issues related to console and vty access, as well as remote transfer tools. Various protocols are covered, including Telnet, SSH, TFTP, HTTP, HTTPS, and SCP.
- **Management Tools Troubleshooting -** This section examines how to use and troubleshoot various management tools, including syslog, SNMP, Cisco IP SLA, Object Tracking, NetFlow, and Flexible NetFlow. In addition, it examines Bidirectional Forwarding Detection (BFD) and Cisco DNA Center Assurance.

Device Management Troubleshooting

- When you have physical access to a device use the console line to access a Cisco IOS router for management purposes. Use vty lines to provide remote connectivity using Telnet or Secure Shell (SSH).
- You may have to troubleshoot problems connecting to a device so that you can troubleshoot another issue that has been presented to you. It may be necessary to transfer configuration files or IOS images while you are solving a problem. You need to be able to troubleshoot issues related to your remote transfers using protocols such as TFTP, HTTP(S), and SCP.
- This section explains why management access to a Cisco IOS router may fail, how you can determine why the problem is occurring, and how you can fix it. This section also discusses what to look out for when troubleshooting remote transfers. .

Console Access Troubleshooting

Here are some questions you should ask when troubleshooting console access:

- Has the correct COM port been selected in the terminal program?
- Are the terminal program's settings configured correctly?
- Is a line password used to authenticate to the console?
- Are a local username and password used to authenticate to the console?
- Is an AAA (authentication, authorization, and accounting) server used to authenticate to the console?
  - Has a method list been created for login authentication?
- Are the correct cable and drivers being used to connect to the console port?
  - New devices use a mini-USB port, older devices use the serial-to-RJ45 console (rollover) cable.

vty Access Troubleshooting and Telnet

Most devices are administered remotely via the vty lines, which support protocols such as Telnet and SSH for remote access. Consider the following when troubleshooting Telnet access to a device:

- Is the IP address of the remote router/switch reachable?
- Are the correct transport protocols defined for the line?
- Is the line configured to ask the user for credentials?
- Is a password specified?
- Is there an ACL (access control list) defining which management stations, based on IP address, can access the router/switch?
- Are all vty lines busy?
- Is there an ACL in the path between the client and the device blocking port 23?

vty Access Troubleshooting and SSH

With Secure Shell (SSH), you may experience the same issues as described with Telnet, in addition to several others. Consider the following additional issues when troubleshooting SSH access to a device:

- Is the correct version of SSH specified?
- Has the correct login command been specified?
- Has the correct key size been specified?
- Is there an ACL in the path between the client and the device blocking port 22?

Password Encryption Levels

By default, all passwords are stored in plaintext within the IOS configuration. For security, passwords should be encrypted or hashed in the configuration. Example 23-8 shows sample output of the passwords stored in the running configuration. The level 0 indicates no encryption. The level 4 indicates that SHA-256 was used. The level 5 indicates that Message Digest 5 (MD5) was used. The level 7 indicates that Type 7 encryption was used. The levels from strongest to weakest are 4, 5, 7, and then 0.

Example 23-8 *Verifying Password Security Levels*

```
SW1# show run | section username
username admin password 0 letme1n
username administrator password 7 082D495A041C0C19
username cisco secret 4 tnhtc92DXBhelxjYk8LWJrPV36S214ntXrpb4RFmfqY
username Raymond secret 5 $1$sHu.$sIjLazYcNOkRrgAjhyhxn0
```

Remote Transfer Troubleshooting - TFTP

TFTP is an unsecure file transfer protocol you can use to transfer files to and from a Cisco device using a TFTP server. TFTP uses UDP port 69 and is considered an unreliable protocol. When troubleshooting TFTP issues consider the following:

- When copying to a TFTP server, make sure the TFTP server has enough storage space.
- When copying from a TFTP server, make sure the storage location on the Cisco device has enough storage space. Use the show flash command to verify the amount of free space available and compare it to the size of the file you want to copy.
- Ensure that the TFTP server is reachable from the Cisco device.
- Check along the path from source to destination for access lists that might be blocking TFTP traffic.
- If you are using a management interface for TFTP traffic, use the **ip tftp source-interface** *interface_type interface_number* command to specify that the management interface will be used for sourcing TFTP traffic.
- Ensure that you are using the copy command correctly
- There is a 63-character limit on filenames in flash memory.

Remote Transfer Troubleshooting – HTTP(S)

To copy Cisco IOS image files, core files, configuration files, log files, and scripts to/from a remote web server, use unsecure protocol HTTP (TCP port 80), or secure protocol HTTPS (TCP port 443). Consider the following when troubleshooting HTTP(S) access for a device:

- Your Cisco device must support the HTTP client. Check with the **show ip http client all** command.
- Your router must connect to the web server. From the Cisco device, ping the URL of the web server or its IP address.
- Ensure that the correct URL or IP address of the web server has been specified in the copy command. When copying to a web server from flash, the destination is the web server.
- Ensure that the correct filename, username and password are specified in the copy command.
- Check that the correct port is specified in the copy command.
- Check that packets to the web server from the Cisco device are being sourced from the correct IP address.
- Make sure you specified the correct protocol: HTTP or HTTPS.
- For additional help with troubleshooting HTTP and HTTPS copy issues, use the **debug ip http client all** command.

Remote Transfer Troubleshooting – SCP

Secure Copy Protocol (SCP) is another way to copy files from a storage location to a Cisco device. It relies on Secure Shell (SSH) to provide a secure and authenticated method of transferring files. SCP requires AAA to be enabled so that the router can determine if the user is authorized to copy. Consider the following when troubleshooting SCP issues:

- Ensure that SSH, authentication, and authorization have been configured correctly on the device.
- Ensure that an RSA key is available and can be used for encryption.
- Ensure that AAA is configured correctly and is functioning.
- Ensure that SCP is enabled on the Cisco device using the **ip scp server enable** command.
- Ensure that the copy command is being used correctly.
- Verify that the correct username and password are being used for copying
- For additional help troubleshooting SCP issues, use the **debug ip scp** command.

Management Tools Troubleshooting

- Being able to monitor your network using various tools will help you stay ahead of any issues. However, when the tools break or don’t provide the results you need, you have to troubleshoot the tools that help you troubleshoot.
- This section examines how to troubleshoot issues with tools such as syslog, SNMP, IP SLA, Object Tracking, NetFlow, and Flexible NetFlow. It also explores the benefits of using BFD and examines how Cisco DNA Center Assurance can assist you with your troubleshooting efforts.

Syslog Troubleshooting

To verify your syslog configuration, confirm that logging is enabled, and view the syslog messages stored in the buffer, use the **show logging** command. In Example 23-11, the console and monitor are configured with the level 'informational', the buffer is configured with the level 'debugging', and the trap logging (server) is configured with the level 'warnings'.

When logging in to a server, specify the correct server IP address. Ensure that the server is reachable. Because syslog uses UDP port 514, ensure that no ACLs are blocking traffic destined to this port.

Finally, if you have remotely connected to a device by using Telnet or SSH, and no syslog messages are appearing, it is because the **terminal monitor** command has not been issued.

Example 23-11 *Verifying Syslog Configuration*

```
R4# show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

Inactive Message Discriminator:
OSPF severity group drops 4

     Console logging: level informational, 116 messages logged, xml disabled,
                      filtering disabled
     Monitor logging: level informational, 0 messages logged, xml disabled,
                      filtering disabled
     Buffer logging: level debugging, 175 messages logged, xml disabled,
                     filtering disabled
     Exception Logging: size (8192 bytes)
     Count and timestamp logging messages: disabled
     Persistent logging: disabled
No active filter modules.

     Trap logging: level warnings, 108 message lines logged
```

SNMP2 Troubleshooting

You need to be able to ping the server from the agent. If Layer 3 connectivity does not exist, the SNMP NMS cannot access the information in the MIB on the agent. Keep the following in mind as you troubleshoot SNMPv2c:

- Ensure that community strings match and the ACLs classifying servers are correct.
- Ensure that configurations for notifications are correct, that traps are enabled.
- Ensure that the host (NMS) IP address, the SNMP version, and the community string are all correct and specified.
- Prevent index shuffling using the **snmp-server ifindex persist** command.

Example 23-12 *SNMPv2c Configuration Example*

```
R4# show run | section snmp
snmp-server community CISCO RO 10
snmp-server enable traps cpu threshold
snmp-server host 10.1.100.100 informs version 2c CISCO
snmp ifmib ifindex persist
R4# show ip access-lists
Standard IP access list 10
 10 permit 10.1.100.100
```

If you do not want all traps to be sent, you must specify the correct ones to send. In Example 23-12, the **snmp-server host** command indicates that SNMPv2c informs will be sent to the NMS at 10.1.100.100 with a community string of CISCO.

SNMP3 Troubleshooting

SNMPv3 offers improved authentication and encryption over SNMPv2c. Keep the following in mind as you troubleshoot SNMPv3:

- Appropriate nesting of users, views, and groups.
- Specifying the correct security level.
- Using the correct hashing and encrypting algorithms, and correct passwords.
- Specifying the correct OIDs in the view.
- Appropriate notification configuration.
- Prevent index shuffling using the **snmp-server ifindex persist** command.

Example 23-13 *SNMPv3 Configuration Example*

```
R2# show run | section snmp
snmp-server group NMSREADONLY v3 priv read MIBACCESS access 99
snmp-server view MIBACCESS sysUpTime included
snmp-server view MIBACCESS ifAdminStatus included
snmp-server view MIBACCESS ifOperStatus included
snmp-server user NMSERVER NMSREADONLY v3 auth sha MYPASSWORD priv aes 256 MYPASSWORD
snmp-server host 10.1.100.100 version 3 priv NMSERVER cpu
snmp ifmib ifindex persist
SW2# show ip access-lists
Standard IP access list 99
 10 permit 10.1.100.100
```

In Example 23-13, the **snmp-server host** command indicates that SNMPv3 will send traps related to the CPU to the NMS at 10.1.100.100, with the authentication and encryption provided by the username NMSERVER.

Cisco IOS IP SLA Troubleshooting

Cisco IOS IP SLA lets you measure network performance and test network availability by generating a continuous, reliable probe (simulated traffic) in a predictable manner. You can collect information about packet loss, one-way latency, response times, jitter, network resource availability, application performance, server response times, and even voice quality.

IP SLA consists of an IP SLA source (which sends the probes) and IP SLA responder (which replies to the probes). Figure 23-1 shows a scenario with just the IP SLA source sending a ping to test connectivity. Figure 23-2 shows a scenario with an IP SLA source and an IP SLA responder measuring jitter (interpacket delay variance).

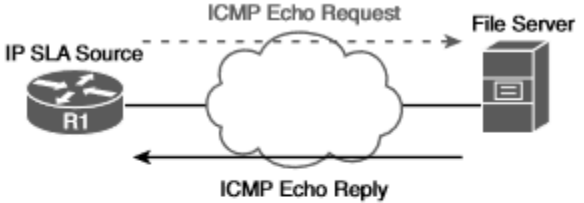

Figure 23-1 *IP SLA Source Topology*

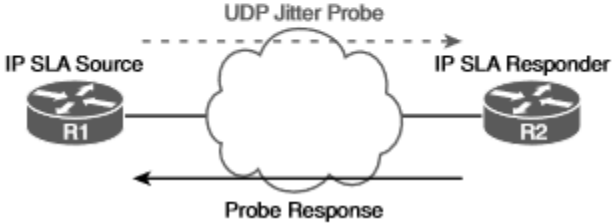

Figure 23-2 *IP SLA Source and Responder Topology*

Cisco IOS IP SLA Troubleshooting (Cont.)

When troubleshooting Cisco IOS IP SLA, consider the following:

- Choose the correct operation for the metrics you intend to measure.
- Ensure that the destination IP address is reachable and correctly defined.
- Ensure that the source IP address is reachable from the destination and correctly defined.
- Ensure that any necessary port numbers are correctly identified.
- The SLA instance needs to be started.
- If the operation needs an IP SLA responder, one must be configured and reachable.

To verify which operations are supported on the platform in addition to how many operations are configured and how many are currently active, use the show ip sla application command, as shown in Example 23-20.

Example 23-20 *Output of show ip sla application*

```
R1# show ip sla application
        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, lsp Group, lspPing, lspTrace
        802.1agEcho VLAN, EVC, Port, 802.1agJitter VLAN, EVC, Port
        pseudowirePing, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 30919230
Estimated system max number of entries: 22645

Estimated number of configurable operations: 22643
Number of Entries configured  : 2
Number of active Entries      : 2
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: 09:29:04.789 UTC Sat Jul 26 2014
```

Object Tracking Troubleshooting

Object Tracking lets you dynamically control what occurs if the result of the tracking object is up or down. For example, you can attach an object to a static route; if the object is up, the route is installed in the routing table. If the object is down, the route is not installed in the routing table. You can track IP routes, IP SLA instances, interfaces, and groups of objects.

To verify the configuration of a tracking object and the status of the tracking object, use the **show track** command. In Example 23-26, tracking object 1 exists on SW1. It is tracking the reachability of an IP route, 10.1.43.0/24. If the route is in the routing table, the object is up. If the route is not in the routing table, the object is down. The object is attached to HSRP Group 10, as shown after Tracked by: in the output.

Example 23-26 *Verifying the Configuration and Status of a Tracking Object (Up)*

```
SW1# show track
Track 1
  IP route 10.1.43.0 255.255.255.0 reachability
  Reachability is Up (EIGRP)
    1 change, last change 00:01:55
  First-hop interface is GigabitEthernet1/0/10
 Tracked by:
   HSRP Vlan10 10
```

NetFlow and Flexible NetFlow Troubleshooting

Cisco IOS NetFlow provides insight into your network traffic patterns. NetFlow distinguishes between different traffic flows. A flow is a series of packets, all of which have shared header information, such as source and destination IP addresses, protocol numbers, port numbers, and type of service (TOS) field information. NetFlow keeps track of the number of packets and bytes observed in each flow. This information is stored in a flow cache in the router's memory. After the NetFlow collector has received flow information over a period of time, analysis software running on the NetFlow collector can produce reports detailing traffic statistics.

Example 23-28 provides a sample NetFlow configuration on a router. Notice that the **ip flow ingress** command is issued for Fast Ethernet 0/0, and **ip flow egress** is configured on Fast Ethernet 0/1.

Example 23-28 *NetFlow Sample Configuration*

```
R4# configure terminal
R4(config)# int fa 0/0
R4(config-if)# ip flow ingress
R4(config-if)# exit
R4(config)# int fa 0/1
R4(config-if)# ip flow egress
R4(config-if)# exit
R4(config)# ip flow-export source lo 0
R4(config)# ip flow-export version 5
R4(config)# ip flow-export destination 192.168.1.50 5000
R4(config)# end
```

NetFlow and Flexible NetFlow Troubleshooting (Cont.)

When troubleshooting NetFlow, consider the following:

- Traffic direction
- Interface (Example 23-30)
- Export destination
- Export source (Example 23-31)
- Version

Flows are temporary on the local Cisco device. If they are not exported to a NetFlow collector, the flows will be removed from the cache at some point to free up resources. Flows are exported to the NetFlow collector only if you set up the device to export the flows and only after the flows expire in the flow cache on the local device.

Example 23-30 *Viewing NetFlow Information with show ip flow interface*

```
R3# show ip flow interface
GigabitEthernet2/0
  ip flow ingress
  ip flow egress
R3#
```

Example 23-31 *Viewing NetFlow Information with show ip flow export*

```
R3# show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       192.168.23.1 (Loopback0)
    Destination(1)  192.168.1.50 (5000)
  Version 5 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
R3#
```

NetFlow and Flexible NetFlow Troubleshooting (Cont.)

Flexible NetFlow lets you customize the traffic analysis parameters for your specific requirements, so you must verify more parameters while troubleshooting. When troubleshooting Flexible NetFlow, you will need to verify the flow records, flow monitors, flow exports, and interface configurations.

Flow records define what will be captured. You need to be able to verify that they are configured to capture what you want. With Cisco-predefined records, use Cisco documentation to identify what is captured as the list will evolve over time. When using user-defined records, use the **show flow record** command to verify that the correct match and collection conditions were specified in the flow record, or the **show running-config flow record** command, as shown in Example 23-33.

Example 23-33 *Viewing Flexible NetFlow Flow Records*

```
R3# show flow record
flow record RNARSI-FLOWRECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  16 bytes
  Fields:
    match ipv4 source address
    match ipv4 destination address
    match application name
    collect interface input

R3# show running-config flow record
Current configuration:
!
flow record RNARSI-FLOWRECORD
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect interface input
!
R3#
```

Bidirectional Forwarding Detection (BFD)

Sometimes no carrier detect signaling mechanism is available to quickly detect whether the link between routers is down. Figure 23-3 illustrates three types of environments where a link failure may not occur on the directly connected interface.

BFD is a “detection” protocol that works with all media types, routing protocols, topologies, and encapsulations. It quickly detects reachability failures between two routers in the same Layer 3 network so that network issues can be identified as soon as possible, and convergence can occur at a far faster rate. BFD is a lightweight protocol which is less CPU intensive than fast routing protocol hellos. In Figure 23-4, R1 and R2 are using BFD to keep track of reachability: BFD packets are being sent every 100 msec, and if three consecutive packets are missed, BFD triggers a session failure and notifies EIGRP.

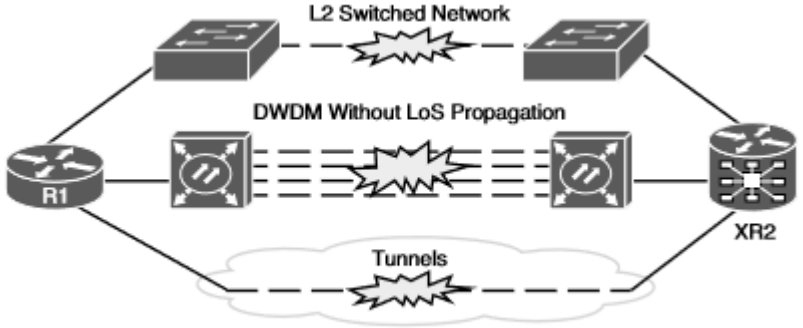

Figure 23-3 *Loss of Signal Detection Challenges*

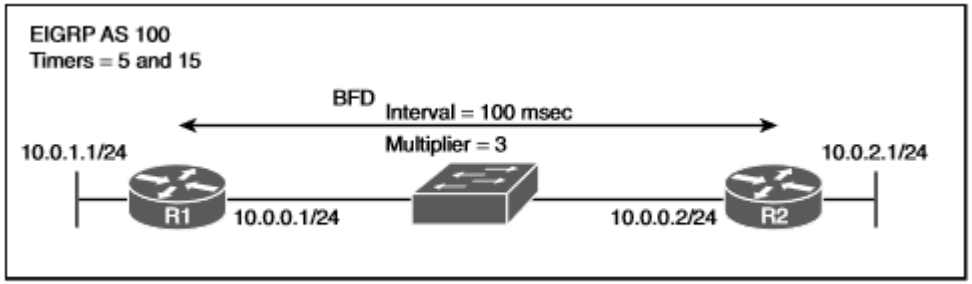

Figure 23-4 *BFD Configured Between Two EIGRP Neighbors*

Cisco DNA Center Assurance

With Cisco DNA Center Assurance, you can predict problems more quickly, thanks to proactive monitoring. Your first valuable troubleshooting tool is the Overall Health page, shown in Figure 23-5. This page provides an overview of the overall health of the networks and clients in the environment, which can be displayed based on information gathered from the most recent 3 hours, 24 hours, or 7 days. You can view health maps as well as hierarchical site/building maps by clicking on the Hide/Show button. The Top 10 Issues area at the bottom of the page displays the issues that should be addressed; when you click on them, you are presented with the issue details, including the impact of the issue, as well as suggested actions to fix the issue.

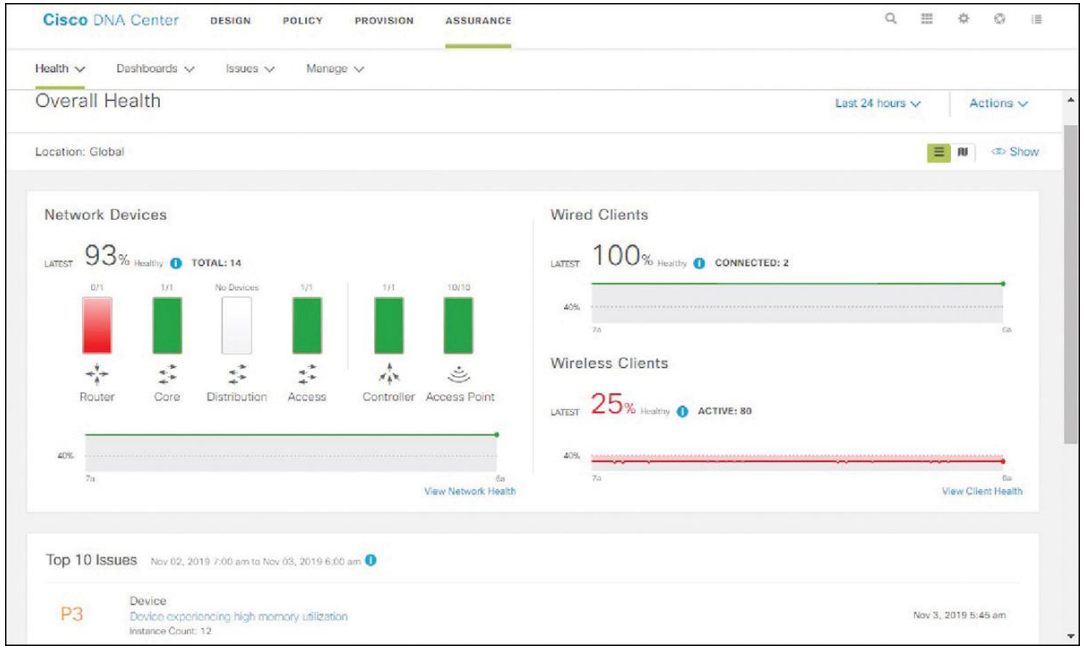

Figure 23-5 Cisco DNA Center Assurance Overall Health Page

Network Health Page

Another valuable troubleshooting tool is the Network Health page, shown in Figure 23-6, which you can access in Cisco DNA Center Assurance by selecting Health and then Network. The Network Devices section lists all the devices on an individual basis and provides information such as the device type, address, OS version, reachability, issue count, and location. In addition, it provides an overall health score. Anything with a health score from 1 to 3 is a critical issue and is displayed in red. You can click on the device to get further details about a device in Device 360.

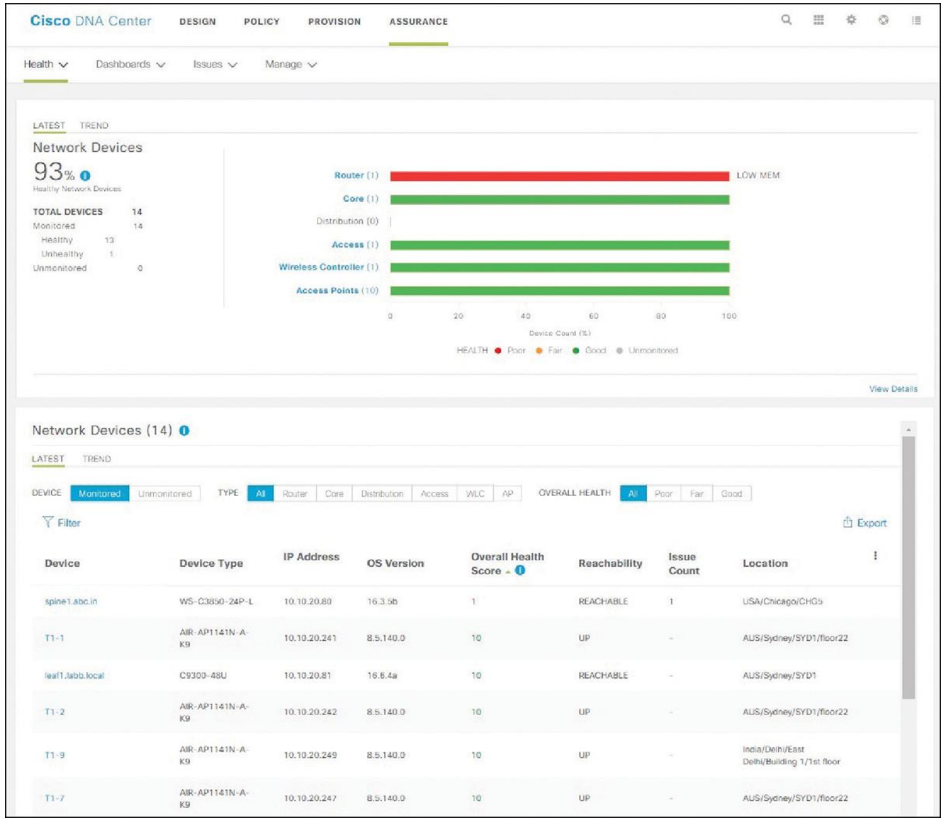

Figure 23-6 Part of the Network Health Page

Client Health Page

Access the Client Health page, shown in Figure 23-7, in Cisco DNA Center Assurance by selecting Health and then Client. The Client Devices section of the Client Health page lists all the clients on an individual basis and provides information such as the identifier, address, type, when it was last seen, the switch or AP it is connected to, and location. In addition, it provides an overall health score. Anything with a health score from 1 to 3 is a critical issue and is displayed in red. You can click on the device to get further details about a device in Client 360.

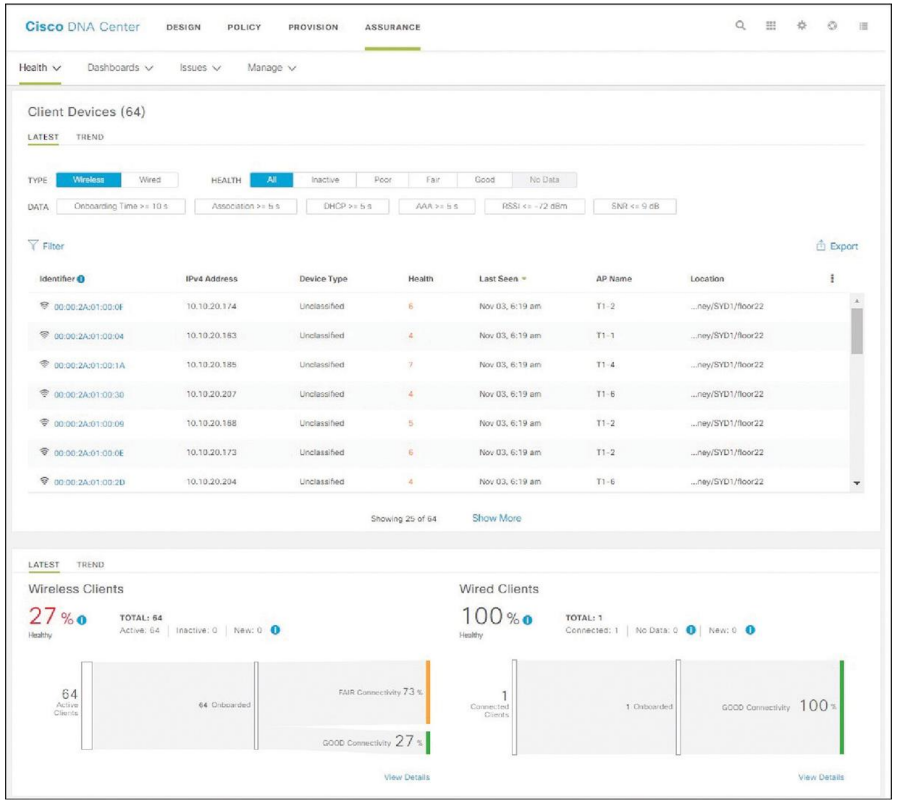

Figure 23-7 Part of the Client Health Page

Client 360 Dashboard

Figure 23-8 shows the Client 360 dashboard for the client with IP address 10.10.20.207. Notice that the client is experiencing poor RF (radio frequency) conditions. In this case, if you click on Wireless Client Experiencing Poor RF Conditions on SSID “sandbox,” you get a description of the issue, the impact of the last occurrence, and possibly suggested remediation actions.

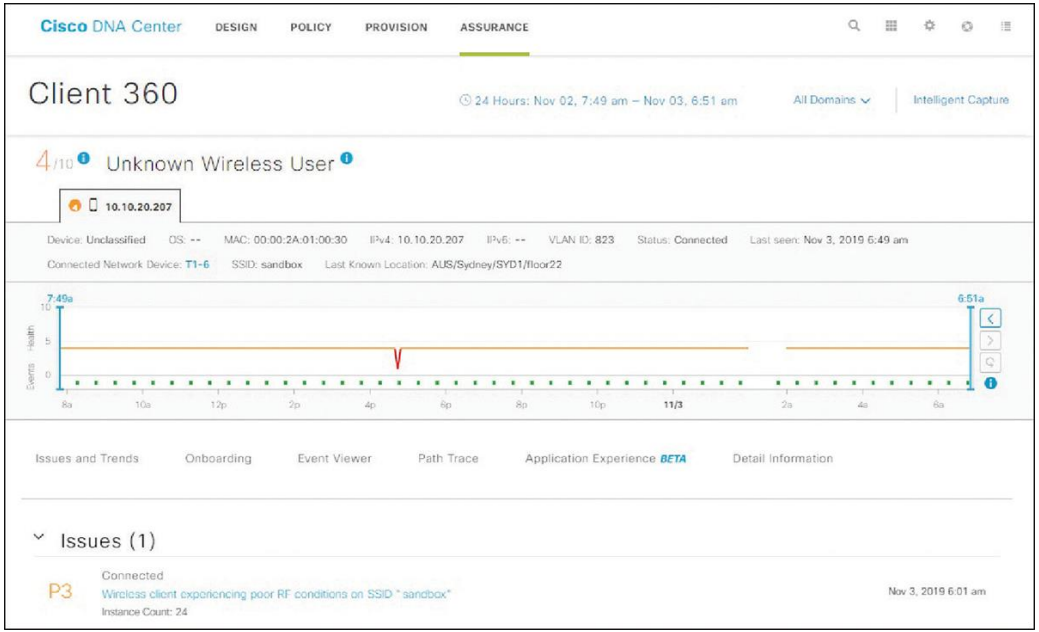

Figure 23-8 Part of the Client 360 Page

Device 360

Figure 23-9 shows the Device 360 page for a switch named spine1.abc.in with IP address 10.10.20.80. Notice in the image that there is one issue: The description states “Device experiencing high memory utilization.” If you click the issue, you get a description of the issue and possibly suggested actions you should take to resolve it (Figure 23-10).

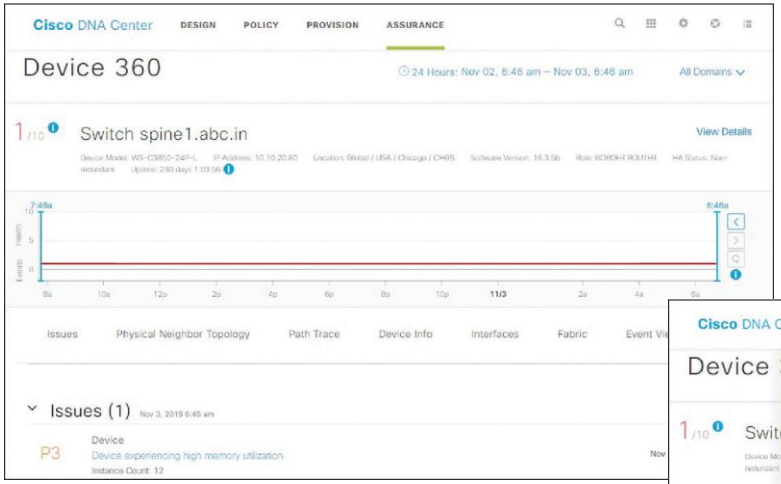

Figure 23-9 Part of the Device 360 Page

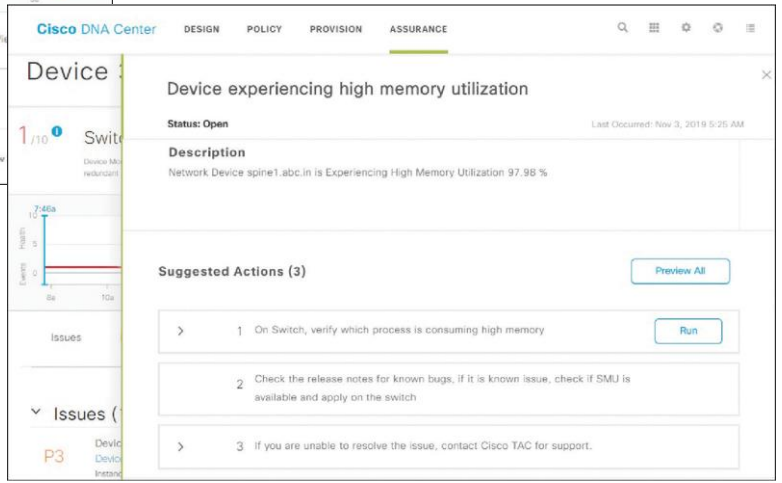

Figure 23-10 Description and Suggested Actions for an Issue

Path Trace

The next troubleshooting feature in DNA Center Assurance is Path Trace. With Path Trace, you can graphically see the path that applications and services running on a client will take through all the devices on the network to reach the destination. With a few clicks, you can use this tool to do multiple troubleshooting tasks that would take you 5 to 10 minutes at the command line. Figure 23-11 shows an example of using Path Trace between two devices. Path Trace can be accessed within Client 360 or Device 360.

Another great tool for troubleshooting in Cisco DNA Center Assurance is Network Time Travel. This tool allows you to hop into a time machine and see the cause of a network issue instead of trying to reproduce the issue.

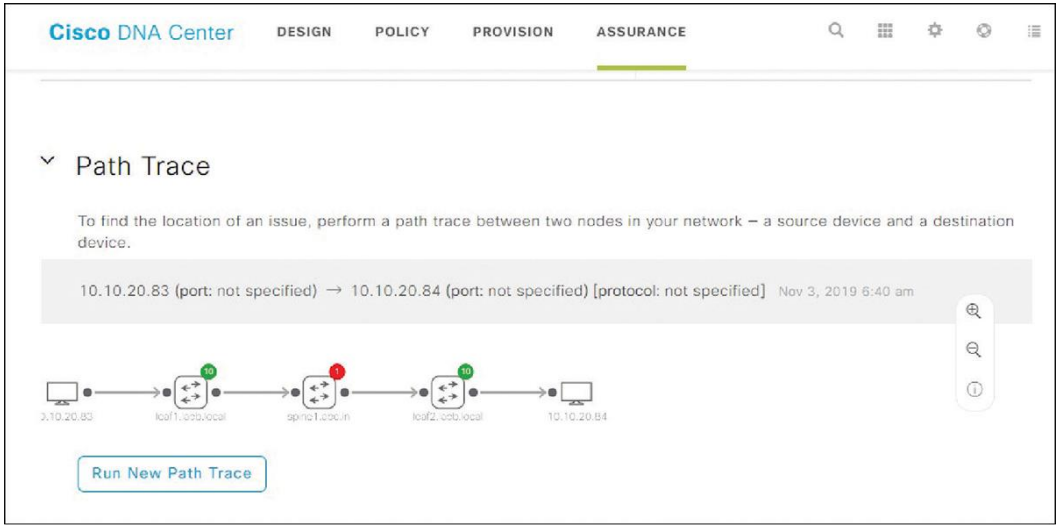

Figure 23-11 Using Path Trace from the DNA Center Assurance Client 360 Page

Global Issues

With the Global Issues page, you can access all open issues, resolved issues, and ignored issues in one place, as shown in Figure 23-12. You can access the Global Issues page from the Issues drop-down.

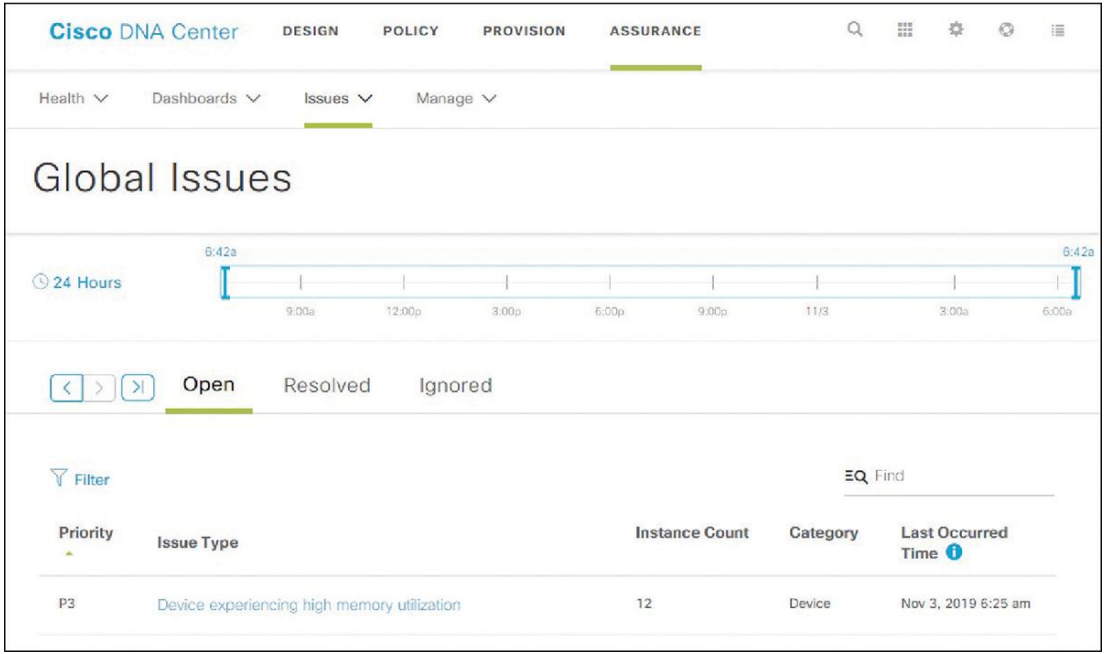

Figure 23-12 Global Issues Page

Global Issues (Cont.)

Select the All Issues option from the Issues drop-down, as shown in Figure 23-13. The following categories are available:

- **Onboarding** - Identifies issues related to wireless and wired client onboarding.
- **Connectivity** - Identifies issues related to network connectivity, including OSPF, BGP, and tunnels.
- **Connected** - Identifies issues related to clients.
- **Device** - Identifies issues related to the device.
- **Availability** - Identifies availability issues related to access points, wireless LAN controllers, etc.
- **Utilization** - Identifies issues related to utilization of access points, wireless LAN controllers, radios, etc.
- **Application** - Identifies issues related to application experience.
- **Sensor Test** - Identifies any global sensor issues.

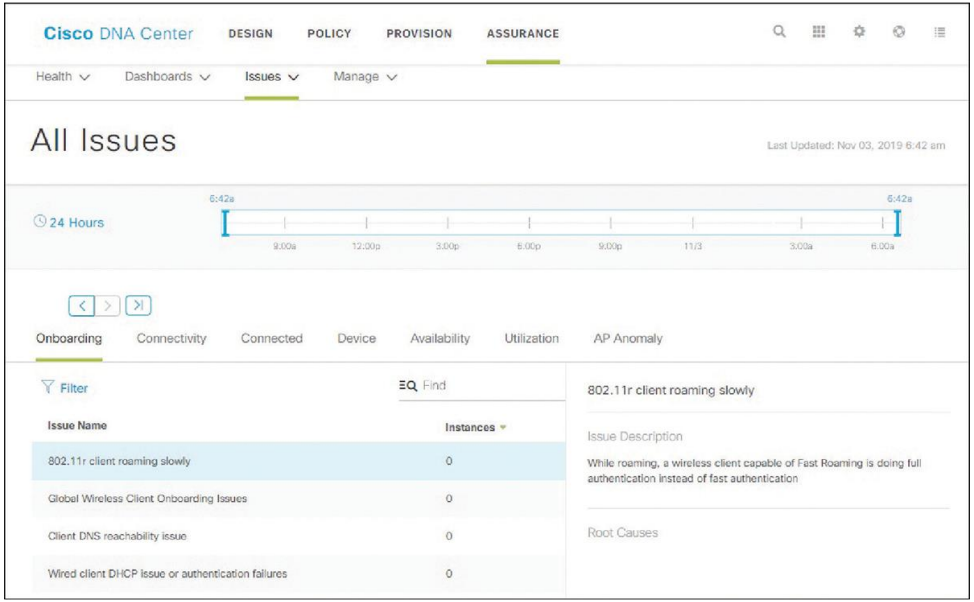

Figure 23-13 All Issues Page

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 23

Description	
Considerations when troubleshooting issues related to console port access	Considerations when troubleshooting issues related to remote transfers with SCP
Considerations when troubleshooting issues related to Telnet	Verifying syslog configuration
Considerations when troubleshooting issues related to SSH	Considerations when troubleshooting issues related to SNMPv2c
Password encryption levels	Considerations when troubleshooting issues related to SNMPv3
Considerations when troubleshooting issues related to remote transfers with TFTP	Considerations when troubleshooting issues related to IP SLA
Considerations when troubleshooting issues related to remote transfers with HTTP(S)	Considerations when troubleshooting issues related to NetFlow

Prepare for the Exam

Key Topics for Chapter 23 (Cont.)

Description	
Viewing Flexible NetFlow flow records	Health scores for the clients connected to the network on the Client Health page of Cisco DNA Center Assurance
Viewing Flexible NetFlow flow monitors	The Client 360 and Device 360 pages of Cisco DNA Center Assurance
Viewing Flexible NetFlow flow monitor cache format records	Path Trace in Cisco DNA Center Assurance
Viewing Flexible NetFlow-enabled interfaces	Categories in All Issues of Cisco DNA Center Assurance
Viewing Flexible NetFlow flow exporter information	
Health scores for the network devices on the Network Health page of Cisco DNA Center Assurance	

Prepare for the Exam

Key Terms for Chapter 23

Term		
AAA	IP SLA	Port 22
BFD	Level 4 encryption	SSH
Cisco DNA Center Assurance	Level 5 encryption	SNMPv2c
Client 360	Level 7 encryption	SNMPv3
Device 360	Line	Syslog
Flexible NetFlow	Login	Telnet
Flow cache	Login local	
Flow exporter	NetFlow	
Flow record	Object Tracking	
Flow monitor	Port 23	

Prepare for the Exam

Command Reference for Chapter 23

Task	Command Syntax
Display the ingress and egress allowed transport protocols on vty line	**show line vty** *line_number* **| include Allowed**
Display only the ingress allowed transport protocols on a vty line	**show line vty** *line_number* **| include Allowed input transports**
Display the vty line configuration in the running configuration	**show run | section line vty**
Display the lines that are currently being used for management connectivity	**show users**
Display whether SSH is enabled or disabled, the version of SSH enabled, and the SSH RSA key	**show ip ssh**
Display the SSHv1 and SSHv2 connections to the local device	**show ssh**

Command Reference for Chapter 23 (Cont.)

Task	Command Syntax
Display information related to syslog, including level settings and messages logged for console, monitor, buffer, and traps logging; verify the buffer size and its contents for buffer logging and the IP address/port number of the syslog server	**show logging**
Display the conditional **debug** commands that have been configured on the router	**show debug condition**
Display SNMP group information, including the group name, the security mode, the read and write views, and any applied ACLs	**show snmp group**
Display any configured SNMP users; output includes the username, the authentication protocol used, the encryption protocol used, and the group the user is applied to	**show snmp user**
Display the local configuration of the SNMP server, including the IP address, UDP port, type, attached user, and security model being used	**show snmp host**

Command Reference for Chapter 23 (Cont.)

Task	Command Syntax
Display the SNMP views configured on the local device	**show snmp view**
Display which IP SLA operations are supported on the platform, how many operations are configured, and how many operations are currently active	**show ip sla application**
Display the IP SLA configuration values for the IP SLA instances	**show ip sla configuration**
Display the IP SLA operational results of IP SLA instances	**show ip sla statistics**
Display the operational results of the IP SLA responder	**show ip sla responder**
Display the configured tracking objects on the local device, including the current state and the service or feature it is attached to	**show track**
Display the local NetFlow flow cache as well as the configured timers	**show ip cache flow**
Display the interfaces enabled for NetFlow and the direction in which they are capturing information	**show ip flow interface**

Command Reference for Chapter 23 (Cont.)

Task	Command Syntax
Display the NetFlow exporter configuration, including the source and destination addresses, port number, and version of NetFlow	**show ip flow export**
Display all user-defined Flexible NetFlow flow records that are configured on the local device	**show flow record**
Display the locally configured Flexible NetFlow flow monitors; verify the attached flow record and flow exporter as well as the configured timers	**show flow monitor**
Display the interfaces enabled for Flexible NetFlow and the direction in which they are capturing information	**show flow interface**
Display the Flexible NetFlow exporter configuration, including the source and destination addresses, port number, and version of NetFlow	**show flow exporter**


CISCO