[Updated Constantly]

HERE

CCNA 4 (v5.0.3 + v6.0) Chapter 8 Exam Answers Full

1. **When should a network performance baseline be measured?**
   - after normal work hours to reduce possible interruptions
   - **during normal work hours of an organization***
   - when a denial of service attack to the network is detected and blocked
   - immediately after the main network devices restarted

   The purpose of a network performance baseline is to record the characteristics of a network during normal operations. This can be used as a standard to determine when a network is performing abnormally. Measurements that are performed during particular circumstances (such as main network device restart or after working hours) will result in an inaccurate set of characteristics for the purpose of a baseline. A DoS attack might cause abnormal network performance, but once it is blocked, network performance should return to normal, so there is no immediate need to measure performance in order to establish a baseline.

2. **What is a purpose of establishing a network baseline?**
   - It provides a statistical average for network performance.
   - **It creates a point of reference for future network evaluations.***
   - It manages the performance of network devices.
   - It checks the security configuration of network devices.

   A baseline is used to establish normal network or system performance. It can be used to compare with future network or system performances in order to detect abnormal situations.

3. **Which three pieces of information are typically recorded in a logical topology diagram? (Choose three.)**
   - device models and manufacturers
   - device locations
   - cable specifications
   - **static routes***
   - **routing protocols***
   - **IP address and prefix lengths***

   There are two types of network topology diagrams: physical topology diagrams and logical topology diagrams. Logical topology diagrams show how devices are logically connected and how data moves through the network. Logical topology diagrams include information such as IP addresses, routing protocols, and static routes.

4. **In which step of gathering symptoms does the network engineer determine if the problem is at the core, distribution, or access layer of the network?**
   - Determine the symptoms.
   - **Narrow the scope.***
   - Determine ownership.
   - Gather information.

- Document the symptoms.

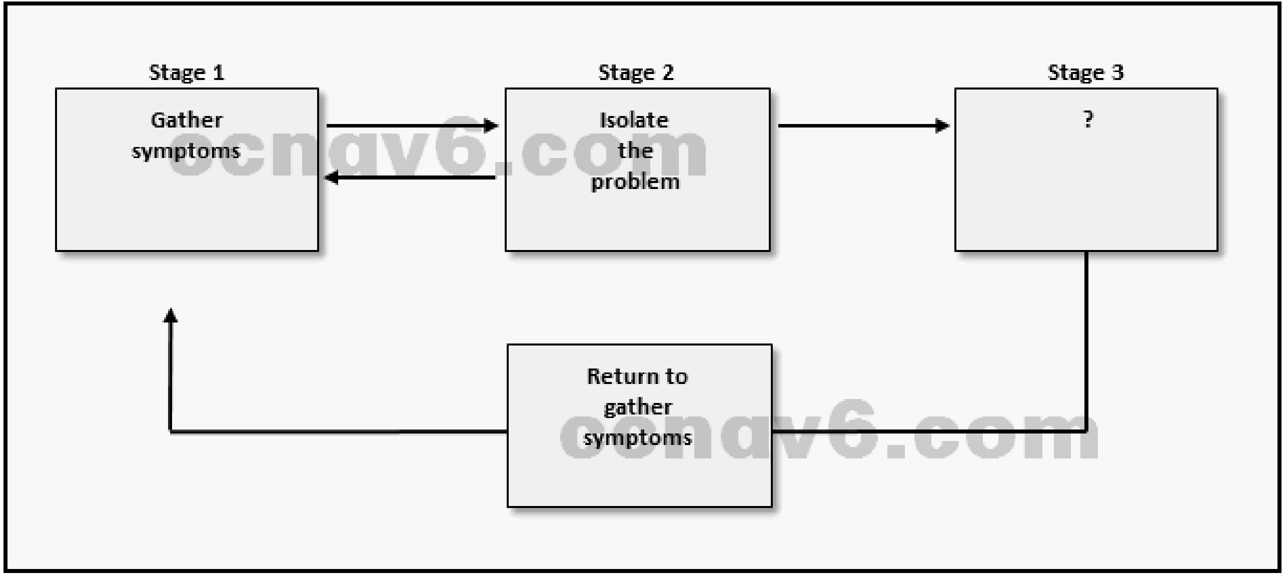
In the “narrow the scope” step of gathering symptoms, a network engineer will determine if the network problem is at the core, distribution, or access layer of the network. Once this step is complete and the layer is identified, the network engineer can determine which pieces of equipment are the most likely cause.

5. **A team of engineers has identified a solution to a significant network problem. The proposed solution is likely to affect critical network infrastructure components. What should the team follow while implementing the solution to avoid interfering with other processes and infrastructure?**

- syslog messages and reports
- one of the layered troubleshooting approaches
- knowledge base guidelines
- **change-control procedures***

Change-control procedures should be established and applied for each stage to ensure a consistent approach to implementing the solutions, and to enable changes to be rolled back if they cause other unforeseen problems.

6. **Refer to the exhibit. What action occurs at stage 3 of the general troubleshooting process?**



- Document symptoms.
- Question end users.
- Narrow the scope.
- **Correct the problem.***

There are three stages in the general troubleshooting process:
Gather symptoms
Isolate the problem
Correct the problem
If the problem is not corrected, the administrator documents the attempted solution, removes any changes made, and returns to gathering symptoms.

7. **After which step in the network troubleshooting process would one of the layered troubleshooting methods be used?**

- documenting symptoms
- determining ownership
- narrowing the scope
- **gathering symptoms from suspect devices***

A layered troubleshooting approach (top-down, bottom-up, or divide-and-conquer) is used to gather hardware and software symptoms from the suspect devices.

8. **A network technician is troubleshooting an email connection problem. Which question to the end-user will provide clear information to better define the problem?**

- How big are the emails you tried to send?
- What kind of equipment are you using to send emails?
- Is your email working now?
- **When did you first notice your email problem?***

To efficiently establish exactly when the user first experienced email problems, an open-ended question should be asked so that the user can state the day and time that the problem was first noticed. Closed questions only require a yes or no answer which will require further questions to determine the actual time of the problem.

9. **A network engineer is troubleshooting a network problem and can successfully ping between two devices. However, Telnet between the same two devices does not work. Which OSI layers should the administrator investigate next?**

- from the network layer to the physical layer
- all of the layers
- only the network layer
- **from the network layer to the application layer***

A successful ping indicates that everything is working on the physical, data link, and network layer. All of the other layers should be investigated.

10. **A network administrator is having issues with a newly installed network not appearing in other routers. At which layer of the OSI model is the network administrator going to start the troubleshooting process when using a top-down approach?**

- internet
- application
- **network***
- session
- transport

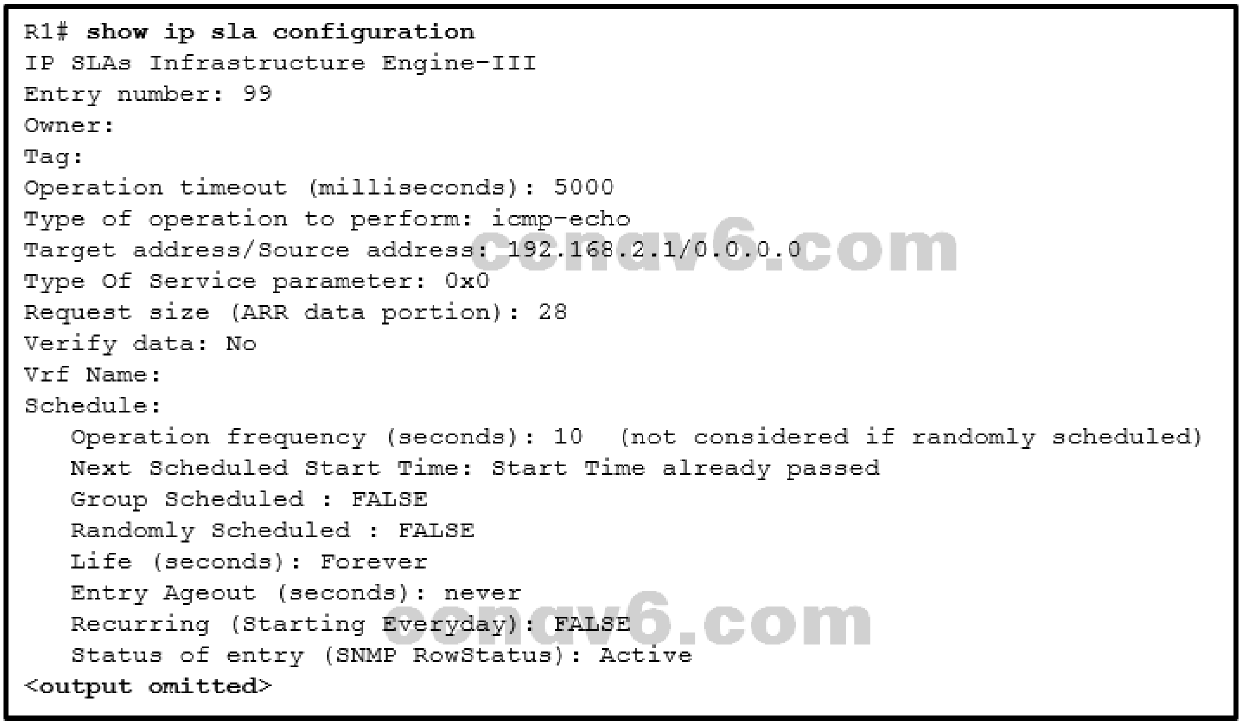
Routing is a Layer 3 process. The network layer is another name for Layer 3. The top-down method of troubleshooting typically starts at the application layer, but when a problem is definitely a routing problem, there is no need for troubleshooting to be performed at the higher levels. The problem can only be a Layer 1, 2, or 3 problem.

11. **Which troubleshooting method begins by examining cable connections and wiring issues?**

- top-down
- divide-and-conquer
- substitution
- **bottom-up***

In troubleshooting with the bottom-up method, a technician would start with the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified.

12. **Refer to the exhibit. On the basis of the information presented, which two IP SLA related statements are true? (Choose two.)**



```
R1# show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 99
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.2.1/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 10  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
<output omitted>
```

- **IP SLA 99 will run forever unless explicitly disabled.***
- IP SLA 99 is measuring jitter.
- IP SLA 99 is configured with the type dns target-addr 192.168.2.1 command.
- IP SLA 99 is sending echo requests from IP address 192.168.2.1.
- IP SLA 99 is scheduled to begin in 2 hours.
- **IP SLA 99 is sending echo requests every 10 seconds.***

From the output, the IP SLA is configured to perform icmp-echo, the target device is 192.168.2.1, and the icmp-echo requests are sent every 10 seconds. “Start Time already passed” indicates that the operation has started. The “Life” parameter indicates that the setting is “Forever”.

13. **A company is setting up a web site with SSL technology to protect the authentication credentials required to access the web site. A network engineer needs to verify that the setup is correct and that the authentication is indeed encrypted. Which tool should be used?**

- baselining tool
- cable analyzer
- **protocol analyzer***
- fault-management tool

To verify that the authentication is indeed encrypted, the authentication process needs to be captured and investigated, which can be accomplished through a protocol analyzer, such as Wireshark. A baselining tool is used for automating the network documentation and baselining process. A fault-management tool is used to manage the fault tolerance of network devices . A cable analyzer is used to test and certify copper and fiber cables for different services and standards.

14. **Which category of software troubleshooting tools provides device-level monitoring, configuration, and fault-management?**
- host-based protocol analyzers
- baselining tools
- knowledge bases
- **network management system tools***

Network management system (NMS) tools include device-level monitoring, configuration, and fault-management tools. Knowledge bases are online repositories of experience-based information. Baselining tools perform tasks of network baselining documentation, network diagram drawings, and network performance statistics establishment. Host-based protocol analyzers capture and decode the various protocol layers in a recorded frame and present the information in a relatively easy to use format.

15. **Which two specialized troubleshooting tools can monitor the amount of traffic that passes through a switch? (Choose two.)**
- DTX cable analyzer
- TDR
- digital multimeter
- **portable network analyzer***
- **NAM***

Network analysis modules and portable network analyzers such as the Fluke OptiView can monitor network traffic to investigate the amount of data going through switch ports. TDRs, DMMs, and DTX cable analyzers are used to investigate physical media errors and lengths.

16. **Which number represents the most severe level of syslog logging?**
- **0***
- 1
- 6
- 7

Syslog levels are numbered 0 through 7, with 0 being the most severe and 7 being the least severe.

17. **A user in a large office calls technical support to complain that a PC has suddenly lost connectivity to the network. The technician asks the caller to talk to nearby users to see if other machines are affected. The caller reports that several immediate neighbors in the same department have a similar problem and that they cannot ping each other. Those who are seated in other departments have connectivity. What should the technician check as the first step in troubleshooting the issue?**
- the power outlet to the PC that is used by the caller
- the cable connection between a PC and a network outlet that is used by a neighbor
- the cable that connects the PC of the caller to the network jack
- **the status of the departmental workgroup switch in the wiring closet***
- the trunks between switches in the wiring closet

18. **A user reports that after an OS patch of the networking subsystem has been applied to a workstation, it performs very slowly when connecting to network resources. A network**

technician tests the link with a cable analyzer and notices that the workstation sends an excessive number of frames smaller than 64 bytes and also other meaningless frames. What is the possible cause of the problem?

- corrupted application installation
- cabling faults
- **corrupted NIC driver***
- Ethernet signal attenuation

The symptom of excessive runt packets and jabber is typically a Layer 1 issue, such as caused by a corrupted NIC driver, which could be the result of a software error during the NIC driver upgrade process. Cable faults would cause intermittent connections, but in this case, the network is not touched and the cable analyzer has detected frame problems, not signal problems. Ethernet signal attenuation is caused by an extended or long cable, but in this case, the cable has not been changed. A NIC driver is part of the operating system, it is not an application.

19. **An administrator is troubleshooting an Internet connectivity problem on a router. The output of the show interfaces gigabitethernet 0/0 command reveals higher than normal framing errors on the interface that connects to the Internet. At what layer of the OSI model is the problem likely occurring?**

- Layer 1
- **Layer 2***
- Layer 3
- Layer 4
- Layer 7

Framing errors are symptoms of problems at the data link layer, Layer 2, of the OSI model.

20. **A group of Windows PCs in a new subnet has been added to an Ethernet network. When testing the connectivity, a technician finds that these PCs can access local network resources but not the Internet resources. To troubleshoot the problem, the technician wants to initially confirm the IP address and DNS configurations on the PCs, and also verify connectivity to the local router. Which three Windows CLI commands and utilities will provide the necessary information? (Choose three.)**

- **ping***
- arp -a
- netsh interface ipv6 show neighbor
- **nslookup***
- tracert
- **ipconfig***
- telnet

The ipconfig and nslookup commands will provide initial IP address and DNS configuration information to the technicians and determine if DHCP is assigning correct information to the PCs. The ping utility would be used to verify, or not, connectivity to the default gateway (router) using the configured default gateway address, or using the known correct default gateway address if these are found to be different. The arp -a or netsh interface ipv6 show neighbor commands could be used if the problem is then suspected to be an IP address to MAC address mapping issue. The telnet and tracert utilities could be used to determine where the problem was located in the network if the default gateway configuration was found to be correct.

21. **Users report that the new web site http://www.company1.biz cannot be accessed. The helpdesk technician checks and verifies that the web site can be accessed with http://www.company1.biz:90. Which layer in the TCP/IP model is involved in troubleshooting this issue?**
    - **transport***
    - application
    - network access
    - internet

    The issue is that the new web site is configured with TCP port 90 for HTTP, which is different from the normal TCP port 80. Therefore, this is a transport layer issue.

22. **Where are IPv4 address to Layer 2 Ethernet address mappings maintained on a host computer?**
    - routing table
    - **ARP cache***
    - neighbor table
    - MAC address table

    The ARP cache is used to store IPv4 addresses and the Ethernet physical addresses or MAC addresses to which the IPv4 addresses are mapped. Incorrect mappings of IP addresses to MAC addresses can result in loss of end-to-end connectivity.

23. **A networked PC is having trouble accessing the Internet, but can print to a local printer and ping other computers in the area. Other computers on the same network are not having any issues. What is the problem?**
    - **The PC has a missing or incorrect default gateway.***
    - The link between the switch to which the PC connects and the default gateway router is down.
    - The switch port to which the PC connects has an incorrect VLAN configured.
    - The default gateway router does not have a default route.

    Since other computers on the same network work properly, the default gateway router has a default route and the link between the workgroup switch and the router works. An incorrectly configured switch port VLAN would not cause these symptoms.

24. **The newly configured ASBR that connects a company to the Internet has a default route configured and has the default-information originate command entered. Devices connected through this router can access the Internet. The problem is that no other OSPF routers have a default route in the routing table and no other users throughout the organization can access the Internet. What could be the problem?**
    - The ASBR should use the exit_interface argument instead of next-hop on the default route.
    - The ASBR does not have OSPF configured.
    - **The ASBR does not have an OSPF neighbor.***
    - The other routers are not configured to accept LSA type 4s.

    Because no other routers have a default route, the most likely problem is the link between the ASBR and other OSPF routers, or the advertisement of that link between the ASBR and the other OSPF routers. Cisco routers configured with OSPF automatically accept the common LSAs such as 1, 2, 3, 4, 5, and 7. The ASBR has OSPF configured or the default-information originate command would not have been able to have been entered.

25. **An internal corporate server can be accessed by internal PCs, but not by external Internet users that should have access. What could be the issue?**
    - The default gateway router for the server does not have a default route.
    - The switch port to which the server connects has an incorrect VLAN configured.
    - The server does not have a private IP address assigned.
    - **Static NAT has not been configured properly or at all.***

    NAT/PAT allows a private IP address to be translated into a public address so that external users can access internal devices. Static NAT assigns one public address to a private address and is used with internal servers.

26. **Fill in the blank.**

    Use the cache to verify IPv4 address to Layer 2 Ethernet address mappings on a host computer.

    Correct Answer: ARP

    The ARP cache is used to store IPv4 addresses and the Ethernet physical addresses or MAC addresses to which the IPv4 addresses are mapped. Incorrect mappings of IP addresses to MAC addresses can result in loss of end-to-end connectivity.

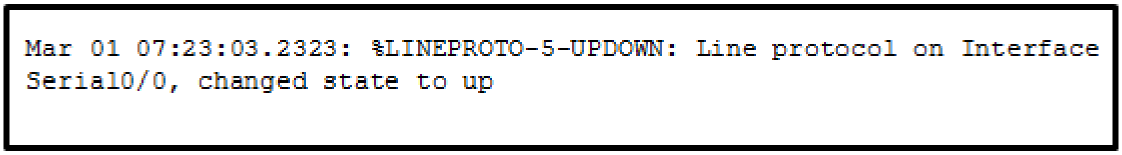
27. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**

    A user reports that PC0 cannot visit the web server www.server.com. Troubleshoot the network configuration to identify the problem. What is the cause of the problem?
    - The clock rate on Branch S0/0/0 is configured incorrectly.
    - **A serial interface encapsulation is configured incorrectly.***
    - The DNS server address on PC0 is configured incorrectly.
    - A default route on HQ is not configured.

    The status of interface S0/0/0 is up but the line protocol is down. A possible problem could be a framing error or an encapsulation error.

    Older Version

28. **What are the most common syslog messages?**
    - those that occur when a packet matches a parameter condition in an access control list
    - **link up and link down messages***
    - output messages that are generated from debug output
    - error messages about hardware or software malfunctions
29. **When logging is used, which severity level indicates that a device is unusable?**
    - Alert – Level 1
    - Critical – Level 2
    - **Emergency – Level 0***
    - Error – Level 3
30. **Refer to the exhibit. Which two conclusions can be drawn from the syslog message that was generated by the router? (Choose two.)**



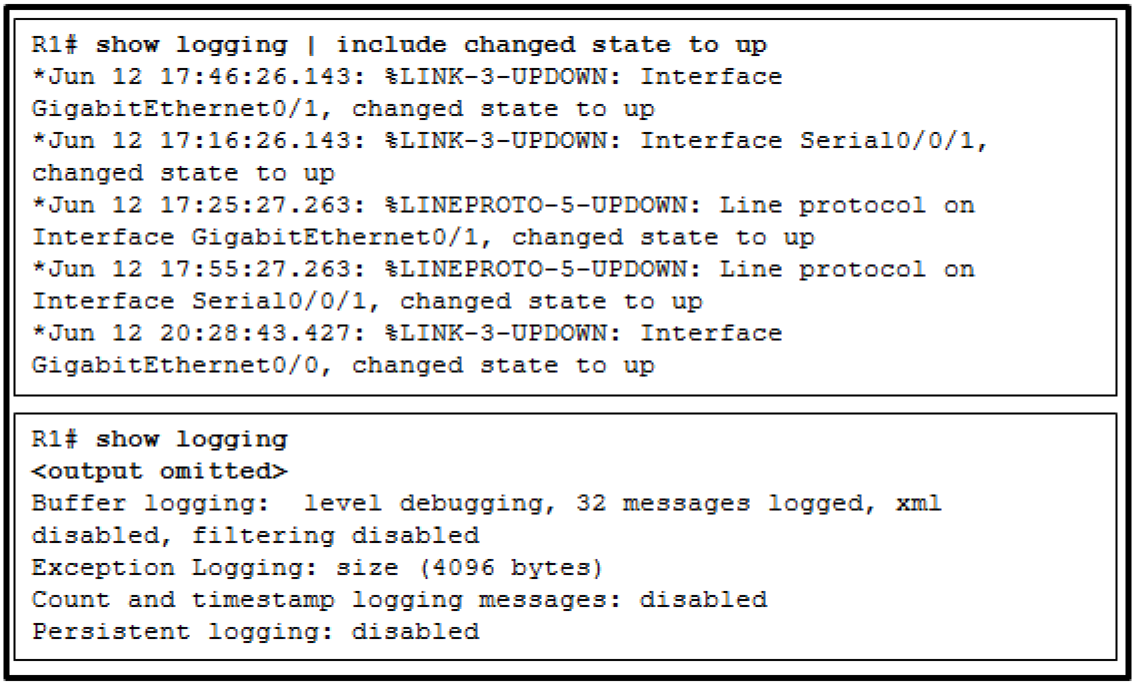
```
Mar 01 07:23:03.2323: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0, changed state to up
```

- This message resulted from an unusual error requiring reconfiguration of the interface.
- This message indicates that the interface should be replaced.
- **This message is a level 5 notification message. ***
- **This message indicates that service timestamps have been configured.***
- This message indicates that the interface changed state five times.

31. **A network technician has issued the service timestamps log datetime command in the configuration of the branch router. Which additional command is required to include the date and time in logged events?**

- Branch1(config)# service timestamps log uptime
- **Branch1# clock set 08:00:00 05 AUG 2013***
- Branch1(config)# service timestamps debug datetime
- Branch1# copy running-config startup-config

32. **Refer to the exhibit. From what location have the syslog messages been retrieved?**

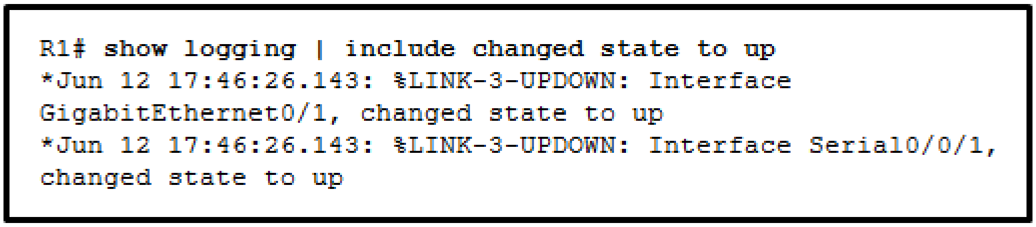


```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:16:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:25:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:55:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
```

```
R1# show logging
<output omitted>
Buffer logging:  level debugging, 32 messages logged, xml
disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

- syslog server
- syslog client
- **router RAM***
- router NVRAM

33. **Refer to the exhibit. What does the number 17:46:26.143 represent?**



```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
```

- the time passed since the syslog server has been started
- **the time when the syslog message was issued***
- the time passed since the interfaces have been up
- the time on the router when the show logging command was issued

34. **Which destination do Cisco routers and switches use by default when sending syslog messages for all severity levels?**

- **console***
- nearest syslog server
- NVRAM
- RAM

35. **A network administrator has issued the logging trap 4 global configuration mode command. What is the result of this command?**

- After four events, the syslog client will send an event message to the syslog server.
- The syslog client will send to the syslog server any event message that has a severity level of 4 and higher.
- **The syslog client will send to the syslog server any event message that has a severity level of 4 and lower.***
- The syslog client will send to the syslog server event messages with an identification trap level of only 4.

36. **Which statement describes SNMP operation?**

- An NMS periodically polls the SNMP agents that are residing on managed devices by using traps to query the devices for data.
- A get request is used by the SNMP agent to query the device for data.
- An SNMP agent that resides on a managed device collects information about the device and stores that information remotely in the MIB that is located on the NMS.
- **A set request is used by the NMS to change configuration variables in the agent device.***

37. **What are SNMP trap messages?**

- messages that are used by the NMS to query the device for data
- **unsolicited messages that are sent by the SNMP agent and alert the NMS to a condition on the network***
- messages that are used by the NMS to change configuration variables in the agent device
- messages that are sent periodically by the NMS to the SNMP agents that reside on managed devices to query the device for data

38. **Which SNMP feature provides a solution to the main disadvantage of SNMP polling?**

- SNMP set messages
- **SNMP trap messages***
- SNMP get messages
- SNMP community strings

39. **When SNMPv1 or SNMPv2 is being used, which feature provides secure access to MIB objects?**

- packet encryption
- message integrity
- community strings*
- source validation

40. **A network administrator has issued the snmp-server user admin1 admin v3 encrypted auth md5 abc789 priv des 256 key99 command. What are two features of this command? (Choose two.)**

- It adds a new user to the SNMP group.*
- It restricts SNMP access to defined SNMP managers.
- It forces the network manager to log into the agent to retrieve the SNMP messages.
- It uses the MD5 authentication of the SNMP messages.*
- It allows a network administrator to configure a secret encrypted password on the SNMP server.

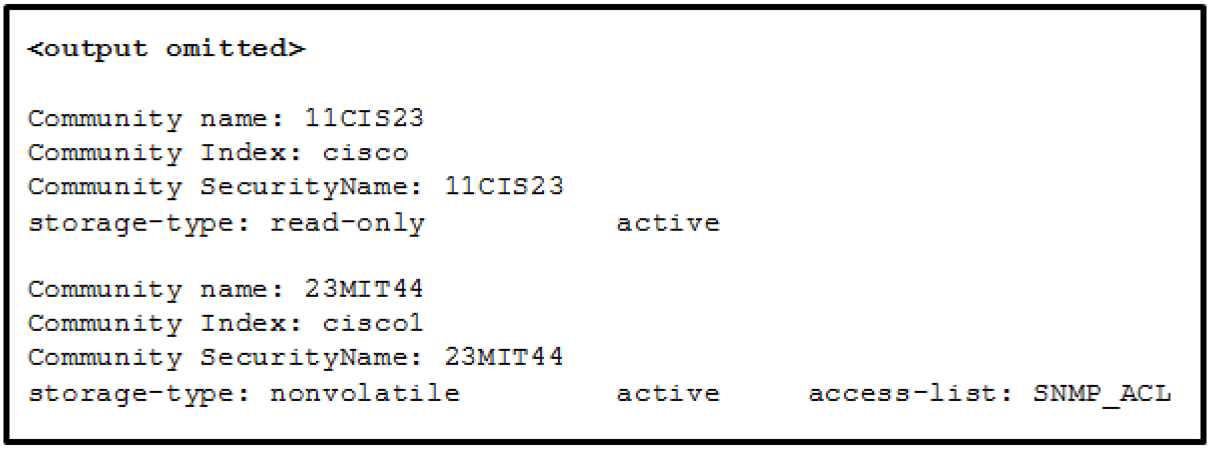
41. **How can SNMP access be restricted to a specific SNMP manager?**

- Use the snmp-server community command to configure the community string with no access level.
- Specify the IP address of the SNMP manager by using the snmp-server host command.
- Use the snmp-server traps command to enable traps on an SNMP manager.
- Define an ACL and reference it by using the snmp-server community command.*

42. **A network administrator issues two commands on a router:**
R1(config)# snmp-server host 10.10.50.25 version 2c campus
R1(config)# snmp-server enable traps
What can be concluded after the commands are entered?

- No traps are sent, because the notification-types argument was not specified yet.
- Traps are sent with the source IP address as 10.10.50.25.
- If an interface comes up, a trap is sent to the server.*
- The snmp-server enable traps command needs to be used repeatedly if a particular subset of trap types is desired.

43. **Refer to the exhibit. What can be concluded from the produced output?**



```
<output omitted>

Community name: 11CIS23
Community Index: cisco
Community SecurityName: 11CIS23
storage-type: read-only          active

Community name: 23MIT44
Community Index: cisco1
Community SecurityName: 23MIT44
storage-type: nonvolatile        active     access-list: SNMP_ACL
```

- An ACL was configured to restrict SNMP access to an SNMP manager.*
- This is the output of the show snmp command without any parameters.
- The system contact was not configured with the snmp-server contact command.
- The location of the device was not configured with the snmp-server location command.

44. **What is a difference between SNMP and NetFlow?**

- Unlike NetFlow, SNMP uses a “push”-based model.
- **NetFlow collects more detailed traffic statistics on IP networks than SNMP does.***
- SNMP only gathers traffic statistics, whereas NetFlow can also collect many other performance indicators, such as interface errors and CPU usage.
- Unlike NetFlow, SNMP may be used to provide IP accounting for billing purposes.

45. **How does NetFlow function on a Cisco router or multilayer switch?**

- Netflow captures and analyzes traffic.
- **One user connection to an application exists as two NetFlow flows.***
- On 2960 switches, Netlow allows for data export.
- NetFlow does not consume any additional memory.

46. **Which type of information can an administrator obtain with the show ip cache flow command?**

- the NetFlow version that is enabled
- whether NetFlow is configured on the correct interface and in the correct direction
- the configuration of the export parameters
- **the protocol that uses the largest volume of traffic***

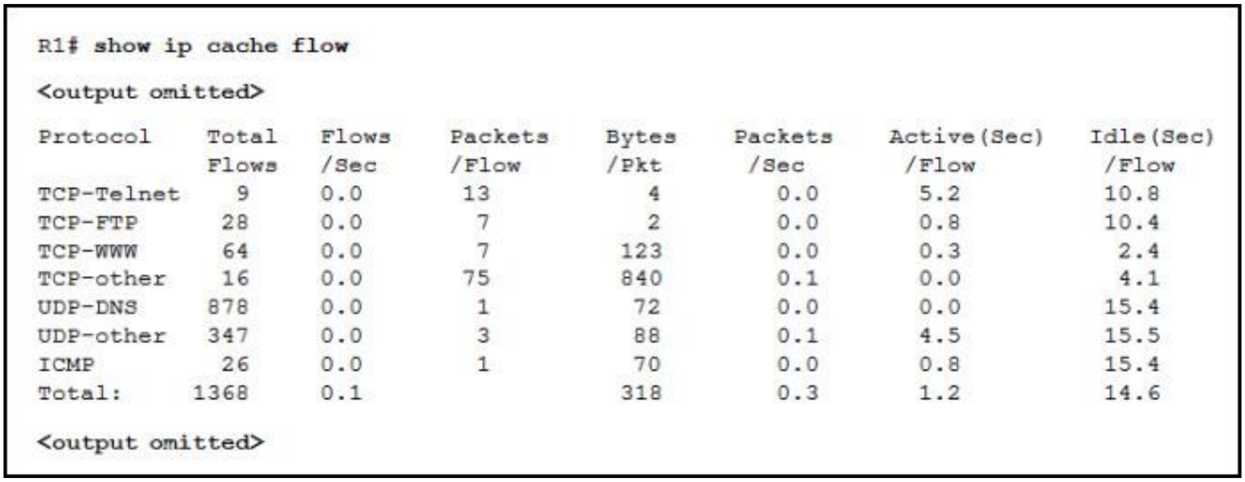
47. **Which two statements describe items to be considered in configuring NetFlow? (Choose two.)**

- Netflow requires both management and agent software.
- Netflow requires UDP port 514 for notification messages.
- **NetFlow consumes additional memory.***
- **Netflow can only be used in a unidirectional flow.***
- NetFlow can only be used if all devices on the network support it.

48. **What is the most common purpose of implementing NetFlow in a networked environment?**

- **to support accounting and monitoring with consumer applications***
- to actively capture traffic from networked devices
- to monitor live data usage and to control traffic flow with set messages
- to passively capture changing events that occur in the network and to perform after-the-fact-analysis

49. **Refer to the exhibit. While planning an upgrade, a network administrator uses the Cisco NetFlow utility to analyze data flow in the current network. Which protocol used the greatest amount of network time?**



```
R1# show ip cache flow

<output omitted>

Protocol      Total   Flows   Packets   Bytes   Packets   Active(Sec)   Idle(Sec)
              Flows   /Sec    /Flow     /Pkt    /Sec      /Flow         /Flow
TCP-Telnet      9     0.0     13          4      0.0       5.2          10.8
TCP-FTP        28     0.0      7          2      0.0       0.8          10.4
TCP-WWW        64     0.0      7        123      0.0       0.3           2.4
TCP-other      16     0.0     75        840      0.1       0.0           4.1
UDP-DNS       878     0.0      1         72      0.0       0.0          15.4
UDP-other     347     0.0      3         88      0.1       4.5          15.5
ICMP           26     0.0      1         70      0.0       0.8          15.4
Total:       1368     0.1               318      0.3       1.2          14.6

<output omitted>
```

- TCP-Telnet
- TCP-FTP

- TCP-other
- UDP-DNS
- **UDP-other ***

50. **Fill in the blank.**
    The **syslog**protocol uses UDP port 514 and is the most common method to access system messages provided by networking devices.
51. **When SNMPvl or SNMPv2 is being used, which feature provides secure access to MIB objects?**
    - message integrity
    - source validation
    - **community strings***
    - packet encryption
52. **A network administrator has issued the snmp-server user adminl admin v3 encrypted auth md5 abc789 priv des 256 key99 command. What are two features of this command? (Choose two.)**
    - It forces the network manager to log into the agent to retrieve the SNMP messages.
    - It restricts SNMP access to defined SNMP managers.
    - **It uses the MD5 authentication of the SNMP messages.***
    - It allows a network administrator to configure a secret encrypted password on the SNMP server.
    - **It adds a new user to the SNMP group.**
53. **Which SNMP version uses weak community string-based access control and supports bulk retrieval?**
    - SNMPv3
    - SNMPv1
    - **SNMPv2c***
    - SNMPv2Classic
54. **Which protocol or service can be configured to send unsolicited messages to alert the network administrator about a network event such as an extremely high CPU utilization on a router?**
    - **SNMP***
    - NetFlow
    - syslog
    - NTP
55. **Which protocol or service allows network administrators to receive system messages that are provided by network devices?**
    - SNMP
    - **syslog***
    - NetFlow
    - NTP
56. **The command ntp server 10.1.1.1 is issued on a router. What impact does this command have?**
    - determines which server to send system log files to
    - **synchronizes the clock of the device to the timeserver that is located at IP address 10.1.1.1***
    - identifies the server on which to store backup configurations

- ensures that all logging will have a time stamp associated with it

57. **Which syslog message type is accessible only to an administrator and only via the Cisco CLI?**
    - alerts
    - **debugging***
    - emergency
    - errors
58. **Which protocol is used by network administrators to track and gather statistics on TCP/IP packets that are entering or exiting network devices?**
    - syslog
    - **NetFlow***
    - NTP
    - SNMP