[Updated Constantly]

HERE

CCNA 1 (v5.1 + v6.0) Chapter 11 Exam Answers Full

How to find: Press "Ctrl + F" in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **A newly hired network technician is given the task of ordering new hardware for a small business with a large growth forecast. Which primary factor should the technician be concerned with when choosing the new devices?**
   - devices with a fixed number and type of interfaces
   - devices that have support for network monitoring
   - redundant devices
   - **devices with support for modularity***

   Explain:
   In a small business with a large growth forecast, the primary influencing factor would be the ability of devices to support modularity. Devices with a fixed type/number of interfaces would not support growth. Redundancy is an important factor, but typically found in large enterprises. Network monitoring is also an important consideration, but not as important as modularity.

2. **Which network design consideration would be more important to a large corporation than to a small business?**
   - Internet router
   - firewall
   - low port density switch
   - **redundancy***

   Explain:
   Small businesses today do need Internet access and use an Internet router to provide this need. A switch is required to connect the two host devices and any IP phones or network devices such as a printer or a scanner. The switch may be integrated into the router. A firewall is needed to protect the business computing assets. Redundancy is not normally found in very small companies, but slightly larger small companies might use port density redundancy or have redundant Internet providers/links.

3. **Which two traffic types require delay sensitive delivery? (Choose two.)**
   - email
   - web
   - FTP
   - **voice***
   - **video***

   Explain:
   Voice and video traffic have delay sensitive characteristics and must be given priority over other traffic types such as web, email, and file transfer traffic.

4. **A network administrator for a small company is contemplating how to scale the network over the next three years to accommodate projected growth. Which three types of information should be used to plan for network growth? (Choose three.)**
   - human resource policies and procedures for all employees in the company
   - **documentation of the current physical and logical topologies ***
   - **analysis of the network traffic based on protocols, applications, and services used on the network***
   - history and mission statement of the company
   - **inventory of the devices that are currently used on the network***
   - listing of the current employees and their role in the company

   Explain:
   Several elements that are needed to scale a network include documentation of the physical and logical topology, a list of devices that are used on the network, and an analysis of the traffic on the network.

5. **Which two statements describe how to assess traffic flow patterns and network traffic types using a protocol analyzer? (Choose two.)**
   - Capture traffic on the weekends when most employees are off work.
   - Only capture traffic in the areas of the network that receive most of the traffic such as the data center.
   - **Capture traffic during peak utilization times to get a good representation of the different traffic types. ***
   - **Perform the capture on different network segments.***
   - Only capture WAN traffic because traffic to the web is responsible for the largest amount of traffic on a network.

   Explain:
   Traffic flow patterns should be gathered during peak utilization times to get a good

representation of the different traffic types. The capture should also be performed on different network segments because some traffic will be local to a particular segment.

6. **Some routers and switches in a wiring closet malfunctioned after an air conditioning unit failed. What type of threat does this situation describe?**
   - configuration
   - **environmental***
   - electrical
   - maintenance

   Explain:
   The four classes of threats are as follows:
   Hardware threats – physical damage to servers, routers, switches, cabling plant, and workstations
   Environmental threats – temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
   Electrical threats – voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
   Maintenance threats – poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling

7. **Which type of network threat is intended to prevent authorized users from accessing resources?**
   - **DoS attacks***
   - access attacks
   - reconnaissance attacks
   - trust exploitation

   Explain:
   Network reconnaissance attacks involve the unauthorized discovery and mapping of the network and network systems. Access attacks and trust exploitation involve unauthorized manipulation of data and access to systems or user privileges. DoS, or Denial of Service attacks, are intended to prevent legitimate users and devices from accessing network resources.

8. **Which two actions can be taken to prevent a successful network attack on an email server account? (Choose two.)**
   - **Never send the password through the network in a clear text.***
   - Never use passwords that need the Shift key.

- Use servers from different vendors.
- Distribute servers throughout the building, placing them close to the stakeholders.
- **Limit the number of unsuccessful attempts to log in to the server.***

Explain:
One of the most common types of access attack uses a packet sniffer to yield user accounts and passwords that are transmitted as clear text. Repeated attempts to log in to a server to gain unauthorized access constitute another type of access attack. Limiting the number of attempts to log in to the server and using encrypted passwords will help prevent successful logins through these types of access attack.

9. **Which firewall feature is used to ensure that packets coming into a network are legitimate responses initiated from internal hosts?**
   - application filtering
   - **stateful packet inspection***
   - URL filtering
   - packet filtering

Explain:
Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network. Packet filtering can be used to permit or deny access to resources based on IP or MAC address. Application filtering can permit or deny access based on port number. URL filtering is used to permit or deny access based on URL or on keywords.

10. **What is the purpose of the network security authentication function?**
    - **to require users to prove who they are***
    - to determine which resources a user can access
    - to keep track of the actions of a user
    - to provide challenge and response questions

Explain:
Authentication, authorization, and accounting are network services collectively known as AAA. Authentication requires users to prove who they are. Authorization determines which resources the user can access. Accounting keeps track of the actions of the user.

11. **A network administrator is issuing the login block-for 180 attempts 2 within 30 command on a router. Which threat is the network administrator trying to prevent?**
    - **a user who is trying to guess a password to access the router***
    - a worm that is attempting to access another part of the network

- an unidentified individual who is trying to access the network equipment room
- a device that is trying to inspect the traffic on a link

Explain:

The login block-for 180 attempts 2 within 30 command will cause the device to block authentication after 2 unsuccessful attempts within 30 seconds for a duration of 180 seconds. A device inspecting the traffic on a link has nothing to do with the router. The router configuration cannot prevent unauthorized access to the equipment room. A worm would not attempt to access the router to propagate to another part of the network.

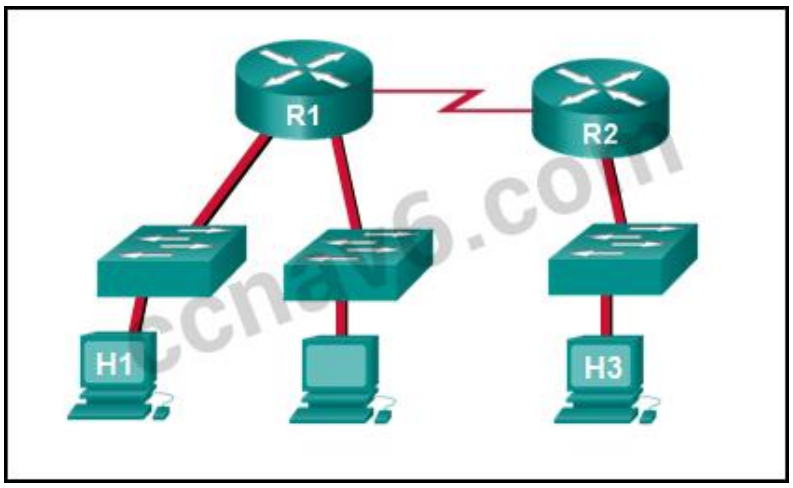
12. **Which two steps are required before SSH can be enabled on a Cisco router? (Choose two.)**
    - **Give the router a host name and domain name.***
    - Create a banner that will be displayed to users when they connect.
    - **Generate a set of secret keys to be used for encryption and decryption.***
    - Set up an authentication server to handle incoming connection requests.
    - Enable SSH on the physical interfaces where the incoming connection requests will be received.

    Explain:

    There are four steps to configure SSH on a Cisco router. First, set the host name and domain name. Second, generate a set of RSA keys to be used for encrypting and decrypting the traffic. Third, create the user IDs and passwords of the users who will be connecting. Lastly, enable SSH on the vty lines on the router. SSH does not need to be set up on any physical interfaces, nor does an external authentication server need to be used. While it is a good idea to configure a banner to display legal information for connecting users, it is not required to enable SSH.

13. **Refer to the exhibit. Baseline documentation for a small company had ping round trip time statistics of 36/97/132 between hosts H1 and H3. Today the network administrator checked connectivity by pinging between hosts H1 and H3 that resulted in a round trip**

time of 1458/2390/6066. What does this indicate to the network administrator?



- Connectivity between H1 and H3 is fine.
- H3 is not connected properly to the network.
- Something is causing interference between H1 and R1.
- Performance between the networks is within expected parameters.
- **Something is causing a time delay between the networks.***

Explain:

Ping round trip time statistics are shown in milliseconds. The larger the number the more delay. A baseline is critical in times of slow performance. By looking at the documentation for the performance when the network is performing fine and comparing it to information when there is a problem, a network administrator can resolve problems faster.

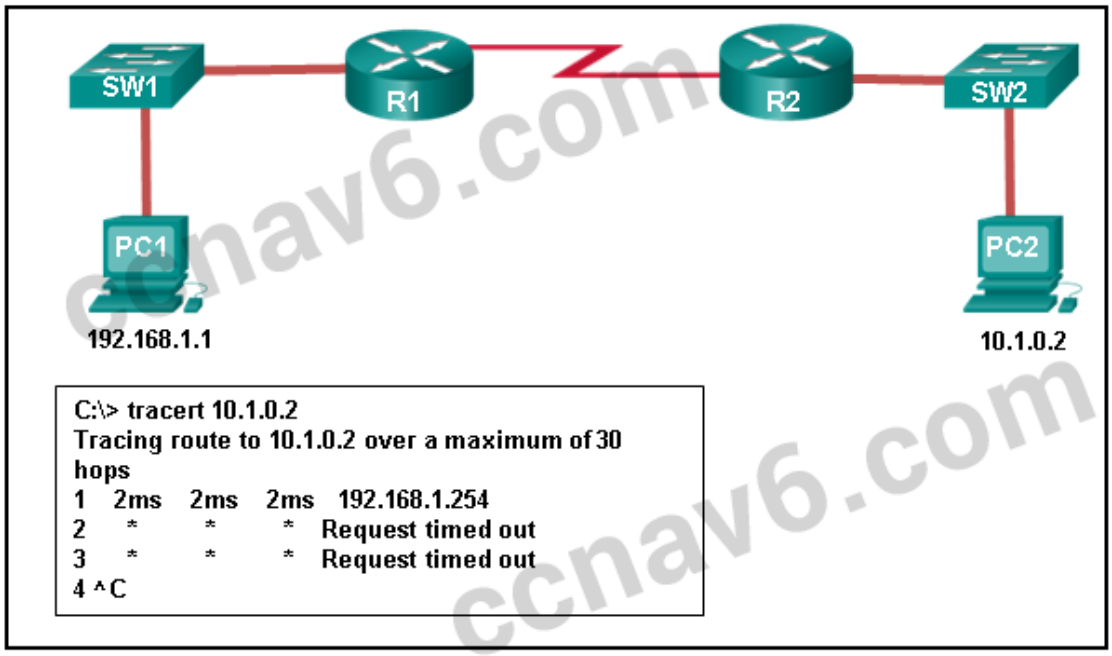
14. **When should an administrator establish a network baseline?**
    - when the traffic is at peak in the network
    - when there is a sudden drop in traffic
    - at the lowest point of traffic in the network
    - **at regular intervals over a period of time***

Explain:

An effective network baseline can be established by monitoring the traffic at regular intervals. This allows the administrator to take note when any deviance from the established norm occurs in the network.

15. **Refer to the exhibit. An administrator is trying to troubleshoot connectivity between PC1 and PC2 and uses the tracert command from PC1 to do it. Based on the displayed**

output, where should the administrator begin troubleshooting?



- PC2
- **R1***
- SW2
- R2
- SW1

Explain:

Tracert is used to trace the path a packet takes. The only successful response was from the first device along the path on the same LAN as the sending host. The first device is the default gateway on router R1. The administrator should therefore start troubleshooting at R1.

16. **Which statement is true about CDP on a Cisco device?**

- The show cdp neighbor detail command will reveal the IP address of a neighbor only if there is Layer 3 connectivity.
- To disable CDP globally, the no cdp enable command in interface configuration mode must be used.
- **CDP can be disabled globally or on a specific interface.***
- Because it runs at the data link layer, the CDP protocol can only be implemented in switches.

Explain:

CDP is a Cisco-proprietary protocol that can be disabled globally by using the no cdp run global configuration command, or disabled on a specific interface, by using the no cdp enable interface configuration command. Because CDP operates at the data link layer, two or more

Cisco network devices, such as routers can learn about each other even if Layer 3 connectivity does not exist. The show cdp neighbors detail command reveals the IP address of a neighboring device regardless of whether you can ping the neighbor.

17. **A network administrator for a small campus network has issued the show ip interface brief command on a switch. What is the administrator verifying with this command?**
    - **the status of the switch interfaces and the address configured on interface vlan 1***
    - that a specific host on another network can be reached
    - the path that is used to reach a specific host on another network
    - the default gateway that is used by the switch

    Explain:
    The show ip interface brief command is used to verify the status and IP address configuration of the physical and switch virtual interfaces (SVI).

18. **A network technician issues the arp -d * command on a PC after the router that is connected to the LAN is reconfigured. What is the result after this command is issued?**
    - **The ARP cache is cleared.***
    - The current content of the ARP cache is displayed.
    - The detailed information of the ARP cache is displayed.
    - The ARP cache is synchronized with the router interface.

    Explain:
    Issuing the arp –d * command on a PC will clear the ARP cache content. This is helpful when a network technician wants to ensure the cache is populated with updated information.

19. **Fill in the blank.**
    VoIP defines the protocols and technologies that implement the transmission of voice data over an IP network

20. **Fill in the blank. Do not use abbreviations.**
    The show **file systems** command provides information about the amount of free nvram and flash memory with the permissions for reading or writing data.

21. **Fill in the blank. Do not use abbreviations.**
    The **show version** command that is issued on a router is used to verify the value of the software configuration register.

    Explain:
    The show version command that is issued on a router displays the value of the configuration register, the Cisco IOS version being used, and the amount of flash memory on the device, among other information.

22. **What service defines the protocols and technologies that implement the transmission of voice packets over an IP network?**
    - **VoIP***
    - NAT
    - DHCP
    - QoS
23. **What is the purpose of using SSH to connect to a router?**
    - **It allows a secure remote connection to the router command line interface.***
    - It allows a router to be configured using a graphical interface.
    - It allows the router to be monitored through a network management application.
    - It allows secure transfer of the IOS software image from an unsecure workstation or server.
24. **What information about a Cisco router can be verified using the show version command?**
    - **the value of the configuration register***
    - the administrative distance used to reach networks
    - the operational status of serial interfaces
    - the routing protocol version that is enabled
25. **A network technician issues the C:\> tracert -6 www.cisco.com command on a Windows PC. What is the purpose of the -6 command option?**
    - **It forces the trace to use IPv6.***
    - It limits the trace to only 6 hops.
    - It sets a 6 milliseconds timeout for each replay.
    - It sends 6 probes within each TTL time period.

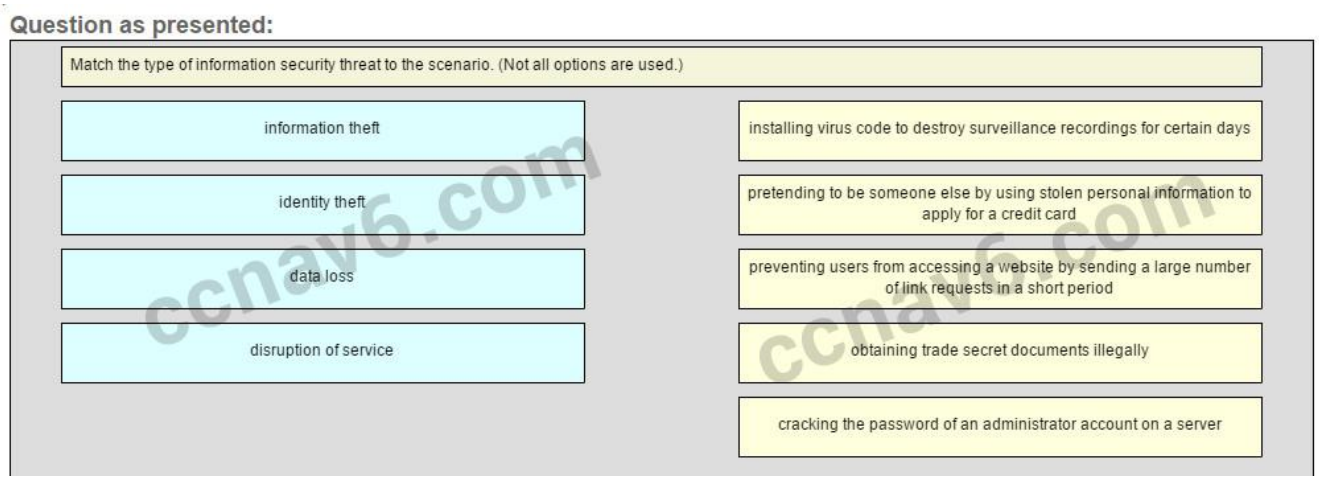
    Explain:
    The -6 option in the command C:\> tracert -6 www.cisco.com is used to force the trace to use IPv6.

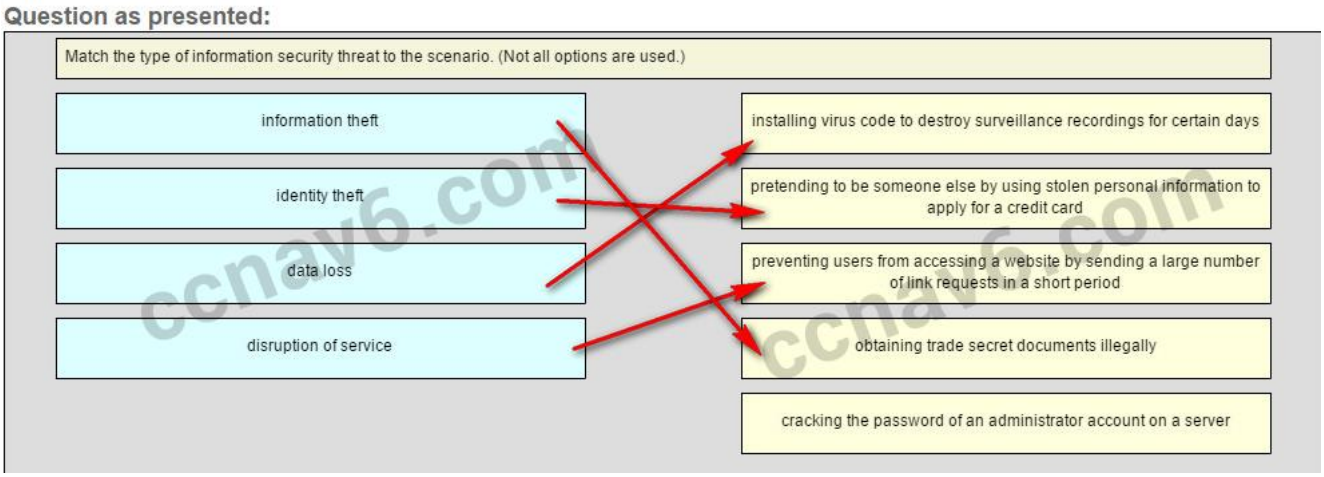
26. **Which command should be used on a Cisco router or switch to allow log messages to be displayed on remotely connected sessions using Telnet or SSH?**
    - debug all
    - logging synchronous
    - show running-config
    - **terminal monitor***

    Explain:
    The terminal monitor command is very important to use when log messages appear. Log messages appear by default when a user is directly consoled into a Cisco device, but require

the terminal monitor command to be entered when a user is accessing a network device remotely.

27. **Match the type of information security threat to the scenario. (Not all options are used.)**





Place the options in the following order.

installing virus code to destroy surveillance recordings for certain days -> data loss

pretending to be someone else by using stolen personal information to apply for a credit card ->identity theft

preventing userd from accessing a website by sending a large number of link requests in a short period -> disruption of service

obtaining trade secret documents illegally -> information theft

— not scored —

Explain:

After an intruder gains access to a network, common network threats are as follows:

Information theft

Identity theft

Data loss or manipulation

Disruption of service

Cracking the password for a known username is a type of access attack.

Older Version

1. **What is the purpose of issuing the commands cd nvram: then dir at the privilege exec mode of a router?**
   - to clear the content of the NVRAM
   - to direct all new files to the NVRAM
   - **to list the content of the NVRAM***
   - to copy the directories from the NVRAM
2. **Which command will backup the configuration that is stored in NVRAM to a TFTP server?**
   - copy running-config tftp
   - copy tftp running-config
   - **copy startup-config tftp***
   - copy tftp startup-config
3. **Which protocol supports rapid delivery of streaming media?**
   - SNMP
   - TCP
   - PoE
   - **RTP***
4. **How should traffic flow be captured in order to best understand traffic patterns in a network?**
   - during low utilization times
   - **during peak utilization times***
   - when it is on the main network segment only
   - when it is from a subset of users
5. **A network administrator checks the security log and notices there was unauthorized access to an internal file server over the weekend. Upon further investigation of the file system log, the administrator notices several important documents were copied to a host located outside of the company. What kind of threat is represented in this scenario?**
   - data loss

- identity theft
- **information theft***
- disruption of service

6. **Which two actions can be taken to prevent a successful attack on an email server account? (Choose two.)**
   - **Never send the password through the network in a clear text.***
   - Never use passwords that need the Shift key.
   - Never allow physical access to the server console.
   - Only permit authorized access to the server room.
   - **Limit the number of unsuccessful attempts to log in to the server.***
7. **Which type of network attack involves the disabling or corruption of networks, systems, or services?**
   - reconnaissance attacks
   - access attacks
   - **denial of service attacks***
   - malicious code attacks
8. **A network administrator has determined that various computers on the network are infected with a worm. Which sequence of steps should be followed to mitigate the worm attack?**
   - inoculation, containment, quarantine, and treatment
   - containment, quarantine, treatment, and inoculation
   - treatment, quarantine, inoculation, and containment
   - **containment, inoculation, quarantine, and treatment ***
9. **What is a security feature of using NAT on a network?**
   - allows external IP addresses to be concealed from internal users
   - **allows internal IP addresses to be concealed from external users***
   - denies all packets that originate from private IP addresses
   - denies all internal hosts from communicating outside their own network
10. **A ping fails when performed from router R1 to directly connected router R2. The network administrator then proceeds to issue the show cdp neighbors command. Why would the network administrator issue this command if the ping failed between the two routers?**
    - The network administrator suspects a virus because the ping command did not work.
    - **The network administrator wants to verify Layer 2 connectivity.***
    - The network administrator wants to verify the IP address configured on router R2.

- The network administrator wants to determine if connectivity can be established from a non-directly connected network.

11. **If a configuration file is saved to a USB flash drive attached to a router, what must be done by the network administrator before the file can be used on the router?**
    - Convert the file system from FAT32 to FAT16.
    - **Edit the configuration file with a text editor.***
    - Change the permission on the file from ro to rw.
    - Use the dir command from the router to remove the Windows automatic alphabetization of the files on the flash drive.
12. **Which two statements about a service set identifier (SSID) are true? (Choose two.)**
    - **tells a wireless device to which WLAN it belongs***
    - consists of a 32-character string and is not case sensitive
    - responsible for determining the signal strength
    - **all wireless devices on the same WLAN must have the same SSID***
    - used to encrypt data sent across the wireless network
13. **What do WLANs that conform to IEEE 802.11 standards allow wireless users to do?**
    - use wireless mice and keyboards
    - create a one-to-many local network using infrared technology
    - use cell phones to access remote services over very large areas
    - **connect wireless hosts to hosts or services on a wired Ethernet network ***
14. **Which WLAN security protocol generates a new dynamic key each time a client establishes a connection with the AP?**
    - EAP
    - PSK
    - WEP
    - **WPA***
15. **Which two statements characterize wireless network security? (Choose two.)**
    - Wireless networks offer the same security features as wired networks.
    - Some RF channels provide automatic encryption of wireless data.
    - **With SSID broadcast disabled, an attacker must know the SSID to connect.***
    - **Using the default IP address on an access point makes hacking easier.***
    - An attacker needs physical access to at least one network device to launch an attack.
16. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. How long will a user be blocked if the user exceeds the maximum allowed number of unsuccessful login attempts?**
    - 1 minute

- 2 minutes
- **3 minutes***
- 4 minutes