Introduction to Networks (Version 7.00) – Modules 16 – 17: Building and Securing a Small Network Exam

Which component is designed to protect against unauthorized communications to and from a computer?

- security center
- port scanner
- antimalware
- antivirus
- **firewall**

Which command will block login attempts on RouterA for a period of 30 seconds if there are 2 failed login attempts within 10 seconds?

- RouterA(config)# login block-for 10 attempts 2 within 30
- **RouterA(config)# login block-for 30 attempts 2 within 10**
- RouterA(config)# login block-for 2 attempts 30 within 10
- RouterA(config)# login block-for 30 attempts 10 within 2

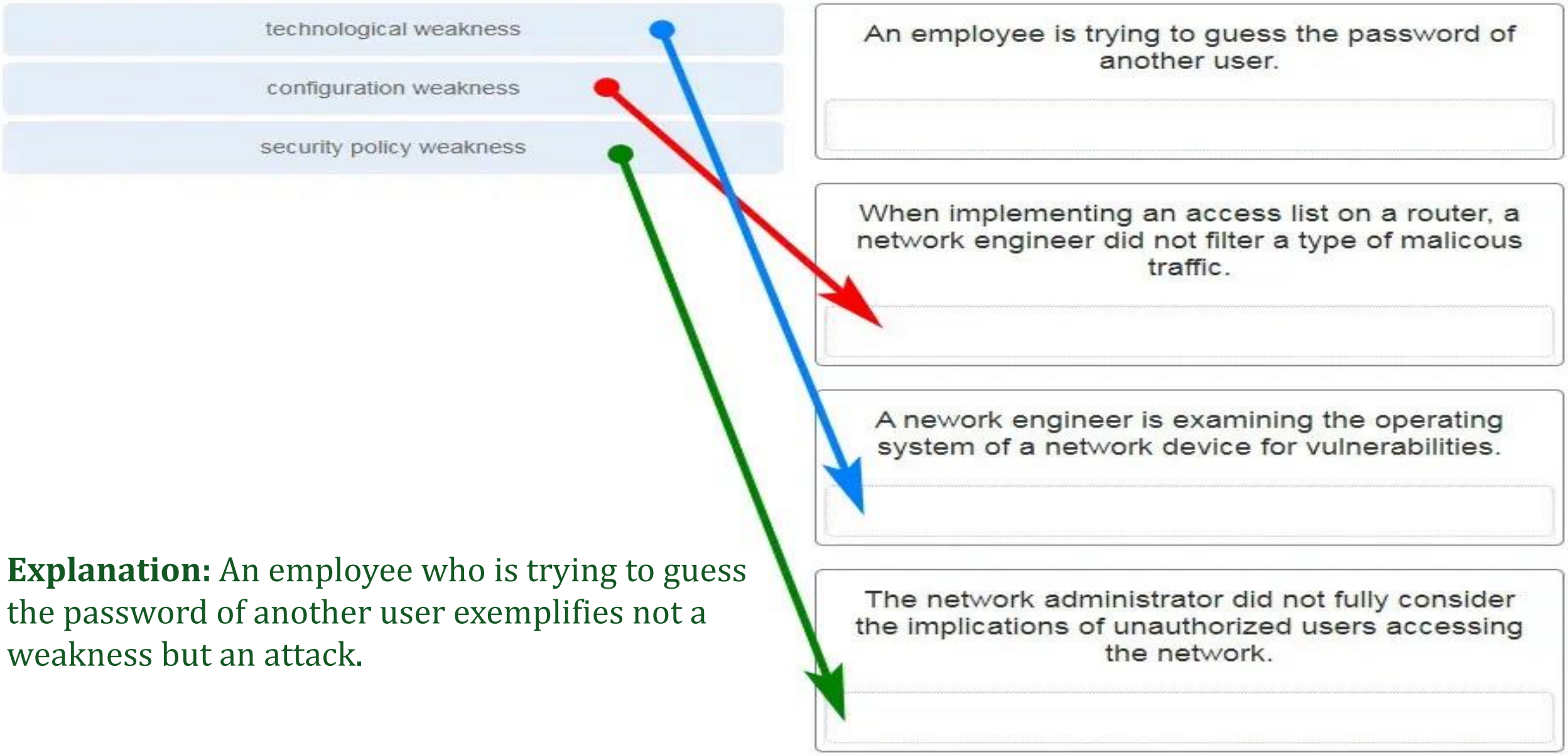
What is the purpose of the network security accounting function?

- o 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

What type of attack may involve the use of tools such as nslookup and fping?

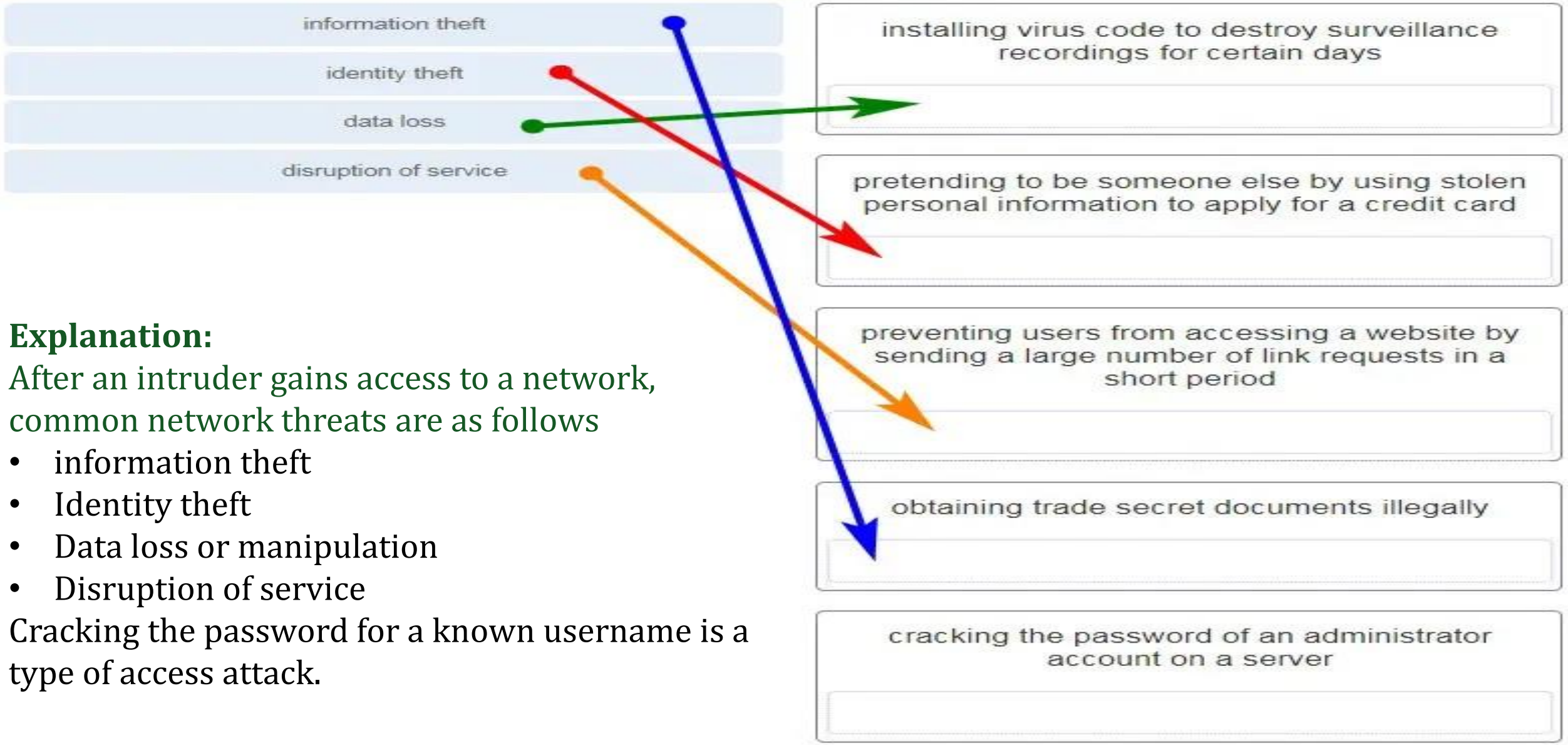
- access attack
- **reconnaissance attack**
- denial of service attack
- worm attack

Match each weakness with an example. (Not all options are used.)



Explanation: An employee who is trying to guess the password of another user exemplifies not a weakness but an attack.

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



Explanation:

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.

Which example of malicious code would be classified as a Trojan horse?

- **malware that was written to look like a video game**
- malware that requires manual user intervention to spread between systems
- malware that attaches itself to a legitimate program and spreads to other programs when launched
- malware that can automatically spread from one system to another by exploiting a vulnerability in the target

Explanation: A Trojan horse is malicious code that has been written specifically to look like a legitimate program. This is in contrast to a virus, which simply attaches itself to an actual legitimate program. Viruses require manual intervention from a user to spread from one system to another, while a worm is able to spread automatically between systems by exploiting vulnerabilities on those devices.

What is the difference between a virus and a worm?

- Viruses self-replicate but worms do not.
- **Worms self-replicate but viruses do not.**
- Worms require a host file but viruses do not.
- Viruses hide in legitimate programs but worms do not.

Explanation: Worms are able to self-replicate and exploit vulnerabilities on computer networks without user participation.

Which attack involves a compromise of data that occurs between two end points?

- denial-of-service
- **man-in-the-middle attack**
- extraction of security parameters
- username enumeration

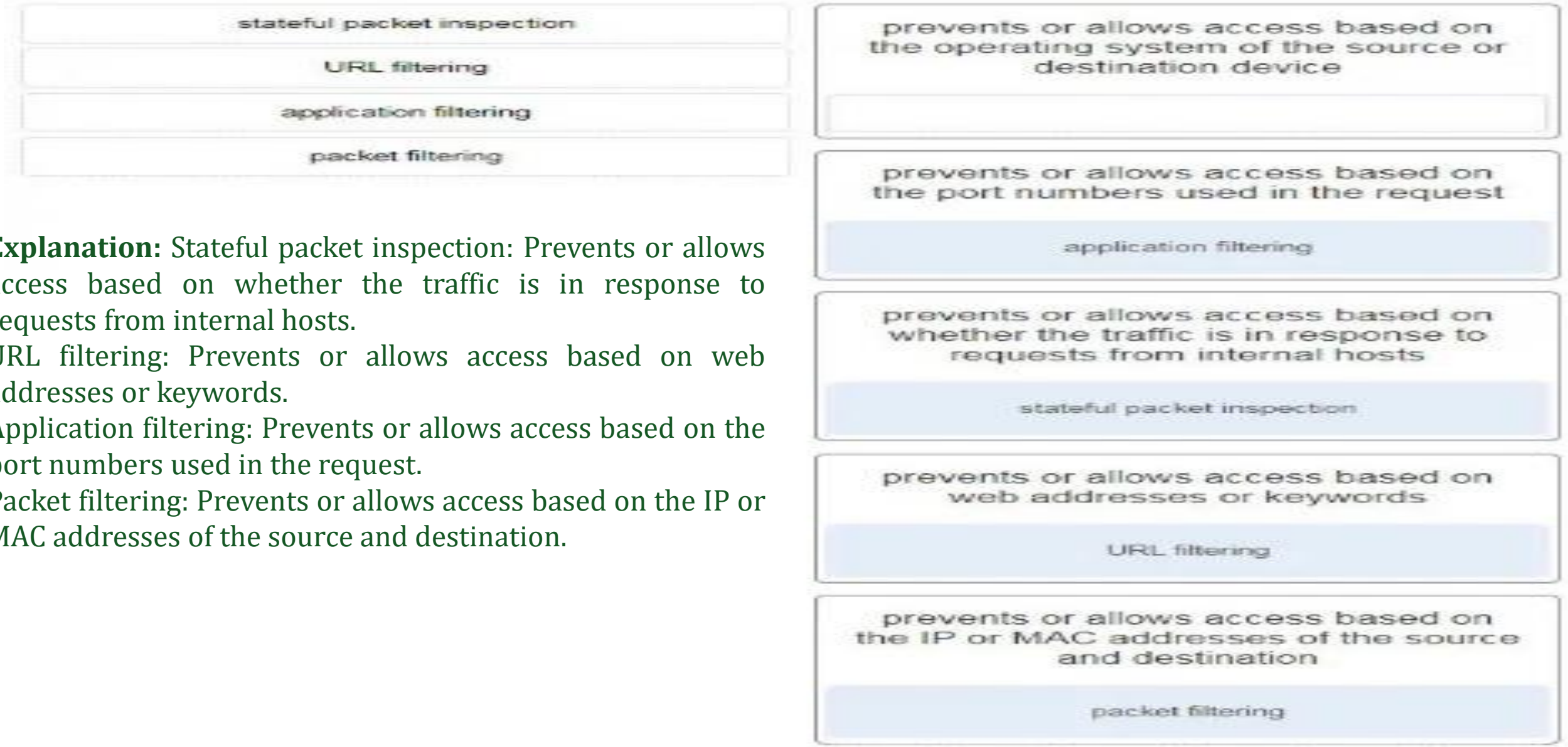
Explanation: Threat actors frequently attempt to access devices over the internet through communication protocols. Some of the most popular remote exploits are as follows:
Man-In-the-middle attack (MITM) – The threat actor gets between devices in the system and intercepts all of the data being transmitted. This information could simply be collected or modified for a specific purpose and delivered to its original destination.
Eavesdropping attack – When devices are being installed, the threat actor can intercept data such as security keys that are used by constrained devices to establish communications once they are up and running.
SQL injection (SQLi) – Threat actors uses a flaw in the Structured Query Language (SQL) application that allows them to have access to modify the data or gain administrative privileges.
Routing attack – A threat actor could either place a rogue routing device on the network or modify routing packets to manipulate routers to send all packets to the chosen destination of the threat actor. The threat actor could then drop specific packets, known as selective forwarding, or drop all packets, known as a sinkhole attack.

Which type of attack involves an adversary attempting to gather information about a network to identify vulnerabilities?

- **reconnaissance**
- DoS
- dictionary
- man-in-the-middle

Explanation: Reconnaissance is a type of attack where the intruder is looking for wireless network vulnerabilities

Match the description to the type of firewall filtering. (Not all options are used.)



Explanation: Stateful packet inspection: Prevents or allows access based on whether the traffic is in response to requests from internal hosts.
URL filtering: Prevents or allows access based on web addresses or keywords.
Application filtering: Prevents or allows access based on the port numbers used in the request.
Packet filtering: Prevents or allows access based on the IP or MAC addresses of the source and destination.

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

Explanation: 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.

Which firewall feature is used to ensure that packets coming into a network are legitimate responses to requests initiated from internal hosts?

- **stateful packet inspection**
- URL filtering
- application filtering
- packet filtering

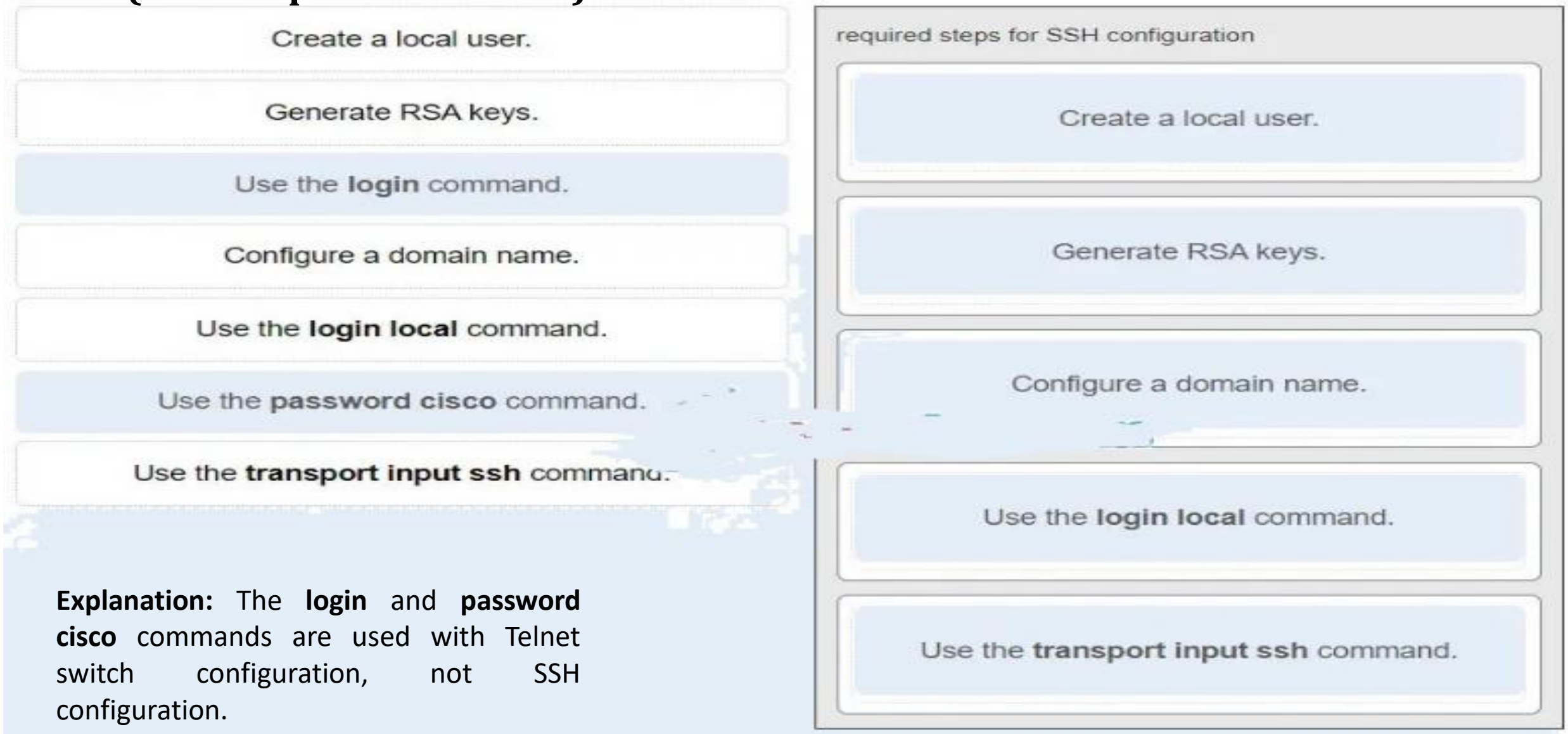
Explanation: Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network. Packet filtering can be used to permit or deny access to resources based on IP or MAC address. Application filtering can permit or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

When applied to a router, which command would help mitigate brute-force password attacks against the router?

- exec-timeout 30
- service password-encryption
- banner motd $Max failed logins = 5$
- **login block-for 60 attempts 5 within 60**

Explanation: The **login block-for** command sets a limit on the maximum number of failed login attempts allowed within a defined period of time. If this limit is exceeded, no further logins are allowed for the specified period of time. This helps to mitigate brute-force password cracking since it will significantly increase the amount of time required to crack a password. The **exec-timeout** command specifies how long the session can be idle before the user is disconnected. The **service password-encryption** command encrypts the passwords in the running configuration. The **banner motd** command displays a message to users who are logging in to the device.

Identify the steps needed to configure a switch for SSH. The answer order does not matter. (Not all options are used.)



Explanation: The **login** and **password cisco** commands are used with Telnet switch configuration, not SSH configuration.

What feature of SSH makes it more secure than Telnet for a device management connection?

- confidentiality with IPsec
- stronger password requirement
- random one-time port connection
- **login information and data encryption**

Explanation: Secure Shell (SSH) is a protocol that provides a secure management connection to a remote device. SSH provides security by providing encryption for both authentication (username and password) and the transmitted data. Telnet is a protocol that uses unsecure plaintext transmission. SSH is assigned to TCP port 22 by default. Although this port can be changed in the SSH server configuration, the port is not dynamically changed. SSH does not use IPsec.

What is the advantage of using SSH over Telnet?

- SSH is easier to use.
- SSH operates faster than Telnet.
- **SSH provides secure communications to access hosts.**
- SSH supports authentication for a connection request.

Explanation: SSH provides a secure method for remote access to hosts by encrypting network traffic between the SSH client and remote hosts. Although both Telnet and SSH request authentication before a connection is established, Telnet does not support encryption of login credentials.

What is the role of an IPS?

- **detecting and blocking of attacks in real time**
- connecting global threat information to Cisco network security devices
- authenticating and validating traffic
- filtering of nefarious websites

Explanation: An intrusion prevention system (IPS) provides real-time detection and blocking of attacks.

A user is redesigning a network for a small company and wants to ensure security at a reasonable price. The user deploys a new application-aware firewall with intrusion detection capabilities on the ISP connection. The user installs a second firewall to separate the company network from the public network. Additionally, the user installs an IPS on the internal network of the company. What approach is the user implementing?

- attack based
- risk based
- structured
- **layered**

Explanation: Using different defenses at various points of the network creates a layered approach.

What is an accurate description of redundancy?

- configuring a router with a complete MAC address database to ensure that all frames can be forwarded to the correct destination
- configuring a switch with proper security to ensure that all traffic forwarded through an interface is filtered
- designing a network to use multiple virtual devices to ensure that all traffic uses the best path through the internetwork
- **designing a network to use multiple paths between switches to ensure there is no single point of failure**

Explanation: Redundancy attempts to remove any single point of failure in a network by using multiple physically cabled paths between switches in the network.

A network administrator is upgrading a small business network to give high priority to real-time applications traffic. What two types of network services is the network administrator trying to accommodate? (Choose two.)

- **voice**
- **video**
- instant messaging
- FTP
- SNMP

Explanation: Streaming media, such as video, and voice traffic, are both examples of real-time traffic. Real-time traffic needs higher priority through the network than other types of traffic because it is very sensitive to network delay and latency.

What is the purpose of a small company using a protocol analyzer utility to capture network traffic on the network segments where the company is considering a network upgrade?

- to identify the source and destination of local network traffic
- to capture the Internet connection bandwidth requirement
- **to document and analyze network traffic requirements on each network segment**
- to establish a baseline for security analysis after the network is upgraded

Explanation: An important prerequisite for considering network growth is to understand the type and amount of traffic that is crossing the network as well as the current traffic flow. By using a protocol analyzer in each network segment, the network administrator can document and analyze the network traffic pattern for each segment, which becomes the base in determining the needs and means of the network growth.

Refer to the exhibit. An administrator is testing connectivity to a remote device with the IP address 10.1.1.1. What does the output of this command indicate?

- Connectivity to the remote device was successful.
- **A router along the path did not have a route to the destination.**
- A ping packet is being blocked by a security device along the path.
- The connection timed out while waiting for a reply from the remote device.

Explanation: In the output of the ping command, an exclamation mark (!) indicates a response was successfully received, a period (.) indicates that the connection timed out while waiting for a reply, and the letter “U” indicates that a router along the path did not have a route to the destination and sent an ICMP destination unreachable message back to the source.

Which method is used to send a ping message specifying the source address for the ping?

- issue the ping command from within interface configuration mode.
- **Issue the ping command without specifying a destination IP address.**
- Issue the ping command without extended commands.
- Issue the ping command after shutting down un-needed interfaces.

Explanation: By issuing the **ping** command without a destination IP address in privileged EXEC mode, the Cisco IOS enters extended ping mode. This allows the user to implement extended commands which include source IP address.

A network engineer is analyzing reports from a recently performed network baseline. Which situation would depict a possible latency issue?

- a change in the bandwidth according to the show interfaces output
- a next-hop timeout from a traceroute
- **an increase in host-to-host ping response times**
- a change in the amount of RAM according to the show version output

Explanation: While analyzing historical reports an administrator can compare host-to-host timers from the **ping** command and depict possible latency issues.

Which statement is true about Cisco IOS ping indicators?

- !’ indicates that the ping was unsuccessful and that the device may have issues finding a DNS server.
- **‘U’ may indicate that a router along the path did not contain a route to the destination address and that the ping was unsuccessful.**
- ‘.’ indicates that the ping was successful but the response time was longer than normal.
- A combination of ‘.’ and ‘!’ indicates that a router along the path did not have a route to the destination address and responded with an ICMP unreachable message.

Explanation: The most common indicators of a ping issued from the Cisco IOS are “!”, “.”, and “U”. The “!” indicates that the ping completed successfully, verifying connectivity at Layer 3. The “.” may indicate that a connectivity problem, routing problem, or device security issue exists along the path and that an ICMP destination unreachable message was not provided. The “U” indicates that a router along the path may not have had a route to the destination address, and that it responded with an ICMP unreachable message.

A user reports a lack of network connectivity. The technician takes control of the user machine and attempts to ping other computers on the network and these pings fail. The technician pings the default gateway and that also fails. What can be determined for sure by the results of these tests?

- The NIC in the PC is bad.
- The TCP/IP protocol is not enabled.
- The router that is attached to the same network as the workstation is down.
- **Nothing can be determined for sure at this point.**

Explanation: In networks today, a failed ping could mean that the other devices on the network are blocking pings. Further investigation such as checking network connectivity from other devices on the same network is warranted.

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.

Why would a network administrator use the tracert utility?

- to determine the active TCP connections on a PC
- to check information about a DNS name in the DNS server
- **to identify where a packet was lost or delayed on a network**
- to display the IP address, default gateway, and DNS server address for a PC

Explanation: The **tracert** utility is used to identify the path a packet takes from source to destination. **Tracert** is commonly used when packets are dropped or not reaching a specific destination.

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.

Explanation: The **show cdp neighbors** command can be used to prove that Layer 1 and Layer 2 connectivity exists between two Cisco devices. For example, if two devices have duplicate IP addresses, a ping between the devices will fail, but the output of **show cdp neighbors** will be successful. The **show cdp neighbors detail** could be used to verify the IP address of the directly connected device in case the same IP address is assigned to the two routers.

A network engineer is troubleshooting connectivity issues among interconnected Cisco routers and switches. Which command should the engineer use to find the IP address information, host name, and IOS version of neighboring network devices?

- show version
- show ip route
- show interfaces
- **show cdp neighbors detail**

Explanation: The **show cdp neighbors detail** command reveals much information about neighboring Cisco devices, including the IP address, the capabilities, host name, and IOS version. The **show interfaces** and **show version** commands display information about the local device.

What information about a Cisco router can be verified using the show version command?

- the routing protocol version that is enabled
- **the value of the configuration register**
- the operational status of serial interfaces
- the administrative distance used to reach networks

Explanation: The value of the configuration register can be verified with the **show version** command.

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**

Explanation: 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.

Which command can an administrator issue on a Cisco router to send debug messages to the vty lines?

- **terminal monitor**
- logging console
- logging buffered
- logging synchronous

Explanation: Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the terminal lines requires the **terminal monitor** command.

By following a structured troubleshooting approach, a network administrator identified a network issue after a conversation with the user. What is the next step that the administrator should take?

- Verify full system functionality.
- Test the theory to determine cause.
- **Establish a theory of probable causes.**
- Establish a plan of action to resolve the issue.

Explanation: A structured network troubleshooting approach should include these steps in sequence:

1. Identify the problem.
2. Establish a theory of probable causes.
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the issue.
5. Verify full system functionality and implement preventive measures.
6. Document findings, actions, and outcomes.

Users are complaining that they are unable to browse certain websites on the Internet. An administrator can successfully ping a web server via its IP address, but cannot browse to the domain name of the website. Which troubleshooting tool would be most useful in determining where the problem is?

- netstat
- tracert
- **nslookup**
- ipconfig

Explanation: The **nslookup** command can be used to look up information about a particular DNS name in the DNS server. The information includes the IP address of the DNS server being used as well as the IP address associated with the specified DNS name. This command can help verify the DNS that is used and if the domain name to IP address resolution works.

An employee complains that a Windows PC cannot connect to the Internet. A network technician issues the ipconfig command on the PC and is shown an IP address of 169.254.10.3. Which two conclusions can be drawn? (Choose two.)

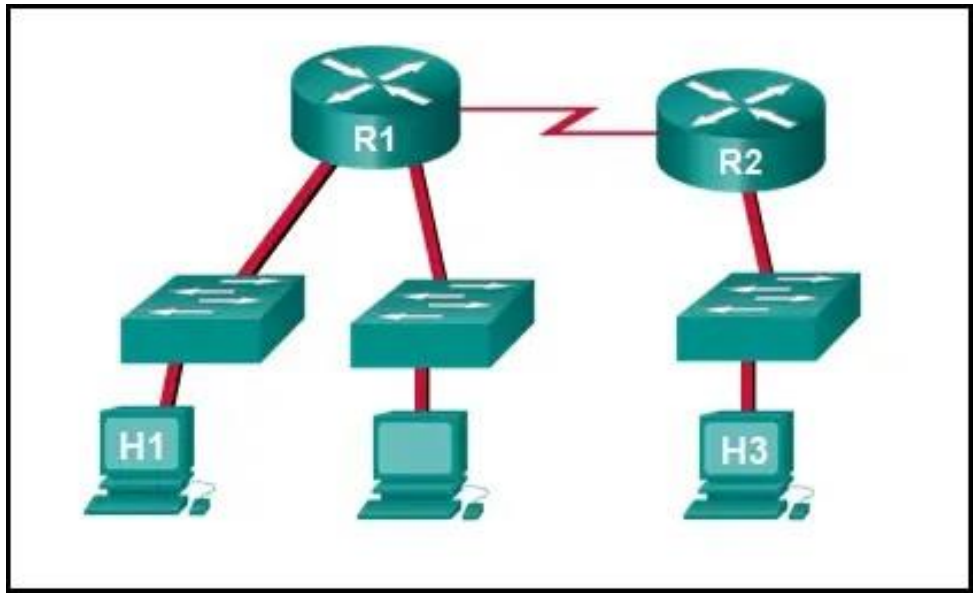
- **The PC cannot contact a DHCP server.**
- The DNS server address is misconfigured.
- The default gateway address is not configured.
- **The PC is configured to obtain an IP address automatically.**
- The enterprise network is misconfigured for dynamic routing.

Explanation: When a Windows PC is configured to obtain an IP address automatically, the PC will try to obtain an IP address from a DHCP server. When the PC cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range.

Refer to the exhibit. Host H3 is having trouble communicating with host H1. The network administrator suspects a problem exists with the H3 workstation and wants to prove that there is no problem with the R2 configuration. What tool could the network administrator use on router R2 to prove that communication exists to host H1 from the interface on R2, which is the interface that H3 uses when communicating with remote networks?

- traceroute
- show cdp neighbors
- Telnet
- **an extended ping**

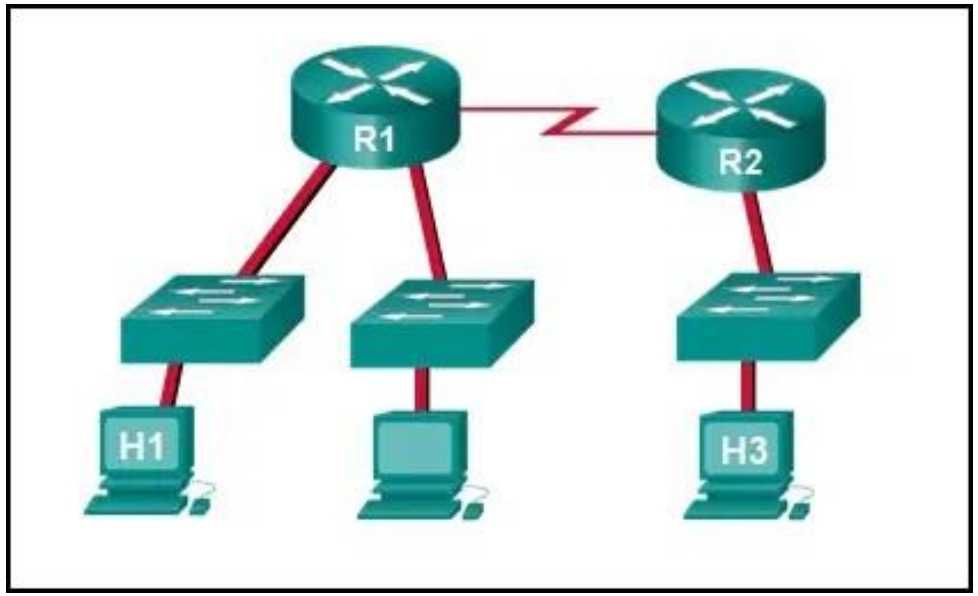
Explanation: An extended ping allows an administrator to select specific ping features. For example in this situation, the network administrator could do an extended ping and specify a source address of the gigabit Ethernet port on the router. The destination address would be the IP address of host H1. If the ping succeeds connectivity exists from the Ethernet router interface on R2 to device H1.



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.**

Explanation: 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.



Which network service automatically assigns IP addresses to devices on the network?

- **DHCP**
- Telnet
- DNS
- traceroute

Explanation: Dynamic Host Configuration Protocol (DHCP) can be used to allow end devices to automatically configure IP information, such as their IP address, subnet mask, DNS server, and default gateway. The DNS service is used to provide domain name resolution, mapping hostnames to IP addresses. Telnet is a method for remotely accessing a CLI session of a switch or router. Traceroute is a command used to determine the path a packet takes as it traverses the network.

Which command can an administrator execute to determine what interface a router will use to reach remote networks?

- show arp
- show interfaces
- **show ip route**
- show protocols

Explanation: The **show ip route** command is used to display the IP routing table of the router. The IP routing table will show a list of known local and remote networks and the interfaces that the router will use to reach those networks.

On which two interfaces or ports can security be improved by configuring executive timeouts? (Choose two.)

- Fast Ethernet interfaces
- **console ports**
- serial interfaces
- **vty ports**
- loopback interfaces

Explanation: Executive timeouts allow the Cisco device to automatically disconnect users after they have been idle for the specified time. Console, vty, and aux ports can be configured with executive timeouts.

When configuring SSH on a router to implement secure network management, a network engineer has issued the login local and transport input ssh line vty commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)

- Set the user privilege levels.
- **Generate the asymmetric RSA keys.**
- **Configure the correct IP domain name.**
- Configure role-based CLI access.
- **Create a valid local username and password database.**
- Manually enable SSH after the RSA keys are generated.

Explanation: SSH is automatically enabled after the RSA keys are generated. Setting user privilege levels and configuring role-based CLI access are good security practices but are not a requirement of implementing SSH.

What is considered the most effective way to mitigate a worm attack?

- Change system passwords every 30 days.
- Ensure that all systems have the most current virus definitions.
- Ensure that AAA is configured in the network.
- **Download security updates from the operating system vendor and patch all vulnerable systems.**

Explanation: Because worms take advantage of vulnerabilities in the system itself, the most effective way to mitigate worm attacks is to download security updates from the operating system vendor and patch all vulnerable systems.

Which statement describes the ping and tracert commands?

- **Tracert shows each hop, while ping shows a destination reply only.**
- Tracert uses IP addresses; ping does not.
- Both ping and tracert can show results in a graphical display.
- Ping shows whether the transmission is successful; tracert does not.

Explanation: The **ping** utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the **traceroute** utility (**tracert** in Windows) traces the route a message takes from its source to the destination. **Traceroute** displays each hop along the way and the time it takes for the message to get to that network and back.

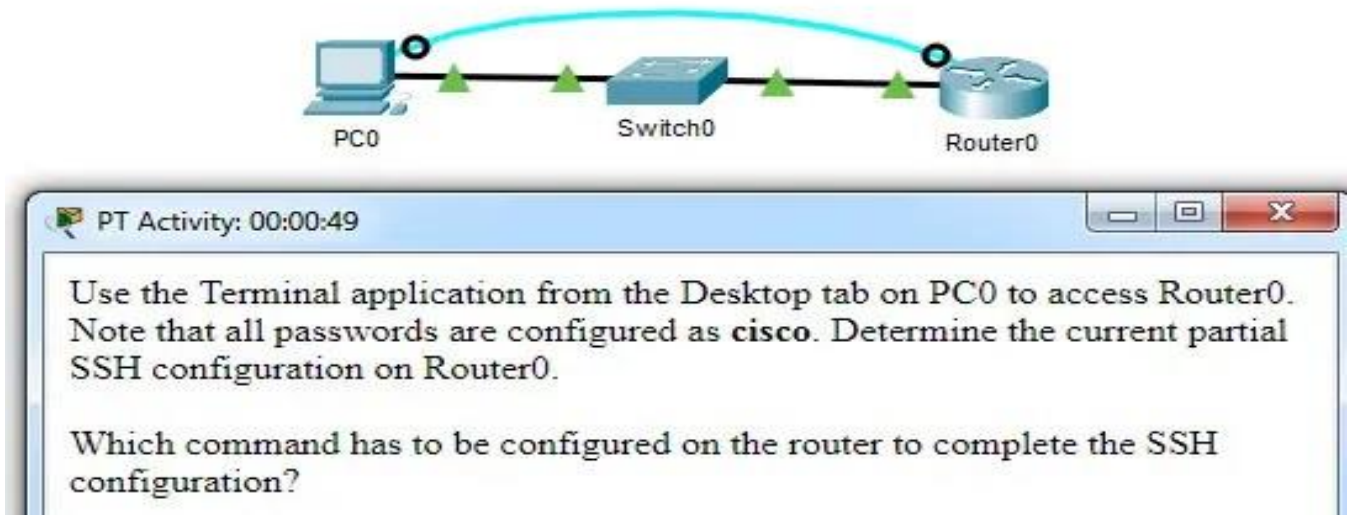
A technician is to document the current configurations of all network devices in a college, including those in off-site buildings. Which protocol would be best to use to securely access the network devices?

- FTP
- HTTP
- **SSH**
- Telnet

Explanation: Telnet sends passwords and other information in clear text, while SSH encrypts its data. FTP and HTTP do not provide remote device access for configuration purposes.

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.
Which command has to be configured on the router to complete the SSH configuration?

- service password-encryption
- **transport input ssh**
- enable secret class
- ip domain-name cisco.com



Explanation: The missing command to complete the SSH configuration is **transport input ssh** in **line vty 0 4** mode.The commands **service password-encryption** and **enable secret class** do configure secure features on the router, but are not required to configure SSH. The command **ip domain-name cisco.com** is not required because the command i**p domain-name span.com** has been used.

An administrator decides to use "WhatAreyouwaiting4" as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it uses a passphrase.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.
- It is weak since it is a word that is easily found in the dictionary.

An administrator decides to use “pR3s!d7n&0” as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it uses a minimum of 10 numbers, letters and special characters.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.
- It is weak since it is a word that is easily found in the dictionary.

An administrator decides to use "5$7*4#033!" as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it contains 10 numbers and special characters.**
- It is weak because it is often the default password on new devices.
- It is weak since it uses easily found personal information.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

An administrator decides to use “pR3s!d7n&0” as the password on a newly installed router. Which statement applies to the password choice?

- **It is strong because it uses a minimum of 10 numbers, letters and special characters.**
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a passphrase.
- It is strong because it contains 10 numbers and special characters.

An administrator decides to use "12345678!" as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak because it uses a series of numbers or letters.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

An administrator decides to use “admin” as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak because it is often the default password on new devices.**
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.
- It is strong because it contains 10 numbers and special characters.

An administrator decides to use "Feb121978" as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak because it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

An administrator decides to use “password” as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak because it is a commonly used password.**
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

An administrator decides to use "RobErT" as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak since it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.
- It is strong because it contains 10 numbers and special characters.

An administrator decides to use "Elizabeth" as the password on a newly installed router. Which statement applies to the password choice

- **It is weak because it uses easily found personal information.**
- It is strong because it uses a passphrase.
- It is weak since it is a word that is easily found in the dictionary.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

Explanation: Rules for strong passwords:
* minimum of 8 characters, preferably 10.
* use complex combinations of numbers, special characters, and upper and lower case letters.
* avoid repetition, common dictionary words, letter or number sequences.
* avoid names of children, relatives, pets, birthdays, or any easily identifiable personal information.
* can be created by misspelling words or replacing vowels with numbers or special characters.

A network technician is troubleshooting an issue and needs to verify the IP addresses of all interfaces on a router. What is the best command to use to accomplish the task?

- **show ip interface brief**
- nslookup
- ipconfig getifaddr en0
- show ip route

Students who are connected to the same switch are having slower than normal response times. The administrator suspects a duplex setting issue. What is the best command to use to accomplish the task?

- **show interfaces**
- ipconfig getifaddr en0
- copy running-config startup-config
- show ip nat translations

A user wants to know the IP address of the PC. What is the best command to use to accomplish the task?

- **ipconfig**
- copy running-config startup-config
- show interfaces
- show ip nat translations

A student wants to save a router configuration to NVRAM. What is the best command to use to accomplish the task?

- **copy running-config startup-config**
- show interfaces
- show ip nat translations
- show ip route

A support technician needs to know the IP address of the wireless interface on a MAC. What is the best command to use to accomplish the task?

- **ipconfig getifaddr en0**
- copy running-config startup-config
- show interfaces
- show ip nat translations

A network technician is troubleshooting an issue and needs to verify all of the IPv6 interface addresses on a router. What is the best command to use to accomplish the task?

- **show ipv6 interface**
- show interfaces
- show ip nat translations
- show ip route

A teacher is having difficulties connecting his PC to the classroom network. He needs to verify that a default gateway is configured correctly. What is the best command to use to accomplish the task?

- **ipconfig**
- copy running-config startup-config
- show interfaces
- show ip nat translations

Only employees connected to IPv6 interfaces are having difficulty connecting to remote networks. The analyst wants to verify that IPv6 routing has been enabled. What is the best command to use to accomplish the task?

- **show running-config**
- show interfaces
- copy running-config startup-config
- show ip nat translations

An administrator is troubleshooting connectivity issues and needs to determine the IP address of a website. What is the best command to use to accomplish the task?

- **nslookup**
- show ipv6 route
- show ipv6 interface
- copy startup-config running-config

What is a characteristic of UDP?

- UDP datagrams take the same path and arrive in the correct order at the destination.
- Applications that use UDP are always considered unreliable.
- **UDP reassembles the received datagrams in the order they were received.**
- UDP only passes data to the network when the destination is ready to receive the data.

Explanation: **UDP has no way to reorder the datagrams into their transmission order, so UDP simply reassembles the data in the order it was received and forwards it to the application**.