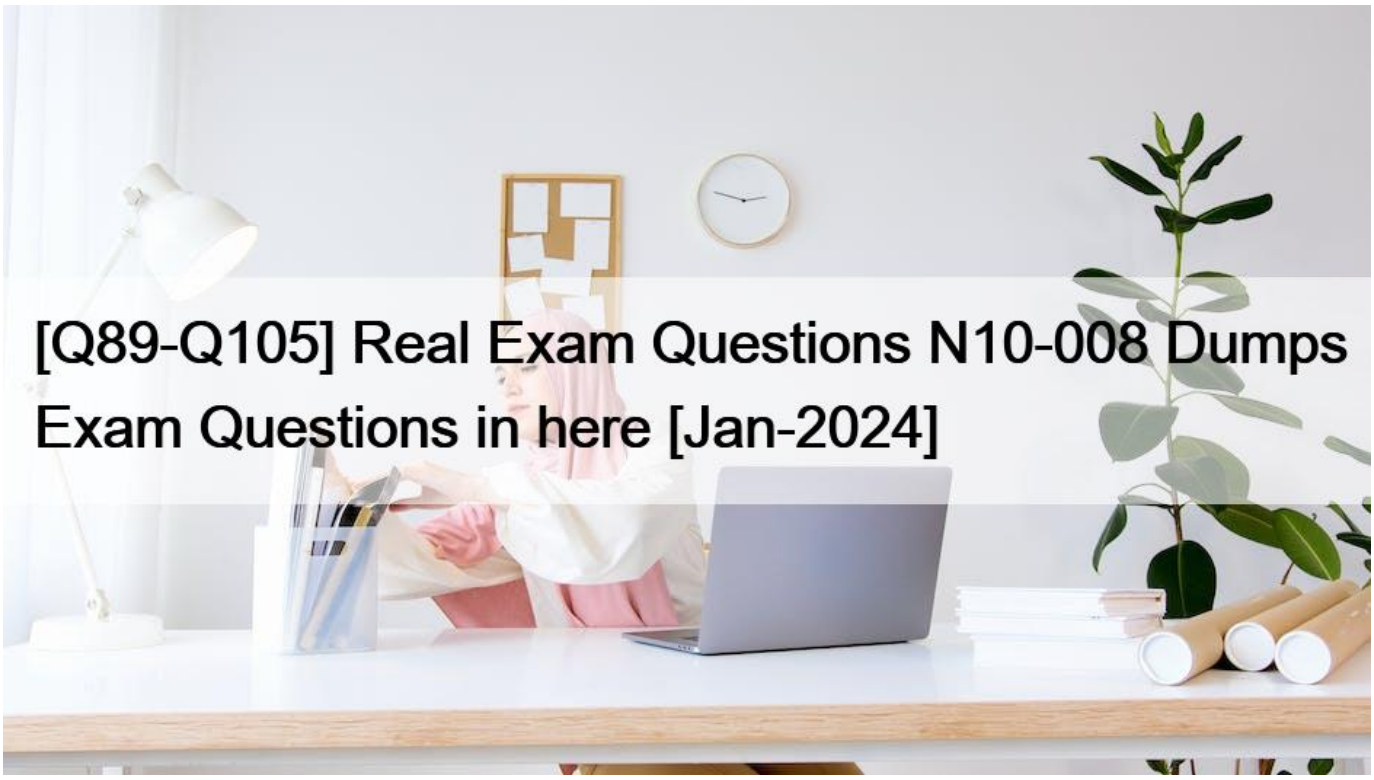
[Q89-Q105 Real Exam Questions N10-008 Dumps Exam Questions in here [Jan-2024



Real Exam Questions N10-008 Dumps Exam Questions in here [Jan-2024]
Get Latest Jan-2024 Conduct effective penetration tests using N10-008

NO.89 Which of the following would be the MOST likely attack used to bypass an access control vestibule?
* Tailgating
* Phishing
* Evil twin
* Brute-force

NO.90 Given the following output:

```
192.168.22.1     00-13-5d-00-c6-23
192.168.22.15    00-15-88-00-58-00
192.168.22.10    00-13-5d-00-c6-23
192.168.22.100   00-13-5d-00-c6-23
```

Which of the following attacks is this MOST likely an example of?
* ARP poisoning
* VLAN hopping
* Rogue access point

* Amplified DoS

Explanation

The output is most likely an example of an ARP poisoning attack. ARP poisoning, also known as ARP spoofing, is a type of attack that exploits the ARP protocol to associate a malicious device’s MAC address with a legitimate IP address on a local area network. This allows the attacker to intercept, modify, or redirect network traffic between two devices without their knowledge. The output shows that there are multiple entries for the same IP address (192.168.1.1) with different MAC addresses in the ARP cache of the device. This indicates that an attacker has sent fake ARP replies to trick the device into believing that its MAC address is associated with the IP address of another device (such as the default gateway). References:

https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html

NO.91 A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport’s performance:

Metric	Value
Uptime	201 days, 3 hours, 18 minutes
MDIX	On
CRCs	0
Giants	2508
Output queue maximum	40
Packets input	136208849
Packets output	64458087024

Based on the information in the chart above, which of the following fs the cause of these performance issues?

* The connected device is exceeding the configured MTU.
* The connected device is sending too many packets
* The switchport has been up for too long
* The connected device is receiving too many packets.
* The switchport does not have enough CRCs

NO.92 The following instructions were published about the proper network configuration for a videoconferencing device:

“Configure a valid static RFC1918 address for your network. Check the option to use a connection over NAT.”

Which of the following is a valid IP address configuration for the device?

* FE80::1
* 100.64.0.1
* 169.254.1.2
* 172.19.0.2
* 224.0.0.12

172.19.0.2 is a valid IP address configuration for the device that uses a static RFC1918 address for the network and allows for a connection over NAT (Network Address Translation). RFC1918 addresses are private IP addresses that are not routable on the public Internet and are used for internal networks. The RFC1918 address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. NAT is a technique that translates private IP addresses to public IP addresses when communicating with external networks, such as the Internet. FE80::1 is an IPv6 link-local address that is not a static RFC1918 address and does not allow for a connection over NAT. 100.64.0.1 is an IPv4 address that belongs to the shared address space range (100.64.0.0/10) that is used for carrier-grade NAT (CGN) between service providers and subscribers, which is not a static RFC1918 address and does not allow for a connection over NAT. 169.254.1.2 is an IPv4 link-local address that is automatically assigned by a device when it cannot obtain an IP address from a DHCP server or manual configuration, which is not a static RFC1918 address and does not allow for a connection over NAT. 224.0.0.12 is an IPv4 multicast address that is used for VRRP (Virtual Router Redundancy Protocol), which is not a static RFC1918

address and does not allow for a connection over NAT.

NO.93 An employee reports to a network administrator that internet access is not working. Which of the following should the administrator do FIRST?
* Establish a theory of probable cause.
* Identify symptoms.
* Determine if anything has changed.
* Ask the user to restart the computer.

Explanation

When a user reports that internet access is not working, it is important to first determine if there have been any recent changes to the network or the user’s computer that could have caused the issue. This could include changes to the network configuration, the installation of new software or hardware, or other events that could have impacted the user’s ability to access the internet. By determining if anything has changed, the administrator can narrow down the possible causes of the issue and focus on addressing the most likely cause.

NO.94 Which of the following is the DNS feature that controls how long a lookup is stored in cache on a server?
* CNAME
* TTL
* SOA
* SRV

TTL stands for Time to Live, and it is a field on DNS records that controls how long each record is valid and cached by the DNS resolver before it expires and requests a new one. The TTL value is measured in seconds, and it affects how quickly DNS changes propagate across the Internet. A lower TTL means that the DNS resolver will refresh the record more frequently, but it also increases the load on the DNS servers. A higher TTL means that the DNS resolver will cache the record longer, but it also delays the update of the record.

NO.95 A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?
* Perform a site survey.
* Review the AP placement
* Monitor channel utilization.
* Test cable attenuation.

NO.96 A help desk technician is concerned that a client’s network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?
* Run the show interface command on the switch
* Run the tracerouute command on the server
* Run iperf on the technician’s desktop
* Ping the client’s computer from the router
* Run a port scanner on the client’s IP address

To determine if a client’s network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch. This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client’s device and the switch.

“Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts.”

NO.97 A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?
* IP scanner
* Terminal emulator
* NetFlow analyzer
* Port scanner

To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

NO.98 A server application requires large amounts of data to be sent at a consistent rate. Which of the following should an engineer most likely configure to meet these requirements?
* Link speed
* Jumbo frames
* Switch Virtual Interface
* Spanning tree

Explanation

Jumbo frames are Ethernet frames that have a payload size greater than the standard 1500 bytes. Jumbo frames can carry more data in each frame, which reduces the overhead and improves the throughput and efficiency of data transmission. Jumbo frames are commonly used in storage area networks (SANs), where large amounts of data need to be transferred between servers and storage devices

NO.99 A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?
* Change default passwords on internet-facing hardware.
* Implement robust ACLs with explicit deny-all entries.
* Create private VLANs for management plane traffic.
* Routinely upgrade all network equipment firmware.

Explanation

Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances.

Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance.

References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 462)

NO.100 A wireless network technician is receiving reports from some users who are unable to see both of the corporate SSIDs on their mobile devices. A site survey was recently commissioned, and the results verified acceptable RSSI from both APs in all user areas. The APs support modern wireless standards and are all broadcasting their SSIDs. The following table shows some of the current AP settings:

Name	Power	Directionality	Wireless standard	Authentication standard	SSID
AP1	Medium	Omnidirectional	802.11b	WPA2 - PSK	CORP01
AP2	High	Directional	802.11a	WPA2 - PSK	CORP02

Which of the following changes would result in all of the user devices being capable of seeing both corporate SSIDs?
* Implementing the WPA2 Enterprise authentication standard
* Implementing omnidirectional antennas for both APs
* Configuring the highest power settings for both APs
* Configuring both APs to use the 802.11ac wireless standard

Explanation

The change that would result in all of the user devices being capable of seeing both corporate SSIDs is configuring both APs to use the 802.11ac wireless standard. 802.11ac is a wireless standard that operates in the 5 GHz frequency band and offers high data rates and performance. However, not all wireless devices support 802.11ac, especially older ones that only operate in the 2.4 GHz frequency band. In the table, AP1 uses 802.11b, which is an outdated wireless standard that operates in the 2.4 GHz frequency band and offers low data rates and performance. AP2 uses 802.11a, which is an older wireless standard that operates in the 5 GHz frequency band and offers moderate data rates and performance. Therefore, some user devices may not be able to see both SSIDs because they are incompatible with either 802.11b or 802.11a. By configuring both APs to use 802.11ac, which is backward compatible with previous wireless standards, all user devices should be able to see both SSIDs. References: CompTIA Network+ N10-008 Certification Study Guide, page 75; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-18.

NO.101 A security team updated a web server to require https:// in the URL. Although the IP address did not change, users report being unable to reach the site. Which of the following should the security team do to allow users to reach the server again?
* Configure the switch port with the correct VLAN.
* Configure inbound firewall rules to allow traffic to port 443.
* Configure the router to include the subnet of the server.
* Configure the server with a default route.

One possible reason why users are unable to reach the site after the security team updated the web server to require https:// in the URL is that the firewall rules are blocking the traffic to port 443. Port 443 is the default port for HTTPS, which is the protocol that encrypts and secures the web communication. If the firewall rules do not allow inbound traffic to port 443, then users will not be able to access the web server using HTTPS12.

To troubleshoot this issue, the security team should configure inbound firewall rules to allow traffic to port 443. This can be done by using the firewall-cmd command on RHEL 8.2, which is a tool that manages firewalld, the default firewall service on RHEL. The command to add a rule to allow traffic to port 443 is:

firewall-cmd –permanent –add-port=443/tcp

The –permanent option makes the rule persistent across reboots, and the –add-port option specifies the port number and protocol (TCP) to allow. After adding the rule, the security team should reload the firewalld service to apply the changes:

firewall-cmd –reload

The security team can verify that the rule is active by using this command:

firewall-cmd –list-ports

The output should show 443/tcp among the ports that are allowed34.

The other options are not relevant to troubleshooting this issue. Configuring the switch port with the correct VLAN may help with network segmentation or isolation, but it will not affect the HTTPS protocol or port. Configuring the router to include the subnet of the server may help with network routing or connectivity, but it will not enable HTTPS communication. Configuring the server with

a default route may help with network access or reachability, but it will not allow HTTPS traffic.

NO.102 Which of the following routing protocols is BEST suited for use on a perimeter router?
* OSPF
* RIPv2
* EIGRP
* BGP

BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router.

NO.103 The network administrator is informed that a user’s email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implements to BEST mitigate this issue? (Choose two.)
* Captive portal
* Two-factor authentication
* Complex passwords
* Geofencing
* Role-based access
* Explicit deny

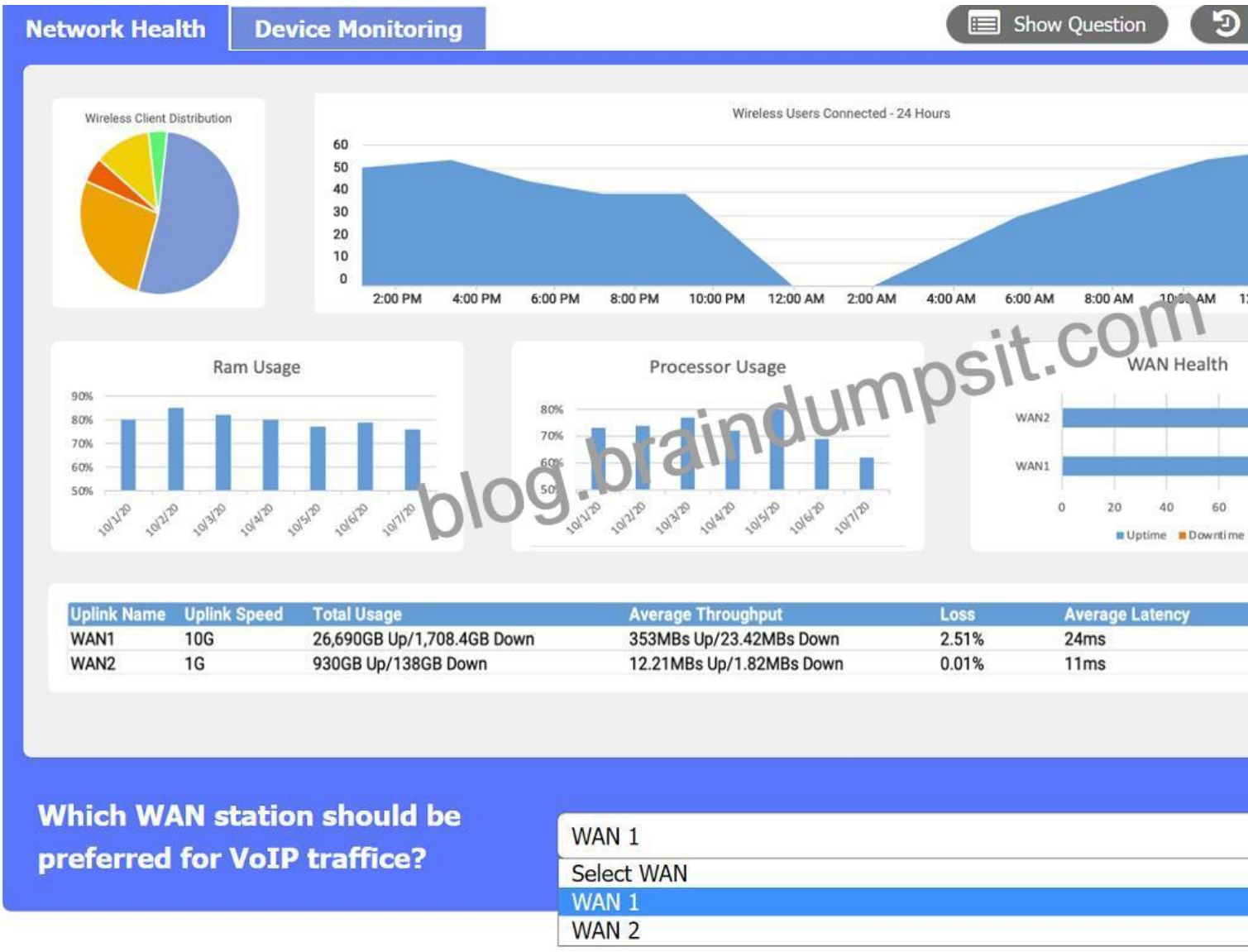
Two-factor authentication (2FA) is a method of verifying a user’s identity by requiring two pieces of evidence, such as something the user knows (e.g., a password) and something the user has (e.g., a token or a smartphone). 2FA adds an extra layer of security that makes it harder for hackers to access a user’s account by brute-force programs. Complex passwords are passwords that are long, random, and use a combination of uppercase and lowercase letters, numbers, and symbols. Complex passwords are more resistant to brute-force attacks than simple or common passwords. Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.csoonline.com/article/3225913/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-you-should.html, https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

NO.104 A technician wants to deploy a new wireless network that comprises 30 WAPs installed throughout a three-story office building. All the APs will broadcast the same SSID for client access. Which of the following BEST describes this deployment?
* Extended service set
* Basic service set
* Unified service set
* Independent basic service set

NO.105 After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

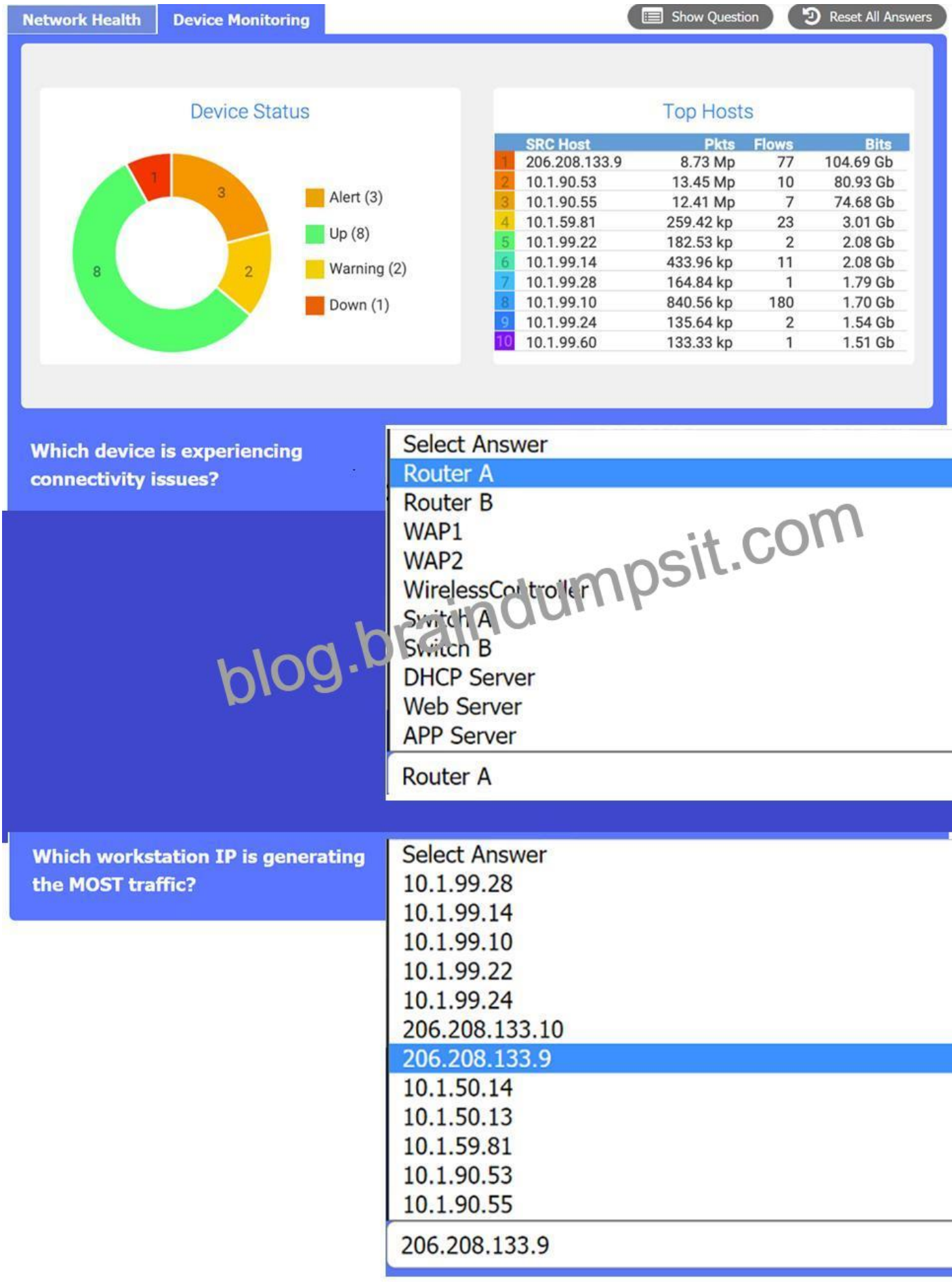


Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms

Which WAN station should be preferred for VoIP traffice?

WAN 1

Select WAN
WAN 1
WAN 2



See the answer and solution below.

Explanation

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here’s the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.

Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down

. This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.

A screenshot of a computer Description automatically generated

Authentic Best resources for N10-008 Online Practice Exam: https://www.braindumpsit.com/N10-008_real-exam.html]