Free Questions for N10-008

Shared by Kelley on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a hybrid routing protocol?

Options:

A- BGP

B- RIPv2

C- OSPF

D- EIGRP

Answer:

D

Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid routing protocol23.It combines the features of Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP), making it an effective solution for larger networks that require scalable and efficient routing

Question 2

Question Type: MultipleChoice

An administrator wants to host services on the internet using an internal server. The server is configured with an RFC1918 address, and the administrator wants to make the services

that are hosted on the server available on one of the company's public IP addresses. Which of the following should the administrator configure to allow this access?

Options:

A- IPv6 tunneling

B- Virtual IP

C- Dual stack

D- EUI-64

Answer:

B

Explanation:

A virtual IP (VIP) is an IP address that is shared by multiple servers or devices on a network. A VIP can be used to provide load balancing, failover, or high availability for services that are hosted on the network. A VIP can also be used to map an internal server's private IP address to a public IP address, allowing the server to host services on the internet. This is also known as network address translation (NAT) or port forwarding.

The other options are not correct because they are not related to mapping an internal server's IP address to a public IP address. They are:

* IPv6 tunneling is a technique that allows IPv6 packets to be encapsulated and transmitted over an IPv4 network.

* Dual stack is a configuration that allows a device to support both IPv4 and IPv6 protocols simultaneously.

* EUI-64 is a method of generating a 64-bit interface identifier for an IPv6 address based on the 48-bit MAC address of the device.

Reference

: What is a Virtual IP Address (VIP)? - Definition from Techopedia

: IPv6 Tunneling - an overview | ScienceDirect Topics

: Dual Stack Definition

: [EUI-64 - an overview | ScienceDirect Topics]

Question 3

Question Type: MultipleChoice

A network engineer installed a new fiber uplink for an office and wants to make sure that the link meets throughput requirements. Which of the following tools should the engineer use to

verify that the new link is sufficient?

Options:

A- tcpdump

B- ping

C- iperf

D- netstat

Answer:

C

Explanation:

iperf is a tool that can measure the bandwidth and quality of a network link by generating and transferring TCP or UDP data streams. iperf can report the maximum achievable throughput, packet loss, jitter, and other statistics for a given link. iperf can be used to test both the uplink and downlink performance of a network link by running it on two endpoints and specifying the direction and duration of the test. iperf can help the engineer verify that the new fiber uplink meets the throughput requirements for the office network.

tcpdump is a tool that can capture and analyze network traffic by filtering and displaying packets based on various criteria. tcpdump can help the engineer troubleshoot network problems, monitor network activity, and inspect packet contents, but it cannot measure the throughput or quality of a network link.

ping is a tool that can test the reachability and latency of a network host by sending and receiving ICMP echo packets. ping can help the engineer check if the new fiber uplink is connected and responsive, and how long it takes for packets to travel between the endpoints, but it cannot measure the throughput or quality of a network link.

netstat is a tool that can display information about the network connections, routing tables, interfaces, and protocols on a network host. netstat can help the engineer view the status and details of the network connections using the new fiber uplink, but it cannot measure the throughput or quality of a network link.

Reference

iperf - The ultimate speed test tool for TCP, UDP and SCTP

How to use iperf to test local network LAN speed in Windows 10

How to Test Network Performance Between Two Linux Servers

What is tcpdump?

8 Common Network Utilities Explained

Monitoring Your Network: ping, netstat, tcpdump, and Ethereal

Netstat vs. Nmap vs. Netcat: Understanding the Differences

Question 4

Question Type: MultipleChoice

A user reports that the internet seems slow on a workstation, but no other users have reported any issues. The server team confirms the servers are functioning normally. A technician suspects something specific to the user's computer is overutilizing bandwidth. Which of the following commands should the technician use to further investigate the issue?

Options:

A- nmap
B- tcpdump
C- netstat
D- nslookup

Answer:

C

Explanation:

netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. It can help the technician identify which processes or applications are using the network bandwidth on the user's computer. netstat can also show the current bandwidth usage in bytes per second for each network interface.

Reference

netstat - Wikipediaprovides an overview of the netstat tool and its features.

How to get current bandwidth usage from command line using built-in Linux tools? - Super Userexplains how to use netstat and other tools to monitor bandwidth usage on Linux systems.

Get network utilization from command line - Super Usershows how to use typeperf and other tools to monitor bandwidth usage on Windows systems.

Question 5

Question Type: MultipleChoice

A technician is documenting an application that is installed on a server and needs to verify all existing web and database connections to the server. Which of the following tools should the technician use to accomplish this task?

Options:

A- Tracert

B- Ipconfig

C- Netstat

D- nslookup

Answer:

C

Explanation:

The correct tool for verifying existing network connections on a server isC. Netstat. Netstat (network statistics) displays active network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Tracert: Tracert (traceroute) is used to trace the route taken by packets from the source to the destination. It helps identify the path and latency between routers.

Ipconfig: Ipconfig is used to view and manage IP configuration settings on a local machine (such as IP address, subnet mask, default gateway, etc.). It does not provide information about existing connections.

Netstat: Netstat displays active network connections, including listening ports, established connections, and associated processes. It's useful for troubleshooting and monitoring network activity.

Nslookup: Nslookup is used for DNS (Domain Name System) queries to resolve domain names to IP addresses. It does not provide information about existing connections.

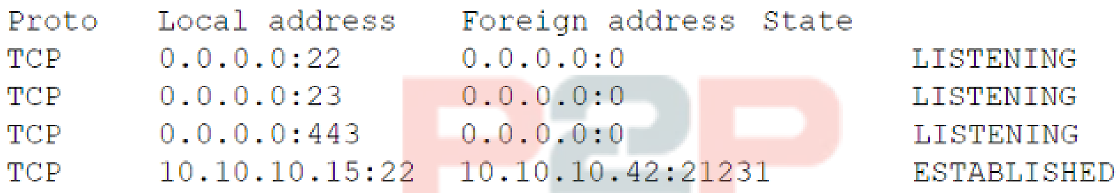
CompTIA Network+ Certification Exam Objectives

Question 6

Question Type: MultipleChoice

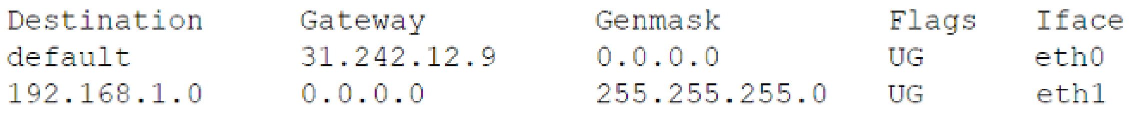
A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician

runs a command on the server and receives the following output:



```
Proto    Local address      Foreign address  State
TCP      0.0.0.0:22         0.0.0.0:0                LISTENING
TCP      0.0.0.0:23         0.0.0.0:0                LISTENING
TCP      0.0.0.0:443        0.0.0.0:0                LISTENING
TCP      10.10.10.15:22     10.10.10.42:21231        ESTABLISHED
```

On the host, the technician runs another command and receives the following:



```
Destination      Gateway          Genmask          Flags    Iface
default          31.242.12.9      0.0.0.0          UG       eth0
192.168.1.0      0.0.0.0          255.255.255.0    UG       eth1
```

Which of the following best explains the issue?

Options:

A- A firewall is blocking access to the server.

B- The server is plugged into a trunk port.

C- The host does not have a route to the server.

D- The server is not running the SSH daemon.

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following most likely occurs when an attacker is between the target and a legitimate server?

Options:

A- IP spoofing

B- VLAN hopping

C- Rogue DHCP

D- On-path attack

Answer:

D

Explanation:

An on-path attack (also known as a man-in-the-middle attack) is a type of security attack where the attacker places themselves between two devices (often a web browser and a web server) and intercepts or modifies communications between the two1. The attacker can then collect information as well as impersonate either of the two agents. For example, an on-path attacker could capture login credentials, redirect traffic to malicious sites, or inject malware into legitimate web pages.

The other options are not correct because they describe different types of attacks:

* IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source2.

* VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag3.

* Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites4.

Reference

2: Understanding Targeted Attacks: What is a Targeted Attack?

3: Types of attacks - Security on the web | MDN

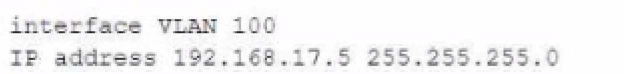
1: What is an on-path attacker? | Cloudflare

4: [What is a Rogue DHCP Server? - Definition from Techopedia]

Question 8

Question Type: MultipleChoice

An engineer recently installed a new distribution switch and connected two servers provisioned with the following IPs: 192.168.17.20 and 192.168.17.30. The servers cannot connect to the Internet, but they can reach themselves. The engineer observes that the distribution switch has the following setup:



```
interface VLAN 100
IP address 192.168.17.5 255.255.255.0
```

The engineer is able to reach the core router 192.168.17.1 from the distribution switch. Which of the following is the most likely cause of this issue?

Options:

A- A routing loop has occurred.

B- The subne1 mask is Incorrect.

C- The servers are not configured with default gateway.

D- There is an improper Layer 1 connection between the router and the ISP modem.

Answer:

C

Explanation:

The servers can communicate with each other but not the internet, indicating local network connectivity is fine. The distribution switch's VLAN and IP configuration are correct, and the engineer can reach the core router, suggesting the issue is not with the switch or the router. The most likely cause is that the servers do not have a default gateway configured, which is necessary for traffic to leave the local network and reach the internet.

Question 9

Question Type: MultipleChoice

A local service provider connected 20 schools in a large city with a fiber-optic switched network. Which of the following network types did the provider set up?

Options:

A- LAN

B- MAN

C- CAN

D- WAN

Answer:

B

Explanation:

MAN stands for Metropolitan Area Network, and it is a type of network that covers a large geographic area, such as a city or a county. MANs are often used to connect multiple LANs (Local Area Networks) within a region, such as schools, offices, or government buildings. MANs typically use high-speed and high-capacity transmission media, such as fiber-optic cables, to provide fast and reliable data communication. MANs can also provide access to WANs (Wide Area Networks), such as the Internet, or other services, such as cable TV or VoIP.

The other options are not correct because they are not the type of network that covers a large city. They are:

LAN. LAN stands for Local Area Network, and it is a type of network that covers a small geographic area, such as a home, an office, or a building. LANs are often used to connect multiple devices, such as computers, printers, or phones, within a single network. LANs typically use low-cost and low-capacity transmission media, such as twisted-pair cables, to provide data communication. LANs can also provide access to other networks, such as MANs or WANs, through routers or gateways.

CAN. CAN stands for Campus Area Network, and it is a type of network that covers a moderate geographic area, such as a university, a hospital, or a military base. CANs are often used to connect multiple LANs within a campus, such as different departments, buildings, or facilities. CANs typically use medium-cost and medium-capacity transmission media, such as coaxial cables, to provide data communication. CANs can also provide access to other networks, such as MANs or WANs, through routers or gateways.

WAN. WAN stands for Wide Area Network, and it is a type of network that covers a very large geographic area, such as a country, a continent, or the world. WANs are often used to connect multiple MANs or LANs across different regions, such as different cities, states, or countries. WANs typically use high-cost and high-capacity transmission media, such as satellite links, to provide data communication. WANs can also provide access to various services, such as the Internet, email, or VPN.

Reference 1:What is a Metropolitan Area Network (MAN)? - Definition from Techopedia 2:Network+ (Plus) Certification | CompTIA IT Certifications 3:What is a Local Area Network (LAN)? - Definition from Techopedia 4:What is a Campus Area Network (CAN)? - Definition from Techopedia 5:What is a Wide Area Network (WAN)? - Definition from Techopedia

Question 10

Question Type: MultipleChoice

The network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new

router to?

Options:

A- Core
B- Leaf
C- Distribution
D- Access

Answer:

C

Explanation:

The distribution layer is the layer that connects the access layer to the core layer in a hierarchical network design. The distribution layer is responsible for routing, filtering, and policy enforcement between the LAN and the WAN. A router is a layer 3 device that can perform these functions and connect to different WAN technologies.

CompTIA Network+ N10-008 Certification Study Guide, page 151

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 322

CompTIA Network+ N10-008 Exam Cram, page 233

Question 11

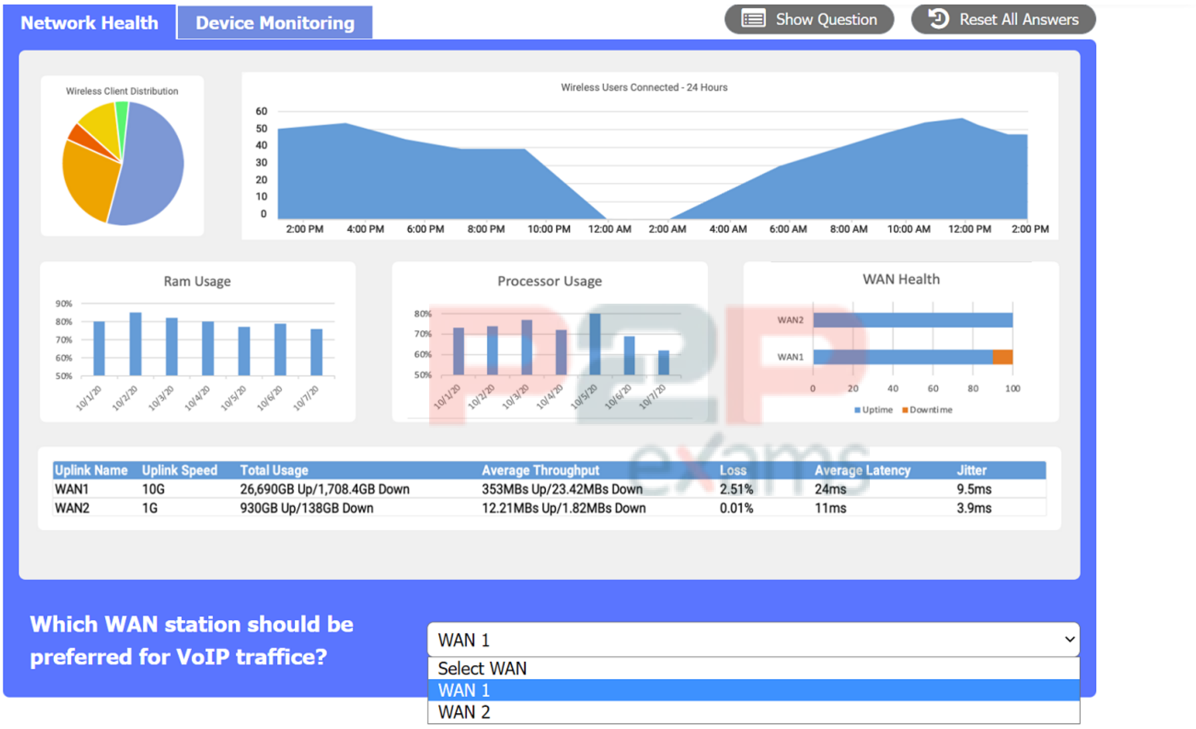
Question Type: MultipleChoice

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

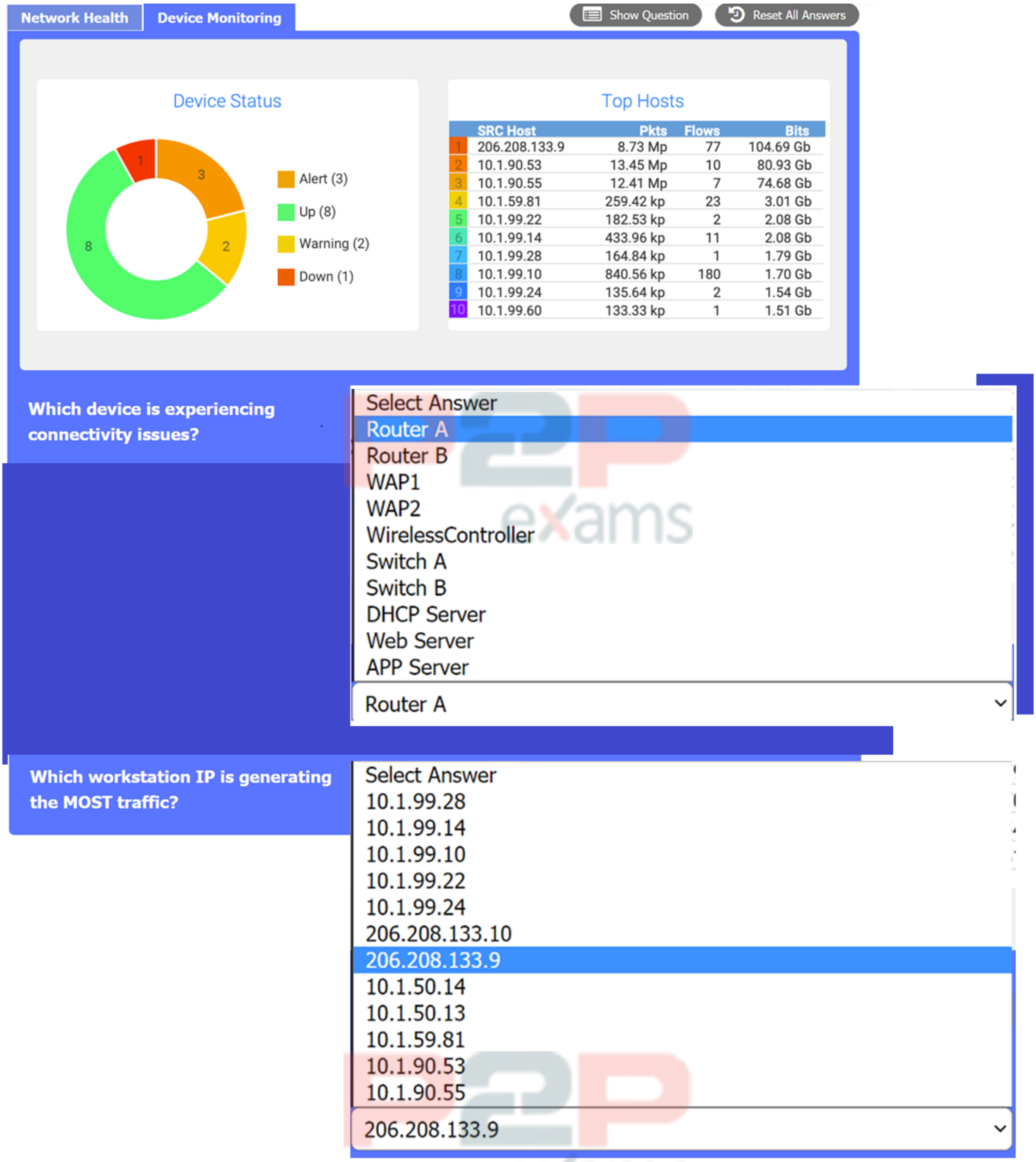
use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffice?

WAN 1



	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22
10.1.99.24
206.208.133.10
206.208.133.9
10.1.50.14
10.1.50.13
10.1.59.81
10.1.90.53
10.1.90.55

206.208.133.9

Options:

A- See the answer and solution below in Explanation

Answer:

A

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

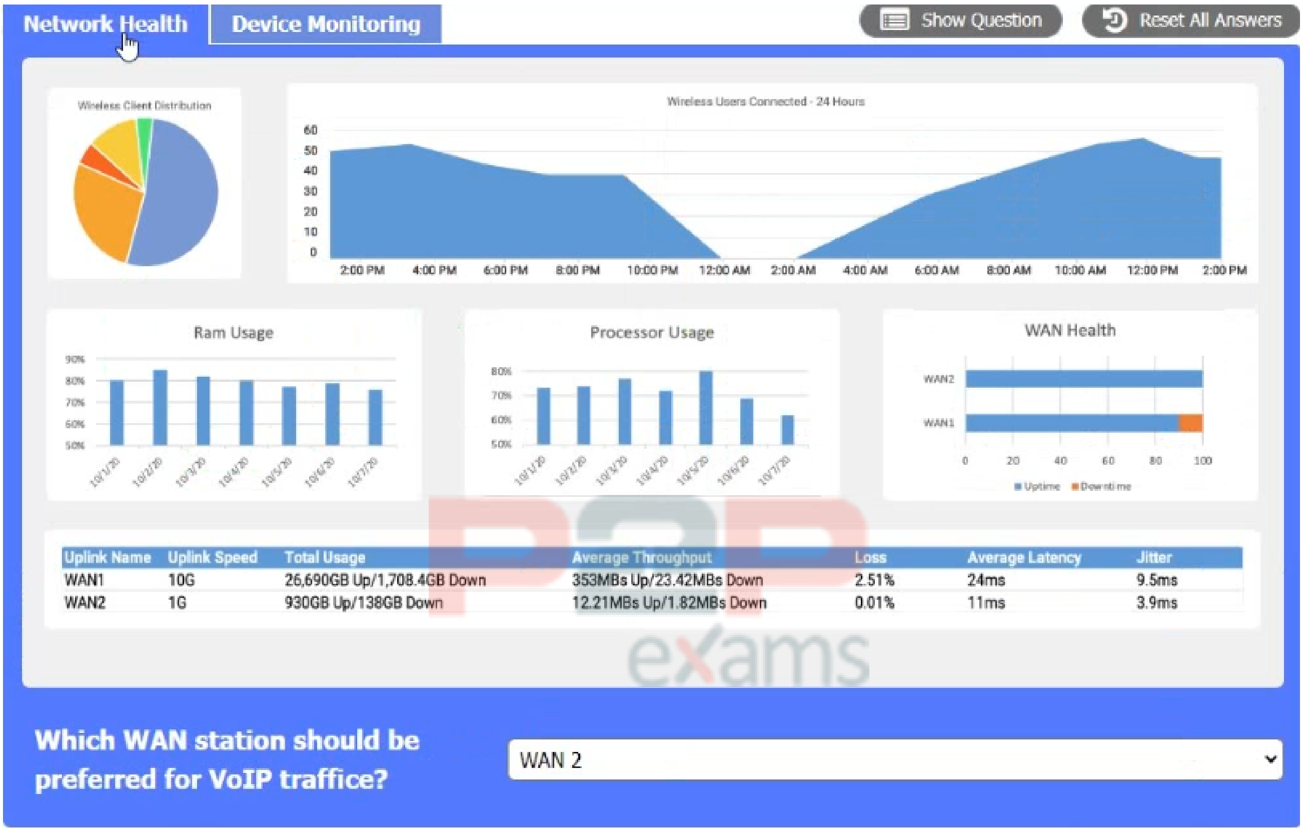
Loss: 0.01%

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.



Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

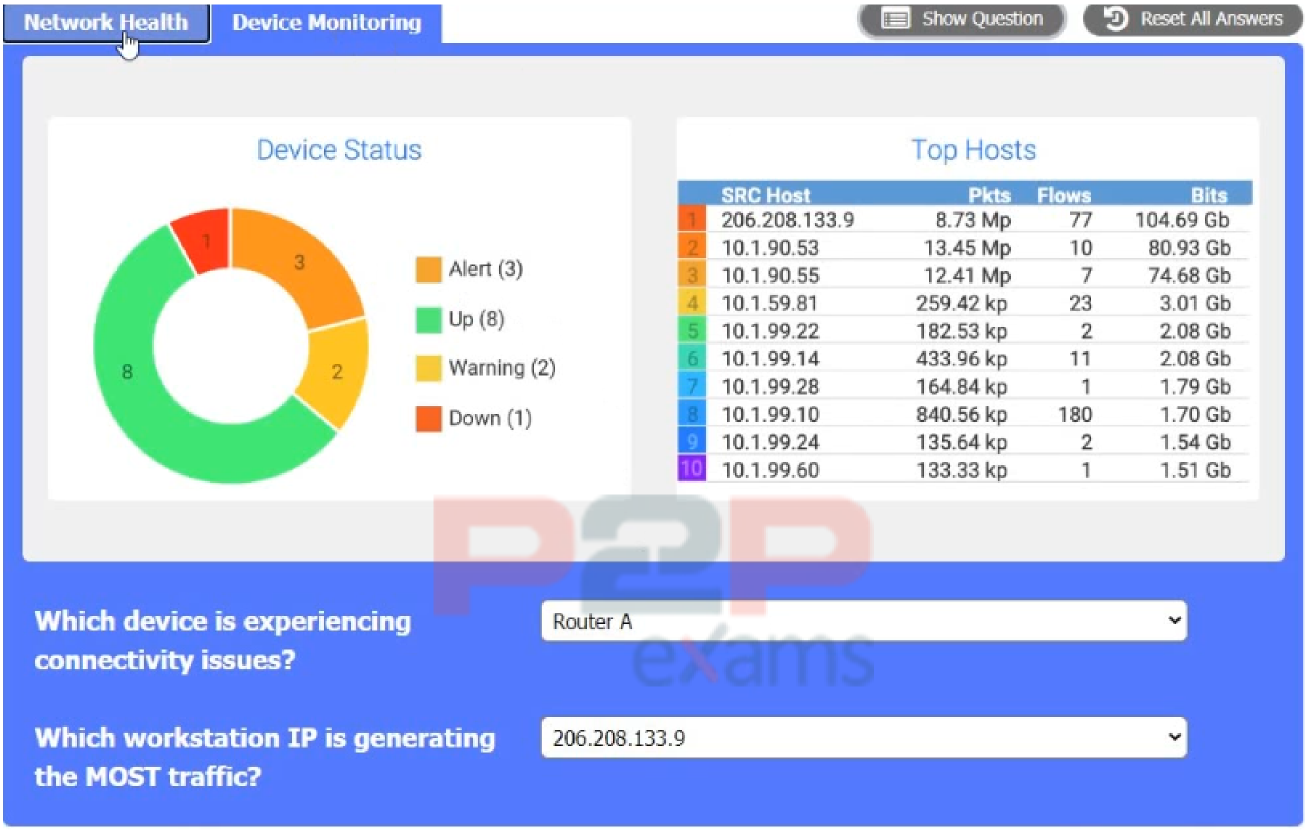
Which WAN station should be preferred for VoIP traffice?

WAN 2

Device Monitoring:

the device that is experiencing connectivity issues is theAPP Server or Router 1, which has a status ofDown. This means that the server is not responding to network requests or sending any dat

a. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues? Router A

Which workstation IP is generating the MOST traffic? 206.208.133.9

20%
DISCOUNT