Vendor: CompTIA

Exam Code: N10-009

Exam Name: CompTIA Network+ N10-009 Certification Exam

Version: DEMO

QUESTION 1
A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?

A. The switch failed.
B. The default gateway is wrong.
C. The port Is shut down.
D. The VLAN assignment is incorrect.

Answer: C
Explanation:
When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.
No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.
Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:
```
bash
Copy code
Switch> enable
Switch# configure terminal
Switch(config)# interface [interface id]
Switch(config-if)# no shutdown
```

The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

QUESTION 2
An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?

A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller

Answer: C
Explanation:
MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.

Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).

QUESTION 3
Which of the following best explains the role of confidentiality with regard to data at rest?

A. Data can be accessed by anyone on the administrative network.
B. Data can be accessed remotely with proper training.
C. Data can be accessed after privileged access Is granted.
D. Data can be accessed after verifying the hash.

Answer: C
Explanation:
Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.

Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.

QUESTION 4
A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?

A. Change the email client configuration to match the MX record.
B. Reduce the TTL record prior to the MX record change.
C. Perform a DNS zone transfer prior to the MX record change.
D. Update the NS record to reflect the IP address change.

Answer: B
Explanation:
Understanding TTL (Time to Live):
TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients. A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:
When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:
To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making the changes. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:
After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.

QUESTION 5
Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP
B. AH
C. GRE
D. UDP
E. TCP

Answer: A
Explanation:
Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data. ESP encrypts the payload and optional ESP trailer, providing data confidentiality.

ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.
ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).

QUESTION 6
A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Choose two).

A. Mesh network
B. 5GHz frequency
C. Omnidirectional antenna
D. Non-overlapping channel
E. Captive portal
F. Ad hoc network

Answer: BD
Explanation:
Switching to the 5GHz frequency can reduce interference because it operates on a different range, thus avoiding the crowded 2.4GHz spectrum.

Using non-overlapping channels within the 2.4GHz frequency can help minimize interference by ensuring that the network uses a clear channel that does not overlap with others, reducing the chance of congestion and interference.

QUESTION 7
Which of the following disaster recovery metrics is used to describe the amount of data that is lost since the last backup?

A. MTTR
B. RTO
C. RPO
D. MTBF

Answer: C

Explanation:
Definition of RPO:
Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.

For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.

Why RPO is Important:
RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.

QUESTION 8
Which of the following can support a jumbo frame?

A. Access point
B. Bridge
C. Hub
D. Switch

Answer: D
Explanation:
Definition of Jumbo Frames:
Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.

Why Switches Support Jumbo Frames:
Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.

QUESTION 9
Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?

A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map

Answer: D
Explanation:
Definition of Heat Maps:
A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.

Purpose of a Heat Map:
Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and

performance.

QUESTION 10
A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file
B. Self-signed certificate
C. Nameserver record
D. IP helper

Answer: A
Explanation:
Role of the Hosts File:
The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.

Common Issues with the Hosts File:
If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.

QUESTION 11
An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?

A. SD-WAN
B. VXLAN
C. VPN
D. NFV

Answer: A
Explanation:
Definition of SD-WAN:
Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.

Benefits of SD-WAN:
Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
Scalability: Easily scales to accommodate additional sites and bandwidth requirements.

QUESTION 12
After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

A. Check to see if the end connections were wrapped in copper tape before terminating.
B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
C. Connect the RX/TX wires to different pins.
D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A
Explanation:
Importance of Proper Termination:
Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).

Interference Troubleshooting:
Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.

QUESTION 13
Which of the following most likely determines the size of a rack for installation? (Choose two).

A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height

Answer: BF
Explanation:
Understanding Rack Size Determination:
The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.

Switch Depth:
Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.
Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.

Server Height:
Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals 1.75 inches. The total height of all equipment determines the overall height requirement of the rack.
Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.

QUESTION 14
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.
B. Configure the native VLAN.

C. Tag the traffic to voice VLAN.
D. Disable VLANs.

Answer: C
Explanation:
Understanding VoIP and VLANs:
VoIP (Voice over IP) phones often use VLANs (Virtual Local Area Networks) to separate voice traffic from data traffic for improved performance and security.

Tagging Traffic to Voice VLAN:
Voice VLAN Configuration: The port on the switch needs to be configured to tag traffic for the specific voice VLAN. This ensures that voice packets are prioritized and handled correctly.
VLAN Tagging: VLAN tagging allows the switch to identify and separate voice traffic from other types of traffic on the network, reducing latency and jitter for VoIP communications.

QUESTION 15
As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing
B. Evil twin
C. MAC flooding
D. DNS poisoning

Answer: C
Explanation:
Definition of MAC Flooding:
MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.

Impact of MAC Flooding:
CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.

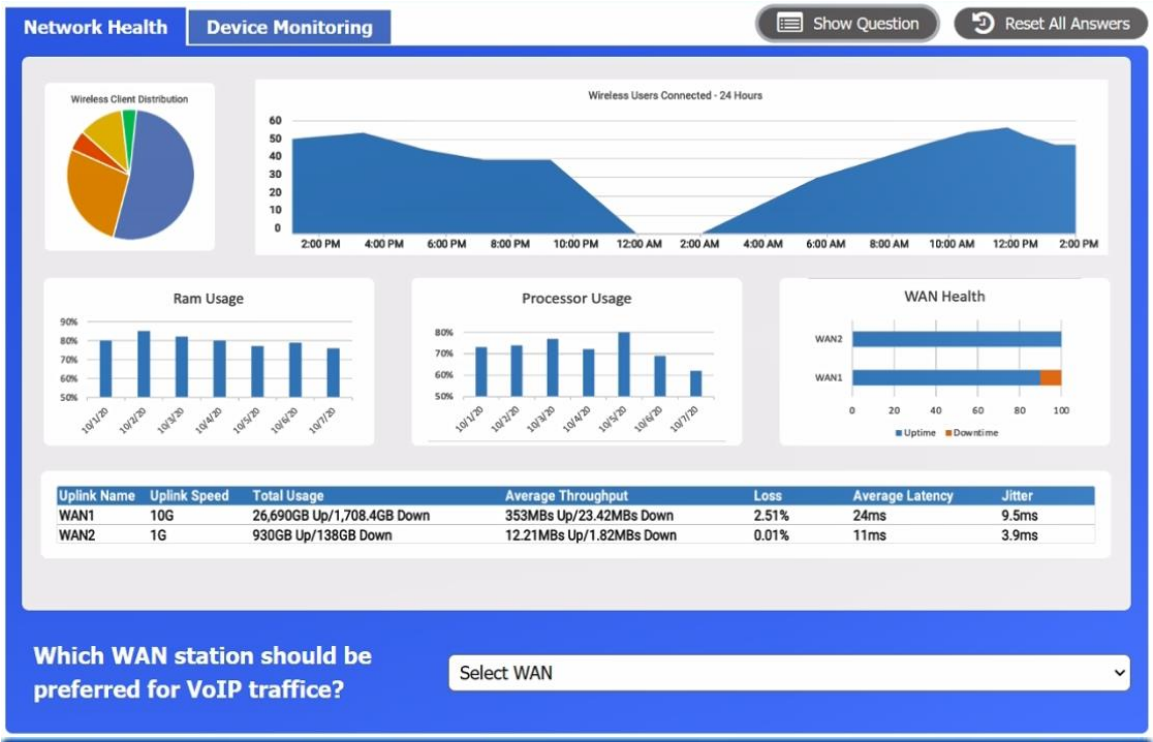
Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.

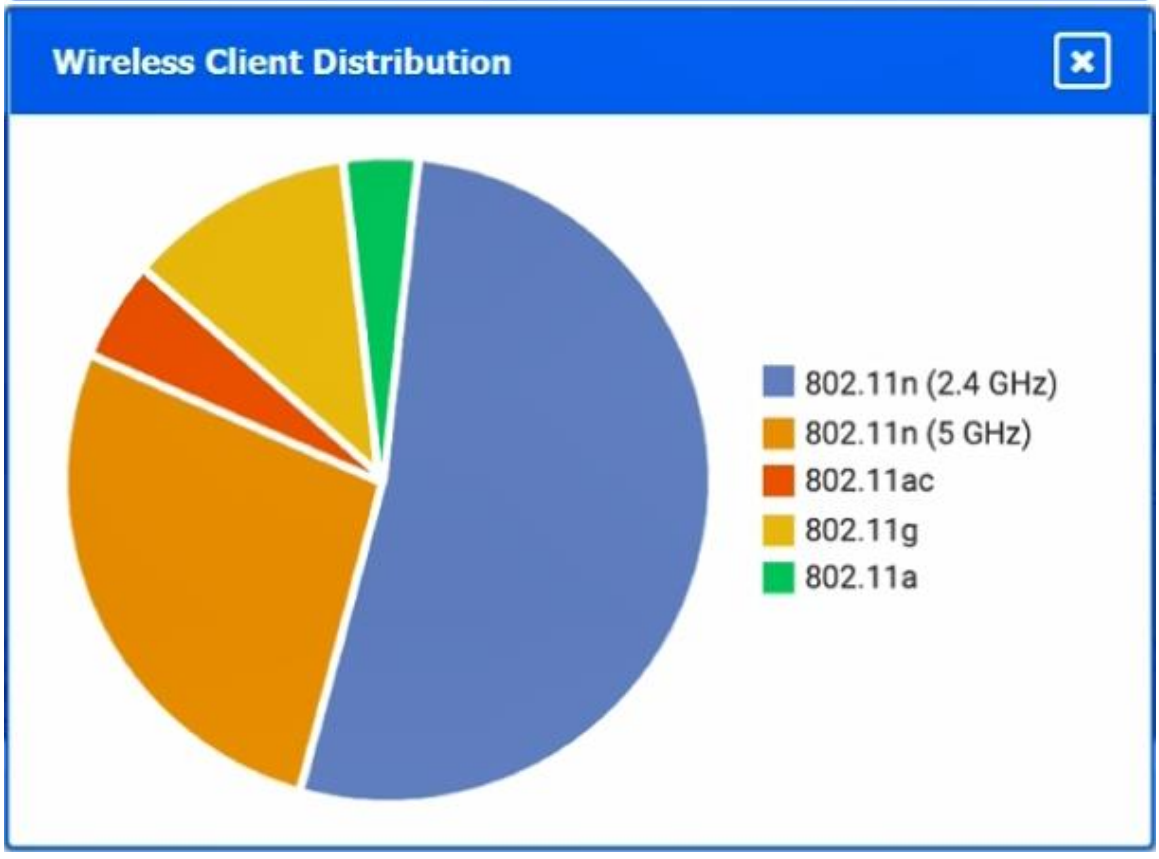
QUESTION 16
SIMULATION

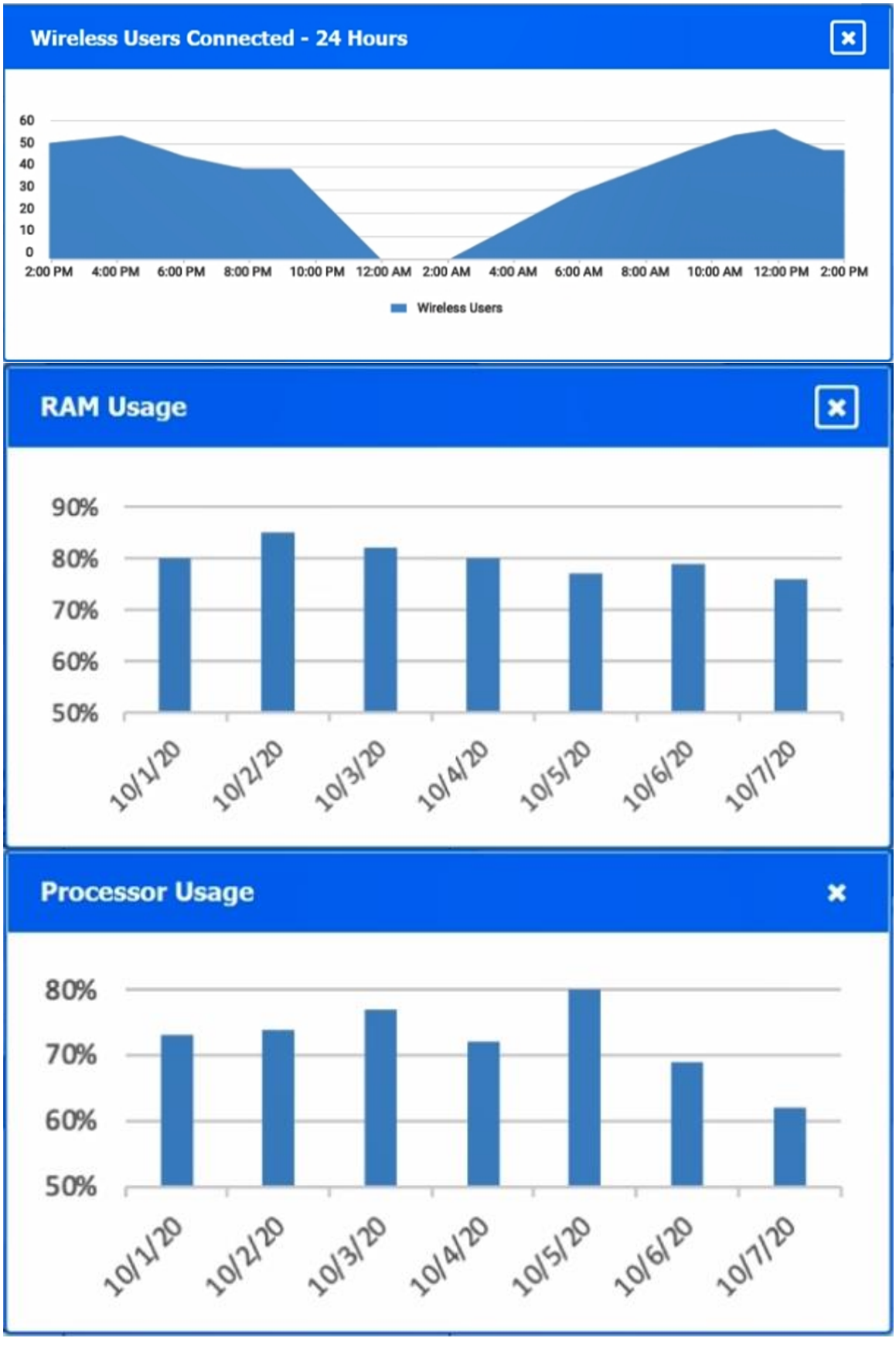
After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

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.

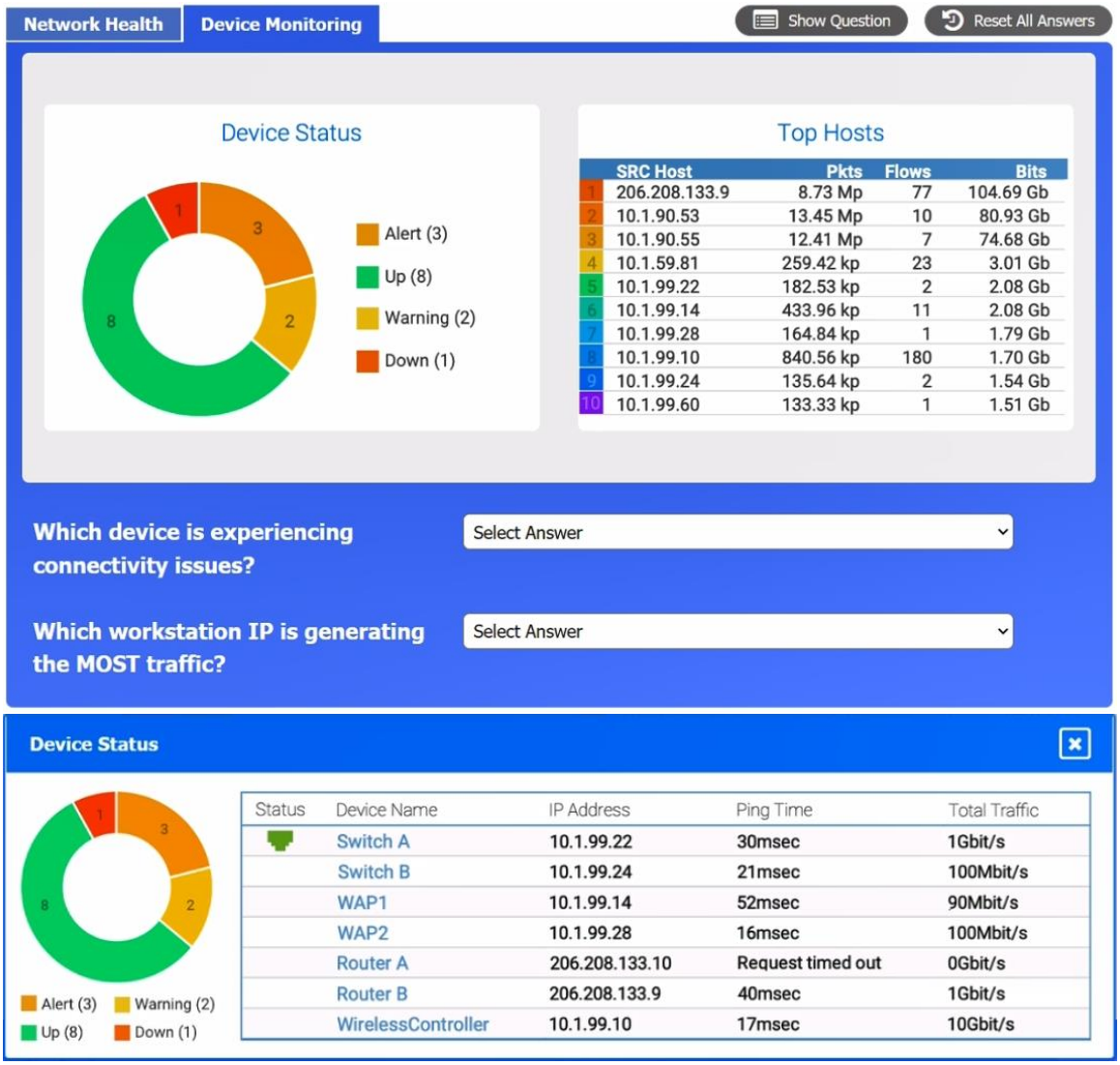
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

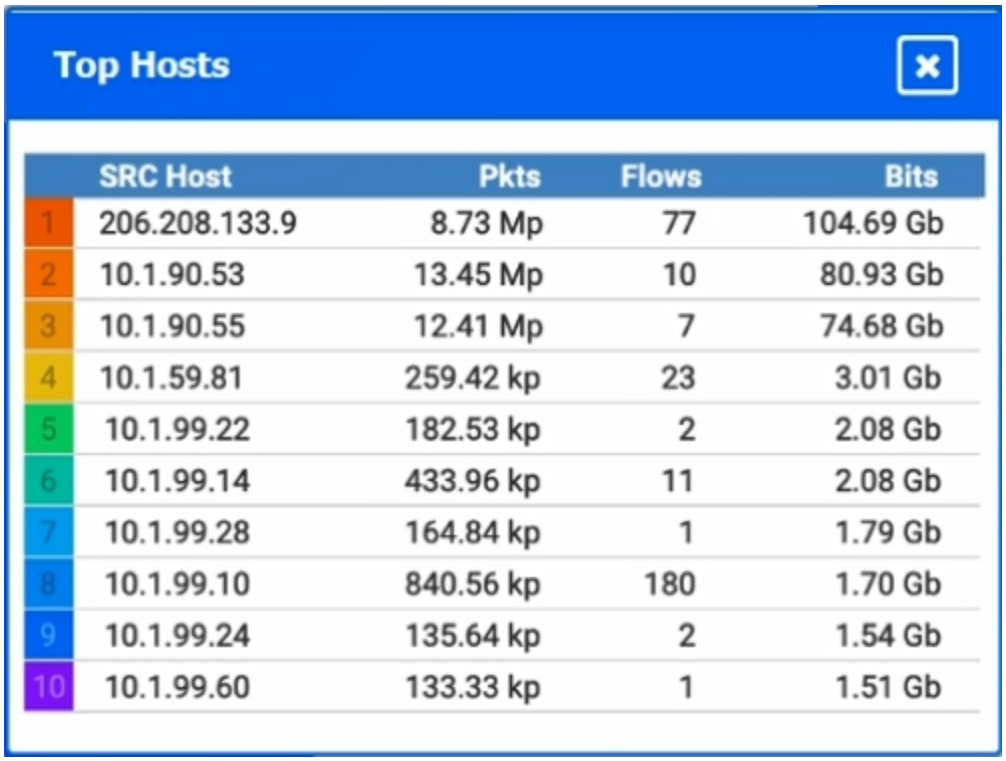

Network Health
Device Monitoring
Show Question
Reset All Answers
Wireless Client Distribution
Wireless Users Connected - 24 Hours
Ram Usage
Processor Usage
WAN Health
WAN2
WAN1
Uptime
Downtime
Uplink Name Uplink Speed Total Usage Average Throughput Loss Average Latency Jitter
WAN1 10G 26,690GB Up/1,708.4GB 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?
Select WAN


Wireless Client Distribution
802.11n (2.4 GHz)
802.11n (5 GHz)
802.11ac
802.11g
802.11a


Wireless Users Connected - 24 Hours
60
50
40
30
20
10
0
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
Wireless Users
RAM Usage
90%
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20
Processor Usage
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20

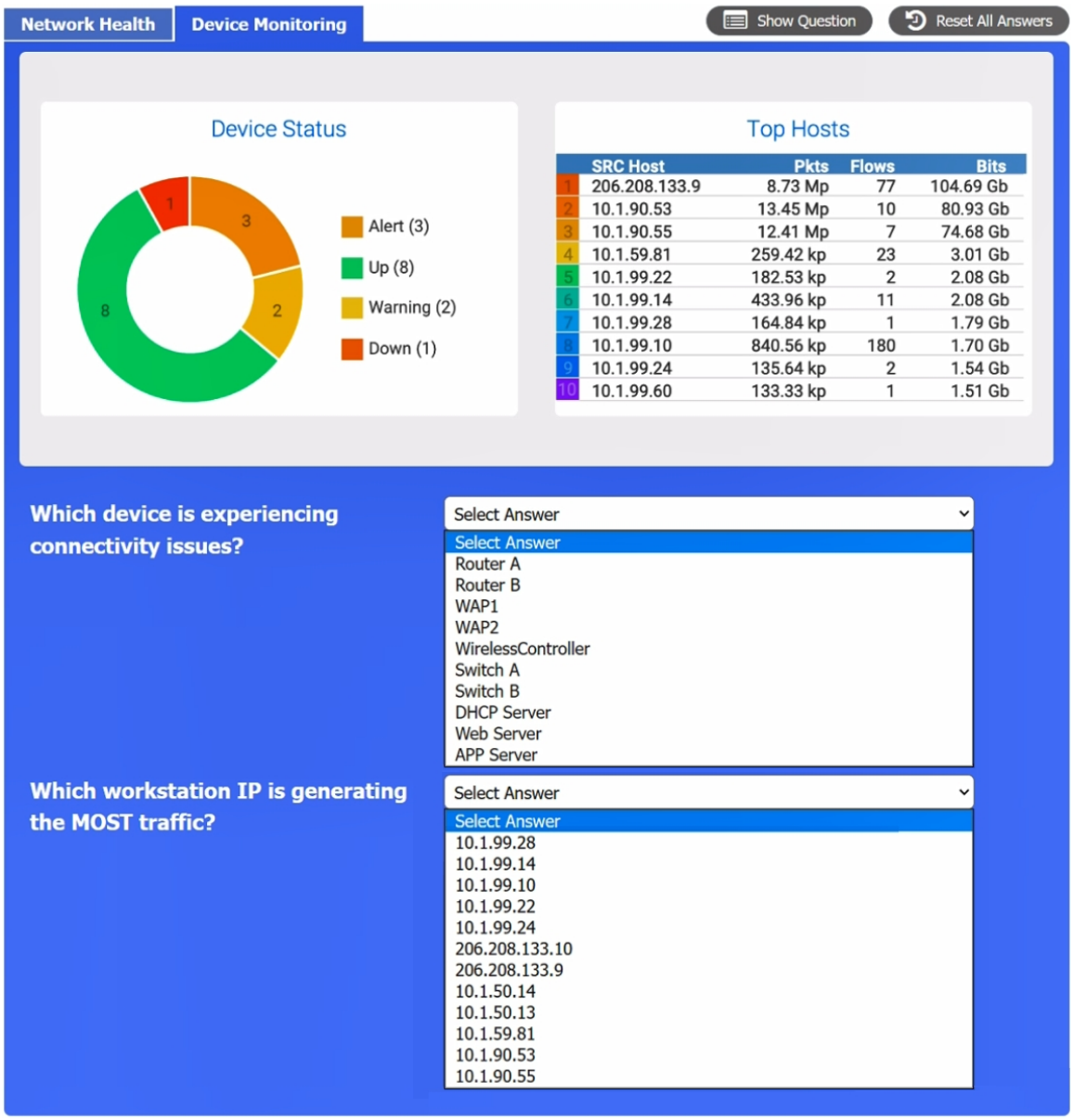

WAN Health
WAN2
WAN1
0
10
20
30
40
50
60
70
80
90
100
Uptime
Downtime
WAN Uplinks
Uplink Name Uplink Speed Total Usage Average Throughput Loss Average Latency Jitter
WAN1 10G 26,690GB Up/1,708.4GB Down 353MBs Up/23.42MBs Down 2.51% 24ms 9.5ms
WAN2 1G 930GB Up/138GB Down 12.21MBs Up/1.82MBs Down 0.01% 11ms 3.9ms
Network Health
Device Monitoring
Show Question
Reset All Answers
Wireless Client Distribution
Wireless Users Connected - 24 Hours
2:00 PM 4:00 PM 6:00 PM 8:00 PM 10:00 PM 12:00 AM 2:00 AM 4:00 AM 6:00 AM 8:00 AM 10:00 AM 12:00 PM 2:00 PM
Ram Usage
Processor Usage
WAN Health
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?
Select WAN
Select WAN
WAN 1
WAN 2


Network Health
Device Monitoring
Show Question
Reset All Answers
Device Status
Alert (3)
Up (8)
Warning (2)
Down (1)
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?
Select Answer
Which workstation IP is generating the MOST traffic?
Select Answer
Device Status
Alert (3)
Warning (2)
Up (8)
Down (1)
Status Device Name IP Address Ping Time Total Traffic
Switch A 10.1.99.22 30msec 1Gbit/s
Switch B 10.1.99.24 21msec 100Mbit/s
WAP1 10.1.99.14 52msec 90Mbit/s
WAP2 10.1.99.28 16msec 100Mbit/s
Router A 206.208.133.10 Request timed out 0Gbit/s
Router B 206.208.133.9 40msec 1Gbit/s
WirelessController 10.1.99.10 17msec 10Gbit/s



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



Answer:

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.

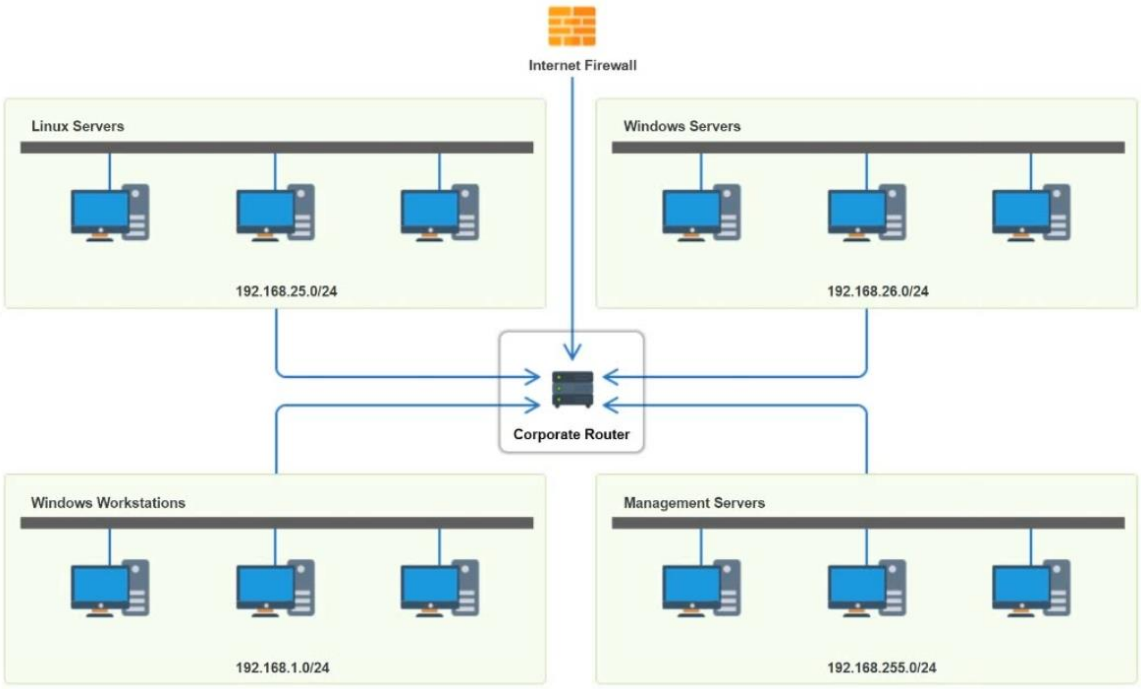
QUESTION 17
SIMULATION

You have been tasked with implementing an ACL on the router that will:

1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments.
2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
3. Prohibit any traffic that has not been specifically allowed.

INSRUCTIONS

Use the drop-downs to complete the ACL.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Internet Firewall
Linux Servers
192.168.25.0/24
Windows Servers
192.168.26.0/24
Corporate Router
Windows Workstations
192.168.1.0/24
Management Servers
192.168.255.0/24

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

Answer:

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 **192.168.255.0** 192.168.26.0 Any	**192.168.1.0** 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP **RDP** VNC SMB Any	**Allow** Deny
2	192.168.1.0 192.168.25.0 **192.168.255.0** 192.168.26.0 Any	192.168.1.0 **192.168.25.0** 192.168.255.0 192.168.26.0 Any	TCP	**SSH** Telnet HTTP RDP VNC SMB Any	**Allow** Deny
3	192.168.1.0 192.168.25.0 **192.168.255.0** 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 **192.168.26.0** Any	TCP	SSH Telnet HTTP **RDP** VNC SMB Any	**Allow** Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	**192.168.1.0** 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 **192.168.25.0** 192.168.255.0 192.168.26.0 Any	TCP	SSH **Telnet** HTTP RDP VNC SMB Any	Allow **Deny**
7	**192.168.1.0** 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 **192.168.26.0** Any	TCP	SSH Telnet HTTP RDP **VNC** SMB Any	Allow **Deny**
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 **Any**	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 **Any**	Any	SSH Telnet HTTP RDP VNC SMB **Any**	Allow **Deny**

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**