

□□□□ □□□□ □□□□ □□□□ □□□□□□□□ □□□□□□ □□□ □ □□ □□□ □□□ □□□ □
□□□ □□□ □ □□□□.
□□

- 1: Network+ (Plus) □□ | CompTIA IT □□
2: □□ □□□□ □□□□? - Techopedia□ □□
3: □□ □□□□ □□□□? - Techopedia□ □□

NEW QUESTION: 2

□□□ □□□□ □□ □□□ □□□□ □□□ □ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□□. □
□ □ □□ □□ □□ □□□□ □□□?

- A. □□ □□□
B. □□□ □□
C. 3□□ □□□
D. □□
E. 7□□ □□□
F. □□□ RSSI□ □□□ □□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

- * □ □□□ □□ □□ □□□□ □□□□ □□ □ □□□ □□□□ □ □□□ □□□□ □□□ □□ □□□□.
 - * □□□□ □□, □□ □□ □□ □□□□ □□□□□□ □ □□ □□□ □□□ □□□ □□□□□□□□.
 - * □□□□□□ □□□□□□ □ □□ □□□ VLAN(□□ LAN)□ □□□□ □□□□. VLAN□ □□□ □□□ □□□
□□□□ □□□ □□□□□□ □□□□ □□□□ □□□ □□ □□□□□□.
 - * VLAN□ □□□ 2 □□ □□□ 3 □□□ □□□□ □□□□□□ □□□ □ □□□□. □□□ 2 □□□□ □□□
□□ □□□□□ □□□□ MAC □□□ □□ □□□□ □□□□□□. □□□ 3 □□□□ □□□□ □□□□□ □
□□□ IP □□□ □□ □□□ □□□□□.
 - * □□□ 3 □□□□ □□□ 2□ □□□ 3 □□□ □□ □□□ □ □□□, □□ □□□ □□□ □□ □□ VLAN □
□ □□□□ □□□□ □ □□□□. □□ □□□□ □□□□ □□ □□□□□□ □□□□ □□□ □□□□.
 - * □□□ □□ C, □ 3□□ □□□□□□□. □ □□□□ □□ □□ □□□ □ □□□ □□□ □ □□□□.
- :

- * CompTIA Network+ N10-008 □□ □□□, 2□: □□□□ □□ □ □□, □□
2.1: □□□□ □□, 74-75□□□□
- * Messer □□□ CompTIA N10-008 Network+ □□, □□□ 2.1: □□□□ □□, 1□
- * □□□□ + N10-008 □□ □□, □□ 977, □□ C, □□

NEW QUESTION: 3

□□□□ □□□□ □□ □□□□□□ □□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□ □□□□
□□□ □□□□ □□□ □ □□□ □□ □□□.
□□ □ □□□□ □□□□ □□□ □□ □□□ □□□□ □ □□□ □□ □□□□□□?

- A. FTP
B. TFTP
C. SMTP

D. SFTP

Answer: D ([LEAVE A REPLY](#))

SFTP(FTP) is a secure file transfer protocol. It uses SSH for secure communication.

NEW QUESTION: 4

Which of the following is the default priority for the Spanning Tree Protocol (STP) on a Cisco switch?

- A. 4096
- B. 8192
- C. 32768
- D. 36684

Answer: ([SHOW ANSWER](#))

STP has several modes: STP, RSTP, MSTP, Per-VLAN STP, Per-VLAN RSTP. The default priority for STP is 32768. The priority is a 16-bit value, and the default is 32768. The priority can be changed using the `spanning-tree priority` command.

<https://community.cisco.com/t5/switching/spanning-tree-default-priorities/td-p/3304365>

NEW QUESTION: 5

Which of the following is the default priority for the Spanning Tree Protocol (STP) on a Cisco switch?

- A. 4096
- B. MAC address
- C. 32768
- D. VLAN ID

Answer: ([SHOW ANSWER](#))

MAC address is not a priority. The default priority for STP is 32768. The priority is a 16-bit value, and the default is 32768. The priority can be changed using the `spanning-tree priority` command. Source: CompTIA Network+ N10-008 Cert Guide, Chapter 7, Section 7.3

NEW QUESTION: 6

A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

- A. FTP
- B. DNS
- C. SSH
- D. RDP

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 7

Which of the following protocols is used to resolve IP addresses to MAC addresses?
A. DNS B. ARP C. DHCP D. RARP

A. DNS

B. ARP

C. DHCP

D. RARP

Answer: (SHOW ANSWER)

Which of the following protocols is used to resolve IP addresses to MAC addresses?
A. DNS B. ARP C. DHCP D. RARP

ARP

CompTIA Network+ N10-008

Studocu -

Network+ N10-008

NEW QUESTION: 8

Which of the following is a characteristic of a virtual machine?
A. It is a physical device. B. It is a software-based environment. C. It is a hardware-based environment. D. It is a network-based environment.

A. It is a physical device.

B. It is a software-based environment.

C. It is a hardware-based environment.

D. It is a network-based environment.

Answer: (SHOW ANSWER)

VM

Which of the following is a characteristic of a virtual machine?
A. It is a physical device. B. It is a software-based environment. C. It is a hardware-based environment. D. It is a network-based environment.

NEW QUESTION: 9

Which of the following is a characteristic of a virtual machine?
A. It is a physical device. B. It is a software-based environment. C. It is a hardware-based environment. D. It is a network-based environment.

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

Which of the following is a characteristic of a virtual machine?

- A. 00000 000
- B. 00 00 0
- C. CRC
- D. 000
- E. 00000

Answer: (SHOW ANSWER)

00

CRC Cyclic Redundancy Check 000, 00 0000 000 000 0000 0 0000 00 00 0
0 00000. 00 00000000 CRC 0000 0000 00 0000 000 00 000 000 000
0 0 000 00000. 00:
0000+ N10-008 00: 2.1 000 000000 0000 000 00 000 00000.

NEW QUESTION: 10

000 0000 00 00000 00000000. 000000 000 000 000 00000 00 00
0 000 0000 0000. 00 0 00 00 00000 000?

- A. 00 00
- B. 200 00
- C. 000
- D. 00 000

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

00 0000 00000 0000000 000 IP 000 0000 00 00000 000. 00 0 00 00
00 0000 00000 00 00000 0 0000 00 00000?

- A. 00000 DHCP 000 00
- B. 00000 000000 00 67/68 00
- C. 00000 000000 000000 0000 000 00 00000.
- D. 000 0000 00 00 000

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12

0000 00 000 0000 0000 00 0000 0000 00 0000 0000 000 000 0 0
0000. 00 0 00 0000 0 000 00 0 000 0 00000?

- A. 00 000 00 0000 00000000 000 00 00000 00000000.
- B. 00 000 0000 0000 00000000 00 000 0000000.
- C. 000 000 0000 0000000 00 000 000 00 000 000000.
- D. 200 0000 Neighbor Resolution Protocol 00000000.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 13

Which of the following is a common cause of a network outage?
A. A single point of failure

A. A single point of failure

B. 60%

C. 100%

D. 70%

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 14

Which of the following is a common cause of a network outage?
A. A single point of failure

B. 60%

C. 100%

D. 70%

Answer: ([SHOW ANSWER](#))

tracert

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

tracert is a command used to trace the route of a packet from the source to the destination. It is a network utility that is used to troubleshoot network connectivity issues.

NEW QUESTION: 15

Which of the following is a common cause of a network outage?
A. A single point of failure

A. A single point of failure

B. SIEM

C. 100%

D. 70%

Answer: B ([LEAVE A REPLY](#))

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

SIEM is a Security Information and Event Management system. It is a network utility that is used to troubleshoot network connectivity issues.

NEW QUESTION: 16

Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

- A. VIP
- B. NAT
- C. APIPA
- D. IPv6
- E. IP

Answer: A (LEAVE A REPLY)

IP is a protocol that allows a network to be extended over the Internet.

N10-008 Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

N10-008 Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

<https://www.dumpstopping.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 17

Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

- A. BGP
- B. OSPF
- C. EIGRP
- D. RIPv2

Answer: D (LEAVE A REPLY)

Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

Which of the following is a protocol that allows a network to be extended over the Internet? A. BGP B. OSPF C. EIGRP D. RIPv2 E. RIPv1

NEW QUESTION: 18

A network administrator is designing a wireless network. The administrator must ensure a rented office space has a sufficient signal. Reducing exposure to the wireless network is important, but it is secondary to the

primary objective. Which of the following would MOST likely facilitate the correct accessibility to the Wi-Fi network?

- A. Polarization**
- B. Channel utilization**
- C. Channel bonding**
- D. Antenna type**
- E. MU-MIMO**

Answer: D (LEAVE A REPLY)

The antenna type is the factor that would most likely facilitate the correct accessibility to the Wi-Fi network, as it determines the shape, direction, and range of the wireless signal¹². Different types of antennas have different characteristics, such as gain, beamwidth, and polarization, that affect how well they can cover a given area and overcome obstacles or interference¹². For example, an omnidirectional antenna can radiate the signal in all directions, while a directional antenna can focus the signal in a specific direction¹². By choosing the appropriate antenna type for the rented office space, the network administrator can ensure a sufficient signal and reduce exposure to the wireless network.

Polarization is the orientation of the electric field of the wireless signal, which can be either vertical, horizontal, or circular¹². Polarization affects the compatibility and performance of the wireless communication, as the transmitter and receiver antennas should have the same polarization to avoid signal loss¹². However, polarization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the antenna type and the environment¹².

Channel utilization is the measure of how much a wireless channel is occupied by data transmission, management frames, or control frames¹³. Channel utilization affects the efficiency and throughput of the wireless network, as a high channel utilization can indicate congestion, interference, or contention¹³. However, channel utilization alone would not facilitate the correct accessibility to the Wi-Fi network, as it depends on the network design, configuration, and demand¹³.

00 000 0 00 000 000 000 0 00 000 0000 00 00000 0000 0000 000
 00 000001. 00 000 00 000 00000 00 00 000 000 000 0000000 00
 00 00000 000 000 0 00001. 000 00 0000000 Wi-Fi 00000 0000 0000
 0 0000. 00 00, 00 000 00, 000 0010 00 0 00 000 0000 00000.

[illegible]

□ □ :

- 1: CompTIA Network+ N10-008 ☐☐ ☐☐☐, 4☐: ☐☐ ☐☐
 2: Messer ☐☐☐ CompTIA N10-008 Network+ ☐☐ ☐☐, 42☐☐☐: ☐☐ ☐☐☐
 3: Messer ☐☐☐ CompTIA N10-008 Network+ ☐☐ ☐☐, 43☐☐☐: ☐☐ ☐☐ ☐☐
 4: Messer ☐☐☐ CompTIA N10-008 Network+ ☐☐ ☐☐, 41☐☐☐: ☐☐ ☐☐
 5: Messer ☐☐☐ CompTIA N10-008 Network+ ☐☐ ☐☐, 40☐☐☐: ☐☐ ☐☐

NEW QUESTION: 19

□□ □ □□□□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□□□?

- A. □□□ □
- B. □□
- C. □□□
- D. □□□ □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 20

□□ □□□□ □□□ □ □□ □□ □□ □□□□□ □□ □□□□□?

- A. □□
- B. □□
- C. □□ □□
- D. □□□□

Answer: D ([LEAVE A REPLY](#))

□□□□ □□□ □□□□ □□□□□ □□□□ □□ □□ □ □□□ □□□□□. □□□□ □□□ □□□ □□
□ □□□ □□□□ □□□□.

<https://www.explainthatstuff.com/□□□□.html>

NEW QUESTION: 21

□□ □ □□ □□□□ □□ 802.11g WAP□ □□ □□ □□□ □□ □ □□□□?
108Mbps?

- A. □□□
- B. MIMO □□
- C. □□ □□
- D. □□□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

□□□□ □□□□ □□□ □□ □□□□□ □□□□ □ □□ □□ □□□□ □□□ □□ □□□ □□□□. □□
□□□□□ □□□ □□□ □□□□□□ □□□ □□□□□.

```
GigabitEthernet0/9 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

- □ □□ □□□ □ □□ □□ □□□□□?
- A. □□□□□□ □□□□□□□.
 - B. □□□□ □□ □□ □□□□.
 - C. □□□□ □□□□ □□□□□.
 - D. □□□ □□□ □□□□□□□.

Answer: A ([LEAVE A REPLY](#))

□□

□□□□□□ □□□□□□□□. □, □□□ □□□□□□ □□□□ □□□ □ □□□□. □□□□□ □□□□□
□□□ "□□"□□ □□□□ □□□ "□□"□ □□ □ □ □□□, □□ □□□ □□ □□□ □□□ □□□ □□□
□□. □□□□ □□□□ □□□, □□□□□ □□ □□□ "□□□" □□□□ □□□□□. □□□□ □□□□ □
□□□, □□□ □□ □□□ "□□□□ □□□□ □□" □□□□ □□□□□. □□□ □□□ □□□□, MTU □
□ □□□ "BW 10000 Kbit/sec" □□□□ □□□□□. □□: [CompTIA Network+ □□ □□ □□], □□□ 3.0 □
□□, □□

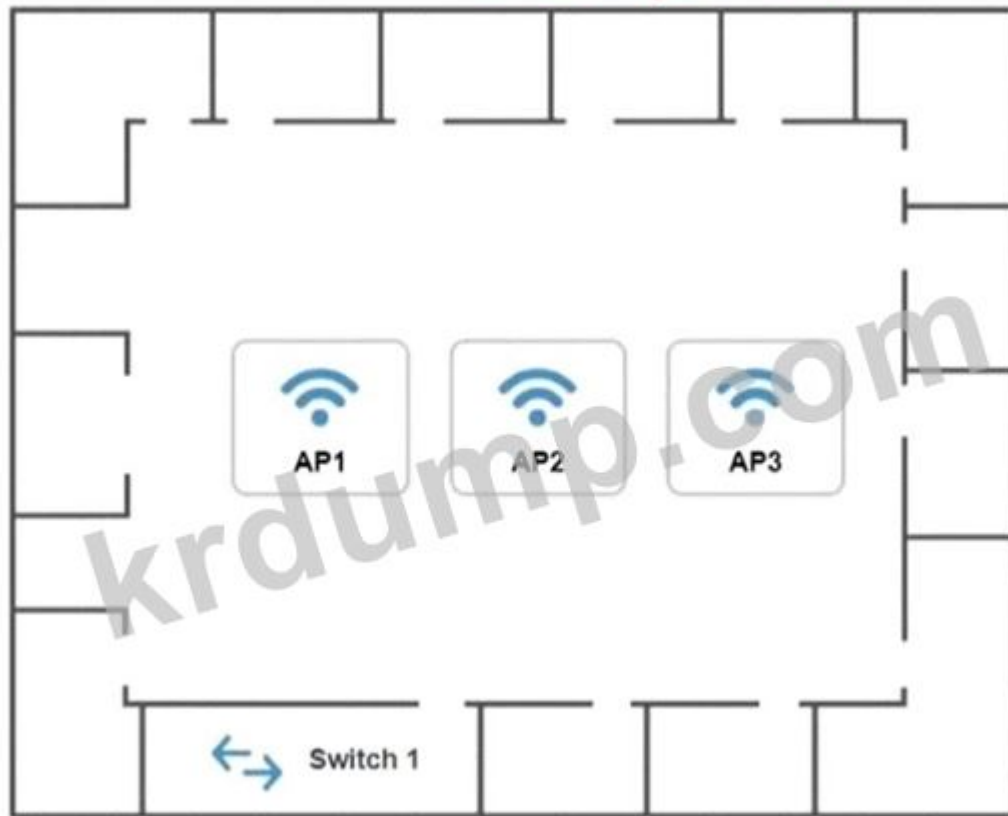
3.1: □□□ □□□□□□ □□□ □□□□ □□□ □□□□□. □□ □□: □□□ □□(ping, netstat, tracert □)

NEW QUESTION: 23

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t!
The wireless signals should not interfere with each other
The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

CompTIA



192.168.1.2
Speed: Auto
Duplex: Auto

AP1 Configuration



https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

CompTIA

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast



Yes



No

Wireless

Mode

B

G

Channel

1

2

3

4

5

6

7

8

9

10

11

Wired

Speed



Auto



100



1000

Duplex



Auto



Half



Full

Security Configuration

Security Settings



None



WEP



WPA



WPA2



WPA2 - Enterprise

Key or Passphrase

Reset to Default

CompTIA

Save

Close

AP3 Configuration



https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto

☒ 100

☐ 1000

Duplex

☐ Auto

☐ Half

☒ Full

Security Configuration

Security Settings

☒ None

☐ WEP

☐ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

Answer:

See explanation below.

Explanation

On the first exhibit, the layout should be as follows

The screenshot shows a web browser window titled "AP1 Configuration" with a URL bar displaying "https://ap1.setup.do". The interface is divided into two main sections: "Basic Configuration" and "Wireless/Wired".

Basic Configuration:

- Access Point Name: AP1
- IP Address: 192.168.1.32
- Gateway: 192.168.1.1
- SSID: CorpNet
- SSID Broadcast: ☒ Yes ☐ No

Wireless:

- Mode: B
- Channel: 3

Wired:

- Speed: ☐ Auto ☒ 100 ☐ 1000
- Duplex: ☐ Auto ☐ Half ☒ Full

Graphical user interface, text, application, chat or text message Description automatically generated

The screenshot shows a web browser window titled "Security Configuration".

Security Settings:

- ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3tl

Graphical user interface Description automatically generated

AP1 Configuration

https://ap1.setup.do

IP Address192.168.1.3227

Gateway192.168.1.1

SSIDCorpNet

SSID BroadcastYesNo

Wireless

ModeB

Channel3

Wired

SpeedAuto1001000

DuplexAutoHalfFull

Security Configuration

Security SettingsNoneWEPWPAWPA2WPA2 - Enterprise

Security Configuration

Security SettingsNoneWEPWPAWPA2WPA2 - Enterprise

Key or PassphraseS3cr3tl

Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated

AP1 Configuration

←

→

↺

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Exhibit 2 as follows

Access Point Name AP2

Graphical user interface Description automatically generated

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

192.168.1.64

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

6

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

Graphical user interface, text, application, chat or text message Description automatically generated

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3tl

Graphical user interface Description automatically generated

AP2 Configuration

https://ap2.setup.do

IP Address: 192.168.1.4 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 6

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

Exhibit 3 as follows

□□□ □□ AP3

□□□ □□□ □□□□□ □□ □□ □□

AP3 Configuration

←

→

↺

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

B

Channel

9

Wired

Speed

☐ Auto

☒ 100

☐ 1000

Duplex

☐ Auto

☐ Half

☒ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☐ WPA

☐ WPA2

☒ WPA2 - Enterprise

Key or Passphrase

S3cr3tl

Reset to Default

Save

Close

□□□ □□□ □□□□□, □□□, □□□□□□□, □□ □□ □□ □□□ □□□ □□□ □□□

Security Configuration

Security Settings

☐ None

☐ WEP

☐ WPA

☐ WPA2

☒ WPA2 - Enterprise

Key or Passphrase

S3cr3tl

□□□ □□□ □□□□□ □□ □□ □□

AP3 Configuration ✕

⬅ ➡ 🔄

IP Address /

Gateway

SSID

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode

Channel

Wired

Speed ☒ Auto ☐ 100 ☐ 1000

Duplex ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default
Save
Close

NEW QUESTION: 24

Which of the following is a function of the IP address 192.168.1.1? (Select two.)

- A. It identifies the network interface card (NIC) of the router.
- B. It identifies the default gateway of the router.
- C. It identifies the network interface card (NIC) of the computer.
- D. It identifies the SSID of the network.

Answer: A (LEAVE A REPLY)

* IGMP is a protocol that is used to manage the membership of hosts in a multicast group. It is used to send and receive data to and from a group of hosts. It is not used to identify the network interface card (NIC) of the router.

* IGMP is a protocol that is used to manage the membership of hosts in a multicast group. It is used to send and receive data to and from a group of hosts. It is not used to identify the network interface card (NIC) of the computer.

* IGMP is a protocol that is used to manage the membership of hosts in a multicast group. It is used to send and receive data to and from a group of hosts. It is not used to identify the SSID of the network. CPU is a component of a computer that is used to process data.

- * IGMP 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。
- * 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。
- * 该 DHCP 数据包 由 路由器 向 主机 发送 数据包 的 过程。 DHCP 数据包 由 路由器 向 主机 发送 数据包 的 过程。
- * 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。
- * AP 的 SSID 数据包 由 路由器 向 主机 发送 数据包 的 过程。 SSID 数据包 由 路由器 向 主机 发送 数据包 的 过程。
- * CompTIA Network+ N10-008 第 3 章: 网络 3.2: IPv4 和 IPv6 第 179-180 页
- * Messer 第 3 章: Network+ N10-008 第 3 章: IPv4 和 IPv6 第 37 页
- * Messer 第 3 章: Network+ N10-008 第 3 章: IPv4 和 IPv6 第 37 页

NEW QUESTION: 25

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

-97dB 数据包 由 路由器 向 主机 发送 数据包 的 过程。

- A. 数据包 由 路由器 向 主机 发送 数据包 的 过程
- B. 数据包 由 路由器 向 主机 发送 数据包 的 过程
- C. 数据包 由 路由器 向 主机 发送 数据包 的 过程
- D. 数据包 由 路由器 向 主机 发送 数据包 的 过程

Answer: A ([LEAVE A REPLY](#))

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

- * 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

该 数据包 由 路由器 向 主机 发送 数据包 的 过程。 该 数据包 由 路由器 向 主机 发送 数据包 的 过程。

* 10000 00 000. 0000 0000 000 00 0000 0000 00 0 0000. 000 00000 0
0000 000 000 00, 0000 00 000 000 000 00 00000.
000 0000 000 000 0000 0000 0000 0000 0000000 00000 0000 0
0 0 0000 000 000 0000 000 0 0000.
001: Network+ (Plus) 00 | CompTIA IT 002: Coaxial Splitter 0 0000? - Techopedia 00 003: Signal
Amplifier 0 0000? - Techopedia 00 00

NEW QUESTION: 26

□□ □□ □ □□ □□□□□ □□ □□ □□ □□□□□ □□□□ □□ □□□□□?

- A. OSPF**
B. LACP
C. STP
D. FHRP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 27

□□□□ □□□□□ □□ □□□ □□□□□ □□□ □□□. □□ □ □□ □□ □□□ □ □□□ □□□ □ □
□□□?

- A.** □□ □□
B. □□ □□□
C. □□ □□
D. □□ □□
E. □□ FTP □□

Answer: B (LEAVE A REPLY)

□□ □□□□ □□ □□□□□ □□, □□□ □□□□ □□□□ CPU □□ □□□□□ □□□□□. □□ □□□ □ □□ □□□(IEEE 802.3) □□□ □□□ 1,518□□□□□ □ □□□□□.

NEW QUESTION: 28

□□ □□ □ □□ □□□□□□ □□ □□ □□ □□□□□ □□□□ □□ □□□□□?

- A. FHRP**
B. LACP
C. OSPF
D. STP

Answer: ([SHOW ANSWER](#))

FHRP(First-hop Redundancy Protocol) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
□ □ □ □ □ □ □ □ □ □.

NEW QUESTION: 29

□□□□ □□□□ □□□ □□ □□ □□□ □□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
 □□ □□□ □ □□□□ □□ □□ □□□ □□□□ □□□□□? (□□□ □□□ □□□□ CompTIA Network+
 □□ □□□ □□ □□□□ □□ □□□ □□□□□)

- Answer: A (LEAVE A REPLY)**

PTR(□□□) □□□□ IP □□□ □□□ □□□ □□□□ □ □□□□, □□ □□□ □□ □□□ □□□□□. □
 □□ □□ □□□ □□ □□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□. PTR □□□□ □□□□ □
 □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □ □□□□ □□□ □ □□□□. CompTIA
 Network+ □□ □□□□ □□□ "PTR □□□□ IP □□□ □□□ □□□ □□□□ □ □□□□, □□ □□□ □
 □□ □□□□□."

□□□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□□ SLA□ □□□ □□ □□□ □□
□□□ □□□□□ □□□. □□ □ □□ □□ □□□□ □□□□ □ □□ □□□ □□□?

- Answer: A (LEAVE A REPLY)**

* □□□□ □□□ □□□□ □□□□□□ □□□□ □□□□□ □ □□□□□ □□ □□□□ □□□□ □□□
□ □□ □□□ □□□□□.

* iPerf TCP 100 UDP 10000 100000 1000, 100, 100, 100 1000 1000 1 100 1000 100000.

* iPerf □□□ □□□□ □□□□□ □□□ □□□□□ □ □□□ □ □□□□. □□□□ □□□ □□□ □□
□□ □□□ □□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□□□.

* iPerf □□□□ □□□ SLA(□□□ □□ □□)□ □□□□□ □□□□ □□□ □□□ □ □□□□.

* □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□.

```
* Ping ICMP 00 0000 00000 0000 00 0000 00 000 0000 0 00 0000
0. Ping 00 000 00 0000 000000 0000 00000 0000 0000 0000 0000 0000 0000 0000.
```

* NetFlow □ □ □ □ IP □□, □□, □□□□, □□□ □□□□ □□ □□□□ □□ □□□□ □□□□ □
□□ □ □□ □□□□□□□. NetFlow □ □□□ □□□□ □□□ □□□ □□ □□□ □□□ □ □□□ □□
□ □□□□ □□□□□□ □□□□□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□□.

* Netstat -s, netstat -s, netstat -s netstat -s netstat -s netstat -s netstat -s
netstat -s. Netstat -s netstat -s netstat -s netstat -s netstat -s. net:

* 1: CompTIA Network+ N10-008 □□ □□□, 1□, 1□: □□□□ □□, p. 14

* 2: CompTIA Network+ N10-008 □□ □□□, 1□, 16□: □□□□ □□□, p. 649

* 3: iPerf - TCP, UDP □ SCTP□ □□ □□□ □□ □□□ □□

* : CompTIA Network+ N10-008 □□ □□□, 1□, 3□: □□□ □□□□, p. 105

* : CompTIA Network+ N10-008 □□ □□□, 1□, 15□: □□□□ □□□□, p. 611
 * : CompTIA Network+ N10-008 □□ □□□, 1□, 4□: IP □□ □□, p. 143
 * : Ping (□□□□ □□□□) - □□□□□
 * : CompTIA Network+ N10-008 □□ □□□, 1□, 15□: □□□□ □□□□, p. 615
 * : NetFlow - □□□□□
 * : CompTIA Network+ N10-008 □□ □□□, 1□, 16□: □□□□ □□□, p. 650
 * : [netstat - □□□□□]

NEW QUESTION: 31

□□□□ □ □□□ □□□ Windows □□□□□□ □□ □□□□□□ □□□□ □□□ □□□□□□□ □□□
 □ □ □□□ □□□□ □□□□□. □□ □ □□ □□□ □□□ □ □□ □□□ □□□□□?

- A. □□ □□□□ □□□□□
- B. □□□
- C. □□□ □ VPN
- D. VNC

Answer: A (LEAVE A REPLY)

□□□ □□□ Windows □□□□□□ □□ □□□□□□ □□□□ □□□ □□□□□□□ □□□□ □ □□□
 □□□ □□□□ □□ □□□□ □□□□(RDP)□ □□□ □ □□□□. RDP□ □□□□ □□□□ □□□ □□
 □□ Windows □□□□ □□□□ □□□□ □□□ □ □□□ □□ Windows □□ □□□ □□ □□ □□□□□.
 RDP□ □□□□□ □□□□ □□□□□ □□ □□□□□□□□ □□ □□□□ □□□ □□□□□ RDP □□□
 □ □□□ □ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□. □□□□ □□ □□ □□□□□ □□□□□
 □□ □□□□□ □ □□□ □□ □□□ □□□□ □□□.

RDP□ □□ □ □□□□ □□ □□□□ □□ □□□□□ □□ □□□□ □□□□□ □□□□ □□□□□
 □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □ □□□□. □□ □□ □□□□ □□ □□□□□□
 □□ □□ □□□ □□□□□□□ □□□□ □□□□ □ □□□□.

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
 □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 32

□□ □□□ □□□□ □□ WAP□ □□□ IT □□□ □□ □□□□ □□□□ □□□□ □□□□. □□□ □□
 □□□□□ □□□□ □□ □□ □ □□ □□ □□□ □□□□ □□□?

- A. WPA2 □□
- B. CDMA □□
- C. □□ □□
- D. 802.11 □□

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 33

□□□□ □□ □□□□□ □□□□□ □□ □□□ □□□ □□□□□. □□□□ □□□□ □□□ □□□ □□ □□□.

IP □□ : 192.168.1.10

□□□ □□□: 255.255.255.0

□□ □□□□□: 192.168.1.254

□□□□ □□□□ □□□ □□ ARP □□□□ □□□□□.

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

□□ □ □□□□ □□ □□□ □□□□ □□ □ □□□ □□□□□?

A. □□□ VLAN□ □□□ □□

B. □□□ □□ □□□ □□ □□□

C. □□□□ IP□ □□□ □□ PC

D. □□□ □□ □□□□ □□ □□□

Answer: C ([LEAVE A REPLY](#))

□□

□□ □□□□ ARP □□□□ 192.168.1.10□ □□□ IP □□□□ □□ □ □□□ □□□ MAC □□□□ □□□□ □ □□□□ □□□ □□□ □□ □□□ □□ □□□□□. □□ □ □□□ □□□ IP □□□□ □□□ □□ □□ □□□□□□ IP □□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.

NEW QUESTION: 34

□□ □ □□□□ □□□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□ □□□□□? (2□ □□)

A. □□ □□ □□

B. □□ □□

C. IP □□□

D. □□ □□ □□ □□

E. □□□ □□

F. □□□□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

□□□□ □□□ □□□ □□□□ □□□□□□ □□ □□□ □□□ TV□ □□□□□, □□□ TV□ □□ Wi-Fi □ □□□ □ □□□□□. □□ □, □□□□ TV□ Wi-Fi□ □□□ □ □□□□, □□ □□□□ □□□ □□□□ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□□□?

- A. DHCP □□ □□
- B. AP □□ □□□
- C. □□□ SSID
- D. □□ □□□

Answer: A ([LEAVE A REPLY](#))

□□

DHCP □□ □□□ DHCP □□□ □□□□□□ □□□ □ □□ □□ □□□ IP □□□ □□□ □□ □□□□ □.DHCP□ Dynamic Host Configuration Protocol□ □□□, □□□□□ □□□□□□ IP □□□ □□ □□ □□ □□□ □□□□ □□□□ □□□□□□□□.DHCP □□□ DHCP □□□ □□□□□□ □□□ □ □□ IP □□ □□□□□.DHCP □□□ □□□□ □ □□□□□□ IP □□□ □□ □□□□□ □□□ □ □□□□.□ □□ □□□ TV□ □□□ □□ Wi-Fi□ □□□ □ □□□ □□□ TV□ □□□ □□ □ □□ □□□□ □□□□ □□□□ □□ □□□ □□□ □ □□□□.□□□□ DHCP □□ □□□ □□□□ □□ DHCP □□□ □□□ □ □□□ IP □□□ □□ □□□ □□□ □□□□.□□□□: [CompTIA Network+ □□ □□ □□], DHCP □□ □□ - □□□□□?□□□ □□□□□?

NEW QUESTION: 36

□□ □ □□ □□ □□□□ □□□ □□□□□□ □□□□□?

- A. □□□□ □□□□ □□□□.
- B. □□□□ □□ □□□ □□□□□□□.
- C. □□□□ □□□□□ □□□□□□□.
- D. □ □□ □□□ □□ □□□ □□□□□ □□□□ □□□□.

Answer: D ([LEAVE A REPLY](#))

□□

□ □□ □□□ □□ □□□ □□□□□ □□□ □ □□□□. □□ □□□□ □□ □□□ □□□□□ □□□□, □□ □□□□□ □□□□□ □□□□ □□ □□□□□ □ □□ □□□ □□ □□ □□, □□□□ □□ □□ □ □□ □□□□ □□□ □□□□□.12 □□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □□□ □□□ □ □□□□□.

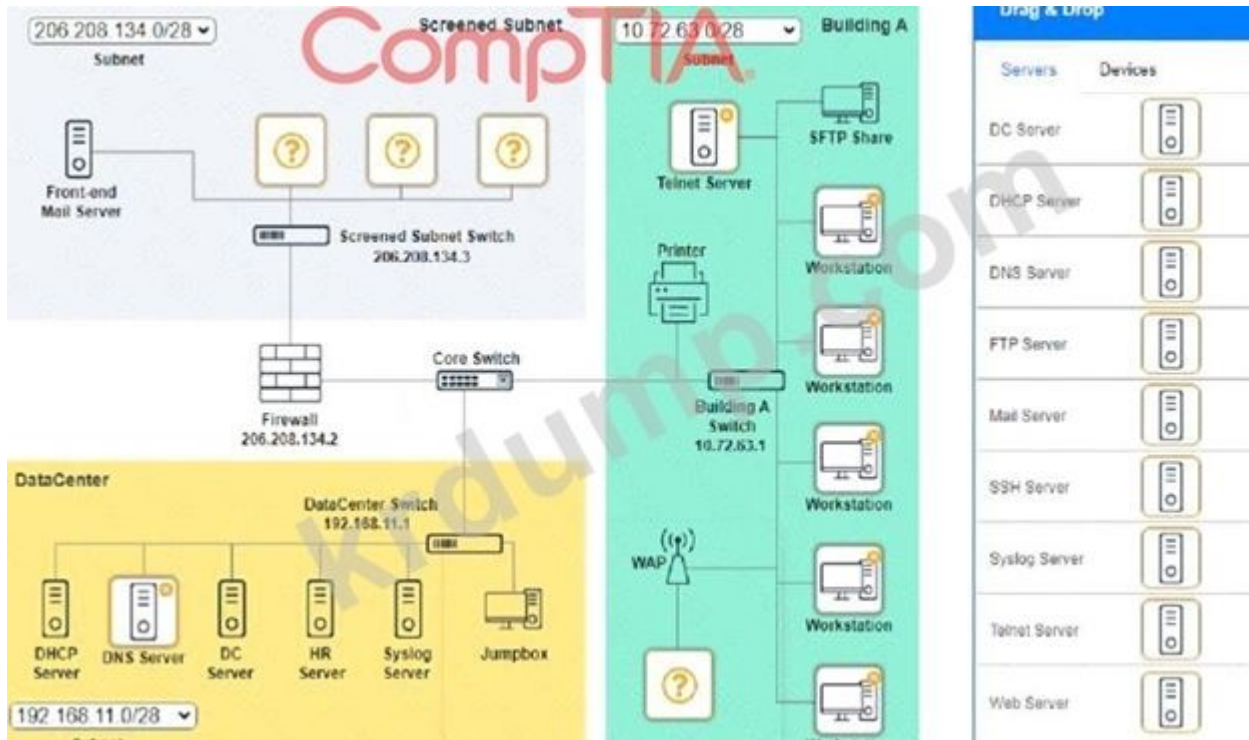
NEW QUESTION: 37

□□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□□.

□□ □□:

□□□□□

□□: □□□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □□□□ □ □□ □□□□□□.IP □□□ □□□ □□□ □□□□ □□□□ □□ 53 □□□□ □□□□ □□ □□□ □□□ □□□□.□□ A □□□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □ □□□ □□□ □□□□□□.5□□ □□ □□□ □□□□ □□□□ □□□ □□□□□□□□.□□ □□□ □□□□ □□□□□□□□.Telnet □□□ □□ □□□ □□□□□ □□□□□□□□.□□□□□ □□□ □□□□□ □□ □□ □



NEW QUESTION: 38

A small SOHO network is shown in the diagram. The network consists of a single PC and a switch. The switch is connected to the PC. The switch is also connected to the Internet. The switch is configured with a default gateway of 192.168.1.1. The switch is also configured with a default route to the Internet. The switch is also configured with a default route to the Internet. The switch is also configured with a default route to the Internet.

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

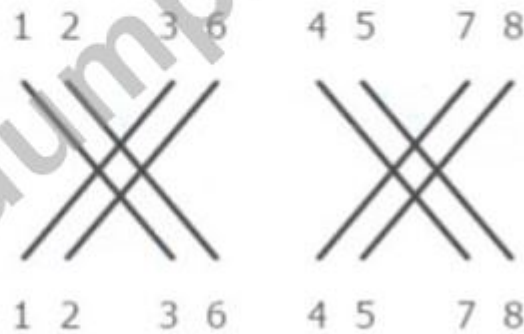
PC3

PC4

PC5

PC6

Connected to Switch 2



CompTIA

Cable Test Results



Switch 1

Length : 16M

Port : GigabitEthernet0/5

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

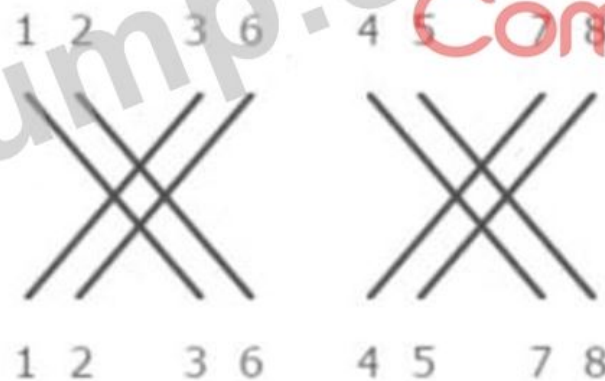
PC3

PC4

PC5

PC6

Connected to Switch 1



Cable Test Results



Switch 1

Length : 22M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

PC3

PC4

PC5

PC6

1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

Cable Test Results



Switch 1

Length : 42M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

PC3

PC4

PC5

PC6

1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

Cable Test Results



Switch 1

Length : 12M

Port : GigabitEthernet0/1

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

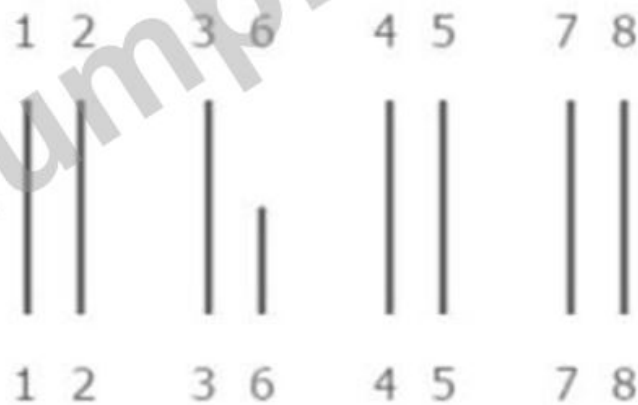
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 20M

Port : GigabitEthernet0/2

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

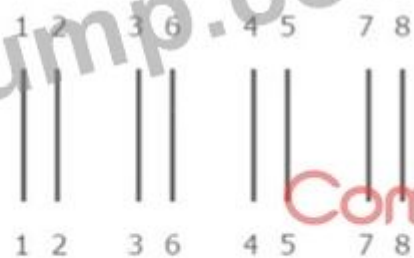
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 18M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 11

Speed : 1000 FDX

Server

PC1

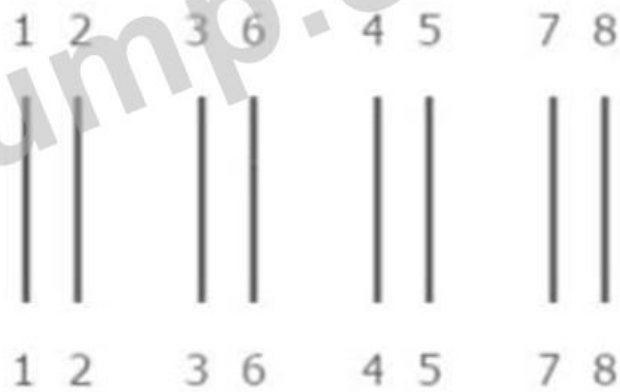
PC2

PC3

PC4

PC5

PC6



CompTIA

Cable Test Results



Switch 1

Length : 33M

Port : GigabitEthernet0/4

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

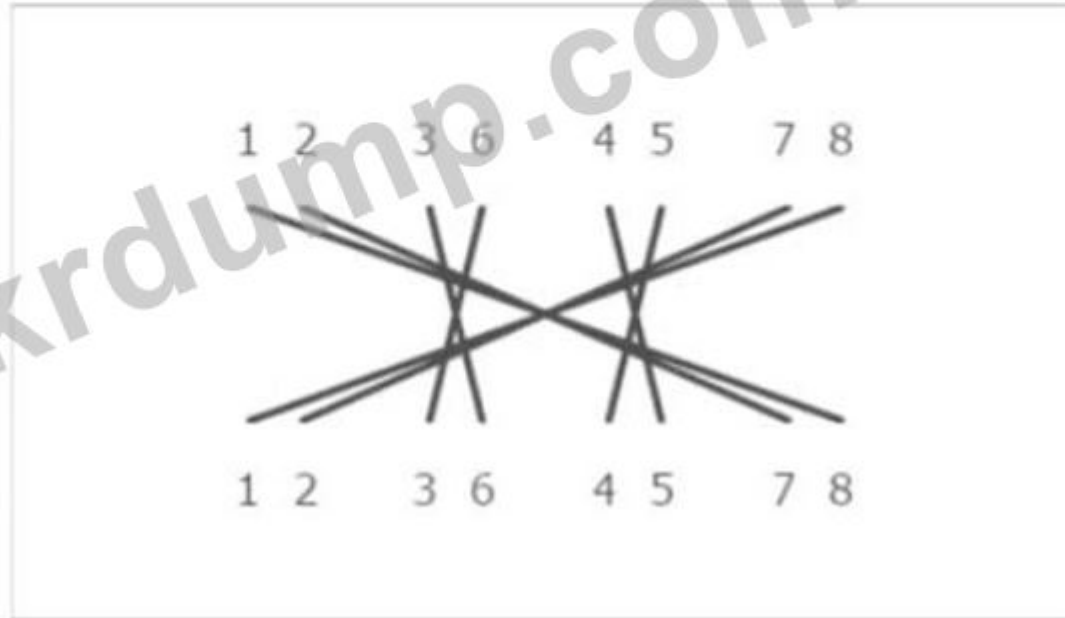
PC2

PC3

PC4

PC5

PC6



Cable Test Results



Switch 1

Length : 90M

Port : GigabitEthernet0/3

Switch 2

VLAN : VLAN 10

Speed : 1000 FDX

Server

PC1

PC2

PC3

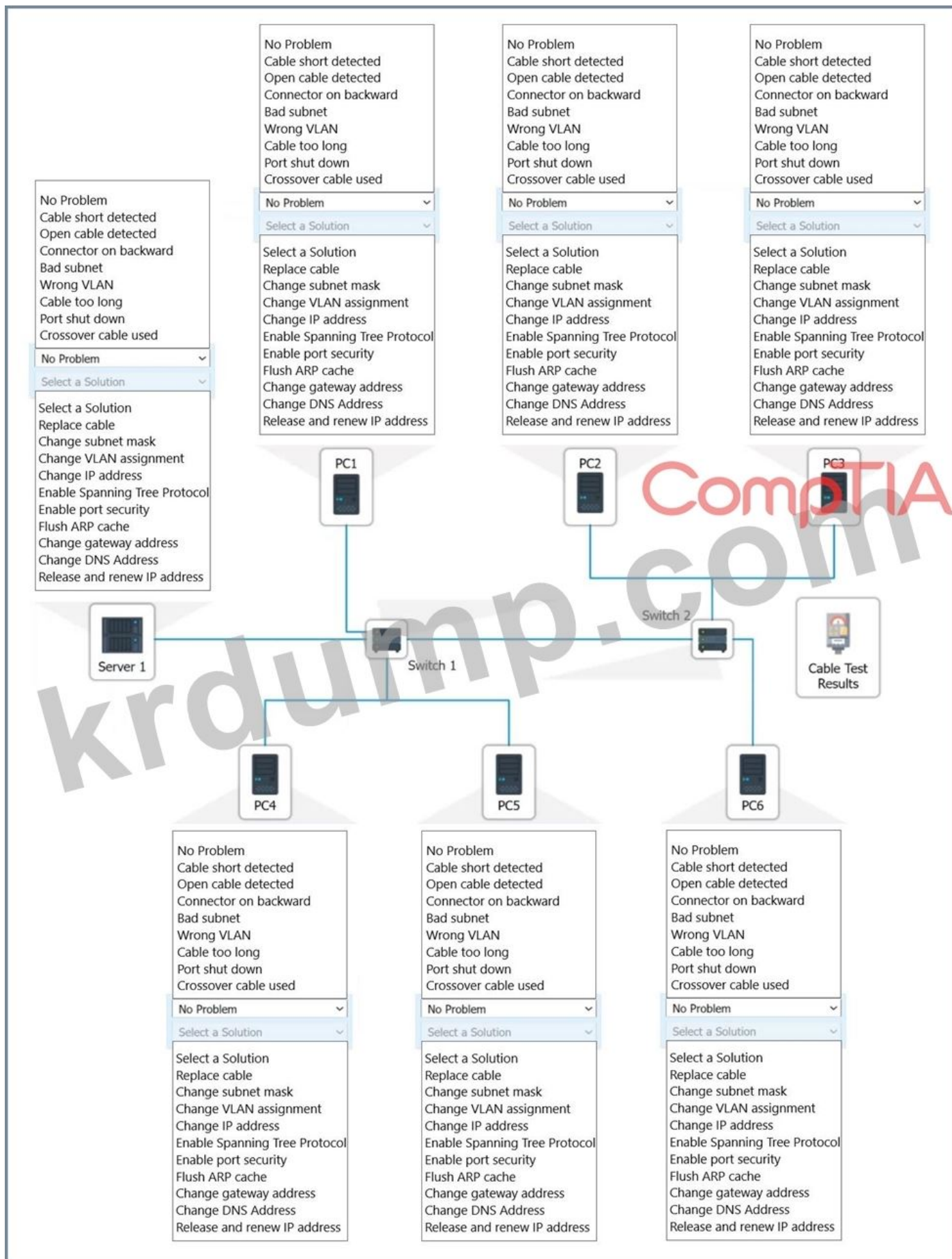
PC4

PC5

PC6

1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

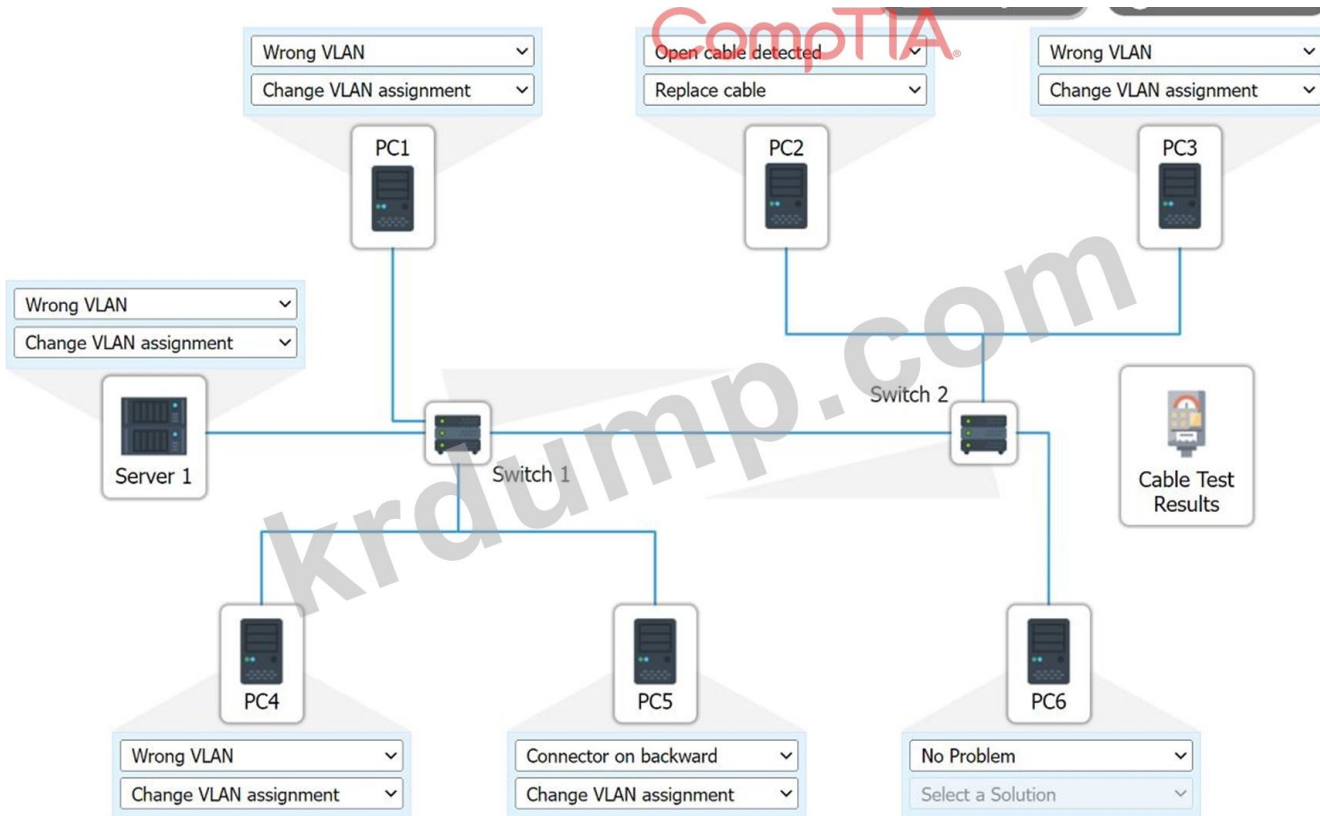
CompTIA



Answer:

□□ □□□□ □□□ □□□ □□□□□□.

□□:



NEW QUESTION: 39

□□□□ □□□□ □□□□□□ □□□□ □□□□ □□ □□□□□ □□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□□□ □□□ □□□□ □□□ □□ □□□□ □□□□ □□□□□.

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

□ □□□ □□□□ □□□□ □ □, □□□□ □□ □□□□ □□□□ □□ □□□□□?

- A. □□□ □□□ □□□ MTU□ □□□□ □□□□.
- B. □□□ □□□ □□ □□ □□□ □□□ □□□□.
- C. □□□□□□ □□ □□□□ □□ □□□□.
- D. □□□ □□□ □□ □□ □□□ □□□□ □□□□.
- E. □□□□□□ CRC□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

□□ □□ □□(MTU)□ □□□□ □□□ □□ □□□ □ □□ □□□ □□□ □□ □□□□□.12 MTU□ □ □□□□ □□□ □ □□□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□□ □□□□ □□□□ □□□□.

□□□ □□□ □□□□□□ MTU□□ □ □□□ □□□ □□□□□ □□□ □□ □□□ □□□□□ □□□ □□.12 □□ □□ □□ □□ □□ □□, □□□□ □□, □□ □□56□ □□ □□ □□□ □□□ □ □□□□.

□□□ □□□ □□□ □□□□□□□ □□78□ MTU□ □□□□ □□□ □□□□□ □□ □□□□. □□ □□ □ □□□ □□□□□□ □□□ MTU□ □□□□ □□ □□□ □□□□ □□□ □□□□□. □□ □□□ □□□ □□□□ □□□□ □□□□. □□□ □□□□ □□□□ □□ □□ □□ □□□□ □□ □□ □□□ □□ □□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□. □□□□ □□ □□□□□ □□□ □□ □□□□□□ □□ □□□ □□□ □□□ □□□ □□□□. CRC(□□ □□ □□) □□ □□□ □□□□ □□□ □ □□□□□□□ CRC□ 0□□□□ □□□ □□□□ □□□□910. □□□ □□ □□ □□ A□□□. □□□ □□□ □□□ MTU□ □□□□ □□□□. □□:

- 1: CompTIA Network+ N10-008 □□ □□ □□□, 67□□□
- 2: CompTIA Network+ □□ □□ □□, 7□□□
- 3: [□□ □□ □□(MTU)□ □□□□□? - WhatIs.com□□ □□]
- 4: [MTU □□ □□ | Network World]
- 5: [MTU □□□ □□□□ □□□ □□□ □□ | SolarWinds MSP]

NEW QUESTION: 40

□□□□ □□□□ IaaS□ □□□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□□. □□□□ □□ □ □□ □□ □□□□ □□□?

- A. □□□□□ □□ □□□□
- B. □□□ □□□□□□ □□
- C. □□□□ □□□□
- D. □□ □□□□ □□ □□

Answer: ([SHOW ANSWER](#))

□□

IaaS□ Infrastructure as a Service□ □□□, □□□□ □□ □□, □□□□, □□□□□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □□□ □□□□□. IaaS□ □□□ □ □□□□ □□□□ □□□□□□ □□□□ □□□ □□□□ □□□□ □ □□□ CPU, RAM, □□□□ □□, □□□□ □□□□ □□ □□ □□□□ □□ □ □□ □□□□ □□□. □□ □□□ □□□□ □□□□ □□ □□□□ □□□□□ IaaS□ □□□ □□□□. □ □□:

<https://www.comptia.org/blog/what-is-iaas>

NEW QUESTION: 41

□□□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □ □□ □ □□□ □□ □□□ □□ □ □□□□□□. □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□□ □□□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □□□. □□□□ □□□ □□□ □□□□ □□ □□ □□□□ □□ □ □□ □□□□?

- A. □ □□ □□ □□ □□□ □ VPN□ □□ □□□□ □□□□□□□□□□ □□□□□□ □□ □□ □□ □□□□ □□ □□□□□.
- B. □□ □□□ □□ □□□□ □□□ □ □□□□□ □□ □□□□□□□□□ VPN□□ □□ □□ □□ □□□□ □□□□□.

CompTIA Network+ (N10-008) □□ □□ □□

802.1Q is a standard protocol used for VLAN tagging on Ethernet networks. It allows multiple VLANs to coexist on a single physical network by adding a VLAN ID to the Ethernet frame header. This process is known as encapsulation. The VLAN ID is a 4-bit field in the frame header that identifies the specific VLAN to which the frame belongs. This enables network devices to route traffic based on the VLAN ID, ensuring that data is delivered to the correct destination within the network. VLANs are used to segment a network into different broadcast domains, improving security and performance. For example, you can create a VLAN for all sales department computers and another for all finance department computers, ensuring their traffic is isolated from each other. This is particularly useful in large enterprises where different departments need to communicate but also maintain some level of separation. The standard 802.1Q is defined by the IEEE. It's a key concept in network engineering, especially when dealing with multi-tenant environments or large-scale networks. Understanding how 802.1Q works is essential for configuring switches and routers to support multiple VLANs effectively. The process involves encapsulating the original frame with a new header that includes the VLAN ID. This tagged frame then travels across the network. When it reaches the destination, the VLAN ID is removed, and the original frame is delivered to the correct destination. This process is transparent to the end users, as they are unaware of the underlying VLAN structure. The standard 802.1Q is widely supported by most network equipment, making it a common choice for VLAN implementation. It's important to note that while 802.1Q is a standard, its implementation can vary slightly between different vendors and network devices. Therefore, it's always a good idea to consult the specific documentation for the equipment you are working with. The standard 802.1Q is a fundamental part of modern network architecture, enabling the efficient and secure management of complex networks. It's a key technology that has enabled the growth of large-scale networks and the ability to manage multiple different types of traffic and users within a single physical infrastructure. The standard 802.1Q is a critical component of network engineering, and understanding its principles and implementation is essential for anyone working in the field. The standard 802.1Q is a key concept in network engineering, and understanding it is essential for configuring and managing modern networks. The standard 802.1Q is a fundamental part of network architecture, enabling the efficient and secure management of complex networks. It's a key technology that has enabled the growth of large-scale networks and the ability to manage multiple different types of traffic and users within a single physical infrastructure. The standard 802.1Q is a critical component of network engineering, and understanding its principles and implementation is essential for anyone working in the field. The standard 802.1Q is a fundamental part of network architecture, enabling the efficient and secure management of complex networks. It's a key technology that has enabled the growth of large-scale networks and the ability to manage multiple different types of traffic and users within a single physical infrastructure. The standard 802.1Q is a critical component of network engineering, and understanding its principles and implementation is essential for anyone working in the field.

□□ □□ □□ □□(AP)□□ □□ □□ □□ □□□□ □□□□ □□□□. □□ □□ □□ □
□ □□ AP□ □□ □□ □□ □□ □□□□ □□□□ □□ AP□ □□ □ □□□ □□□ □ □□□□. □□ □
□ □□□□ □□□ □□ □□□ AP□ □□□□ □□ □□ □□ □□ AP□ □□□ □ □□□□. □□□□ □□
□□ AP□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□ □□□. □□:

Which of the following is a valid SSID? AP1 2.4GHz 802.11b AP2 5GHz 802.11a 802.11b 802.11ac

Answer: D (LEAVE A REPLY)

NEW QUESTION: 48

Which of the following is a valid SSID? AP1 2.4GHz 802.11b AP2 5GHz 802.11a 802.11b 802.11ac

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

Which of the following is a valid SSID? AP1 2.4GHz 802.11b AP2 5GHz 802.11a 802.11b 802.11ac

- A. 802.11b
- B. 802.11a
- C. 802.11g
- D. 802.11n
- E. 802.11ac

Answer: D (LEAVE A REPLY)

NEW QUESTION: 49

Which of the following is a valid SSID? AP1 2.4GHz 802.11b AP2 5GHz 802.11a 802.11b 802.11ac

- A. 802.11b
- B. 802.11a
- C. 802.11g
- D. 802.11n
- E. 802.11ac

Answer: A (LEAVE A REPLY)

NDA 1 - 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

NEW QUESTION: 50

Which of the following is a valid SSID? AP1 2.4GHz 802.11b AP2 5GHz 802.11a 802.11b 802.11ac

- A. 1
- B. 2
- C. 3
- D. 4

Answer: (SHOW ANSWER)

IP address is a 32-bit number, which is divided into two parts. The first part is the network address and the second part is the host address.

For example:

CompTIA Network+ 10101, 10101 N10-007, 4, 2: 10101, p. 82

NEW QUESTION: 51

Which of the following is a type of network interface card (NIC)?

- A. Ethernet
- B. NIC
- C. Fiber optic
- D. Wireless

Answer: (SHOW ANSWER)

NEW QUESTION: 52

Which of the following is a type of cloud service?

- A. PaaS
- B. IaaS
- C. SaaS
- D. DRaaS

Answer: B (LEAVE A REPLY)

IaaS: Infrastructure as a Service. It is a type of cloud service where the provider manages the infrastructure and the user manages the applications. IaaS is the most basic type of cloud service. PaaS: Platform as a Service. It is a type of cloud service where the provider manages the infrastructure and the user manages the applications. PaaS is a more advanced type of cloud service.

SaaS: Software as a Service. It is a type of cloud service where the provider manages the infrastructure, the platform, and the applications. SaaS is the most advanced type of cloud service. Disaster recovery as a Service (DRaaS) is a type of cloud service where the provider manages the infrastructure, the platform, and the applications. DRaaS is a more advanced type of cloud service.

NEW QUESTION: 53

Which of the following is a type of cloud service?

- A. IaaS
- B. PaaS

□□ □□□ □□, □□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□. □□□□ □□□□ □ □□□ □ □□□ □ □□□ □□ □□ □□ □□□□ □□□□. □□ □□ □□□ □□, □ □□ □□□□□ □□ □□ □□□ □□ □□□□ □□□ □□□□ □□□ □□ □□ □□□□□. □□□ □□□ □□□□ □ □□□ □ □□□, □ □□□ □□ □□ □□ □□□ □□□□□ □□ □□.

□□□ □□□ D□□□. □□□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □ □□ □□□□□. □□:

CompTIA Network+ N10-008 □□ □□ □□□, 2□: □□□□ □□ □ □□, 66□□□ Messer □□□ CompTIA N10-008 Network+ □□ □□, □□ 2.5: □□□□ □□ □□ □ □□, 23□□□

NEW QUESTION: 55

A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site.

Which of the following concepts should the company select?

- A. Cold site
- B. Hot site
- C. Warm site
- D. Cloud site

Answer: C (LEAVE A REPLY)

A warm site is a type of disaster recovery site that has equipment ready to go in the event of a disaster at the main datacenter, but does not have live data or applications. A warm site requires some time and effort to restore the data and services from backups, but it is less expensive than a hot site that has live data and applications. A cold site is a disaster recovery site that has no equipment or data, and requires a lot of time and money to set up after a disaster. A cloud site is a disaster recovery site that uses cloud computing resources to provide data and services, but it may have issues with bandwidth, latency, security, and cost. Reference:

<https://www.comptia.org/blog/what-is-a-warm-site>

NEW QUESTION: 56

□□□□ □□□ □□□ □ □□ □□□ □□ □□ □□□□ □□□ □□□□ □□□□. □□ □ □ □□□ □□ □ □□□ □ □□ □□□ □□□□□?

- A. Wi-Fi □□□
- B. □□□□ □□□
- C. □□
- D. IP □□□

Answer: B (LEAVE A REPLY)

□□

□□□□ □□□□ □□□□ □□□□ □□□□ □□ □□, □□ □□ □□ □□ □□□ □□□ □□ □□ □□□ □□□ □ □□ □□□□□.

Wi-Fi □□□□ □□ □□□□□ □□ □□, □□, □□ □□□□ □□□ □ □□ □□□□□, □□□□ □□□ □□ □□□ □□□ □□□ □□ □□□□.

Nmap IP address range scan option, scan all IP addresses in the range, scan all ports on each IP address, scan all open ports on each IP address.

NEW QUESTION: 57

Which of the following is a common method for identifying a wireless network? A. WAP B. WEP C. WPA D. WPA2

- A. WAP
- B. WEP
- C. WPA
- D. WPA2

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 58

Which of the following is a common method for identifying a wireless network? A. WAP B. WEP C. WPA D. WPA2

- A. WAP
- B. WEP
- C. WPA
- D. WPA2

Answer: ([SHOW ANSWER](#))

Which of the following is a common method for identifying a wireless network? A. WAP B. WEP C. WPA D. WPA2

NEW QUESTION: 59

- A. WAP
- B. WEP
- C. WPA
- D. WPA2

Answer: A ([LEAVE A REPLY](#))

Which of the following is a common method for identifying a wireless network? A. WAP B. WEP C. WPA D. WPA2

OSI model - N10-008 CompTIA Network+ : 1.11
CompTIA Network+ exam objectives, 920000

NEW QUESTION: 60

□□□□ □□□□ □□ □□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□□ □□□□□. □
□□□□ URL□ □□□□□ □□□□ □□□□ PC□□ ping□ □□□□ □ □□□ IP □□□ □□□□□□□. □
□□ □□□ □ □□□□ DNS □□ □□□ □□□□□□ □□□□□□.
□□ □ □□ □□□ □□□□ □□ □□□□□?

- A. □□ DHCP □□
- B. □□ □□□ HSRP
- C. DNS □□□□
- D. IP □□ □□□

Answer: A ([LEAVE A REPLY](#))

□□□□ DHCP□ □□□□ IP □□ □□□ □□□□ □□, □□ DHCP □□□ DNS □□□ □□ IP □□□ □
□□□□.

https://en.wikipedia.org/wiki/Rogue_DHCP

NEW QUESTION: 61

□□□ □□ ISP□ □□□ □□ □□□□. □□□ □□□□ □□□□ □□□□ □□□ ISP□ □□ □□ □□□
□□ □□ □□□ □□ □□□□□□□□. □□ □ □ □□□ □□ □ □□□□ □□ □□□□□?

- A. □□□ □
- B. □□ □□
- C. □□ □□
- D. □□ □□□ □□ □□□□

Answer: A ([LEAVE A REPLY](#))

* □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□ □□□ □□□ □□□ □□□□ □□□□
□.

* □□□ □□□ □□ □□□□ □□□ □□ □ □□□□ □□ □□□ □□□□ □ □□□□ □□□□ □□ □□
□□ □□□□□.

* □ □□□□□□ □□□ □□□ ISP□ □□ □□□ □□□ □□□, □□□ □□□ □□ □□□□ □□ □□□
□□□□□.

* □□□ □□□□ □□□ □□□ 2□ □□□ □□ □□ □□ □ □□□□.

* □□ □□□□ □□□ □□□□ □□□□□ □□ □□□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□
□.12 □□ □□□□ □□□ □□□ □□□ □□□□□ □□□□. □□□□ □□□□ □□□□ □□ □□□□□
□□□ □□□ □□□ □ □□ □□□□□.12

* □□□□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □ □ □□□ □□□ □□□ □
□□□ □□ □□□□□.12 □□□□□ □□, □□□ □ □□ □□□□ □□□ □ □□□ □□□ □□ □□ □□
□□ □□ □□ □□□ □□□ □ □□□□ □□□ □□□ □□□□ □□□□.12

* □□ □□□ □□ □□□□(VRRP)□ □□ □□□□ □□□□ □□□□12□ □□□ □□□ □□ □□ □□ □
□□□ □□□ □ □□□ □□ □□□□□□□. VRRP□ □□ □□□□□□ □□ □□□□ □□ □□□ □□□
□□ □□□□ ISP12 □□ □□□□ □□ □□□ □□□□ □□□□. □□:

* 1: CompTIA Network+ N10-008 □□ Cram, 6□, 2□: □□□□ □□ □ □□, p. 59-60

* 2: CompTIA Network+ N10-008 00 000, 10, 30: 0000 00, p. 97-98

N10-008 00 000 00000 00 DumpTop 00 0000 000 N10-008 00! DumpTop 0 00

N10-008 00 000 000000, DumpTop N10-008 00 000 00000000 000 00000
00. 0000 000 0000 00 DumpTop N10-008 000 00000.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 62

00000 00 0000 00 0000 00 000 00 000 0000 0000. 00 00000 00 0
00 00 0000 000 00 000 0000 00 EIRP 00 0000 0000. EIRP 00 00 000
000 00000 00 0 00 00 00000 0000 000? (0 000 00000.)

- A. AP 00 00
- B. 00 00
- C. 00 00
- D. ARP 000 0000
- E. 000 00
- F. AP 00 00

Answer: A,E ([LEAVE A REPLY](#))

EIRP 00 00000 AP 00 0000 000 000 00 0 0000.

00 0000 00 000 EIRP 00 0000 000 000 000, ARP 0000 AP 00 000 00 0
00 000 0000.

NEW QUESTION: 63

0 000 0000 000 0000 00 000 PSK 00000 000. 00 0 000 00000 00
00 00000 00000?

- A. VPN
- B. SSL
- C. TLS
- D. IPSec

Answer: ([SHOW ANSWER](#))

IPSec 0 0000 00 000 0 00 00000 00 0 0000 00 000 00 00 000 0000 0
000000. IPSec 0 000 0 000 0000 0000 00, 00 0 00 000000 00000.

IPSec 00 00 00 00 000 00 00 0 000 00 00 0(PSK) 00000.

NEW QUESTION: 64

000 0000 0000 000000 00 000 0000 00 41200 0000 00 000 000 0
000 IP 00000 00000 000. 0000 000 0 000 000. 000 000 0000 00 0
00 000 0000 0000 000?

- A.** 255.255.0.0
B. 255.255.252.0
C. 255.255.254.0
D. 255.255.255.0

Answer: B (LEAVE A REPLY)

255.255.252.0 是一个 B 类子网掩码，1022 个 IP 地址，412 个主机地址，1022 个 IP 地址。B 类 IP 地址范围是 172.16.0.0 到 172.31.255.255。B 类子网掩码 255.255.0.0 表示前 16 位是网络地址，后 16 位是主机地址。B 类子网掩码 255.255.252.0 表示前 18 位是网络地址，后 14 位是主机地址。B 类子网掩码 255.255.254.0 表示前 19 位是网络地址，后 13 位是主机地址。B 类子网掩码 255.255.255.0 表示前 24 位是网络地址，后 8 位是主机地址。

NEW QUESTION: 65

[illegible]

- A.** ☐☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐.
- B.** ☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐☐.
- C.** ☐☐☐ ☐☐ TX/RX ☐☐☐ ☐☐☐.
- D.** ☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐ ☐☐.
- E.** ☐☐☐ RSSI ☐ ☐☐ ☐☐ ☐☐☐.
- F.** ☐☐☐ ☐ ☐ ☐☐ ☐☐☐ ☐☐☐.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

□□□□ □□□ □□ □□□□ □□□□ □□□□ □ □□□ WAP□ □□□□□ □□□. AP□ □□ □ □□ □
□□ □□□ □□□□ □□□?

- A. ☐ ☐
- B. ☐ ☐ ☐
- C. ☐ ☐
- D. ☐ ☐ ☐ ☐

Answer: A (LEAVE A REPLY)

AP 00 0000 0000 000 00 0000 0000 0000 000. 00 0000 360 00 00
000 00 000 00000. 000 00 00000 00000 00 0000 00 00000 000 0
0000. 0000 AP 000 00 00 000 00000.1 00:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION: 67

□□□□ □□□□ □□ □□□□ □□ □□□□□ □□□□ □□□□. □□ □ IEEE
 □□ □□□□□□ □□□ □□□□ □□ 802.11 □□□ □□□□ □□ □□ □□□□?

- Answer: C (LEAVE A REPLY)**

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

□□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□□.

□ □□□ □□ □□□□□ □□ □ □□□ □□□□□ □□□?

- Answer: D (LEAVE A REPLY)**

NEW QUESTION: 69

A. Single sign-on
B. Kerberos
C. Multifactor
D. Network access control

Multifactor authentication is a method of verifying a user's identity by requiring more than one factor, such as something the user knows, something the user has, or something the user is. A password is something the

user knows, and a fingerprint is something the user is. Therefore, a user who needs to enter a password and scan a fingerprint is using multifactor authentication.

NEW QUESTION: 70

□□□□ □□ □□□□□ □□ □□□ □□□□ □□□□. □□□□□ □□□□ □□ □□ □□□ □□□ □□
 □□ □□ □□□□ □□□ □□□□□ □□□□□. □□□□ □□ □□□□□ □□ □ □□ □□ □□□□ □□
 □?

- A.** □□□□ □□□ □□
B. □□ □□
C. □□□ □□
D. □□□ □□

Answer: ([SHOW ANSWER](#))

1. **Introduction**
 The purpose of this document is to provide a comprehensive overview of the project's objectives, scope, and deliverables. It serves as a reference for all stakeholders involved in the project.
 The document is organized into several sections, each detailing a specific aspect of the project. The first section, 'Introduction', outlines the project's goals and the document's structure. The subsequent sections, 'Scope', 'Deliverables', 'Timeline', and 'Risk Management', provide further details on the project's boundaries, outputs, schedule, and potential challenges.
 This document is intended for use by project managers, team members, and stakeholders. It is a living document that will be updated as the project progresses and new information becomes available.
 2. **Scope**
 The project's scope is defined by the following key areas:
 - Project Objectives: The primary goals of the project are to develop a new software application that improves user experience and increases operational efficiency.
 - Deliverables: The project will produce a functional software application, user manuals, and training materials.
 - Timeline: The project is scheduled to start on January 1, 2021, and is expected to be completed by June 30, 2021.
 - Risk Management: The project team will identify, assess, and mitigate risks throughout the project lifecycle.
 3. **Deliverables**
 The project will deliver the following outputs:
 - A fully functional software application.
 - Comprehensive user manuals and documentation.
 - Training materials and sessions for end-users.
 - Regular progress reports and communication with stakeholders.
 4. **Timeline**
 The project timeline is as follows:
 - Phase 1: Planning and Requirements Gathering (January 1 - February 15, 2021)
 - Phase 2: Design and Development (February 15 - April 15, 2021)
 - Phase 3: Testing and Deployment (April 15 - June 30, 2021)
 5. **Risk Management**
 The project team will implement the following risk management strategies:
 - Regular risk assessments and reviews.
 - Proactive communication and collaboration with stakeholders.
 - Contingency planning for potential risks.
 - Regular reporting and documentation of risks and mitigation efforts.

NEW QUESTION: 71

□□□□ □□□ VoIP □□□ □□□ □□□□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□ □ □□
□ □□□□□. □□□□ □□□□ □□□ □□□□□ □□ □ □□ □□ □□ □□□□ □□□□□ □□□?

- A.** ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
- B.** ☐ ☐ ☐ ☐
- C.** ARP ☐ ☐
- D.** VLAN ☐ ☐
- E.** MDIX ☐ ☐

Answer: D (LEAVE A REPLY)

□□
VLAN(□□ LAN) □□□ □□□ □□ VLAN□ □□□□ □□□□ □ □□□□□. VLAN□ □□□□□ □□□
□□ □□□□□ □□□□ □ □□□□ □ VLAN□□ □□□ VLAN □□□ □□□□□. VLAN □□□ □□□□□
□□□□ □□□ □□□□ □□□□ □□□□ □□□□□ □□ □ □□□□□.

NEW QUESTION: 72

□□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □ □□ □□ □□□ □□□□ □□
□□ □□□□□□. □□ □ □□□□□ □□ □ □□□□ □□ □□□□□?

- A.** NIC ☐ ☐ ☐ ☐
- B.** ☐ ☐ ☐ ☐
- C.** FHRP
- D.** ☐ ☐ ☐ ☐

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 73

Which of the following is a feature of the Spanning Tree Protocol (STP)?

- A. STP uses the Spanning Tree Protocol (STP) to prevent loops.
- B. STP uses the Spanning Tree Protocol (STP) to prevent loops.
- C. MAC address table is used to prevent loops.
- D. STP uses the Spanning Tree Protocol (STP) to prevent loops.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 74

Which of the following is a feature of the Spanning Tree Protocol (STP)?

- A. STP
- B. STP
- C. STP
- D. STP

Answer: ([SHOW ANSWER](#))

Which of the following is a feature of the Spanning Tree Protocol (STP)?

NEW QUESTION: 75

Which of the following is a feature of the Spanning Tree Protocol (STP)?

- A. IP
- B. STP
- C. NetFlow
- D. STP

Answer: A ([LEAVE A REPLY](#))

Which of the following is a feature of the Spanning Tree Protocol (STP)?

NEW QUESTION: 76

Answer: B (LEAVE A REPLY)

□□

AP1□ AP2□ □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□ □□□□ □□ □□
RSSI □□□ □□□□ □□ □□ □ □□ □□ □□ □□□□□. RSSI□ □□ □□ □□ □□□□ □□□□, □
□□ □□□ □□□(AP)□□ □□ □□□ □□□ □ □□□ □ □□□□ □□□□ □□□□. AP□ □□□□□
□□ □□□ □□□□ □□□□□. □□□□ □□□□ □□□□□ □□□□ □□□□□. □□□ □□□□ □□
□□□ □□ □□□□ □□□□ □ □□ □□□ □ □ □□□ □□□□ □□□□□□□. □□ □□ □ □□□ □□
AP1□ AP2□ □□□ □□□□ □□□□ □□□□ □□ □□□□□ □□ □□ □□□ □□□ □□ □□□ □□
□□□ □□□ □ □□□□. □□□□: [CompTIA Network+ □□ □□ □□], RSSI□ □□□□ □□ □□□□□
□□ □□□ □□□□?, □□□ □□□: □□□ □ □□ □

NEW QUESTION: 78

□□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□□.

□□ □□:

□□□□□

□□: □□□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □□□□ □
□□ □□□□□□.IP □□□ □□□ □□□ □□□□ □□□□ □□ 53 □□□□ □□□□ □□ □□□ □□□
□□□.□□ A □□□□□ □□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □
□□□ □□□ □□□□□□.5□□ □□ □□□ □□□□ □□□□ □□□ □□□□□□.□□ □□□ □□□□
□□□□□□.Telnet □□□ □□ □□□ □□□□□ □□□□□□.□□□□□ □□□ □□□□□ □□ □□ □
□□ □□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□ □□□□ □□□ □□□□□□.□□
80/443 □□□□ □□□□ □□□ □□□□□□.□□ 20/21 □□□□ □□□□ □□□ □□□□□□.□□ □□
□ □□□ □□□ □□□ □□□□.□□□ □□ □ □□□ □ □□□ □□ □□ □□□□ □□ □□□ □□□□.
□□ □□□ □□□ □□□ □ □□ □□□ □□ □ □□ □□ □□ □□□□. □□□□ □□□□□□ □□ □□
□ □□□□□ □□ □□□ □□□ □□□□□.

Answer:

□□ □□□ □□□□□.

□□

Screened Subnet □□ - □ □□, FTP □□

□□ A □□ - □□ □□□ SSH □□, □□□□ 5□ □□ □□□ □□□□□□□ □□, □□ □□□ □□□□ □
□□□. □□□□□ □□ - DNS □□.

NEW QUESTION: 79

□□□□ □□□□ □ □□□□ □□ □□ □□□□ □□□□ □□□□. □□ □□ □□ □□□ □□□□ □□
□□□□ □□□□ □□ □□ □□ □ □□□□□?

A. VIP

B. NAT

C. APIPA

D. IPv6 □□□

E. □□□□□□ IP

Answer: A ([LEAVE A REPLY](#))

□□

Which of the following is a valid IPv4 address? A. 192.168.1.1 B. 192.168.1.1.1 C. 192.168.1.1.1.1 D. 192.168.1.1.1.1.1

Answer: A

CompTIA Network+ Study Guide, 6th Edition, N10-007, 4th Edition, 6th Edition: 6th Edition, p. 300

NEW QUESTION: 80

Which of the following is a valid IPv4 address? A. 192.168.1.1 B. 192.168.1.1.1 C. 192.168.1.1.1.1 D. 192.168.1.1.1.1.1

A. 192.168.1.1

B. 192.168.1.1.1

C. 192.168.1.1.1.1

D. 192.168.1.1.1.1.1

Answer: D (LEAVE A REPLY)

NEW QUESTION: 81

Which of the following is a valid IPv4 address? A. 192.168.1.1 B. 192.168.1.1.1 C. 192.168.1.1.1.1 D. 192.168.1.1.1.1.1

A. DHCP

B. 192.168.1.1

C. 192.168.1.1

D. 192.168.1.1.1.1.1

Answer: (SHOW ANSWER)

192.168.1.1

Which of the following is a valid IPv4 address? A. 192.168.1.1 B. 192.168.1.1.1 C. 192.168.1.1.1.1 D. 192.168.1.1.1.1.1

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/sec

NEW QUESTION: 82

Which of the following is a valid IPv4 address? A. 192.168.1.1 B. 192.168.1.1.1 C. 192.168.1.1.1.1 D. 192.168.1.1.1.1.1

A. 192.168.1.1

B. 192.168.1.1.1

C. 192.168.1.1.1.1

D. 192.168.1.1.1.1.1

Answer: A (LEAVE A REPLY)

uses frames as its unit of data, and adds a header and a trailer to each frame that contain information such as source and destination MAC addresses, frame type, and error detection code. The data link layer can check for errors by using techniques such as parity check, checksum, or cyclic redundancy check (CRC). The network layer is the third layer of the OSI model, which is responsible for providing logical addressing and routing of packets across different networks. The network layer uses packets as its unit of data, and adds a header to each packet that contains information such as source and destination IP addresses, protocol type, and hop count. The network layer can check for errors by using techniques such as Internet Control Message Protocol (ICMP), which can send and receive error messages or diagnostic information. References: [CompTIA Network+ Certification Exam Objectives], Data Link Layer - an overview | ScienceDirect Topics, Network Layer - an overview | ScienceDirect Topics

NEW QUESTION: 90

Which of the following is a characteristic of the network layer?

- A. It is responsible for error detection.
- B. It is responsible for error correction.
- C. It is responsible for logical addressing.
- D. It is responsible for physical addressing.

Answer: (SHOW ANSWER)

The network layer is responsible for logical addressing and routing of packets across different networks. It uses packets as its unit of data and adds a header to each packet that contains information such as source and destination IP addresses, protocol type, and hop count. It can check for errors using techniques such as Internet Control Message Protocol (ICMP).

NEW QUESTION: 91

Which of the following is a characteristic of the network layer?

- A. DNS resolution
- B. IP addressing
- C. IP routing
- D. DHCP

Answer: A (LEAVE A REPLY)

* DNS resolution is a process where a domain name is converted into an IP address. This is done by a DNS server. The DNS server stores a database of domain names and their corresponding IP addresses. When a client requests a domain name, the DNS server looks up the IP address in its database and returns it to the client. This process is essential for the network layer to route packets correctly.

* IP addressing is a process where a unique address is assigned to each device on a network. This address is used to identify the device and route packets to it. IP addressing is done by a DHCP server. The DHCP server assigns IP addresses to devices on the network. This process is essential for the network layer to route packets correctly.

* IP routing is a process where packets are sent from one device to another. This is done by a router. The router looks up the destination IP address in its routing table and forwards the packet to the next device. This process is essential for the network layer to route packets correctly.

* DNS resolution is a process where a domain name is converted into an IP address. This is done by a DNS server. The DNS server stores a database of domain names and their corresponding IP addresses. When a client requests a domain name, the DNS server looks up the IP address in its database and returns it to the client. This process is essential for the network layer to route packets correctly.

* IP 192.168.1.100 IP 192.168.1.100 192.168.1.100 192.168.1.100. 192.168.1.100 192.168.1.100 192.168.1.100 192.168.1.100, 192.168.1.100 192.168.1.100, 192.168.1.100 192.168.1.100.2 192.168.1.100 IP 192.168.1.100 192.168.1.100 DNS 192.168.1.100 DNS 192.168.1.100.

* DHCP 192.168.1.100 192.168.1.101 IP 192.168.1.100 DHCP 192.168.1.101. 192.168.1.100 192.168.1.101 IP 192, 192.168.1.100 192 DNS 192 192.168.1.100 192.168.1.101 192 192.168.1.100 192 192.168.1.1012.

□□ IP □□□ □□□□ □□ □□□ DNS □□□□ □□□ □□□□ DNS □□□□□□ □□□□.

□ □ □ □ :

* 1: □□□ □□□□ □ DNS □□□□: □□□□ □□ □□□□? - Heimdal Security

* 2: □□□ □□□□? - Cloudflare

* 3: DNS □□□□ □□□ □□□□□? - □□ □□ □□ □□

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 92

[illegible]

A. SSO

B. +

C. ☐ ☐ ☐ ☐ ☐ ☐

D. ☐ ☐ ☐ ☐

E. ☐ ☐ ☐ ☐

Answer: B (LEAVE A REPLY)

TACACS+(Terminal Access Controller Access Control System Plus) □ □□ □□□ □□□ □□ □□
 □ □□ □□□ □□ □□ □□□ □□□□ □□□□ □ □□□ □ □□□□. □ □□□□□ □□, □□ □□ □
 □□(AAA) □□□ □□□□ □□□□ □□□□ □□ □□□□ □□ □□□□□ □□□ □ □□□ □□□.
 □□:

Network+ N10-007 □□ □□ □□, □□ 4.2: □□□ □□□□□□ □□□ □□□□ □□ □□□ □□□□□□.

NEW QUESTION: 93

□□□□ □□ WAP□ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□□.

□□□□ □□□ □□□ □□□□ □□□ □□ WAP□ □□ 5□ □□□□□ □□ □□□□□□.

□□ □□ □□ □□□ □□□ □□□□ □□ □□□□?

A. ☐ ☐

B. □□

NEW QUESTION: 96

Which of the following is the MOST likely cause of the CRC errors?

- A. Insufficient power at the antennas
- B. PoE and UTP incompatibility
- C. Electromagnetic interference
- D. 802.1Q VLAN tagging

Answer: C ([LEAVE A REPLY](#))

1. Which of the following is the MOST likely cause of the CRC errors?
2. Which of the following is the MOST likely cause of the CRC errors?
3. Which of the following is the MOST likely cause of the CRC errors?
4. Which of the following is the MOST likely cause of the CRC errors?
5. Which of the following is the MOST likely cause of the CRC errors?
6. Which of the following is the MOST likely cause of the CRC errors?

NEW QUESTION: 97

Which of the following is the MOST likely cause of the CRC errors?

- A. Insufficient power at the antennas
- B. PoE and UTP incompatibility
- C. Electromagnetic interference
- D. 802.1Q VLAN tagging

Answer: A ([LEAVE A REPLY](#))

Which of the following is the MOST likely cause of the CRC errors?

CompTIA Network+ N10-008 91000
CompTIA Network+ Cert Guide: 172000

NEW QUESTION: 98

An office area contains two PoE-enabled WAPs. After the area was remodeled, new cable uplinks were installed in the ceiling above the fluorescent lights. However, after the WAPs were reconnected, users reported slowness and application errors. An intern reviewed the network and discovered a lot of CRC errors. A network engineer reviewed the intern's work and realized UTP cabling was used. Which of the following is the MOST likely cause of the CRC errors?

- A. Insufficient power at the antennas
- B. PoE and UTP incompatibility
- C. Electromagnetic interference

D. Wrong cable pinout

Answer: (SHOW ANSWER)

CRC errors in this section is a duplicate in the objectives, and appears in the previous section. They occur when packets contain invalid values, and possible causes include a faulty port, poor wiring, and even electromagnetic interference (EMI).

EMI is a problem when cables are installed near electrical devices, such as air conditioners or fluorescent light fixtures. If a network medium is placed close enough to such a device, the signal within the cable might become corrupt. Network media vary in their resistance to the effects of EMI. Standard unshielded twisted-pair (UTP) cable is susceptible to EMI, whereas fiber cable, with its light transmissions, is resistant to EMI. When deciding on a particular medium, consider where it will run and the impact EMI can have on the installation.

NEW QUESTION: 99

An IT technician successfully connects to the corporate wireless network at a bank. While performing some tests, the technician observes that the physical address of the DHCP server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

- A. Server upgrade
- B. Duplicate IP address
- C. Scope exhaustion
- D. Rogue server

Answer: D (LEAVE A REPLY)

A rogue server is a DHCP server on a network that is not under the administrative control of the network staff. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker.

NEW QUESTION: 100

_____ HTTP _____ PAT(____) _____
_____. PAT _____ IP _____ NAT(____) _____. PAT _____ IP _____
_____. _____ IP _____(____ 80) _____ IP _____(____: 8080)

- A. NAT
- B. _____
- C. STP
- D. SNAT
- E. ARP

Answer: (SHOW ANSWER)

_____ HTTP _____ PAT(____) _____
_____. PAT _____ IP _____ NAT(____) _____. PAT _____ IP _____
_____. _____ IP _____(____ 80) _____ IP _____(____: 8080)

□□ □□ □□□□ □□ □□□ □□□□□□ PAT □□□ □□□ □ □□□□. □□:

<https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

NEW QUESTION: 101

□□□□ □□□□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□. □□□□ □□□ □□, □□□□ □ □□□□□□□ □□ □□ CRC □□□ □□□□□□. □□ □ □□□ □□□ □□ □□□ □□ □□□ □□ □□□?

- A. Cat 5e □□□□ □□□ □□□□□.
- B. □□□□□□ □□□ VLAN □□
- C. □□□□ QoS □□□ □□ □□□□□□□.
- D. □□□ □□□ □□□ □ □□□□□ □□□

Answer: ([SHOW ANSWER](#))

CRC□ □□ □□ □□□ □□□□, □□□ □□□□ □□□ □□□□ □□□□□. CRC □□□ □□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □ □□□□, □□ □□ □□ □□ □□□ □□□□□□ □□□□□.

CRC □□□ □□□□□ □□□, □□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□□□□. □□□ Cat 5e □□□□ □□ □□□□ □□□ □□□ □□□□□ □□□□ □□□ □□□ □ □□□□ □□ □□ □□ □ □□□ □□ □□□ □□□□ □□□□.

□□ B□ CRC □□□ □□□ □□ □□□□ □□□□. □□□□□□ □□□ VLAN□ □□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□. □□□ VLAN □□□□ □□ □□□□ □□□□ □□□ □□□ □ □□□□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□□.

□□ C□ CRC □□□ □□□ □ □□□□ □□□□. □□□□ QoS □□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□□. QoS □□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□□.

□□ D□ CRC □□□ □□□ □ □□□□ □□□□. □□□ □□□□ □□□ □ □□□□□ □□□□ □□□ □□□ □□□ □□□ □□ □□□□□. □ □□□□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□ □ □□□ □□□□□. □□, □ □□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□□ □□□□ □□□□□.

□□:

CompTIA Network+ N10-008 □□ □□□, 2□: □□□□ □□ □ □□, □□ 2.2: □□□□ □□□□ □□ □□, 941□□□ Professor Messer□ CompTIA N10-008 Network+ □□ □□, □□ 2.2: □□□□ □□□□ □□ □ □, 162□□□ □□□: [□□ □□] CRC □□ - Cisco Community3 □□□□□□□ CRC □□ □□ □□ □□ - Huawei4 CRC □ □□ □□ □□, □□□ □□□ - site5

NEW QUESTION: 102

MAC □□□ OSI □□□ □□ □□□□ □□□□□?

- A. □□□□
- B. □□□
- C. □□ □□□□
- D. □□□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 103

Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

- A. Syslog
- B. Session Initiation Protocol
- C. Secure File Transfer Protocol
- D. Server Message Block

Answer: (SHOW ANSWER)

Explanation

Syslog is a protocol that provides a standard way for network devices and applications to send event messages to a logging server or a security appliance. Syslog messages can contain information about security incidents, errors, warnings, system status, configuration changes, and other events. A security appliance that is correlating network events from multiple devices can rely on Syslog to receive event messages from different sources and formats. References: <https://www.comptia.org/blog/what-is-syslog>

NEW QUESTION: 104

□□□ □□□ □□ □□□ □□□□□□. □ □□□ □□□□□ □□□□ □□□□.

□ □□□ IP □□ □□□ □□□ □□□□.

- □□□ □□ : 10.0.0.0/16

- □□ □□ : 10.0.0.0/24

□□□□ □□□□□ □ □□□ □□□ □□□□ □□ □ □ □□ □□ □□ □ □□□□□?

A. □ □□□ □□□ IP □□ □□□ □□□□□.

B. □□ □□□ □□□□□ □□□□ □□ □□ □□□□ □□□□□.

C. □□ □□□ NAT □□□ □□□□□.

D. □□ □□□ □□□ IP □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 105

□□□□ □□□□ □□ 492□□(150m) □□□ □ □□ □□□□ □□□□ □□□□ □□□. □□□□ □□□

□□□ □□ □ □□ □□□ □□□ □□□□ □□□?

A. □□□□ □□□

B. STP

C. DAC

D. □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 106

□□□□ □□□□ □□□□ □□□□ □□ 1/3□ □□□ □□□□□ PC□ □□ □□□ □□ □□□□ □□□

□. □□□□ □□□□□ □□□ □□ □□ □□□ □□□□□.

1/1	Client PC	Connected	Full	1000
1/2	Client PC	Connected	Full	1000
1/3	Client PC	Connected	Full	10

□□ □ □□ 1/3□□ □□□ □□□ □□□ □□□□□?

A. VLAN

B. □□

C. □□

D. □□□□

Answer: B ([LEAVE A REPLY](#))

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 107

A network technician receives a report from the server team that a server's network connection is not working correctly. The server team confirms the server is operating correctly except for the network connection. The technician checks the switchport connected to the server and reviews the following data;

Metric	Value
Bytes input	441,164,698
Bytes output	2,625,115,257
Runts	0
CRCs	5,489
Collisions	1
MDIX	On
Speed	1,000
Duplex	Full

Which of the following should the network technician perform to correct the issue?

A. Replace the Cat 5 patch cable with a Cat 6 cable

B. Install a crossover cable between the server and the switch

C. Reset the switchport configuration.

D. Use NetFlow data from the switch to isolate the issue.

E. Disable MDIX on the switchport and reboot the server.

Answer: A ([LEAVE A REPLY](#))

Explanation

"Bad cables, incorrect pinouts, or bent pins: Faulty cables (with electrical characteristics preventing successful transmission) or faulty connectors (which do not properly make connections) can prevent successful data transmission at Layer 1. A bad cable could simply be an incorrect category of cable being used for a specific purpose. For example, using a Cat 5 cable (instead of a Cat 6 or higher cable) to connect two 1000BASE-TX

devices would result in data corruption. Bent pins in a connector or incorrect pinouts could also cause data to become corrupted."

NEW QUESTION: 108

A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

- A.** 802.11a
- B.** 802.11b
- C.** 802.11g
- D.** 802.11n

Answer: D ([LEAVE A REPLY](#))

Explanation

802.11n is the best choice for setting up a wireless connection that utilizes MIMO on non-overlapping channels.

802.11n is a wireless standard that offers faster speeds and longer range than previous standards.

802.11n uses multiple-input multiple-output (MIMO) technology, which allows multiple antennas to transmit and receive multiple spatial streams of data simultaneously. MIMO can improve wireless performance, reliability, and capacity by exploiting multipath propagation and spatial diversity. 802.11n also uses non-overlapping channels in both the 2.4 GHz and 5 GHz frequency bands to avoid interference and increase bandwidth. Non-overlapping channels are channels that do not share any part of their frequency spectrum with other channels.

References: [CompTIA Network+ Certification Exam Objectives], 802.11n - Wikipedia

NEW QUESTION: 109

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks. A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it. Other machines in the building are able to retrieve files from the file server.

Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

- A.** The lab environment's IDS is blocking the network traffic. The technician can whitelist the new application in the IDS.
- B.** The lab environment is located in the DM2, and traffic to the LAN zone is denied by default. The technician can move the computer to another zone or request an exception from the administrator.
- C.** The lab environment has lost connectivity to the company router, and the switch needs to be rebooted. The technician can get the key to the wiring closet and manually restart the switch.
- D.** The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back. The technician can submit a request for upgraded equipment to management.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 110

A client who shares office space and an IT closet with another company recently reported connectivity issues throughout the network. Multiple third-party vendors regularly perform on-site maintenance in the shared IT closet. Which of the following security techniques would BEST secure the physical networking equipment?

- A. Disabling unneeded switchports
- B. Implementing role-based access
- C. Changing the default passwords
- D. Configuring an access control list

Answer: [\(SHOW ANSWER\)](#)

Role-based access is a security technique that assigns permissions and privileges to users or groups based on their roles or functions within an organization. Role-based access can help secure the physical networking equipment by limiting who can access, modify, or manage the devices in the shared IT closet. Only authorized personnel with a valid role and credentials should be able to access the networking equipment. Disabling unneeded switchports is a security technique that prevents unauthorized devices from connecting to the network by turning off unused ports on a switch. Changing the default passwords is a security technique that prevents unauthorized access to network devices by replacing the factory-set passwords with strong and unique ones. Configuring an access control list is a security technique that filters network traffic by allowing or denying packets based on criteria such as source and destination IP addresses, ports, or protocols.

NEW QUESTION: 111

A network technician is working to upgrade an existing wireless system in order to improve the coverage of APs throughout the building. Which of the following should the technician perform to determine the optimal placement of APs for the new wireless system?

- A. Network assessment
- B. Packet capture
- C. Site survey
- D. Cable testing

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 112

□□ □ □□□ □□ □□□ □□ □□□□□□□□ □□□□ □ □□ □□ □□□□ □□□□ □□□□□?

- A. □□□ □□□
- B. □□□□ □□□
- C. □□ □□□
- D. □□□ □□□

Answer: D [\(LEAVE A REPLY\)](#)

* □□ □□□□ □□□□ □□, □□ □□ □□□□ □□ □□ □□□ □□□ □□□□ □□ □□□□□□. □
□□ □□ □□ □□□ □□ □□□ □□□□□ □□ □□ □ □□□□□□□ □□□□ □□□□ □ □□ □□
□□□ □□□ □□□□□.12

* □ □□□□ □□□ □□□ □□ □□, □□ □ □□□□ □□□ □□□□□ □□ □□□□□□□ □□□□ □
□□□□□ □□□□ □□ □□ □□□□□□. □□ □□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□
□□□□□12.

[illegible]

* □□□□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□□□ □□□□ □□□□□ □□ □□□□ □□. □□□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□, □□□ □ □□□ □□□ □ □□□□. □□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□□13.

* □□□□□ □□ □□□□□□□□ □□, □□□□ □ □□ □□□ □□□□ □□□ □□□□ □□ □□□ □□ □
□ □□□□ □□ □□□□□ □□ □□□□ □□□ □ □□□□. □□□□ □□□ □□ □□ □□□□ □□ □□
□□□ □□□□□□□ □□□□ □□□□ □ □□ □□ □ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□□
□□□. □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□ □□ □□□ □□□ □□□□12. □□:

* 1: CompTIA Network+ N10-008 □□ □□ □□□, 11□: □□□□ □□, □□

11.4: $\square\square \square\square 2$

* 2: Messer □□□ CompTIA N10-008 Network+ □□ □□, 51□□□: □□ □□4

* 3: Messer □□□ CompTIA N10-008 Network+ □□ □□, 52□□□: □□□□ □□□4

* 4: Messer □□□□ CompTIA Network+ N10-008 □□□□5

NEW QUESTION: 113

□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□ □□□□. □□□□ □□□□□ □□□□ □
□□□□ □□ □□□ □□□□□.

SSID	Signal (RSSI)	Channel
Corporate	-50	9
Corporate	-69	10
Corporate	-67	11
Corporate	-63	6

[illegible]

A. ☐ ☐ ☐ ☐ ☐

B. ☐ ☐ ☐ ☐ ☐

C. □□ □□□ □□□□□□□

D. □□□ □□□ □□

Answer: A ([LEAVE A REPLY](#))

00 00 00 00 00000 00000 000 000 000 0000 000 00 000 0000 0
 0000. 0000 000 00 SSID 00 9, 10, 11 0 6 0000 000, 00 00 0000 00 00
 0 00 000000 00000. 00 00 00 000 000 0000, 0000 00 000 0000, 0
 000 0 00 000 000 0 0000. 00 000 00000 2.4GHz 0000 1, 6 0 11 00 000
 0 00 000 00000 0000 5GHz 0000 0000 00 000012.

□ □ □ □

1 - wifi □□□ □□□ □□□ □□□? - □□ □□

2 - Which 2.4GHz Wi-Fi channels 1, 6, 11 are non-overlapping? Select "three channels" 3, 4, 8 and 9 are overlapping - Super User

NEW QUESTION: 114

Which two statements are true?

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which two statements are true regarding PC A and PC B? Select two correct answers.

- A. PC A is connected to switch 1.
- B. PC B is connected to switch 2.
- C. PC A is connected to switch 2.
- D. PC B is connected to switch 1.

Answer: (SHOW ANSWER)

NEW QUESTION: 115

Which two statements are true regarding the IEEE 802.11 standard? Select two correct answers.

- A. 2.4GHz
- B. 5GHz
- C. 6GHz
- D. 900MHz

Answer: B (LEAVE A REPLY)

NEW QUESTION: 116

Which two statements are true regarding the IEEE 802.11 standard? Select two correct answers.

- A. 2.4GHz
- B. 5GHz
- C. 6GHz
- D. 900MHz

Answer: A (LEAVE A REPLY)

NEW QUESTION: 117

Which two statements are true regarding the IEEE 802.11 standard? Select two correct answers.

- A. DHCP □□
- B. □□ DHCP □□
- C. DNS □□ □□
- D. □□□ □□□ □□□□□□.

Answer: [\(SHOW ANSWER\)](#)

Each DHCP request with a different MAC address is regarded by the DHCP server as a new network client request. If the attacker sends an ample number of requests, the server's address pool will ultimately be exhausted. Hence, new network clients will be denied the DHCP service and will be unable to join the network.

NEW QUESTION: 118

□□ □ □□□ □ □□□ □□□□ □□ □□□ □□□ □□□□□?

- A. IPSec
- B. GRE
- C. VXLAN
- D. □□□

Answer: A [\(LEAVE A REPLY\)](#)

NEW QUESTION: 119

□□□□ □□□□□□ □□□ TCP □□□ □□□□□ □□□. □□□□□□ □□ □□□□ □□ □□ □□□□
□□ □ □□ □□□□?

- A. □□□□
- B. □
- C. ICMP □□ □□
- D. □□□□

Answer: A [\(LEAVE A REPLY\)](#)

If a network client is trying to connect to the wrong TCP port, the most likely response it would receive is a RST (reset) packet from the server. A RST packet is used to terminate a TCP connection abruptly, either because the server does not recognize the port number, or because the server has no application listening on that port, or because the server detects an error or an attack on the connection. A RST packet tells the client to stop sending any more data and close the connection immediately¹² The other options are not as likely to be the responses for connecting to the wrong TCP port. A FIN (finish) packet is used to gracefully end a TCP connection, after both parties have exchanged all the data they need. A FIN packet indicates that the sender has no more data to send and is ready to close the connection. A FIN packet does not imply an error or a rejection, but rather a normal termination of the connection¹² An ICMP (Internet Control Message Protocol) Time Exceeded message is used to inform the sender that a packet has been discarded because its time to live (TTL) value has reached zero. A TTL value is a counter that decrements by one every time a packet passes through a router. When the TTL value reaches zero, the packet is dropped and an ICMP Time Exceeded message is sent back to the sender. This message is used to prevent packets from looping endlessly in the network, and also to implement the traceroute tool, which shows the path and the hops that a packet takes to reach a destination. An ICMP Time Exceeded message is not related to the TCP port number, but rather to the IP routing and the TTL value³ A Redirect message is another type of ICMP message that is used to inform the

RFC 792: Internet Control Message Protocol

□□ Cat 5e □□□ □□ □□ □□□□ □□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□□ □□ □
 □ □□□□ □□□□□.

DEBUG □□□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□□□□. □□□ □□
 □□ □□□ □□ □ □□□ □□□ □□□□ □□□□ □□□ □ □□ □□□□□. □□□ □□□□ □□□□□
 □□□□ □□□ □□□□, □□ □ □□□□ □ □□□ □ □ □□□□. □□ □□□ □□ □□□□ □□□ □□
 □□□□ □□□□ □□□□□. □□ □□□□ □□ □□□ □□□ □□□ □□ □□□□. DEBUG □□ □□
 □□ □□□□, □□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□ □□□□
 □. DEBUG □□□□ □□□□□ □□ □□, □□□ □□□□ □□ □□□ □□ □□□ □□□□ □ □□□ □
 □ □□□□. □□□ DEBUG □□ □□□□ □□□□□ □□□ □□ □□□, □□ □□□□ □□□ □□□ □
 □□□ □□□ □□ □ □□□□. □□□ DEBUG □□□□ □□□ □□□□ □□□□ □□□□. □□: [CompTIA
 Network+ □□ □□ □□], □□ □□ □□ - Cisco

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

NEW QUESTION: 122

□□□ □□□ □□ □□ □□□ □□ □□□□ □□□□□.

□□ □ □ □□□ □□ □□ □□□□□?

A. □□

B. □□

C. □□

D. □□

Answer: D (LEAVE A REPLY)

The false camera is seen by people. They think it is real and this prevents them from doing something wrong.

NEW QUESTION: 123

An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

A. TFTP

B. TLS

C. SSL

D. SNMP

Answer: D (LEAVE A REPLY)

SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.

The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:

TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic,

email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.

Reference 1: What is SNMP? - Definition from WhatIs.com 2: Network+ (Plus) Certification | CompTIA IT Certifications 3: What is TFTP? - Definition from WhatIs.com 4: What is TLS? - Definition from WhatIs.com 5: What is SSL? - Definition from WhatIs.com

NEW QUESTION: 124

Which of the following is a routing protocol that uses IP as the transport protocol?

- A. EIGRP
- B. BGP
- C. IPv6
- D. MPLS

Answer: B ([LEAVE A REPLY](#))

BGP is a routing protocol that uses IP as the transport protocol. RIP, OSPF, and EIGRP are all IGP protocols.

NEW QUESTION: 125

Which of the following is a layer 2 protocol?

- A. Ethernet
- B. IP
- C. TCP
- D. UDP

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 126

Which of the following is a layer 3 protocol?

- A. Ethernet
- B. IP
- C. TCP
- D. UDP

Answer: D ([LEAVE A REPLY](#))

OSI is a layer 3 protocol. Ethernet, IP, TCP, and UDP are all layer 2 protocols.

OSI is a layer 3 protocol. Ethernet, IP, TCP, and UDP are all layer 2 protocols.

UDP is User Datagram Protocol. It is a layer 3 protocol.

- A.** □ □ □ □ □ □ □ □
- B.** □ □ □ □ □ □
- C.** □ □ □ □ □ □ □

Answer: C (LEAVE A REPLY)

□□□□: Network+ □□ □□□ □□ 1.4: TCP/IP □ □□ □ □□ □□

□□ □ □□ □□ □□ □ □□□□?

- A.** □ □ □ □ □ □
- B.** □ □ □ □ □ □
- C.** □ □ □ □
- D.** □ □ □ □
- E.** □ □ □ □ □

[illegible]

□□ □□□ VPN □□□□□□□ □□□ DHCP □□□ □□□□□.

□□□□ □□□□ □□ □□□ □ □□□ □□□□□ □□□ □□ □□□□ 300□ □□□, □ □ 252□□ □
□ □□ VPN□ □□□ □ □□□□. □□□□ □□ □□□□ □□ □□ VPN□ □□□ □ □□□□. □□ □□□□
□□□□ □□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □ □□□□?

- A.** □□□□□ □□□□□.
- B.** DHCP □□□ □□□□□□.
- C.** □□□ VPN □□□□□□□ □□□□□□
- D.** □ □□□ □□

Answer: A (LEAVE A REPLY)

□□

DHCP □□□□ □□ □□□ □□□ □□□□□□ IP □□ □□□ □ □□ □□□□ □□ □□ □□□□□□ □
□□ □ □□ IP □□□ □□□□□. □□□□: CompTIA Network+ □□ □□ □□□, 3□: IP □□ □□.

NEW QUESTION: 132

SIMULATION

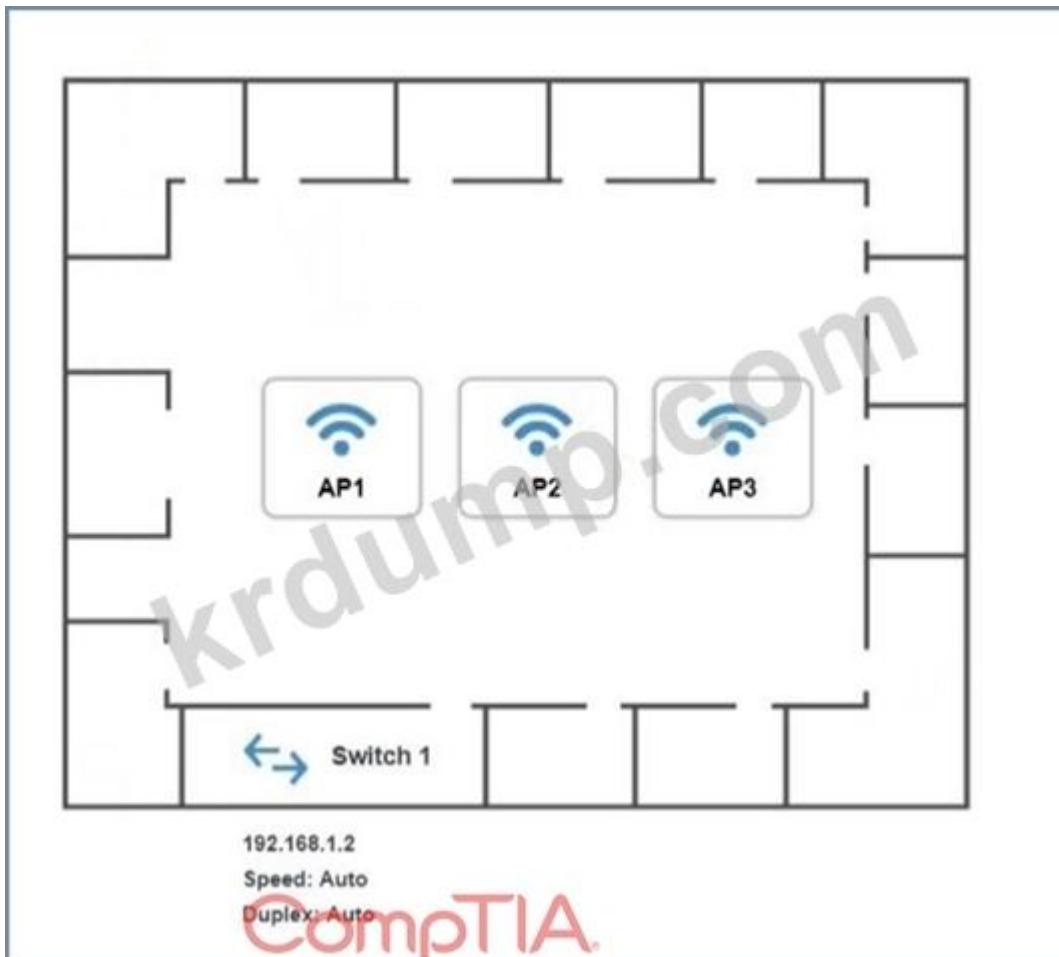
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

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



AP1 Configuration



https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
 G

Channel

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

CompTIA

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration



https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
 G

Channel

1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

Answer:

On the first exhibit, the layout should be as follows

The screenshot displays the 'AP1 Configuration' web interface. At the top, there is a blue header bar with the title 'AP1 Configuration' and a close button. Below the header is a navigation bar with back, forward, and refresh icons, followed by a URL field containing 'https://ap1.setup.do'. The main content area is divided into four sections: 'Basic Configuration', 'Wireless', 'Wired', and 'Security Configuration'. The 'Basic Configuration' section includes fields for 'Access Point Name' (AP1), 'IP Address' (192.168.1.32), 'Gateway' (192.168.1.1), 'SSID' (CorpNet), and 'SSID Broadcast' (Yes). The 'Wireless' section has 'Mode' (B) and 'Channel' (3) dropdown menus. The 'Wired' section has 'Speed' (100) and 'Duplex' (Full) radio button selections. The 'Security Configuration' section has 'Security Settings' (WPA2 - Enterprise) and 'Key or Passphrase' (S3cr3tl).

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name: AP1

IP Address: 192.168.1.32

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 3

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3tl

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.32 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B

Channel

3

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Security Configuration

Security Settings

☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto ☐ 100 ☐ 1000

Duplex

☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings

☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

Exhibit 2 as follows
Access Point Name AP2

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

192.168.1.64

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

6

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3tl

AP2 Configuration

CompTIA

https://ap2.setup.do

IP Address: 192.168.1.4 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 6

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

Exhibit 3 as follows
Access Point Name AP3

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

9

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

AP3 Configuration

https://ap3.setup.do

IP Address
192.168.1.5 / 27

Gateway
192.168.1.1

SSID
CorpNet

SSID Broadcast
☒ Yes ☐ No

Wireless

Mode
G

Channel
9

Wired

Speed
☒ Auto ☐ 100 ☐ 1000

Duplex
☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings
☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase
S3cr3t!

Reset to Default
Save
Close

NEW QUESTION: 133

A network administrator is configuring a new network. The network is a 10.0.0.0/16 network. The administrator wants to use a 10.0.0.0/24 network. Which of the following is the correct configuration?

A. 10.0.0.0/16

B. 10.0.0.0/24

C. 10.0.0.0/24

D. 10.0.0.0/24

- A. 10.0.0.0/16
- B. 10.0.0.0/24
- C. 10.0.0.0/24
- D. 10.0.0.0/24

Answer: (SHOW ANSWER)

A

The network administrator is configuring a new network. The network is a 10.0.0.0/16 network. The administrator wants to use a 10.0.0.0/24 network. Which of the following is the correct configuration?

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

NEW QUESTION: 134

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

- A. 12.1.1.1
- B. 12.1.1.1
- C. 12.1.1.1
- D. 12.1.1.1

Answer: (SHOW ANSWER)

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

<https://www.comptia.org/blog/what-is-a-honeypot>

NEW QUESTION: 135

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

- A. 12.1.1.1
- B. 12.1.1.1
- C. NIC 12.1.1.1
- D. 12.1.1.1

Answer: A (LEAVE A REPLY)

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

<https://www.educba.com/sql-cluster/>

NEW QUESTION: 136

Which of the following is a valid IPv4 address? NAT is not a valid IPv4 address.
12.1.1.1: IP address 12.1.1.1 is a valid IPv4 address. 2: 12.1.1.1(NAT) is not?

- A. VIP
- B. NAT
- C. APIPA
- D. IPv6 12.1.1.1
- E. 12.1.1.1 IP

Answer: A (LEAVE A REPLY)

□□ □□ □□ □□□□ □□ IP(VIP) □□□ □□□□ □□□. VIP □□□ □□ □□ □□□□ □□ □□□ □□□ □□ IP □□□□□. □ □□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□□ VIP □ □□ □□ □□□ □□□□□ □□□□□□ □□ □□ □□□□ □□ □□□□ □ □□□□.

□□:

CompTIA Network+ □□ □□ □□□, □□ N10-007, 4□, 6□: □□□□ □□, p. 300

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□ □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 137

□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□ □□□ □ □□□□□. □□□□ □□ □□□□ □□□□□□□ □□□□ □□□ □□ □ □□ □□□ □□□□□□□.

□□ □ □□□□ □ □□□ □□□ □□□ □□□ □□ □□□□□?

- A. □□□□ □□□ □□□□ □□□ □□□□ □□□□□.
- B. □□□□ □□ □□□ □□□□□ □□□□ □□□□□.
- C. □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□□.
- D. □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 138

□□□□ □□ □□□ □□□□□, □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□.
□□ □□□□ □□ □□□□ □□□ □□ □□□□ □□□ □□□□□ □□□□ □□□□□. □□□□ □□ □ □□ □□□ □□□□ □□□?

- A. 802.11ac
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: ([SHOW ANSWER](#))

802.11ac□ □□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□□. 802.11b/g/n□ □□ □ □□□ □□□□□□ □□ □□□□□ □□□ □ □□□□□. 802.11b□ □□ □□□□ □□ □□ □□□□, 802.11g□ □ □□□□ □□□ □□□□□, 802.11n□ □ □□□□ 802.11ac□□ □□□□ □□ □□□ □□□ □□.

NEW QUESTION: 139

A network administrator needs to query the NSs for a remote application. Which of the following commands would BEST help the administrator accomplish this task?

- A. dig
- B. arp
- C. show interface
- D. hostname

Answer: (SHOW ANSWER)

The Linux/Unix dig (short for domain information groper) utility does the exact same thing as nslookup. It's primarily a command-line utility that allows you to perform a single DNS lookup for a specific entity, but it can also be employed in batch mode for a series of lookups.

NEW QUESTION: 140

□□□□ □□□□ □□ □□□□□ □□ □□□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□ □□□ □□□□ □□ □□□. □□ □ □□ □□ □□□□ □□□□ □□□ □□ □□□ □□□ □ □□ □□□?

- A. FTP
- B. TFTP
- C. SMTP
- D. SFTP

Answer: D (LEAVE A REPLY)

SFTP□ Secure File Transfer Protocol□ □□□, SSH(Secure Shell) □□□ □□ □□□□ □□□□ □□ □□ □ □□□□ □□□□ □□□□□□□. SFTP□ □□ □□ □□□ □□ □□□□□ □□□ □□□ □ □□□, □ □□□□□ □□ □□□ □□ □□ □ □□ □□ □□□□□ □□□□□.

FTP, TFTP, SMTP□ □□ □□ □□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□ □□□□. FTP(□□ □□ □□□□)□ TFTP(□□ □□ □□ □□□□)□ □□□ □□ □□□ □□□□ □ □□□□ □□ SMTP(□□ □□ □□ □□□□)□ □□□ □□□□ □□□ □□ □ □□□□□. □□□ □□□□□ □□□□ □□ □□□□□, □□□□□, □□□□□ □□□ □□□□□ □□□, □□□, □□□□□ □□□□ □ □□□□. □□:

CompTIA Network+ N10-008 □□ □□□, 4□: □□□□ □□□□ □ □□□, p. 173-174 Professor Messer□ Network+ N10-008 □□ □□, □□ 1.3: □□□□ □□□, p. 14 Professor Messer□ Network+ N10-008 □□□ □□ □□, 1.3 □□□□ □□□ - 2□, 8:00-9:00

NEW QUESTION: 141

□□□□ □□ □□□□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□. □□□□□ □ □□□ □□□ □ □□□ SSID□ □□□□□□□□□□ □□□□□. □□□□ □ □□ □□□ □□ □□ □ □□ □□ □□□□ □□□?

- A. MIMO
- B. □□
- C. □□ □□
- D. □□ □□□ □□

Answer: (SHOW ANSWER)

ESSID(ESS)은 SSID와 함께 무선 LAN을 구성하는 데 사용되는 이름입니다.
ESSID는 AP의 이름을 나타냅니다. ESSID를 사용하여 무선 LAN을 구성할 수 있습니다.
ESSID를 사용하여 무선 LAN을 구성할 수 있습니다.

NEW QUESTION: 142

□□□□ □□ □□□□□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□ □□□. □□ □
□□ □□□ □□ □□ □ □□□□□□?

- A.** □ □ □ □ □ □
- B.** □ □ □ □ □ □ □
- C.** □ □ □ □ □ □
- D.** □ □ □ □ □ □ □ □ □

Answer: (SHOW ANSWER)

NEW QUESTION: 143

□□□□ LACP □□□ □□□ □□□□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□ □□ □ □□
□□□□?

- A.** □□□□□ □□
- B.** □□ □□
- C.** □□
- D.** arp □□

Answer: (SHOW ANSWER)

show interface GigabitEthernet0/29, 30, GigabitEthernet0/31
GigabitEthernet0/29. 802.1Q VLAN ID= 100,
GigabitEthernet0/30. 802.1Q VLAN ID= 100,
GigabitEthernet0/31.

[illegible]

LACP(Link Aggregation Control Protocol)□ □□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □□□
□ □□□ □□□□ □□□ □ □□ □□□□□□□. LACP□ IEEE 802.3ad □□ EtherChannel□□□□ □□
□.

show config , IP , ,

LACP .

```
show route 0.0.0.0 0.0.0.0, 0.0.0.0 0.0.0.0, 0.0.0.0 0.0.0.0, 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0. LACP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0.
```

```
show arp [interface] [protocol] [IP] [MAC] [show] [detail] [ARP]([interface]
[protocol]) [show] [detail] [LACP] [show] [detail] [show] [show]:
```

CompTIA Network+ N10-008 ☐☐ ☐☐☐, 2☐: ☐☐☐☐ ☐☐ ☐ ☐☐, ☐☐ 2.1: ☐☐☐ ☐☐☐☐ ☐☐☐ ☐☐
☐ ☐☐ ☐☐, 77-78☐☐☐ Messer ☐☐☐ Network+ N10-008 ☐☐ ☐☐, 13☐☐☐ Messer ☐☐☐ Network+
N10-008 ☐☐☐ ☐☐ ☐☐, ☐☐ 2.1: ☐☐☐☐ ☐☐, ☐☐☐ 2.1.6: ☐☐ ☐☐

NEW QUESTION: 144

Which of the following is a valid IPv4 address?

- A. 192.168.0.0
- B. 192.168.0.1
- C. 192.168.0.255
- D. 192.168

Answer: B ([LEAVE A REPLY](#))

IPv4 addresses are 32-bit numbers, typically written in decimal notation, separated by dots. The four octets of an IPv4 address range from 0 to 255. 192.168.0.0 is a valid IPv4 address, but it is a reserved address for private networks. 192.168.0.1 is a valid IPv4 address for a host. 192.168.0.255 is a valid IPv4 address, but it is a reserved address for broadcast. 192.168 is not a valid IPv4 address because it only has three octets.

NEW QUESTION: 145

Which of the following is a valid MAC address?

- A. 802.11ac
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: ([SHOW ANSWER](#))

802.11ac is a Wi-Fi standard, not a MAC address. 802.11b/g/n are Wi-Fi standards, not MAC addresses. 802.11b is a Wi-Fi standard, not a MAC address. 802.11g is a Wi-Fi standard, not a MAC address. 802.11n is a Wi-Fi standard, not a MAC address. 802.11ac is a Wi-Fi standard, not a MAC address.

NEW QUESTION: 146

Which of the following is a valid IPv4 address?

- A. 192
- B. 192.168
- C. 192.168.0.0
- D. 192.168.0.1

Answer: A ([LEAVE A REPLY](#))

192 is a valid IPv4 address, but it is a reserved address for private networks. 192.168 is not a valid IPv4 address because it only has two octets. 192.168.0.0 is a valid IPv4 address, but it is a reserved address for private networks. 192.168.0.1 is a valid IPv4 address for a host.

□□, □□□, □□□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□. □□□ □□□□ □□□□□ □
□□ □□□ □□□□ □□□□ □□□ □□□ □ □□□□.

□□□□:

* □□ □ □□□ □□ - CompTIA Network+ □□(N10-008): □□ □□ □□□

* CompTIA Network+ □□ □□ □□, 141□□□

NEW QUESTION: 147

□□ □ □ □□ □□ □□ □□ □□□□ □ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□? (□ □□ □
□□□□)

A. IDS

B. □□ □□

C. 2□□ □□□

D. 3□□ □□□

E. □□□

F. □□□ □□□

Answer: D,E ([LEAVE A REPLY](#))

* □□□ 3 □□□□ □□□□ □□□ □□□ □□ □□□ □□□□□. □□ IP □□□ □□□□ □□□
□□□ □ □□□, □□ □□ □□ □□□□□ □□□□ □ □□□□ □□□□□. □□□ 3 □□□□ □□ □□□
□□□□ □□ □□□ □□ □□□□□ □□ VLAN□ □□□□ □□□ □ □□□□. □□□ □□□ 3 □□□□
□ □□ □□ □□ □□□□ □□ □□□ □□□ □ □□□□.

* □□□□ □□ IP □□□□□ □□□□ □□□ IP □□□ □□ □□□ □□□□ □□□□□. □□□□ □□ □
□□□ □□ □□(NAT)□ □□□ □ □□□, □□ □□ □□ IP □□□ □□ □□□ □□ IP □□□ □□ □□□
□□□ □ □□□□. □□□ □□□□ □□ □□ □□ □□ □□□ □□□□ □□ □ □□ □□ □□ □□ □□□
□ □□ □□□ □□□ □ □□□□.

* IDS(□□ □□ □□□)□ □□□□ □□□□ □□□□□□ □□□□□□ □□□□□ □□□ □□□□ □□□
□□. IDS□ □□□ □□□□□ □□ □□□□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□
□□ □□□□□ □□ □□□ □□□□.

* □□□□ □□□□ □□ □□□ □□ □□□□□ □□□ □ □□□ □□ □□□□□. □□□ □□□□ □□□ □
□□□□ □□ □□□□ □□ □□□ □□□□ □□□, □□□□□ □□ □ □□ □□□□ □□ □□□ □□□
□□□.

* □□□ 2 □□□□ □□ MAC □□□ □□□□ □□□□ □□□□ □□□, □□ □□□ □□□□□□ □□ □
□□ □□□□ □ □□□□ □□□□□. □□□ 2 □□□□ □□□□□ □□□□ □□□□ □□□□ □□□□
□□ □□ □□□□□□ □□ □□□ □□□ □ □□□□.

* □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□□. □□□□ □
□□□□ □□□ □□□□□ □□ □□□□ □□ □□□ □□□□ □□□, □□□□ □□□□□□ □□ □□□ □□
□ □□□□□ □□□ □ □□□ □□□.

□□□□:

* □□□□ □□

* □□□ □ □□□ □□ □□

* CompTIA Network+ N10-008 □□ □□□, 2□: □□ □ □□□, 58-63, 72-75□□□.

NEW QUESTION: 148

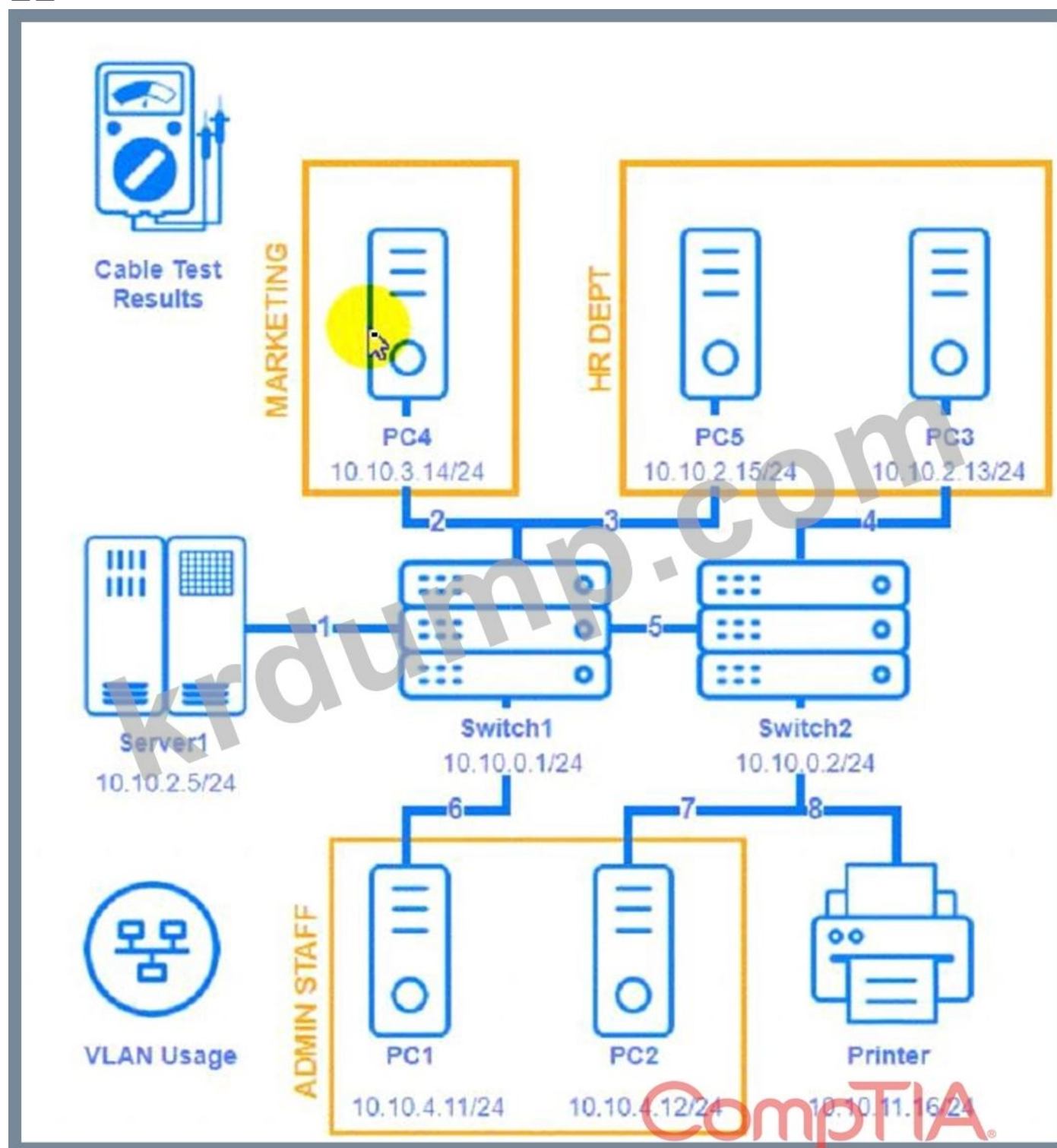
A small SOHO network is shown in the exhibit. The network is configured with a single VLAN. The network administrator is troubleshooting a connectivity issue. The network administrator is unable to ping PC4 from the network administrator's workstation. What is the most likely cause of the problem?

A. The network administrator's workstation is not configured with the correct IP address.

B. The network administrator's workstation is not configured with the correct subnet mask.

C. The network administrator's workstation is not configured with the correct default gateway.

D. The network administrator's workstation is not configured with the correct DNS server.



PC1 - ADMIN STAFF



C:\>

CompTIA

krdump.com

PC4 - MARKETING



C:\>

krdump.com

CompTIA

PC5 - HR DEPT



C:\>

CompTIA

krdump.com

Server1



C:\>

krdump.com

CompTIA

□□□ □□□ □□:

□□□ 1:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 22M VLAN: VLAN 2 Speed: 1000 FDX Port: GigabitEthernet0/1							

□□□ 2:

Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 103M VLAN: VLAN 3 Speed: 1000 FDX Port: GigabitEthernet0/4						

□□□ 3:

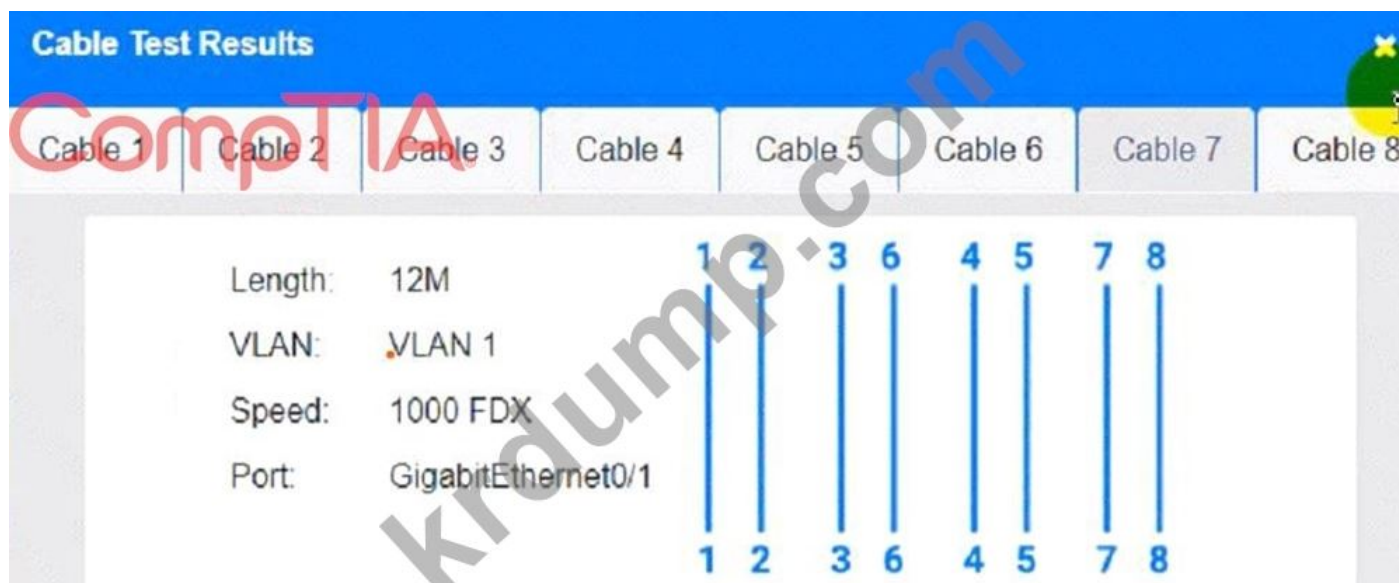
Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 18M VLAN: VLAN 2 Speed: 1000 FDX Port: GigabitEthernet0/3							

□□□ 4:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 20M VLAN: VLAN 1 Speed: 1000 FDX Port: GigabitEthernet0/2							

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 16M VLAN: VLAN 1 Speed: 1000 FDX Port: GigabitEthernet0/5							

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 42M VLAN: VLAN 4 Speed: 1000 FDX Port: GigabitEthernet0/2							





HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC, http://192.168.2.9
Firmware Revision	FDP1CN1347A
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c:b6:54:4d:30:ec
------------------------	-------------------



Internet

Not Connected

802.3 Wired

Hardware Address (MAC)

9c:b6:54:4d:30:ec

Link Configuration

None

IPv4

IP Address

10.10.11.56

Subnet Mask

255.255.255.0

Default Gateway

10.10.11.1

Configuration Source

DHCP

Primary DNS Server

8.8.8.8

Secondary DNS Server

8.8.4.4

Total Packets Transmitted

15655

Total Packets Received

394068

CompTIA

GRE □□□□□ □□□□□ □□□ □□□ □□□ □□□ □ □□ □□ □ □□□ A. □□ □□□□□□. □□ □□□□ □□□□ □□□ 1500□□□□□ □ □□□ □□□□□, □□□□ □□ □□ □□ □□(MTU)□□□. □□ □□□□ □□□□ □ □□□□ □ □□ □□□□ □□□ □ □□ □□□□ □□□ □□□ □□□□ □□□ □ □□□□.

□□ □□ □□ □□□□□(MDI), □□□□□ □□□□□ □ □□ □□□ □□□ □□ □□ □□□ □□□ □□ □□□ GRE □□□□□ □□□□□□ □□□ □□□ □□□□□.

NEW QUESTION: 153

□□□ □□ □□□□ □□□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□ □
□□ □□□□□ □□ □ □□□□□?

- A.** □□ □□□ □□□□ □□□□□□ □□□□□□□.
- B.** □□ □□□ NDA□ □□□□□ □□□□□.
- C.** □ □ □□ □□□□ □□□ □□□□□ MAC □□□□ □□□□□□.
- D.** □□ □□□ Wi-Fi □□□ □□□□ □□ □□□ □□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 154

□□□□ □□□□ □□ DNS □□□□ □□□□□ □□□ □□□□ □□□. □ □□□ □□□□ □□ □□□□
□□□□□□□□ □□ □□□□ □ □□ □□ □□□□ □□□□ □□□□?

- A.** NS
- B.** □□□ □□ □□□□(SOA)
- C.** □□
- D.** □□

Answer: A ([LEAVE A REPLY](#))

NS Name Server
□□□, □□□□ □□ □□ □□□ □□□ □□□□ DNS □□□□□□. □□□□
□□□ □□ □ □□□ □□□□ □□□□, □ □□□□ □□ NS □□□□ □□ □□□□□. □□ DNS □□□□
□□□□□ □□□ □□□□□ □□□□ □□□□ □□□□ NS □□□□ □□□□ □□ DNS □□□□ □□□
□ □ DNS □□□ □□□□ □□□.

11

DNS □□□ □□ - N10-008 CompTIA Network+ : 1.61

CompTIA Network+ N10-008 □□ □□□, 1472□□□

NEW QUESTION: 155

□□□□ □□ □□ SSiD □□ □□□□□ □□□ □□□ SSiD □□□ □□□□ □□□□. □ □□□ □□ □
□ □□ □ □□ □□□ □□□□□?

- A.** □□□ □□
B. □□ □□□ □□
C. WPA
D. MU-MIMO

Answer: A (LEAVE A REPLY)

□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □ □□□ □□□(AP)□□ □□ □□□ □□□
(AP)□ □□□ □ □□ □□□ □□□□.

□□ □□□□□ □□ SSID□ □□□□ □□ □ SSID□ □□ □□ □□, □□□□ □□ □ □□ □□□□□ □□
□□□□ □□□□□ □□□□□□2.

□, □□ □□□ □□ AP □□ □□□ □ □□□ SSID□□ □□□ □□ □□ SSID□ □□ □□□□ □□, □□ □□ □□ □ □□ □□□ □□□ □ □□□□.

[illegible]

□□□ □□ □□□ □□□ SSID□ □□□□□□□□ □□ AP□ □□□□, □□ □□□□□ □□ □□□□□□
□□□□□□ □□□ □□ AP □□ □□□ □ □□□□.

□□ □□ □□□ □□□□ □□ □□□□□ □□□□□ □□□□□ □□□□□.2 □□:

1: CompTIA Network+ N10-008 ☐☐ Cram, 6☐, 6☐: ☐☐ ☐☐☐☐ ☐☐, p. 212

2: CompTIA Network+ N10-008 □□ □□□, 1□, 9□: □□ □□□□ □□ □ □□ □□, 367-368□

NEW QUESTION: 156

00 00 ISP 00 00 00 00 000 0000 00000. 000 0000 000 00000 000
 00 00 00 000-00 000 00000 000 00 AP 00000. 0 0000 000000 000
 AP 00 0000 00 000 00000. AP 00000000 000 00 000 0000 0000. 0
 00 0000 000 000 000 00 0000 00 000000 00000. 000 0000 00 0
 0 000 00000 000?

- A.** □□□□□□ □□□□□□ □□□□□□.
- B.** □□□ □□□ □□□□ □□□□□.
- C.** □□□ □□□□ □□□□□.
- D.** □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

□□□ □□□□ □ □□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□□□. □□□ □□□
□ □ □□□ □□□□ □□ □□□□ □□ □□□□ □□□ □ □□ □□, □□, □□ □□ □□ □□ □□□ □□
□□□. □□□ □□□□ □□ □□ □□□ □□□□□ □□□□ □□□□ □ □□ □ □□□ □□□□ □□ □
□□ □□ □□ □□□ □□□ □□□ □□ □□□□ □□□□. □□□ □□□ □□ □□□□ □ □□□ □□□
□□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□□ □ □□□□.

NEW QUESTION: 157

□□□□□ □□ □□□□□ □□ □□ UPS□ □□□□ □□□□ □□ □□□□ □□□□ □□□□. □□□□
□ □□ □□□□ □□□□ □□□□ □□□□ □ □□□ □ □□ □□□□ □□□□□?

- A.** ☐☐ ☐☐
- B.** NetFlow ☐☐☐
- C.** SNMP ☐☐
- D.** ☐☐☐☐☐ ☐☐

Answer: (SHOW ANSWER)

Which of the following is a valid IPv4 address? (Select two.)
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

NEW QUESTION: 158

Which of the following is a valid IPv4 address? (Select two.)
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 is a valid IPv4 address? (Select two.)
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

- A. 192.168.22.1
- B. 192.168.22.15
- C. 192.168.22.10
- D. 192.168.22.100

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 159

Which of the following is a valid IPv4 address? (Select two.)
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

- A. 7 10 10 10
- B. 6 10 10
- C. Cat5
- D. 10 10 10 5e

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 160

Which of the following is a valid IPv4 address? (Select two.)

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 is a valid IPv4 address? (Select two.)

- A. ARP 10 10
- B. VLAN 10 10
- C. 10 10 10 10 10
- D. 10 10 10 DoS

Answer: A ([LEAVE A REPLY](#))

Which of the following is a valid IPv4 address? (Select two.)

Which of the following is a valid IPv4 address? (Select two.)
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

□□□. □□ □□ □□□□ □ □□ □□ □□□□ □□□□ □□□□ □□□
□□ □ □□□□. □□□ □□□ ARP □□□ □□ MAC □□□ □□ □□□ IP □□(192.168.1.1)□ □□ □□
□□□ □□□ □□□□□. □□ □□□□ □□ ARP □□□ □□ □□□ □□ MAC □□□ □□ □□(□: □□
□□□□□)□ IP □□□ □□□□ □□□ □□ □□□ □□ □□□□□. □□:

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

NEW QUESTION: 161

□□□□ □□□□ □□ □□ □□□□ □□ □□ IDF□ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□
□□ □□□□□□ □□□? (□ □ □□)

- A. □□□ □□ □□ □□
- B. BYOD □□
- C. □□ □□ □□
- D. □□ □□ □□
- E. □□ □□ □□
- F. □□□ □□□□ □□□□□

Answer: E,F ([LEAVE A REPLY](#))

□□ □□ □□□ □□, □□, □□, □□□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□ □□
□ □□□□ □□ □□□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□, □□ □ □□ □□, □□□
□□□ □□, □□□ □ □□ □□ □□, □□□□ □□ □ □□□ □□□□□ □□□□□. □□ □□ □□□
MDF(Main Distribution Frame)□ □□ □□□ □□□□ □□□□ □□ IDF(Intermediate Distribution Frame) □
□□ □□ □□□□ □□□□, □□ □□ □□□ □□ □□□ □□□□□ □□□□□□ □□□. □□ □□ □□
□ □□□□□□ □□□□ □□□□ □□ □□ □ □□□□□ □□□□ □ □□□ □□ □□□□ □□ □□□ □
□ □ □□□□.

□□□ □□□□ □□□□□□ □□□, □□□, □□□, □□, □□□□□□, □□□, □□□□ □□ □□□□ □
□□ □□□ □□□□□ □□□ □□□□□ □□□ □□□□. □ □□□ □□, □□, IP □□, MAC □□, □□ □
□□ □ □□□□ □□, □□, □□□ □□□□□. □□□ □□□□ □□□□□□ □□□□□ □ □□ □□□ □
□□□ □□□□ □□ IDF □□□ □□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□□ □□□. □□
□ □□□□ □□□□□□ □□□□□□ □□□□ □□□□ □□□□ □□□ □□□ □□ □□, □□□□ □ □
□□□□ □ □□□ □□□.

□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□ □□□□ □□ □□ □□□, □□, □□ □□ □□□
□□□□ □□ □□□ □□□ □□□□ □□□□□. □□□□ □□□ □□, □□□ □ □□ □□, □□□ □□ □
□□ □□□□, □□ □ □□ □□, □□ □□ □ □□ □□□□□ □□□□□. □□□ □□ □□ □□□ □□ IDF
□□□ □□□□□ □□□□□ □□□ □□□□. □, IDF□ □□□□□ □□□ □□□□ □□□□ □□□ □□
□□ □□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□.

BYOD(Bring Your Own Device) □□□ □□□□, □□□, □□ □□ USB □□□□□ □□ □□ □□□ □□□
□ □□□ □□□□ □□□□□. □□□□ □□□ □□ □□ □ □□ □□, □□□□ □□□ □ □□ □□, □□□
□□ □ □□, □□ □ □□ □□ □□□, □□ □ □□□ □□□ □□□□□. BYOD □□□ □□ IDF □□□ □□
□□□ □□□□□ □□□ □□□□. □, IDF□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□□ □□
□□□ □□□ □□□□ □□ □□□ □□□ □□ □□□.

□□ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□ □□
□ □□□ □□□□□. □□□□ □□□□□ □□□ □□, □□ □□□ □□□ □□, □□□ □□ □□□ □□, □
□□□ □□ □ □□□ □□□□□. □□ □□ □□□ ID□ □□□□□ □□□□ □□□ □□□□ □□ □ □□
ID□ □□□ □□□□□ □□□□□ □□□ □□□□. □ □□ □□□ □□□□□ □□ □□□ □□□ □□□ □
□□.

□□ □□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□□ □
□ □3□□ □□□□ □□□ □□□□ □□ □□□□□. □□□□ □□ □□□ □□ □ □□, □□ □□ □ □□,
□□ □ □□, □□□ □ □□ □□, □□□□ □□ □ □□□ □□□□□. □□ □□ □□□ □□ ID□ □□□ □
□□□□ □□□□□ □□□ □□□□. □, ID□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□
□□□□□ □□□□ □ □□□ □□□□ □□□. □□:

CompTIA Network+ N10-008 □□ □□□, 3□: □□□□ □□, □□ 3.1: □□□ □ □□□□□□ □□□ □□,
131-136□□□ Messer □□□ Network+ N10-008 □□ □□, 20□□□ Messer □□□ Network+ N10-008 □□
□ □□ □□, □□ 3.1: □□□□ □□□, □□□ 3.1.1: □□□□ □□□ □□

NEW QUESTION: 162

Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

- A. QoS
- B. RIPv2
- C. STP
- D. OSPF

Answer: (SHOW ANSWER)

NEW QUESTION: 163

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

- A. Incorrect VLAN setting
- B. Improper NIC setting
- C. Duplicate IP address
- D. Insufficient DHCP scope

Answer: D (LEAVE A REPLY)

NEW QUESTION: 164

□□□□ □□□□□ □□ □□□□ □□□ □□ □□□ □□ □□□□□.
□□□□ □□□ □□□□ □ □□ □□□□ □□□□ □□□□□.
□□□□□□□ LACP □□
□□□ □□□□□□□ □□□ □□□ □□□□□.
□□ □ □□□□ □□□□ □□ □□ □□□□□?

- A. □□ □□□

- B. □□ □□
- C. NIC □ □□
- D. □□□□□

Answer: C (LEAVE A REPLY)

NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)),

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming>

NEW QUESTION: 165

□□□ □ □□ □□□□□ □□□□□□ □□ □□□ □□□□ □□□□□. □ □□□□ □□□□□ □□□ □ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□ □ □ □□ □□□ □□□□ □□ □ □□□□?

- A. CVE
- B. SSO
- C. Exploits
- D. Zero day

Answer: A (LEAVE A REPLY)

NEW QUESTION: 166

□□□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □ □□ □ □□□ □□ □□□ □□ □ □□□□□□. □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□□ □□□□□ □□□□ □□□□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□□. □□□□ □□□ □□□ □□□□ □□ □□ □□□□ □□ □ □□ □□□□?

- A. □ □□ □□ □□ □□□ □ VPN□ □□ □□□□ □□□□□-□□□ □□□□□□ □□ □□ □□ □□□□ □□ □□□□□.
- B. □□ □□□ □□ □□□□ □□□ □ □□□□□ □□ □□□□□-□□□ VPN□□ □□ □□ □□ □□□□ □□□□□.
- C. □ □□ □□ □□ □□□□□-□□□ VPN □ □□ □□ □□ □□□□ □□ □□ □□□□ □□□-□□□ □ □□□□
- D. □□□ □□ □□ □□ □□□ □ VPN □ □□ □□ □□ □□□□ □□ □□ □□□□ □□□ □ □□□□□

Answer: A (LEAVE A REPLY)

□□□□□ □ □□ □□ □□ □□□ □ VPN□ □□ □□ □□ □□□□ □□ □□□ □□□ □□ □□□□□ □ □□□□□□ □□□□ □□□ □□ □□□ □□□ □□□□ □□ □□□□. VPN(□□ □□□)□ □□□□ □ □□ □□□□□ □□ □□□□ □□□□ □□□ □□□ □□□□□. □□ □□□□ □□□□ □□ □□□ □ □□ □□□□□ □□□□ □ □□□ □□□. □□□□ □ VPN□ □ □□□□ VPN □□□□□ □□□ □□ □□ □□□ □□□ □□□ □□ □ □□□ □□□□□ □□□□□. □□□□□ □ VPN□ □□□ □□□□ □□ □□□□ □□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □□□□□. □ □□□□□

NEW QUESTION: 169

A network engineer is configuring a 802.11ac AP in a multi-tenant environment. The engineer wants to ensure that the AP is configured to operate in the 5GHz band and that the channel width is set to 40MHz. The engineer also wants to ensure that the AP is configured to operate in the 802.11n mode. Which of the following configurations is correct?

- A. EIRP is set to 100mW, channel width is set to 40MHz, and mode is set to 802.11n.
- B. 802.11n is selected, channel width is set to 40MHz, and mode is set to 802.11ac.
- C. Channel width is set to 40MHz, mode is set to 802.11n, and EIRP is set to 100mW.
- D. Channel width is set to 40MHz, mode is set to 802.11ac, and EIRP is set to 100mW.

Answer: C (LEAVE A REPLY)

* The correct configuration is to set the channel width to 40MHz, mode to 802.11n, and EIRP to 100mW. This configuration ensures that the AP is configured to operate in the 5GHz band and that the channel width is set to 40MHz.

* The 802.11n mode is selected, and the channel width is set to 40MHz. The AP is configured to operate in the 802.11n mode, which is a legacy mode. The 802.11ac mode is not selected, which means that the AP is not configured to operate in the 5GHz band. The EIRP is set to 100mW, which is the maximum power level for a 802.11n AP.

* EIRP is set to 100mW, channel width is set to 40MHz, and mode is set to 802.11ac. EIRP is Effective Isotropic Radiated Power, which is the power level of the AP. The channel width is set to 40MHz, which is the maximum channel width for a 802.11ac AP. The mode is set to 802.11ac, which is the latest mode for a 802.11ac AP.

* Switching to 802.11n, disabling channel auto-selection, and enforcing channel bonding on the configuration is also not the best solution, because it may degrade the performance and compatibility of the WLAN. 802.11n is an older standard than 802.11ac, which has lower maximum data rates and fewer features. Disabling channel auto-selection may prevent the AP from adapting to the changing environment and finding the optimal channel. Enforcing channel bonding may increase the bandwidth, but it may also increase the interference and reduce the number of available channels.

* Deactivating the band 5GHz to avoid interference with the government radio is not the best solution, because it may limit the functionality and capacity of the WLAN. The 5GHz band has more channels and less congestion than the 2.4GHz band, which makes it suitable for high-performance applications and devices. Deactivating the band 5GHz may force the WLAN to use only the 2.4GHz band, which may reduce the speed, range, and reliability of the wireless network. References:

- * Channel Bonding
- * Dynamic Frequency Selection
- * Radio Regulations
- * [EIRP Calculator]
- * [EIRP and Regulatory Domains]
- * [802.11n vs 802.11ac]
- * [Channel Auto-Selection]
- * [Channel Bonding and Interference]

- * [5GHz vs 2.4GHz]
- * [5GHz Band Deactivation]

NEW QUESTION: 170

□□□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□□□ □□□□□□.

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

□□□ □□□ □□□ □ □ □ □, □□□□□ □□ □□ □□□ □ □□□ □□□□ 5GHz □□□□□ □□ □ □□□ □□□ □□ □□□ □□□□ □□□□□□. '□□□ □□□□ □□ □□□□□ □□ □ □□ □□□ □ □□ □□□?

- A. □□□ □□ □□ □□
- B. 2.4GHz□ □□□□□ □□□□□ □□□□□□.
- C. WPA3□ □□□□□□□□.
- D. □□□ □□□□ □□-

Answer: (SHOW ANSWER)

□□

5GHz □□□□□□ □□ □□ □ □□ □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □□ □□. □□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□□□□. □□□ □□□□ □□ □□□ □□□□□□ □□□ □ □□ □□□□□ □□□ □□ □□□ □□□□□. □□□□□ □ □□ □□□□ 2.4GHz □□□□□□ □□□ □□ □□□□ □□ 5GHz □□□□□ □□ □□□ □□□□ □ □ □□ □□ □□ □□ □□□□. □□□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□ □□□□. □□ □□: CompTIA Network+ N10-008 □□ □□ □□□, 76□□□; □□ CompTIA Network+ □□ □□□(□□ N10-008), 2-19□□□.

NEW QUESTION: 171

□□□□ □□ □□□□ □□□ □□ □□□□ □□□□ □□□ □□□ □□ □□□ □□ □□ □□□□ □□. □□ □□□□□ □□ □□□ □□□□ □□□□□. □□□□ □□□□ □ □□□ □□□□ □□ □□ □ □□□ □□□□ □□ □□ □□□□□?

- A. □□ □□ □□ □□
- B. □ WAP □□
- C. SSID□ □□□ □□□□ □□
- D. □□ □□ □□□□ □□□□

Answer: (SHOW ANSWER)

□□ □□□□□ □□ □□□ □□□ □□□□ □□□ □□ □ □□□□5. □□□ □□ □□□□ □□□□ □□ □ □□□ □□□ □□ □□□ □□ □□ □□ □□ □□□□ □□□□□ □□□□□ □□□□ □□ □ □□□□. □□ □□ □□□□□ □□□□□□ □ □□□ □□□ □ □□□□.

DHCP 192.168.0.0/24 192.168.0.1~192.168.0.254 IP 192.168.0.1. 192.168.0.1, 192.168.0.2 192.168.0.3 192.168.0.4 192.168.0.5. 192.168.0.6 DHCP 192.168.0.7 IP 192.168.0.8 192.168.0.9 192.168.0.10 169.254.0.1~169.254.255.254 192.168.0.11 APIPA 192.168.0.12 192.168.0.13. APIPA 192.168.0.14 192.168.0.15 192.168.0.16 192.168.0.17 192.168.0.18 192.168.0.19. 192.168.0.20 APIPA 192.168.0.21 192.168.0.22 192.168.0.23 DHCP 192.168.0.24 DHCP 192.168.0.25 IP 192.168.0.26 192.168.0.27.

NEW QUESTION: 174

Which of the following is the LARGEST MTU for a standard Ethernet frame?

- A.** 1452
B. 1492
C. 1500
D. 2304

Answer: C (LEAVE A REPLY)

The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\),](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),)

https://en.wikipedia.org/wiki/Maximum_transmission_unit

NEW QUESTION: 175

[illegible]

- A. OSPF**
B. RIPv2
C. EIGRP
D. BGP

Answer: D (LEAVE A REPLY)

BGP□ Border Gateway Protocol□ □□□ □□□□ □□ □□□(AS) □□ □□□ □□□ □□□□ □ □□□
 □□. □□ □□□□ AS□ □□ AS □□ □□□□ □□□□ □□□□□□. □□□□ BGP□ □□ □□□□ □□
 □□□□ □□□□ □□□□□□□□.

□□□□: Network+ □□ □□□ □□ 2.4: □□□□ □□□□, □□ □ □□□ □□□ □□□□□.

NEW QUESTION: 176

□□□□ □□□□ □□□□ □□□□ □□□ □ □□ □□ □□ □□□□ □□ □□□ □□ □□□□. □□□□
 □□□□□ □□□ □ □□□□ □□□ □□□ □□□□ □□□□. □□ □ □ □□ □□□□ □□□ □□□ □□
 □□□ □□□□ □□□□□. □□ □ □□ □□□ □□ □□□ □□□ □□□□□?

- A.** □□ □□□□□ □□□ □□□ □□□□ □□□□.
- B.** □□□□□ DHCP □□□ □□□ □□□□□□□.
- C.** SNMP □□□ □□□□ □□□□.
- D.** □□□ □□□□□□ □□ □□□□ □□□□.

E. □□ □□□ □□□□ □□ □□□□ □□□.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 177

□□ □ □□ □□□□ TCP/IP □□ □□□ □□□ □□□□ □□□□ □□□□□□□ □□□□ □□□ □□□ □□□?

- A. 3
- B. 4
- C. 5
- D. 6
- E. 7

Answer: B ([LEAVE A REPLY](#))

□□

4□□□ TCP/IP □□ □□□ □□□ □□□□ □□□□ □□□□□□□ □□□ □□□□ □□□ □□□□ □□ □□□. 4□□□ TCP/IP □□ □□ OSI □□□□ □□ □□□□□□ □□□. □□ □□□ □□□□□ □□□ □□ □□□□□□ □□□□□ □□ □□□□□ □□□ □□□ □□□□ □□□ □□□. □□ □□□ □□ □□□ □ □□□ □□□□□ □□ □□□□ □□□ □□□□□□□□ □□□□□ □□□□ □□□□□□. □□ □□□ 0~65535 □□□ 16□□ □□□□ □ □□□ □□(0~1023), □□□ □□(1024~49151), □□ □□ (49152~65535)□ □ □□ □□□ □□□□□. □ □□□ □□ □□□ □ □□ □□□ HTTP□ □□ 80, HTTPS □ □□ 443, SMTP□ □□ 25□ □□□□. □□□□: [CompTIA Network+ Certification Exam Objectives], □□ □□ - □□ | ScienceDirect Topics

NEW QUESTION: 178

□□ □□□□□ □□□ □ □□□□□ □□□ □□□ □□ □□□□. □□ □ □□ □□□ □□□ □□□□ □ □□ □□□ □□□?

- A. □□□
- B. □□
- C. ipconfig
- D. □

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 179

□□□□ □□□□ 53□□ □□□□ □□□ □□ □□ □□□□ □□ □□□□ □□□ □□□□. □□ □□ □□ □ □□ □□□□ □□□□ □□□□ □□□□. □□ CIDR □□□ □ □□□□ □□ □□□ □□ □□ □□□ IP □□ □□ □□□□ □□ □□□□□? (□□□□ □□□□ □□□□□ CompTIA Network+ □□ □□□ □□ □□□□ □□ □□□ □□□□□)

- A. /24
- B. /26
- C. /28
- D. /32

Answer: ([SHOW ANSWER](#))

□□

□ CIDR □□□□ 64□□ IP □□□ □□□ □ □ 62□□ □□□□ □□□ □□ □□□□□□.

□□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□ □□□□ □□□□ □□□□.

53□□ □□□□ □□. CompTIA Network+ □□ □□□□ □□□, "□□□□□□ □□□□ □□□ □ □□□□□□ □ □□ □□□□ □□ □□□□ □□ □□□□□□ □□ □ □□□□□."

NEW QUESTION: 180

□□□□ □□□□ □□ 80□□ □□ □□□□ □ □□□ □□ LAN□□ □□□□ □□□ □□ □□□□□□ □□ □□□□. □ □□□ □□ 80□ □□ □□ □□□□ □□□□ □ □□□ □□□ □□ LAN□□□□ □□□□ □□□□□□. □□ □□□□□□ □ □□□□□□□□ □□ IP □□ □□ □□□ □□□□ □□□□ □□ □□□□□□ □□□□□ □□□□□.

□□□□ □□ □ □□ □□ □□□□ □ □□□ □□□□ □□□? □□□ □□□□ □□ □ □□ □□□ □□□ □□□□ □□□?

A. □ □□□ □□□ □□ 80□ □□ □□□□ □□□□ □□ eth2 □□□□□□□□ eth1□□ □□□□ □□□ □ □□ □□□ □ □□□ □□□□□□.

B. □ □□□ □□□ □□ 80□ □□ □□□□ □□□□ □□ eth0 □□□□□□□□ eth1□□ □□□□ □□□ □ □ DMZ□ □ □□□ □□□□□□.

C. □ □□□ □□□ □□ 80□ □□ □□□□ □□□□ □□ eth1 □□□□□□□□ eth0□□□ □□□□ □□□ □□ DMZ□ □ □□□ □□□□□□.

D. □ □□□ □□□ □□ 80□ □□ □□□□ □□□□ □□ eth0 □□□□□□□□ □□□□ □□□ □□ □□ □□□ □□□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 181

□□ □ □□ □□ □□□□□□ □□□ □□□ □□□ □□□□□□?

A. □□□

B. □□

C. □□

D. □□

Answer: ([SHOW ANSWER](#))

□□

□□□□□□□ □□ □□□□□□ □□□ □□□□ □□□ □□□□□□□□. □□□□□ □□□□ □□ □□, □□□□□ □□□□□□□, □□□□ □□□ □□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□□□ □ □□□, □□ □□, □□□□□□ □□, □□ □□ □□ □□□ □□□□ □□ □□□ □ □□□□□. □□ □□, □□ □ □□ □□ □□ □□□ □□□□□ □□□ □□□□ □□□ □□□ □ □□ □□□□□□□□. □□: CompTIA Network+ N10-008 □□ □□ □□□, 342□□□□; □□ CompTIA Network+ □□ □□□(□□ N10-008), 13-7□ □□.

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 182

□□ □ □□□ □□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□ □□□□□? (2□ □□)

- A. □□ □□ □□
- B. □□□□ □□
- C. IP □□□
- D. □□□ □□
- E. □□ □□ □□ □□
- F. □□ □□

Answer: (SHOW ANSWER)

□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □□□□□, □□□□□ □□ □□□ □□(DDoS) □
□□ □□□□, □□□ □□□, □□□□ □□□, □□ □□□□ □□□ □□□ □□□□ □□□□□.

□□□ □□□ □□□□ □□□ □□□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□□□. □□□□
□□, □□□□ □□ □□□□ □□□□ □□□□□ □□□ □□ □□□□□□□□□. □□□□ □□ □□□, □□
□□□□, □□□□□□ □□□□ □□ □□□ □□□2□ □□ □□□ □□□ □□ □□□ □ □□□□. □□□
□ □□□ □□□□□ □□ □□□□ □□□ □□□□□, □□□ □□□ □□□□□□□□, □□□ □□□ □ □□
□ □□□ □ □□□□3.

□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□ □□□□□ □□ □□□ □□□ □□□ □ □□ □□□
□ □□□□□. □□ □□ □□□ □□□, □□□ □□ □□□□ □□ □□ □□□□ □□ □□□□□ □□ □□
□ □□□ □□□ □□□□ □□□□□. □□ □□ □□□ □□ □□□□□ □□□□□ □□ □□, □□ □□□
□ □□□ □□□ □ □□ □□□□ □□□□. □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□ □□
□□ □□□ □□□ □ □□ □□□□ □□ □□□ □ □□□ □□□□□□.

□□ □□ □□□ □□□□ □□□ □□□ □□□(AP)□ □□□□ □□ □□ □□□□ □□ □□□□ □□□□
□□ □□□□□□ □□□□ □□ □□□ □□ □□ □□□□□. □□ □□ □□□ □□□ □□□ □□□□
□, □□□□ □□□ □□□□□, □□□ □□□□ □□ □□□□□□ □□□□ □□ □□ □□ □□□ □□□□
□ □□□□. □□□ □□ □□ □□□ □□□ □□□□□□ □□□ □□□ □□ □□□□.

IP □□□□ □□□ □□ IP □□□ □□□□ □□ □□□ □□□□ □ □□□ □□□ □□ □□□□□. IP □□
□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □ □□□ □ □□□
□. □□□ IP □□□□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□ □ □□□ □□□□□
□ □□□ □□□ □□ □□□□.

□□□ □□□ □□□ □□□, □ □□ □□□ □□□ □□□□ □□□□□□ □□ □□, □□□□ □□, □□□
□ □□ □□ □□□□ □□□□□ □□ □□□ □□□ □□□□□ □□□□ □□□□□. □□□ □□□ □□□
□□□□□□ □□□□ □□□ □□□□ □ □□ □□ □ □□□□. □□□ □□□ □□□ □□□□ □□ □□□
□ □□□□ □□□□ □□□□ □□ □□□□ □□ □ □□□ □□□□□□ □□□ □□□ □□ □□□□.

□□ □□□ □□, □□□□□□ □□ □□ □□□□ □□□ □□ □□ □□□□□□ □□□ □□ □□□□ □□
□ □□□□ □□□ □□ □□□ □□□□□ □□□□□ □□□ □□ □□□ □ □□□□□. □□ □□□ □□□
□□□□□ □□□ □□□ □□□ □ □□□ □ □□□ □□□ □□□□□ □□□□ □□ □□□ □□□□ □□
□□□. □□□ □□ □□□ □□□ □□□□□ □□□□ □□□ □□□ □□ □□ □□ □□ □□ □□ □□ □□ □□
□□ □□□□□.

□□:

1: □□

2: □□ □□□□□

3: □□□□ □□□ □□□ □□□□ □□ □ □□□

4: [□□ □□ □□]

5: [□□ □□ □□□ IoT □□□□ □□□ □ □□ □□]

6: [□□ □□ □□]

7: [IP □□□]

8: [□□□ □□]

9: [□□□□]

NEW QUESTION: 183

□□ □ 40Gbps □□□□ □ □□□□ □□□□ □ □□ □□□ □□ □□□□□?

A. □□□□ 5e

B. 6a □□□□

C. □□□□ 7

D. 8□□

Answer: ([SHOW ANSWER](#))

Cat 7□ □□ 40Gbps □□□□ □□ 100m □□□ □□□ □□□□ □□ □ □□ □□□ □□□□□. Cat 7□ □
□ □□□ □□□ □□□ □ □□□□ □□□□□. Cat 7□ □□ □□□ □□□□□ □□ □ □□□□□ □□ □
□□ □□□□□.

NEW QUESTION: 184

□□□ □□ □□□□□□ □□□ □□□□□ □□□□. □□□ □□□□ □□□ □□□□, □□□ □ □□□ □
□□ □□□ □ □□□□. □□ □ □□□□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□
□?

A. □□□□ □□□

B. nmap

C. ipconfig

D. □□ □□□

Answer: A ([LEAVE A REPLY](#))

□□

□□□□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□□□. □□ □□□ □□ □□□
□ □□□□□□ □□ □□□□ □□□□ □□□□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□□□
□. □□□□ □□□□ □ □□□ □□ □ □□ IP □□, □□, □□□□ □ □□□□□ □□□□ □□□ □□ □

□ □□□ □□□ □ □□□□. □□□□ □□□□ □□ □□□ □□□ □□, □□□□ □□□ □□ □□ □□ □□ □□ □□12□ □□ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□□ □ □□□ □ □ □□□□. □□□□ □□□□ □□□□ □□□□ □□□□ □□□□□ □□□ □□ □□□ □□□□.

Wireshark3 □□ Microsoft Network Monitor4□ □□ □□□ □□□ □□□□□ □□□ □□□ □□□□ □□ □ □□ □□□□□.

□□□□ □□□□ □ □□□□ □□□□ □□□□□□ □□□□ □□□□ □□□ □□□ □□□□□.

□□□□ IP □□□□ □□□ □□□ □□□□□, □□□□□□ □□□□□ □□□□ □□ □□□ □□□□□ □□ □□ □□□□ □□□□□□.

□□□□□ □□□□□ □□□□ TCP SYN, ACK, RST □□□□□ ICMP □□□□ □ □□ □□ □□□ □□ □□□ □ □□ □□□□.

□□□□□ □□ □□□ □□ □□, □□□□□ □□□ □□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□ □ □□□□.

□□ □□□ □□□□□ □□□□ □□□□□ □□□ □□, □□ □□□□ □□□ □□□ □□□ □□ □□□□ □ □□□ □□□□ □□ □ □□□□.

□□ □□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□. nmap□ □□□□□ □□ □□ □□□□ □□□□ □□□ □ □□ □□□□□, □□□□ □□□ □□□□□ □□□□ □□□ □□ □□□ □.

ipconfig□ □□□ IP □□□□ □□□□ □□□ □ □□ □□□□□ □□ □□□□ □□□□ □□□ □□□□□□ □ □□□□ □□ □□□□. Speed test□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□ □□□□□ □ □□□□ □□□ □□□□□ □□□ □□ □□□□.

NEW QUESTION: 185

□□ □ □□ □□□□□ □□□ □□ □□□ □□ □□ □□ □□ □□□ □□□?

A. □□□ □ □□ □□□□□□□□

B. Qwerty!@#\$

C. □□□□!1

D. T5!8j5

Answer: D ([LEAVE A REPLY](#))

□□□: □□□□ "T5!8j5"□ □□□, □□, □□ □□□ □□ □□ □ □□□ □□□□. □ □□□□ □□□□□ □□□ □□□ □□□ □□ □□□ □ □□□□□.

□□: □□□□□ □ □□□□□ □ □□□□□ □ □□ □□ □□□□□ □ □□□□□.

"T5!8j5" is still strong due to its complexity.

NEW QUESTION: 186

□□□□ □□ □ 8□□ □□□□□ □□ □□□ □□□□ □□ IP □□□ □□□□ □□ □□□□□. □□□□ □□□□ □ IP □□□ □□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□□□□□ IP □□□ □□□□ □□□□□.

□□ □ □□ □□□□ □□ □□□ □□□ □ □□□□?

A. □ □□□ □□□ □□□□ □□ □□

B. □□□□ VLAN □□□□

C. ACL ☐☐

D. IP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 187

□□□□ □□□□ □□□ □□ □□□□□ □□□□ □ □□ □□ □□□□ □□□ □□ □□□ □□□□. □□
□□□□□ □□□ □□□ □□□□□□ □□□ □□□□□.

```
GigabitEthernet0/9 is down, line protocol is down (noconnect)
  Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

□□ □ □□ □□□ □ □□ □□ □□□□□?

A. □□□□□□ □□□□□□□□.

B. ☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐.

C. .

D. □□□ □□□ □□□□□□□.

Answer: ([SHOW ANSWER](#))

11

000000 00000000. 0, 000 000000 0000 000 0 0000. 00000 00000
 000 "00"00 0000 000 "00"0 00 0 0 000, 00 000 00 000 000 000 000
 00. 0000 0000 000, 00000 00 000 "000" 0000 00000. 0000 0000 0
 000, 000 00 000 "0000 0000 00" 0000 00000. 000 000 0000, MTU 0
 0 000 "BW 10000 Kbit/sec" 0000 00000. 00: [CompTIA Network+ 00 00 00], 000 3.0 0
 00, 00

3.1: □□□ □□□□□□ □□□ □□□□ □□□ □□□□□. □□ □□: □□□ □□(ping, netstat, tracert □)

NEW QUESTION: 188

□□ □ □□ □□□ □□ □□□ ISP□ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □
TCP □□□□ □□□□ □□□ □□□□□ □□□ □□□ □□□□□?

A. ☐ ☐ ☐ ☐ ☐ ☐

B. □ □ □ □

C. ☐ ☐ ☐ ☐

D. ☐☐ ☐☐☐☐ ☐☐

Answer: A (LEAVE A REPLY)

□□□□ □□□□ □□□□ □□□□□□ □□□□□□ □□□ □□□ □□ □□ □□□□ □□□□
 □. □ □□□ □□□□□ □□□ □□□ □□□□ ISP□ □□□ □□□ □□□□ □□ □□□ □□□ □
 □□□□ □□□ □ TCP □□□□ □□□□ □□□□ □□□. □□□□ □□□□ □□□ □□□□ □□□□
 □□ □□□□ □ □□□ □□□□ □□□ □ □□ □□ □□□□ □□□□ □ □□□□.

NEW QUESTION: 189

□□□ □□□□□□□□ □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□
□ 100 □ □□□□(FD)□ □□□□□ □□ □□□□□□.
□□□ CLIP□ □□□□□ □□□ □□□□ □□ □□□□ □□□ IOOFD□□ □□□□□ □□ RX □ TX □□
□ □□□□ □□□□□□. □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□□.
□□ □ □□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□□□?

A. □□□ □□□ □□□□□.

B. □□□□ □□

C. □□□ □□

D. □□□ □□□

Answer: D ([LEAVE A REPLY](#))

* □□□□ □□□□□□ □□□□ □□□□ □ □□□, □□□ □□□□ □□□□ □□□ □□□□□. □□□□
□□□□□-□□(straight-through)□ □ □□□, □□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□ □□
□ □□□□□ □□ □□□□, □□□□□(crossover)□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□
□□ □□ □□□□□.

* □□□ □□□□ □□□□□□□□ □□□ □□ □□□ □□□ □□□ □ □□□□ □□ □□□ □□□ □□ □
□□ □□□ □□□□ □□□□. □□□□ □□□ □□□ □□□□ □□□ □□□ □□□□□ □□□□□ □□
□□□□□ □□□ □□ □□□ □□□ □ □□□□. □□ □□ □□□□□□□□ □□□□ 10BASE-T □
1000BASE-T□ □□ □□ □□ □□□ □□□ □□□□ □□ □□□□ □□□□□ □□ □□ □□□□ □□□
□ □□□□. □□□□□ □□□□ □□□□ □□□□ □□□ □□□□□□□ □□□□ □□□ □□□ □□ □
□□ □□□□ □□□ 100 □ □□□□□ □□ □ □□ □□□ □□□ □□□□□ □□ RX □ TX □□□ □□□
□ □□□□.

* □□□ □□ D□ □□ □□□ □□ □□□□. □□□ □□□ □□□ □□ □□□ □□□□□ □□□ □□□□
□□□□□ □□ □□□□□. □□□□ □□□ □ □□□ □□, □□ □ □□□□ □□□□ □□□□□□□ □□□
□□□ □□ □□□ □□□ □□□□ □□□.

* □□ A□ □□□ □□ □□ □□□□. □□ □□□ □□□ □□□□□□□□ □□□ □□□ □□ □□□ □□
□□ □□□ □□□ □□□ □□□□□. □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□
□□□ □□□ □□□ □□□ □□□□□□, □□□ □□ □□□□ □□□ □□ □□□□□.

* □□ B□ □□□ □□ □□ □□□□. □□□□ □□□ □□□□□□□ □□□ □□ □□□ □□ □□□ □□
□ □□ □ □□□ □□□ □□ □□□□ □□□ □□□ □□ □□□□□. □□□□ □□□ □□□(□□□□ □
□□ □ □□□□ □□□ □ □□□ □□)□□□ □□□(□□□□ □□□ □□□□□ □□□ □ □□□ □□)□
□ □□□□. □□□□□□□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □□ □□□□ □□□ □□
□ □ □□□, □□□ □□□ 100 □ □□□□□ □□□□□ □□ RX □ TX □□□ □□□□□ □□□□.

* □□ C□ □□□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□ □□□□.

* □□□ □□□□ □□□ □□□ □□ □□□ □□□□. □□□ □□□ □□□ □□ □□ □□ □□□ □□□ □
□□ □□□□ □□□□ □□□ □□□□□□ □□□ □ □□□□. □□□ □□□ □□□ □□□ □□□□□ □
□□ □ □□□ □□□ □□□ 100 □ □□□□□ □□□□□ □□ RX □ TX □□□ □□□□□ □□□□.
□□□□:

* CompTIA Network+ N10-008 □□ □□□, 2□: □□□□ □□ □ □□, □□

2.1: □□□□ □□□ □ □□□, 661□□□

* Messer □□□ CompTIA N10-008 Network+ □□ □□, □□ 2.1: □□□□ □□□□ □ □□□, 92□□□

- * □ □ □ □ □ □ □ □ - Cisco

NEW QUESTION: 190

[illegible]

- D.** ☐ ☐ ☐ ☐ VPN ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ IP ☐ ☐ ☐ ☐ ☐ ☐.

Answer: (SHOW ANSWER)

□. □□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □□ ISP□ □□□□ □ □ □□□□.

NEW QUESTION: 191

□□ □□□ □□ □ □□ □□ □□ IP □□□ 1.1.1.2/24□ □□ □□□□□ □□ Telnet □□□□ □□□□□□?

- D.** □□ □□ 23□□ □□□□□□ □□ □□ □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 192

□ □ □ □ □ ?

- ### D. BGP

Answer: (SHOW ANSWER)

□ □□ □ □□(BGP)□ □□ □□□ □□□□.

NEW QUESTION: 193

Which of the following is a valid IPv4 address?

- A. 192.168.0.0
- B. 192.168
- C. 192.168
- D. 192.168.0.0

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 194

Which of the following is a valid IPv4 address?

- A. VLAN 192.168
- B. 192.168.0.0 MAC 192.168.0.0
- C. 192.168.0.0
- D. 192.168.0.0

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 195

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Static assignment
- B. Exclusion
- C. Reservation
- D. Dynamic assignment
- E. Scope options

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 196

Which of the following is a valid IPv4 address?

- A. 192.168.0.0
- B. 192.168.0.0
- C. 192.168.0.0
- D. 192.168.0.0

Answer: ([SHOW ANSWER](#))

Which of the following is a valid IPv4 address?

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

NEW QUESTION: 197

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

A. WPA2 Enterprise ☐ ☐ ☐ ☐ ☐

B. □ AP□ □□ □□□ □□□ □□

C. AP □□ □□ □□ □□

D. ☐ AP ☐☐ 802.11ac ☐☐ ☐☐☐ ☐☐☐☐

Answer: D (LEAVE A REPLY)

11

NEW QUESTION: 198

□□□ □□ □□ □□□□ □□ SOHO □□□□ □□□□ □□□□ WiFi □□□□□. □□□
□□ □□□ □ □□□□ □□□□ □□ □□□□ WiFi □□□□□ □ □□ □□□ □ □□ □□□ □ □□ □□

Which of the following is a common method for securing a wireless network? (Select all that apply.)

- A. WPA2-PSK
- B. WEP
- C. WPA3-Enterprise
- D. WPA2-Enterprise

Answer: (SHOW ANSWER)

WPA2-PSK is a common method for securing a wireless network. WPA3-Enterprise is a newer method that provides stronger security. WEP is an older method that is no longer recommended. WPA2-Enterprise is a method that uses a central authentication server. SOHO stands for Small Office/Home Office. WiFi is a common wireless networking technology. WPA2-PSK is the correct answer.

<https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network>

NEW QUESTION: 199

Which of the following is a valid IPv4 address? (Select all that apply.)

- A. 80.87.78.1 - 80.87.78.158
- B. 80.87.78.1 - 80.87.78.62
- C. 80.87.78.0 - 80.87.78.110
- D. 80.87.78.0 - 80.87.78.14

Answer: B (LEAVE A REPLY)

NEW QUESTION: 200

Which of the following is a common method for securing a wireless network? (Select all that apply.)

WPA2-PSK is a common method for securing a wireless network. WPA3-Enterprise is a newer method that provides stronger security. WEP is an older method that is no longer recommended. WPA2-Enterprise is a method that uses a central authentication server. SSID stands for Service Set Identifier. S3cr3t is a common password. CorpNet is a common network name. TKIP is a common encryption algorithm. WPA2-PSK is the correct answer.

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name: AP1

IP Address: 192.168.1.32 /

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 3

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Answer:

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name: AP1

IP Address: 192.168.1.32 /

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: B

Channel: 3

Wired

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3tl

AP1 Configuration



https://ap1.setup.do

IP Address

192.168.1.32

/ 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B

Channel

3

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Security Settings

☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3tl

AP1 Configuration

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

□2□□ □□□ □□□□.
□□□ □□ AP2

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

192.168.1.64

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

6

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3tl

AP2 Configuration

CompTIA

← → ↺

https://ap2.setup.do

IP Address

192.168.1.4 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

ModeG

Channel6

Wired

Speed☒ Auto ☐ 100 ☐ 1000

Duplex☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or PassphraseS3cr3t!

Reset to Default

Save

Close

□3□□ □□□ □□□ □□.
□□□ □□ AP3

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

9

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

AP3 Configuration ✕

← → ↻

IP Address /

Gateway

SSID

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode

Channel

Wired

Speed ☒ Auto ☐ 100 ☐ 1000

Duplex ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

NEW QUESTION: 201

Which of the following is a common wireless network security protocol? (Select TWO)

Options: A. WEP, B. WPA, C. WPA2, D. WPA2 - Enterprise, E. WPA3

- A. WEP
- B. WPA
- C. WPA2
- D. WPA2 - Enterprise
- E. WPA3

Answer: (SHOW ANSWER)

WPA and WPA2 are common wireless network security protocols. WPA3 is a newer protocol that is not yet widely deployed. WEP is an older protocol that is considered insecure. WPA2 - Enterprise is a more complex protocol that is used in enterprise environments. The correct answers are B and C.

Source: CompTIA Network+ Study Guide, 2.0 (Exam #: N10-006), Chapter 1.0, Section 1.8, Wireless Networking

NEW QUESTION: 202

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a divide-and-conquer approach.
- B. a bottom-up approach.
- C. a top-to-bottom approach.
- D. implementing a solution.

Answer: A ([LEAVE A REPLY](#))

Explanation

A divide-and-conquer approach is a troubleshooting method that involves breaking a complex problem into smaller and more manageable parts, and then testing each part to isolate the cause of the problem.

In this scenario, the technician is using a divide-and-conquer approach by pinging the default gateway and DNS server of the workstation, which are two possible sources of connectivity issues.

By pinging these devices, the technician can determine if the problem is related to the local network or the external network.

NEW QUESTION: 203

□□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□□.

ISP□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□□.

□□ □□ □ □□□□ □□□□ □□□□ □□□ □□□□□? (□ □□ □□□□□.)

- A. TCP□□
- B. □□ □□
- C. □□□ □□
- D. □□□□
- E. □□□□□
- F. IP arp □□

Answer: B,D ([LEAVE A REPLY](#))

show config □□(□□ □□ □□□ □□)□ □□□□ □□□ □□□ □□□□ □ □□□□□. □□ □□, Cisco
□□□□□ show running-configuration □□□ □□□□ □□□ RAM□ □□□ □□□ □□ □□□ □ □□□
□□. □□□□ □□□□ □ □□□□ □□□ □□□ □□□ □□□ show startup-configuration □□□ □□□ □ □□
□□.

show route □□(□□ □ □□)□ □□□□ □□□ □□□ □□□ □□□ □□ □ □□□□□. Cisco □□□□□□

show ip route□ □□□□ IPv4 □□□ □□□□ □ □□□□□.

□□□ □□□□ □□□□ netstat(Win/UNIX)□ □□□□ □□□□□.

NEW QUESTION: 204

□□ □ □□ □□□ VPN □□□□□ □□□□□?

- A. WAN □□
- B. □□
- C. □□
- D. □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 205

Which of the following is a security feature of WPA3? (Select two.)

Which of the following is a security feature of WPA3? (Select two.)

- A. WPA3 uses 128-bit encryption.
- B. WPA3 uses 256-bit encryption.
- C. WPA3 uses 192-bit encryption.
- D. WPA3 uses 256-bit encryption.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 206

Which of the following is a security feature of WPA3? (Select two.)

Which of the following is a security feature of WPA3? (Select two.)

- A. WPA3 uses 128-bit encryption.
- B. WPA3 uses 256-bit encryption.
- C. WPA3 uses 192-bit encryption.
- D. WPA3 uses 256-bit encryption.

Answer: C ([LEAVE A REPLY](#))

Which of the following is a security feature of WPA3? (Select two.)

Which of the following is a security feature of WPA3? (Select two.)

NEW QUESTION: 207

Which of the following is a security feature of WPA3? (Select two.)

Which of the following is a security feature of WPA3? (Select two.)

- A. QoS
- B. WPA3
- C. WPA3
- D. WPA3
- E. CRC
- F. WPA3

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 208

□□□□ □□□□ □□□□ □□□ □□□□ □□□□. □ □□□ 12.31 69.1□□ 12.31.69.29 □□□ □□□ □□□. □□ □ □□ □□ □ □□ □□□ □□□□□?

- A. DNS
- B. □□ □□
- C. □□□□
- D. □□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 209

□□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□ □□□□. □□ □ □□ □□□ □□□ □□□□ □□ □□□ □□□□□□?

- A. □□□
- B. □□□
- C. □□□□ □□
- D. □□□

Answer: B ([LEAVE A REPLY](#))

□□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□□ □□ □□□ □□□□□. □ □□□□ □□ □□ □ □□□ □□ □ □□□□ □□ □□□ □□ □□□□ □□□□ □□ □ □□ □□□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□. □□: CompTIA Network+ □□ □□ □□

NEW QUESTION: 210

□□□□ 3□□□ □□□ □□ □□□ □□□ 30□□ WAP□ □□□ □□□ □□ □□□□□ □□□□□ □□ □. □□ AP□ □□□□□ □□□□ □□ □□□ SSID□ □□□□□□□□□□. □□ □ □ □□□ □□ □ □□ □□ □□ □□□□□?

- A. □□ □□□ □□
- B. □□ □□□ □□
- C. □□ □□ □□□ □□
- D. □□ □□□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 211

□□□□ □□□□ □□□ □□ □□□□□ □□□□ □ □□ □□ □□□□ □□□ □□ □□□ □□□□. □□ □□□□□ □□□ □□□ □□□□□□ □□□ □□□□□. □□ □ □□ □□□ □ □□ □□ □□□□□?

- A. □□□□□□□ □□□□□□□.
- B. □□□□ □□ □□ □□□□.
- C. □□□□ □□□□ □□□□□.
- D. □□□ □□□ □□□□□□□.

Answer: A ([LEAVE A REPLY](#))

□□□□□□ □□□□□□□□. □, □□□ □□□□□□ □□□□ □□□ □ □□□□. □□□□□ □□□□□
□□□ "□□"□□ □□□□ □□□ "□□"□ □□ □ □ □□□, □□ □□□ □□ □□□ □□□ □□□ □□□
□□. □□□□ □□ □□□, □□□□□ □□ □□□ "□□□" □□□□ □□□□□. □□□□ □□□□ □□□
□, □□□ □□ □□□ "□□□□ □□□□ □□" □□□□ □□□□□. □□□ □□□ □□□□, MTU □□ □
□□ "BW 10000 Kbit/sec" □□□□ □□□□□. □□: [CompTIA Network+ □□ □□ □□], □□□ 3.0 □□□, □□ 3.1: □□□ □□□□□□ □□□ □□□□ □□ □□, □□ □□: □□□ □□(ping, netstat, tracert □)

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 212

□□ □ □□ □□□ □□□ □□□□ □□□ □□□ □□ 4□□ □□□ □□□□□?

- A. 1000BASE-FX
- B. 1000BASE-T
- C. 1000BASE-LR
- D. 1000BASE-SX

Answer: B (LEAVE A REPLY)

□□□ 1000BASE-T□□□. □ □□□ □□□ □□□ □□□□ 4□□ □□□□ 5 □□□ □□ □□□□ □□□
□□. □□ 100m □□□□ □□ 1000Mbps(1Gbps)□ □□□□ □□□ □□□ □□□□□ □□□□□ □□□□□
□□□. □□□ □□□ □□(1000BASE-FX, 1000BASE-LR □ 1000BASE-SX)□ □□□ □□□ □□ □□□ □
□ 1000BASE-T□ □□ □□□ □□□□ □□□ □□□□□ □ □□□ □□□ □□□□□.

NEW QUESTION: 213

A network technician crimped a length of IJTP with TIA\EIA-568A on one end and TINE-IA-5688 on the other. Which of the following cable types did the technician create?

- A. Crossover cable
- B. Patch cable
- C. Twinaxial cable
- D. Rollover cable

Answer: A (LEAVE A REPLY)

Explanation

The cable type that the technician created is a crossover cable. A crossover cable is a type of twisted-pair cable that has the transmit and receive pairs reversed on one end. A crossover cable is used to connect two devices of the same type, such as two switches or two computers, without using a hub or a switch. A crossover cable can be made by crimping one end of the cable with TIA/EIA-568A standard and the other end with

TIA/EIA-568B standard, or vice versa. These standards define the color coding and pin assignments for RJ-45 connectors on twisted-pair cables. References: CompTIA Network+ N10-008 Certification Study Guide, page 53; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-4.

NEW QUESTION: 214

□□ □□ □□□□ TCP/IP □□ □□□ □□□ □□□□ □□□□ □□□□□□□□ □□□□ □□□ □□□
□□?

- A. 5**
B. 3
C. 4
D. 7
E. 6

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 215

□□□□ □□□□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□□□.

Building construction type	Brick
Layout:	10,764 ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

□□□ □□□ □□□ □ □ □ □, □□□□□ □□ □□ □□□ □ □□□ □□□□ 5GHz □□□□□ □□□□
□ □□□ □□ □□□ □□□□ □□□□□. □□□□□ □□ □ □□ □□ □□ □□□ □□ □ □□□□ □
□□?

- A.** WPA3 □ □ □ □ □ □ □ □ .
- B.** □ □ □ □ □ □ □ □ □ □ □ □ .
- C.** □ □ □ □ □ □ □ □ □ □ □ □ □ □ .
- D.** 2.4GHz □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ .

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 216

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

- A. SSO**
- B. TACACS+**
- C. Zero Trust**
- D. Separation of duties**
- E. Multifactor authentication**

Answer: ([SHOW ANSWER](#))

Terminal Access Controller Access Control System (TACACS+) is often used in authenticating administrative access to routers and switches.

NEW QUESTION: 217

□□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□ □□ □ □□ □□ □□
□□□?

- A.** □□□ □□□□□.
- B.** □□□ □□□ □□□.
- C.** □□□ □□□□□.
- D.** □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

CompTIA □□ □□ □□□1□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□□ □□
 □□□□□ □□□□ □□□□□. □ □□□□ □□□ □□ □□, □□ □□ □□ □□ □□ □□□□ □□□□
 □□□ □□□ □□□□□ □□□□ □□ □□□□□.

□ □ :

□□ □□ □□□ | IT □□ □ □□ □□□ | CompTIA1

NEW QUESTION: 218

□□□□ □□□□ Cat 6(□□□□ □□) □□□□ □□ □□ □□□□□□ □□□□ □□□□ □ □□□□ □□
 □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□□□□. □□ □ □□ □□ □□ □□□□ □□□□ □□□□
 □ □□□ □□□□ □ □□□□?

- A. CSMA/CD**
B. LACP
C. PoE+
D. MDIX

Answer: D (LEAVE A REPLY)

11

MDIX(□□ □□ □□□□ □□□□)□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□
 □□□□□ □□□□ □□ □□ □□□ □□□□□. □□□□□ MDIX□ □□□□□ □□□□ □□ Cat 6 □□
 □□ □□□□ □□□□□ □□□□ □□ □□□□.

□□□□: CompTIA Network+ □□ □□ □□□, Glen E. Clarke □□, 6□

NEW QUESTION: 219

□□□□□ □□□ □□ □□ □□□□ □□□ □□□□ □□□□. □□□□□ □□□□ □□□ □□□□ □□□
□ □□□ □□ □ □□ □□ □□□□□ □□□□?

- A.** 802.1Q
B. STP
C. □□ □□
D. CSMA/CD

Answer: B (LEAVE A REPLY)

□□□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□ □□□□(STP)□ □□□□ □□□. STP□ □ □
□ □□□ □□ □□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□.

□ □ :

CompTIA Network+ ☐☐ ☐☐ ☐☐☐

NEW QUESTION: 220

[illegible]

```
c:\user> nslookup newmail.company.com
```

□ □ □ □ □ □ :

☐☐: newmail.company.com

IP: 3.219.13.186, 64.58.225.184, 184.168.131.243

[illegible]

- A.** □□ DNS □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□.
- B.** □□□ ACL□ □□□□ □□□ □□ IP □□□ □□□□ □□□ □□□□□.
- C.** □□□ □□□ PAT □□□ □□□□ □□□□□□ □□□□□.
- D.** □□□□ □□□ □□□□ □□□□□ □□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 221

A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are allowed?

- A.** Geofencing
B. Secure SNMP
C. Private VLANs
D. Captive portal

Answer: D (LEAVE A REPLY)

NEW QUESTION: 222

A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

- A.** Cold site
B. Hot site
C. Warm site
D. Cloud site

Answer: A (LEAVE A REPLY)

NEW QUESTION: 223

□□□□ □□□□ □□□ □□□ □□□□ PoE□ □□ □□□ □□□□ □□□□. □□□□ □□□□
□ □ PoE□ □□□□□ □□□□ □□ □□ □ □□ □□ □□□□? (□ □□□ □□□□□.)

- A.** □□□
- B.** □□□
- C.** □□□ □□
- D.** VoIP □□

E. UPS

F. □□□

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 224

□□ □□□ □□□□ □ □□ □□ □□□□□ ISP □□ □□□ □□□□□ □□ □□□ □□□□□ □□□□ □□□?

A. BGP

B. EIGRP

C. □□□ □□□

D. OSPF

Answer: A ([LEAVE A REPLY](#))

BGP(Border Gateway Protocol): BGP□ □□□□ □□ □□ □□□(AS) □ □□□□ □□ □□□□□□□. ISP, □□ □ □□ □□□□ □□ □□□ □ □□ □□□ □□□ □□□□□. BGP□ □□□ □□□□□ □□□□ □□ □□ □□□ □□□ □□□□ □ □□□□□.

NEW QUESTION: 225

□□□ □□ □□ □□□ □□□□ □□□ □□□□ □□□□□□□□. □□□□ □□□ □□□□□ □ □□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□□. □□ □ □□ □□□ □□□ □□ □□□ □□ □ □□ □□□?

A. □ □□□□□□ □□□ □□ □□□□ □□ □□ □□

B. □□□□□ □□□□ □□ □□ □□

C. □ □□□ □□ □□ OTDR□ □□□□ □□ □□ □□□ □□□□.

D. □□□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□□□.

Answer: ([SHOW ANSWER](#))

* □ □□ □□ □□□(OTDR)□ □□, □□, □□ □□ □□ □□ □□□□ □□□ □□□ □ □□ □□□□□.

* OTDR□ □□□□ □□ □□□ □ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □ □□□□.

* OTDR□ □□□ □□ □□□□ □□□□ □□□□ □□ □□□□□ □□□ □□ □□□□ □□□□ □□□ □ □□□□.

* OTDR□ □□□□□□ □□□ □□□□ □□□ □□□ □□□ □ □□□, □□ □□□□ □□ □□□ □□□ □□□□□.

* OTDR□ □□□□ □□□ □□ □□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□□ □□ □ □□□ □ □□□ □□□□.

* □□ □□□ □□□ □□□ □□□□ □□□□ □□□□.

* □ □□□□□ □ □□□ □□ □□ □ □□ □□ □□□□ □□ □□ □□□□ □□□□ □ □□ □□□□□.

* □□ □□□□ □□ □□□ □□□ □□□ □□ □□□□□□3. □□ □□ □□ □□□□ □□□ □□□□ □ □□□ □ □□□□1.

* □□□□□ □□, □□, □□□ □□ □□□ □□□ □□□ □ □□ □□□□□.4 □□ □□□ □□□□ □□ □ □□ □□□□ □□□□ □ □□□□.1

NEW QUESTION: 231

Which of the following is a benefit of using a VPN?

- A. It provides a secure connection between two devices.
- B. It allows users to access resources on a remote network.
- C. It provides a secure connection between two networks.
- D. It provides a secure connection between two users.

Answer: D ([LEAVE A REPLY](#))

A VPN is a secure connection between two devices. It allows users to access resources on a remote network. It provides a secure connection between two networks. It provides a secure connection between two users.

<https://www.auvik.com/franklyit/blog/vpn-split-tunneling/>

NEW QUESTION: 232

Which of the following is a command used to view the DNS configuration on a Linux system?

- A. ipconfig
- B. nslookup
- C. ping
- D. netstat

Answer: B ([LEAVE A REPLY](#))

nslookup is a command used to view the DNS configuration on a Linux system. It provides information about the DNS server, the IP address of the DNS server, and the DNS records for a domain. It is used to troubleshoot DNS issues. MX, NS, SOA are DNS records. Linux command IP nslookup provides information about the DNS server. IP: <https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/>

NEW QUESTION: 233

Which of the following is a command used to view the ARP table on a Linux system?

- A. netstat
- B. nslookup
- C. arp
- D. netstat

Answer: B ([LEAVE A REPLY](#))

nslookup is a command used to view the DNS configuration on a Linux system. It provides information about the DNS server, the IP address of the DNS server, and the DNS records for a domain. It is used to troubleshoot DNS issues. MX, NS, SOA are DNS records. Linux command IP nslookup provides information about the DNS server. IP: <https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/>

NEW QUESTION: 234

A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

- A. Fusion splicer
- B. Tone generator
- C. Cable tester
- D. PoE injector
- E. OTDR

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 235

Which of the following is a common method for testing a network's performance? (Select two.)

- A. Ping
- B. Traceroute
- C. Netstat
- D. nslookup

Answer: D ([LEAVE A REPLY](#))

Which of the following is a common method for testing a network's performance? (Select two.)

NEW QUESTION: 236

Which of the following is a common method for testing a network's performance? (Select two.)

- A. SNMP
- B. Ping
- C. Netstat
- D. nslookup

Answer: D ([LEAVE A REPLY](#))

SIEM is a type of security tool that can help organizations monitor and analyze their network traffic. SIEM can help organizations detect and respond to security incidents. SIEM can also help organizations prevent security incidents. SIEM can help organizations improve their overall security posture.

<https://www.comptia.org/blog/what-is-siem>

NEW QUESTION: 237

Which of the following is a common method for testing a network's performance? (Select two.)

- A. ThisIsMyPasswordForWork

B. Qwerty!@#\$

C. □□□□! 1

D. T5!8j5

Answer: D ([LEAVE A REPLY](#))

□□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□
□□. □□□□□ □□ □□□□□ □□□ □□ □□□□ □□□□ □□□□□. □□□ □□ □□□ □□ □□□
□□ □□□ □□ □□□□□ □□□□ □□□, □□, □□ □□□ □□□□□ □□ □□□ □ □□□ □□□. □
□□□ T5!8j5□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□ □□□□□ □□ □□□□□□.
□□□□:

□□□□ □□ - N10-008 CompTIA Network+ : 4.21

CompTIA Network+ □□ □□□: □□ □□ □ □□, 25□□□

<https://www.pearsonitcertification.com/articles/article.aspx?p=3021579&seqNum=2>

NEW QUESTION: 238

□□□□ 30□□□ □□ □□□ □□ □□ □□□□□ □□□□ □□ □□□ □□□ □□□ □□□□□. □ □□
□□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□. □□ □ □□ □□□ □□□ □□□ □
□□□ □□ □□□□?

A. □□ □□□□

B. □□ □□□

C. □□□ □□

D. □□□ □□□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 239

□□□□ □□□□□ □□□ □□ □□ □□□□□ □□□□ □□□□. □□□□□ □□□ □□ □□ □□□ □
□□□□.

1 □□ □□□ □□□□□ □□□□ □ □□□.

2. □□□ □□□□□ □□□.

3. □□□□□ □□ □□□□□□ □□□.

□□□□□ □□ □ □□ □□□ □□□□ □□?

A. TWP-RC4

B. WPA2

C. CCMP-AES

D. EAP-TLS

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 240

□□□□ □□□□ □□□ □□ □□□□□ □□□□ □ □□ □□ □□□□ □□□ □□ □□□ □□□□. □□
□□□□□ □□□ □□□ □□□□□□ □□□ □□□□□.

GigabitEthernet0/9 is down, line protocol is down (notconnect)
Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set

□□ □ □□ □□□ □ □□ □□ □□□□□?

- A. □□□□□□ □□□□□□□.
- B. □□□□ □□ □□ □□□□.
- C. □□□□ □□□□ □□□□□.
- D. □□□ □□□ □□□□□□□.

Answer: A ([LEAVE A REPLY](#))

□□

□□□□□□ □□□□□□□. □, □□□ □□□□□□ □□□□ □□□ □ □□□□. □□□□□ □□□□□
□□□ "□□"□□ □□□□ □□□ "□□"□ □□ □ □ □□□, □□ □□□ □□ □□□ □□□ □□□ □□□
□□. □□□□ □□□□ □□□, □□□□□ □□ □□□ "□□□" □□□□ □□□□□. □□□□ □□□□ □
□□□, □□□ □□ □□□ "□□□□ □□□□ □□" □□□□ □□□□□. □□□ □□□ □□□□, MTU □
□ □□□ "BW 10000 Kbit/sec" □□□□ □□□□□. □□: [CompTIA Network+ □□ □□ □□], □□□ 3.0 □
□□, □□

3.1: □□□ □□□□□□ □□□ □□□□ □□□ □□□□□. □□ □□: □□□ □□(ping, netstat, tracert □)

NEW QUESTION: 241

ARP □□□□ □□□□□ □□□ □□□□□.

- A. □□□ □□.
- B. DNS □□□□.
- C. DoS □□.
- D. □□□□ □□□ □□□.

Answer: A ([LEAVE A REPLY](#))

ARP □□□□ □□ ARP □□□□ □□ □□□□ MAC □□□ □□□□□ □□□□ □□□ IP □□□ □□□□
□ □□□□□. □□ □□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□□ □□□□ □□□ □
□□□□. □□ □□□□ □ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□ □ □□ □□□ □□□
□□ □□ □□□ □□□□□□ □□□. ARP □□□□ □□□ □□ □□□, □□ □□□□, □□□ □□□□ □
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □ □□□□. DNS □□□□, DoS □□ □ □□ □
□□ □□□□ ARP □□□□ □□ □□□ □□□ ARP □□□□ □□ □□ □ □□□ □□□ □ □□□□. DNS
□□□□□ □□□ □□□ □□□ □□□ IP □□□ □□□□ □□ □□ □□ □□ □□□□□□ DNS □□□ □
□□ □□□ □□□□□ □□□□□. □□ □□□□ □□ □□□□, □□ □□□ □□ □□□ □□□□□ □□□
□□□ □ □□□ □ □□□□. DoS □□□ SYN □□□, ICMP □□□ □□ UDP □□□□ □□ □□□ □□□
□ □□□□□ □□ □□□□□ □□□□□ □□□□ □□□□□. □□ □□ □□□□□ □□□□□ □□, □□
□ □□ □□□ □□□□□ □ □□□ □ □□□□. □□ □□□ □□□□ □□□□□ □□ □□ □□□□□ □
□□ □□ □□□ □□□□□□. □□ □□□□□ □□ □□ □□□□ □□□□□, □□□□□ □□□□□ □□□□
□, □□ □□□ □□□□ □ □□□ □ □□□□. □□:

* ARP □□□

* □□□ □□

- * DNS □□□□
- * [DoS □□]
- * [□□ □□ □□□]
- * [□□□□+N10-008 □□□□]
- * [CompTIA N10-008 □□ □□ □□ □□]

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
 □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 242

After a critical power issue, the network team was not receiving UPS status notifications. The network team would like to be alerted on these status changes. Which of the following would be BEST to use for these notifications?

- A. MB
- B. Syslog
- C. NetFlow
- D. Traps

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 243

□□□□ □□□□ □□□□□□ □□□ □□□□ □□□□. □□□□ □□ □□□□ □□□ □□□ □ □□□
 □. □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□?

- A. □□□ □□ □□□ □□ □□□ □□□□□.
- B. □□□ □□□□ □□□□□.
- C. □□□ □□□□ □□ □□□□ □□□□□.
- D. □□ □□□□□ □□□ □□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 244

□□□ □□□□□□□ □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□
 □ 100 □ □□□□(FD)□ □□□□□ □□ □□□□□□.
 □□□ CLI□□ □□□□□ □□□ □□□□ □□ □□□□ □□□ IOOFD□□ □□□□□ □□ RX □ TX □□
 □ □□□□ □□□□□□. □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□.
 □□ □ □□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□ □□□□□?

- A. □□□ □□□ □□□□□.
- B. □□□□ □□

C. 10BASE-T

D. 100BASE-T

Answer: D ([LEAVE A REPLY](#))

Networks are often configured with different types of cables, and the type of cable used can affect the network's performance. The most common types of cables used in networks are straight-through (straight-through) and crossover (crossover). Straight-through cables are used to connect a computer to a switch or a router, and crossover cables are used to connect two computers directly.

10BASE-T and 100BASE-T are both types of Ethernet networks. 10BASE-T is a standard for 10 Mbps Ethernet, and 100BASE-T is a standard for 100 Mbps Ethernet. Both standards use twisted-pair cabling, and both are commonly used in networks. 10BASE-T is typically used in small networks, while 100BASE-T is typically used in larger networks. Both standards are compatible with each other, and both can be used to connect a computer to a switch or a router.

10BASE-T is a standard for 10 Mbps Ethernet, and 100BASE-T is a standard for 100 Mbps Ethernet. Both standards use twisted-pair cabling, and both are commonly used in networks. 10BASE-T is typically used in small networks, while 100BASE-T is typically used in larger networks. Both standards are compatible with each other, and both can be used to connect a computer to a switch or a router.

10BASE-T is a standard for 10 Mbps Ethernet, and 100BASE-T is a standard for 100 Mbps Ethernet. Both standards use twisted-pair cabling, and both are commonly used in networks. 10BASE-T is typically used in small networks, while 100BASE-T is typically used in larger networks. Both standards are compatible with each other, and both can be used to connect a computer to a switch or a router.

10BASE-T is a standard for 10 Mbps Ethernet, and 100BASE-T is a standard for 100 Mbps Ethernet. Both standards use twisted-pair cabling, and both are commonly used in networks. 10BASE-T is typically used in small networks, while 100BASE-T is typically used in larger networks. Both standards are compatible with each other, and both can be used to connect a computer to a switch or a router.

CompTIA Network+ N10-008 100 questions, 2.1: 100 questions, 2.1: 100 questions, 661 questions Messer 100 CompTIA N10-008 Network+ 100 questions, 2.1: 100 questions, 92 questions 100 questions? | 100 questions 3 questions 100 questions - Cisco 100 questions 100 questions - Cisco

NEW QUESTION: 245

Networks are often configured with different types of cables, and the type of cable used can affect the network's performance. The most common types of cables used in networks are straight-through (straight-through) and crossover (crossover). Straight-through cables are used to connect a computer to a switch or a router, and crossover cables are used to connect two computers directly.

A. 10BASE-T

B. 100BASE-T

C. 100BASE-T

D. IP .

Answer: D (LEAVE A REPLY)

00000000 0000 0000 00 IP 00000000, 00 0000 0000 0000 0000 0 00 0
 00 00 0 000000. 00 IP 0000 0000 0000 0000 0000 0000 00 IP 0000
 0. 00 IP 0000 0000 0000 00 00000000 00 000000 000000 00 0000 0000 0 0
 0000. 0000 0000 000000 00 0 0000 0000 00 IP 0000 0000 00 00 IP 00 0000 00
 0 0 00000. IP 00 0000 0 0000 0000 0000 IP 0000 000000 0 0 00000 000000 00 0
 00 0000 000000. IP 00 0000 00 00000 00000 00000 00 IP 0000 000000 00 00
 00 00000 000000 00 0 00000. 00000: [CompTIA Network+ 00 00 00], IP 00 00000?
 | HowStuffWorks

NEW QUESTION: 246

□□□□ SNMPv3 □□□□ □□□□ □□□ □□□□□□ □□□□. □□□ □□□□ □□□ □□ □□□□
□□ □ □□ □□□ □□ □□□□□?

- A.** □□ □□□□ UDP□ □□ □□□□ □□□□□□□□ □□□□□.
- B.** SET □□□ MIB □□□□□□□ □□□ □□□□□.
- C.** □□□□□□ □□□□□□ □□ □□□□ □□□□□.
- D.** □□ □□□□ □□ □□□□ □□ □□ □□□□ □□□□□.

NEW QUESTION: 247

- A.** □□ □□ □□
- B.** □□□□ □□□ □□
- C.** □□□ □□ □□
- D.** □□ □□

□□□ □□□□ □□□□ □, □□ □□□ □□□□□□. □ □□□ □□□□ □□□□ □□ □□□□ □□□
□□ □□□ □□□□ □□□□□ □□□ □□□□□□ □□□. □□□□ □□□□ □□□ □□□ □□ □□□ □
□□□.

□□□ □□ □□: □ □□□ □□□□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□□□. □□
□□, □□□ □□ □□□ □□ a□ □□□□ □□ z□□ □□□□, □□□□ □□ aa□□ zz□□ □□□□ □□
□□□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□□ □□□, □□ □□□ □□□ □□□ □□□ □
□□□□ □□□□ □□□ □□ □□□ □□□□ □ □□□ □ □ □□□□.

□□ □□□□ □□: □ □□□ □□□□□ □□□□ □□□□□ □□ □ □□□ □□□.

[illegible]

NEW QUESTION: 248

E. ☐ ☐ ☐ ☐ ☐

Answer: A ([LEAVE A REPLY](#))

□□ □□□□ □□□□□□□□ □□ □□□ □□□□ □□□□□ □□ □□□□□□. □□ □□□□ VLAN□ □□□□ □□□ □ □□□□. VLAN□ □□□□□ □□□ □□□□□□, □□ □□ □□ □□ □□ □□□□ □□ □□□. □□□ □□ □□□□ □□□□ □ □□□□ □□ □□□ VLAN□ □□□□ □□ □□□ □□□ □□□ □ □□□□□□□ □□□ □ □□□□ □□□ □ □□□□. □□: <https://www.comptia.org/blog/what-is-a-virtual-switch>

NEW QUESTION: 252

□□□□ □□ □□ □□□□ □ □□□ □□ IP □□□ □□□□ □□□□. □□ □□□□ □□ □□ □□□ □ □□□□.

- IP □□□ □□□□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
- □□ □□□□□□ 172.28.85.94□ □□□□ □□□.
- □□□ □□□□ 255.255.255.224□□ □□□.

□□□□□ □□ □□ □ □□ □□□ □□□ □□□□ □□□?

- A. 172.28.85.254
- B. 172.28.85.95
- C. 172.28.85.93
- D. 172.28.85.255

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 253

□□□ □□□□□□ □□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□□.

□□□ □□ □□ □ □□ □□□ □□□ □□□ □ □□□□?

- A. □□□ □□□
- B. □□□□
- C. MAC □□□
- D. VLAN □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 254

IT □□□□ □ □□ □□ □□ □□□□□ □□□□□ □□□□□. □□□□ □ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□ □□□□□ DHCP □□□ □□□ □□□ □□□ □□ □□□□□. □□ □ □□ □□ □ □□□ □□ □ □□□□□?

- A. □□ □□□□□
- B. IP □□□ □□□□□□□
- C. □□ □□
- D. □□ □□

Answer: D ([LEAVE A REPLY](#))

□□

□□ □□□ □□□□ □□□ □□ □□□ □□ □□ □□□□□ DHCP □□□□□.

1. □□□□□ □□□ □□□ IP □□□ □□ □□□□ □□ □□□ □□□ □□□ □□□
 □ □ □□□□.2. □□ □□□ □□□□□ □□□ IP □□□ □□□□ □□□ □□□ DHCP □□□ □□□ □□
 □ □□□ □ □□□□. □□ DHCP □□□□ □□□□□□□ RogueChecker□ □□ □□□ □□□□ □□□
 □ □□□□.

NEW QUESTION: 255

□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□ □ □□□ □□□□. □ □□□□
□□ □ □□ □□ □□ □□□ □□ □□□ □□□□□? (□ □□□ □□□□□.)

- A.** □□ □□
B. □□ □□
C. □□□ □□
D. □□
E. □□ □□ □□
F. □□ □□

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 256

□□□□□ □□□ □ □□□□ □□ □□□□ □□□ IP □□ □□□ □□□□□□. □ □□□ □□ SLAAC□
□□□□□□□. □□ □ □□ □□ □□□ □□□□ □□□□?

- A.** ☐☐ DHCP ☐☐
- B.** MAC ☐☐☐ ☐☐☐☐☐☐☐☐.
- C.** ☐☐☐ ☐☐☐ ☐☐
- D.** ☐☐☐ VLAN ☐☐

Answer: B ([LEAVE A REPLY](#))

SLAAC(Stateless Address Autoconfiguration) □ IPv6 □□□□□ □□□ □□□□□ □□□□ □□ □□ □□□
 □□□□ □□□□ □□□□ □□□□ □□ IP □□□ □□□□ □ □□□□ □□□□□. □□□□□ □ □□□
 □□□ MAC □□□ □□ □□ □□ □□ □□ □□□ IP □□□ □□□ □□□ □□□ □ □□□□. SLAAC□□
 □□□ IPv6 □□□□ EUI-64 □□□ MAC □□□ □□□□□ □□□ MAC □□□ □□□ IPv6 □□□ □□□
 □□. □□ DHCP □□, □□□ □□□ □□, □□□ VLAN □□□ □□ □□□ □□ □□□ □□ MAC □□□□
 □□□□□ □□□□□ SLAAC□□ □□□ IP □□ □□□ □□□□ □□□□.

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
 □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 257

[illegible]

- A. □□
- B. □□□
- C. □□
- D. □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 258

□□□□ □□□□ SSH□ □□ □□□ □□□□ □□ □□□ □□□ □□□□. □□□□ □□ □□□
 □□□ □□□□ □□ □□□□ □□□□□□ □□ □□□□. □□□□ □□□□ □□□ □□□□ □□□ □□
 □□□ □□□□.

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

□□□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.

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

□□ □ □ □□□ □□ □ □□□□ □□ □□□□□?

- A. □□□□ □□ □□□ □□□□ □□□□.
- B. □□□ SSH □□□ □□□□ □□ □□□□.
- C. □□□ □□□ □□□ □□□□ □□□□.
- D. □□□□ □□□□ □□□ □□□□.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 259

A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

- A. RST
- B. FIN
- C. ICMP Time Exceeded
- D. Redirect

Answer: ([SHOW ANSWER](#))

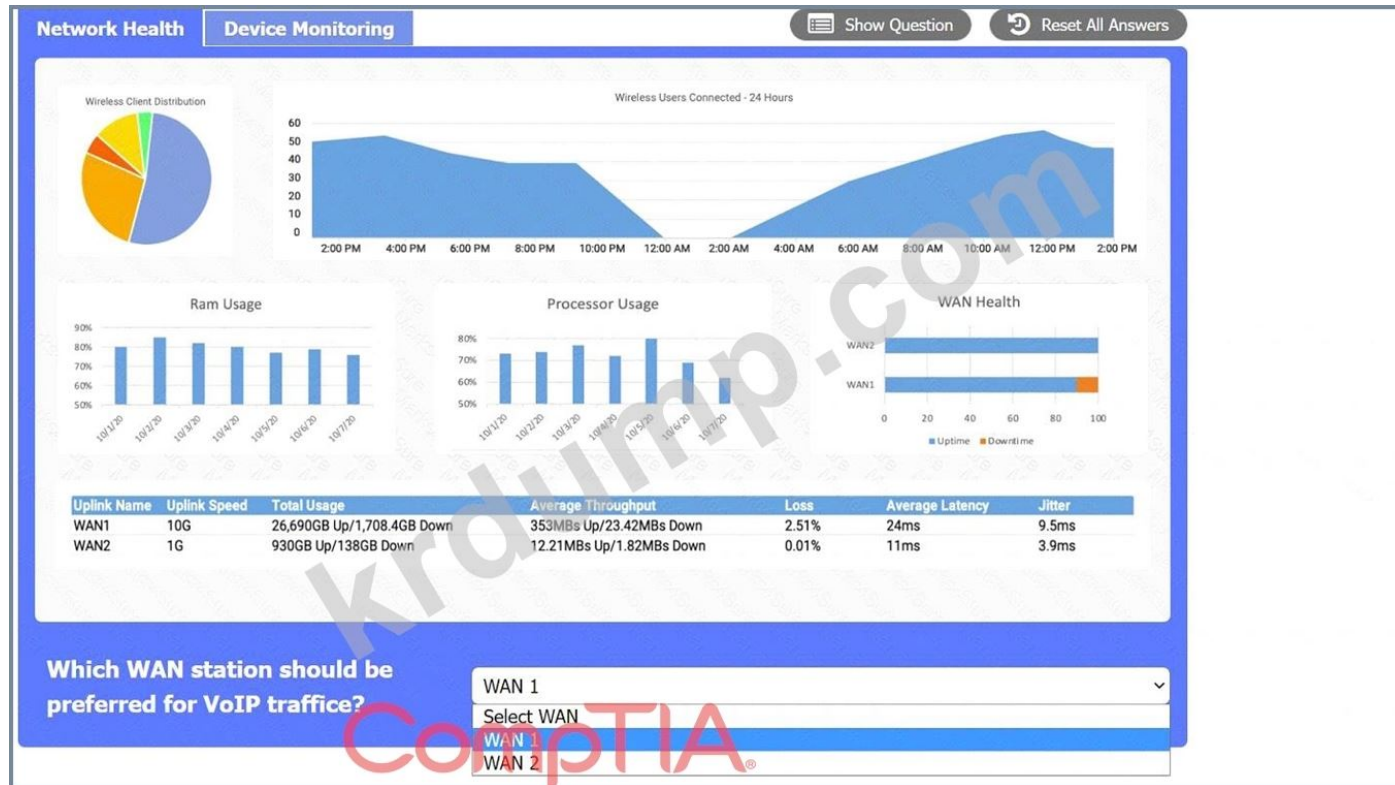
A RST response is generated by the server when a client attempts to connect to a TCP port that is not open. The RST message informs the client that the port is not available, and the client should reset its connection. The RST response is generated by the server to immediately terminate the connection attempt and prevent the client from wasting resources attempting to connect to a port that will not respond.

NEW QUESTION: 260

Which WAN station should be preferred for VoIP traffic?

Answer:

WAN 2. VoIP traffic requires low latency and low jitter. WAN 2 has a lower average latency (11ms) and lower jitter (3.9ms) compared to WAN 1 (24ms latency, 9.5ms jitter).



Answer:

WAN 2. VoIP traffic requires low latency and low jitter.

Answer:

WAN 2.

WAN 2 is preferred for VoIP traffic because it has a lower average latency (11ms) and lower jitter (3.9ms) compared to WAN 1 (24ms latency, 9.5ms jitter). VoIP traffic requires low latency and low jitter to ensure clear communication. WAN 1 has a higher average latency (24ms) and higher jitter (9.5ms), which can lead to poor VoIP quality.

WAN 1 has a higher average latency (24ms) and higher jitter (9.5ms) compared to WAN 2 (11ms latency, 3.9ms jitter).

* 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

- * 930GB / 138GB
- * 12.21Mbps Up/1.82Mbps Down
- * 0.01%
- * 11ms
- * 3.9ms

VoIP traffic is sensitive to latency and jitter. WAN 1 has a higher average latency (24ms) and jitter (9.5ms) compared to WAN 2 (11ms and 3.9ms respectively). Therefore, WAN 2 is preferred for VoIP traffic.



VoIP traffic is sensitive to latency and jitter. WAN 2 has a lower average latency (11ms) and jitter (3.9ms) compared to WAN 1 (24ms and 9.5ms respectively). Therefore, WAN 2 is preferred for VoIP traffic.



NEW QUESTION: 261

Which two statements are true regarding the configuration of a network device? (Choose two.)

Options:

- 1. The configuration of a network device is stored in the configuration register.
- 2. The configuration of a network device is stored in the configuration file.

Answer:

1. The configuration of a network device is stored in the configuration register.

2.

(Note: ips is a typo for ip. The correct statement is: The configuration of a network device is stored in the configuration file.)

3. The configuration of a network device is stored in the configuration file.

show ip interface brief shows the IP address of the interface.

show vlan brief shows the VLANs configured on the switch.

show cdp neighbors shows the neighbors of the switch.

show ip interface brief shows the IP address of the interface.

Core Switch 1 IP address is 192.168.1.1.

Core Switch 1 IP address is 192.168.1.1.

Core Switch 1 VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

Core Switch 1 is connected to Access Switch 1 and Access Switch 2.

Core Switch 1 Access Switch 1 GigabitEthernet0/1 GigabitEthernet0/2.
Core Switch 1 Access Switch 2 GigabitEthernet0/3 GigabitEthernet0/4.
Access Switch 1 Access Switch 2

NEW QUESTION: 262

Which of the following is a characteristic of a honeypot?

- A. It is a real system.
- B. It is a virtual system.
- C. It is a physical system.
- D. It is a logical system.

Answer: (SHOW ANSWER)

A honeypot is a computer system that is designed to attract and trap attackers. It is a virtual system that is designed to look like a real system. It is a physical system that is designed to look like a real system. It is a logical system that is designed to look like a real system.

<https://www.comptia.org/blog/what-is-a-honeypot>

NEW QUESTION: 263

Which of the following is a characteristic of a honeypot?

- A. It is a real system.
- B. It is a virtual system.
- C. It is a physical system.
- D. It is a logical system.

Answer: C (LEAVE A REPLY)

A honeypot is a computer system that is designed to attract and trap attackers. It is a virtual system that is designed to look like a real system. It is a physical system that is designed to look like a real system. It is a logical system that is designed to look like a real system.

- * Microsoft Community1
- * Tom's Hardware2
- * CompTIA Network+ N10-008

<https://www.comptia.org/certifications/network#examdetails>

NEW QUESTION: 264

Which of the following is a characteristic of a honeypot?

- A. 300 000
- B. IPS
- C. 00
- D. 00

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 265

0000 00000 500 VLAN0 000 0 00 0000 0000 000. 0 VLAN0 0000 0000 0 00 000 0000.

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

00 0 000 000 0000, 00 000000 00 0 00 00 0 00 000 00 00 00 0000 0 0000?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 266

0000 0000 00 000 00 RJ45 00 000000 0000 RJ45 000 000000 0000 00 0. 00 00 0 0000 000000 00 00 000 000000?

- A. 000000
- B. 000 000
- C. 0 000
- D. 0000 000

Answer: B ([LEAVE A REPLY](#))

00 000 00 RJ45 00 000000 0000 RJ45 000 000000 000000 0000 0000 00 0 0 00 00 00 000 000 000000. 0 000 000 0000.

00 000: 00 00 0000 00 000 0000 0000 0 000000.

000 000: 0 000 000 0000 0000, 00 000 0000, 00 000 00 000 0000 0000 0 0000 000.

0 000: 0000 000 00 000 0000 0000 0 000000, 00 00 00 000000 000 0.

0000 000: 000 000 00 000 000 000 00000 0 000000.

000 000 B. 000 0003000.

NEW QUESTION: 267

Which of the following is a valid IPv4 address? (Select one)

- A. 192.168.1.1.1
- B. 192.168.1.1
- C. 192.168.1.1.1.1
- D. ACL 192.168.1.1

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 268

Which of the following is a valid IPv4 address? (Select one)

- A. 192
- B. 192
- C. 192
- D. 192

Answer: D ([LEAVE A REPLY](#))

192

Which of the following is a valid IPv4 address? (Select one)

192.168.1.1

192.168.1.1 + N10-008 192.168.1.1: 2.2 192.168.1.1 192.168.1.1 192.168.1.1

NEW QUESTION: 269

Which of the following is a valid IPv4 address? (Select one)

- A. 192.168.1.1
- B. WLAN 192.168.1.1
- C. PoE 192.168.1.1
- D. 192.168.1.1

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 270

Which of the following is a valid IPv4 address? (Select one)

- A. 192.168.1.1
- B. 192.168.1
- C. 192.168.1
- D. 192.168.1 VPN

Answer: D ([LEAVE A REPLY](#))

192

Which VPN protocol is used to create a secure tunnel between two devices over an untrusted network? **Answer:** CompTIA Network+ Question 5: Which VPN protocol is used to create a secure tunnel between two devices over an untrusted network?

NEW QUESTION: 271

ISP 20Mbps. Which of the following is the most appropriate bandwidth for a video stream? **Answer:** CompTIA Network+ Question 271: Which of the following is the most appropriate bandwidth for a video stream?

- A. 10Mbps
- B. 15Mbps
- C. 20Mbps
- D. 25Mbps

Answer: (SHOW ANSWER)

N10-008 Which of the following is the most appropriate bandwidth for a video stream? **Answer:** CompTIA Network+ Question N10-008: Which of the following is the most appropriate bandwidth for a video stream? **N10-008** Which of the following is the most appropriate bandwidth for a video stream? **Answer:** CompTIA Network+ Question N10-008: Which of the following is the most appropriate bandwidth for a video stream? <https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 272

Which of the following is a Layer 2 protocol? **Answer:** CompTIA Network+ Question 272: Which of the following is a Layer 2 protocol?

- A. EIGRP
- B. VRRP
- C. MPLS
- D. STP

Answer: B (LEAVE A REPLY)

VRRP(Virtual Router Redundancy Protocol) is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. VRRP is a Layer 2 protocol that provides a backup for the default gateway. [https://www.comptia.org/training/books/network-n10-008-study-guide\(230111\)](https://www.comptia.org/training/books/network-n10-008-study-guide(230111))

NEW QUESTION: 273

Which of the following is a Layer 2 protocol? **Answer:** CompTIA Network+ Question 273: Which of the following is a Layer 2 protocol?

- A. EIGRP
- B. VRRP

C. 200 000

D. 00 00

Answer: C ([LEAVE A REPLY](#))

000 2 0000 00 0000 0000 00 VLAN 000 MAC 000 00 0000 0000 0000
0. 000 2 0000 300 0000 0000 000 0000 000000 00 00000. 000 000
000, 000, 0000 00 00 000 00000 0000 00000. 000 2 0000 00000 0
0000 00000 0000 000 00 000 000 0000 0000 000 0 0000. 0000:
[https://www.comptia.org/training/books/network-n10-008-study-guide\(139000\)](https://www.comptia.org/training/books/network-n10-008-study-guide(139000))

NEW QUESTION: 274

0000 0000 00000 00 Linux 0000 0000 000. 0000 00 000 000 0000.
Linux 000 00 00:

Interface	IP address	MAC address
eth0	10.1.2.24	A1:B2:C3:F4:E5:D6

000 00 00 00 00 00:

Interface	IP address	MAC address
eth1	10.1.2.3	A1:B2:C3:D4:E5:F6

Linux 0000 0000 00 000 0000 0, 0000 Linux 00000 00 00 0 00 000 0000
000?

A. ifconfig eth0 promisc

B. ifconfig eth1 0

C. ifconfig eth0 10.1.2.3

D. ifconfig eth1 0000 000 A1:B2:C3:D4:E5:F6

Answer: A ([LEAVE A REPLY](#))

00

ifconfig eth0 promisc 000 Linux 00000 0000 000 000 00000 000. 0 000 0000
0000 000 00 000 0000 00 0000 0000 000 0 0000. 00:
CompTIA Network+ 00 00 000, 70: 0000 00.

NEW QUESTION: 275

0000 00000 000 00 0000 00 000 0000 0 000 0000. 00 0 00 0000
0 000 00 00000?

A. 2.4GHz

B. 5GHz

C. 5.9GHz

D. 6GHz

Answer: A ([LEAVE A REPLY](#))

2.4GHz 0000 0000 0000 00 00 0000 000000 0000 000 0 0000.
00:

Which of the following is a valid IEEE 802.11a/b/g channel number?
A. 128
B. 132
C. 136
D. 140

NEW QUESTION: 276

Which of the following is a valid IEEE 802.11a/b/g channel number?

- A. 128
- B. 132
- C. 136
- D. 140

Answer: (SHOW ANSWER)

NEW QUESTION: 277

A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage. However, users in the offices adjacent to the warehouse have noticed a large amount of signal overlap from the new network. Additionally, warehouse employees report difficulty connecting to the wireless network from the other side of the building; however, they have no issues when they are near the antenna. Which of the following is MOST likely the cause?

- A. The wireless signal is being refracted by the warehouse's windows
- B. The antenna's power level was set too high and is overlapping
- C. An omnidirectional antenna was used instead of a unidirectional antenna
- D. The wireless access points are using channels from the 5GHz spectrum

Answer: C (LEAVE A REPLY)

Explanation

An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building.

References:
<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION: 278

Which of the following is a valid IEEE 802.11a/b/g channel number?

- A. 128
- B. CSU/DSU
- C. 136
- D. MDF

Answer: B (LEAVE A REPLY)

NEW QUESTION: 279

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

- A. ThisIsMyPasswordForWork
- B. Qwerty!@#\$
- C. 12345! 1
- D. T5!8j5

Answer: D ([LEAVE A REPLY](#))

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network? The answer is D. T5!8j5. This is because it is a strong password that includes uppercase letters, lowercase letters, numbers, and special characters. The other options are either weak passwords or not passwords at all.

Source: N10-008 CompTIA Network+ : 4.21

CompTIA Network+ 10101: 10101 10101, 25000:

<https://www.pearsonitcertification.com/articles/article.aspx?p=3021579&seqNum=2>

NEW QUESTION: 280

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

- A. 12345678
- B. 12345678
- C. 123456
- D. 12345678

Answer: D ([LEAVE A REPLY](#))

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network? The answer is D. 12345678. This is because it is a strong password that includes uppercase letters, lowercase letters, numbers, and special characters. The other options are either weak passwords or not passwords at all.

NEW QUESTION: 281

Which of the following is the MOST secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

- A. Site-to-site VPN
- B. Full-tunnel VPN
- C. Split-tunnel VPN
- D. SSH

Answer: ([SHOW ANSWER](#))

The MOST secure connection would be a full-tunnel VPN. This is because all traffic from the remote device is sent through the VPN and encrypted, rather than just specific traffic as with a split-tunnel VPN.

NEW QUESTION: 282

A. ☐☐☐☐ ☐☐☐☐

B. nmap

C. ipconfig

D. ☐☐ ☐☐☐

1. 本報告係根據本公司及子公司之會計帳簿及記錄，以公允合理之方式彙整而成，其中並未包含任何可能影響報告準確性之重大會計估計或判斷。

[illegible]

□□□□ □□□□ □□□□ TCP SYN, ACK, RST □□□□ ICMP □□□ □ □□ □□ □□□ □□ □□□ □
□□ □□□□.

□□ □□□ □□□□ □□□□ □□□□ □□□ □□, □□ □□□□ □□□ □□□ □□□ □□ □□□□ □
□□□□ □□□□ □□ □ □□□□.

[illegible][illegible]

- Answer: B (LEAVE A REPLY)**

11

Which of the following are valid channel numbers for 802.11n in the 2.4GHz band? (Select three.)
A. 1, 6, 11
B. 1, 5, 9
C. 1, 6, 13
D. 1, 11, 16
E. 1, 16, 21
F. 1, 21, 26

NEW QUESTION: 284

Which of the following is the maximum channel width for 802.11n in the 2.4GHz band?

- A. 2.4GHz
- B. 5GHz
- C. 850MHz
- D. 900MHz

Answer: A ([LEAVE A REPLY](#))

2.4GHz is the maximum channel width for 802.11n in the 2.4GHz band. The 2.4GHz band is divided into 14 channels, each 5MHz wide. The channels are numbered 1 through 14. Channels 1, 6, and 11 are the only channels that do not overlap with any other channels in the band.

Channels 2, 7, and 12 overlap with channels 1, 6, and 11 respectively. Channels 3, 8, and 13 overlap with channels 2, 7, and 12 respectively. Channels 4, 9, and 14 overlap with channels 3, 8, and 13 respectively.

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html>

NEW QUESTION: 285

Which of the following is a cloud-based service? (Select three.)
A. IaaS
B. PaaS
C. SaaS
D. VPN
E. VDI
F. VNC

- A. IaaS
- B. PaaS
- C. SaaS
- D. VPN

Answer: C ([LEAVE A REPLY](#))

SaaS is a cloud-based service. IaaS, PaaS, and VDI are also cloud-based services. VPN and VNC are not cloud-based services.

NEW QUESTION: 286

Which of the following is a valid channel number for 802.11n in the 5GHz band? (Select three.)
A. 36
B. 40
C. 44
D. 48
E. 52
F. 56

- A. AP 36 WLAN 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224, 228, 232, 236, 240, 244, 248, 252, 256, 260, 264, 268, 272, 276, 280, 284, 288, 292, 296, 300, 304, 308, 312, 316, 320, 324, 328, 332, 336, 340, 344, 348, 352, 356, 360, 364, 368, 372, 376, 380, 384, 388, 392, 396, 400, 404, 408, 412, 416, 420, 424, 428, 432, 436, 440, 444, 448, 452, 456, 460, 464, 468, 472, 476, 480, 484, 488, 492, 496, 500, 504, 508, 512, 516, 520, 524, 528, 532, 536, 540, 544, 548, 552, 556, 560, 564, 568, 572, 576, 580, 584, 588, 592, 596, 600, 604, 608, 612, 616, 620, 624, 628, 632, 636, 640, 644, 648, 652, 656, 660, 664, 668, 672, 676, 680, 684, 688, 692, 696, 700, 704, 708, 712, 716, 720, 724, 728, 732, 736, 740, 744, 748, 752, 756, 760, 764, 768, 772, 776, 780, 784, 788, 792, 796, 800, 804, 808, 812, 816, 820, 824, 828, 832, 836, 840, 844, 848, 852, 856, 860, 864, 868, 872, 876, 880, 884, 888, 892, 896, 900, 904, 908, 912, 916, 920, 924, 928, 932, 936, 940, 944, 948, 952, 956, 960, 964, 968, 972, 976, 980, 984, 988, 992, 996, 1000
- B. AP 40 WLAN 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224, 228, 232, 236, 240, 244, 248, 252, 256, 260, 264, 268, 272, 276, 280, 284, 288, 292, 296, 300, 304, 308, 312, 316, 320, 324, 328, 332, 336, 340, 344, 348, 352, 356, 360, 364, 368, 372, 376, 380, 384, 388, 392, 396, 400, 404, 408, 412, 416, 420, 424, 428, 432, 436, 440, 444, 448, 452, 456, 460, 464, 468, 472, 476, 480, 484, 488, 492, 496, 500, 504, 508, 512, 516, 520, 524, 528, 532, 536, 540, 544, 548, 552, 556, 560, 564, 568, 572, 576, 580, 584, 588, 592, 596, 600, 604, 608, 612, 616, 620, 624, 628, 632, 636, 640, 644, 648, 652, 656, 660, 664, 668, 672, 676, 680, 684, 688, 692, 696, 700, 704, 708, 712, 716, 720, 724, 728, 732, 736, 740, 744, 748, 752, 756, 760, 764, 768, 772, 776, 780, 784, 788, 792, 796, 800, 804, 808, 812, 816, 820, 824, 828, 832, 836, 840, 844, 848, 852, 856, 860, 864, 868, 872, 876, 880, 884, 888, 892, 896, 900, 904, 908, 912, 916, 920, 924, 928, 932, 936, 940, 944, 948, 952, 956, 960, 964, 968, 972, 976, 980, 984, 988, 992, 996, 1000
- C. AP 44 MU-MIMO 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224, 228, 232, 236, 240, 244, 248, 252, 256, 260, 264, 268, 272, 276, 280, 284, 288, 292, 296, 300, 304, 308, 312, 316, 320, 324, 328, 332, 336, 340, 344, 348, 352, 356, 360, 364, 368, 372, 376, 380, 384, 388, 392, 396, 400, 404, 408, 412, 416, 420, 424, 428, 432, 436, 440, 444, 448, 452, 456, 460, 464, 468, 472, 476, 480, 484, 488, 492, 496, 500, 504, 508, 512, 516, 520, 524, 528, 532, 536, 540, 544, 548, 552, 556, 560, 564, 568, 572, 576, 580, 584, 588, 592, 596, 600, 604, 608, 612, 616, 620, 624, 628, 632, 636, 640, 644, 648, 652, 656, 660, 664, 668, 672, 676, 680, 684, 688, 692, 696, 700, 704, 708, 712, 716, 720, 724, 728, 732, 736, 740, 744, 748, 752, 756, 760, 764, 768, 772, 776, 780, 784, 788, 792, 796, 800, 804, 808, 812, 816, 820, 824, 828, 832, 836, 840, 844, 848, 852, 856, 860, 864, 868, 872, 876, 880, 884, 888, 892, 896, 900, 904, 908, 912, 916, 920, 924, 928, 932, 936, 940, 944, 948, 952, 956, 960, 964, 968, 972, 976, 980, 984, 988, 992, 996, 1000

FTP(□□ □□ □□□□)□ □□□□ □□□□□ □□ □□ □□□□ □□□□□□. □□□□ □□□ □□ □□ □□□□ □□ □□ □□□□ □□□□□□ □□ □□ □□□□ □□□□ □□□□ □□□□□□□□. □□ □□ □□□□□ □□ □□□1□□ □□□□□ □□□□ □□ □□ □□□□□ □□□□ □□ □□□ □□□□□ □□□□ □□□□□. □□□□ □□□□ □□□□□ □□□, □□□ □□ □□ FTP □□□ □□ □□ □□ □□□□ □□ □□□□□ □□ □□□□ □□□□□□. □□:

<https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%20or%20triple-homed%20firewall%2C%20refers%20to,a%20perimeter%20network%20to%20isolate%20or%20separate%20the> 1

NEW QUESTION: 289

A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

- A. WLAN controller
- B. Cable modem
- C. Load balancer
- D. Switch
- E. Hub

Answer: D (LEAVE A REPLY)

A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

NEW QUESTION: 290

□□□□□ □□□ □□□□□ □□ MX □□□□ □□□□□□□ □□□ □□□□□. □□ □□ □□ □□ □□ □□ □□□□ □□□ □□□ □□□□ □□ □□□□?

- A. □□□
- B. □
- C. □□
- D. □□□□□□

Answer: A (LEAVE A REPLY)

□□
MX □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□ DNS □□□ □□□□
□. □□□ MX □□□□ □□□□□□ □□ □□□□□ □□□ □□ □□□□□ □□ □□ □□□□ □□ □□
□□.

NEW QUESTION: 291

□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□ □□□. □□□□ □□ □□□ □□□□
60□ □□□ □□□□ □□□ □ □□□ □□□ □□□□□.

□□ □ □□ □□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□□?

- A. RPO
- B. □□ □□ □□(MTTR)

C. FHRP

D. 60 分钟

Answer: B ([LEAVE A REPLY](#))

解析

MTTR 是指网络故障从发生到修复所需的时间。3 小时等于 180 分钟。如果 MTTR 为 60 分钟，那么网络故障从发生到修复所需的时间为 60 分钟。MTTR 是指 Mean Time To Repair，即平均修复时间。如果 MTTR 为 60 分钟，那么网络故障从发生到修复所需的时间为 60 分钟。

NEW QUESTION: 292

Which of the following is a layer of the OSI model? (Select all that apply.)

A. Network

B. Data Link

C. Session

D. Transport

Answer: A ([LEAVE A REPLY](#))

The OSI model is a seven-layer model of network communication. The layers are: Physical, Data Link, Network, Transport, Session, Presentation, and Application. The Network layer is responsible for routing data between devices. The Data Link layer is responsible for error detection and correction. The Transport layer is responsible for end-to-end communication. The Session layer is responsible for establishing, managing, and terminating sessions. The Presentation layer is responsible for data representation. The Application layer is responsible for the application software. NGFW (Next-Generation Firewall) is a type of firewall that can inspect traffic at the Network layer. NGFW can also inspect traffic at the Transport layer. NGFW can also inspect traffic at the Session layer. NGFW can also inspect traffic at the Presentation layer. NGFW can also inspect traffic at the Application layer. NGFW can also inspect traffic at the Data Link layer. NGFW can also inspect traffic at the Physical layer.

解析

Which of the following is a layer of the OSI model?

A. Network

B. Data Link

C. Session

CompTIA Network+ 认证考试题目，8000 (N10-008)

NEW QUESTION: 293

Which of the following can be used to identify users after an action has occurred?

A. Access control vestibule

B. Cameras

C. Asset tag

D. Motion detectors

Answer: C (LEAVE A REPLY)

□□□□ □□, □ □□ □□ □□□ □□□ □□□□ □□□ □□□ □ □□□ □□□□ □ □□□ □ □□□ □
□. □□□□ □□ □□ □□□□ □□ □ □□□□ □□□ □□□□□. □□ □□ □□, □□ □□ □ □□ □□
□□ □□□□ □□□□ □ □□□□□ □□□ □□ □□, □□ □□ □ □□□ □□□□ □□□□□□.
□□□ □ □ □□□ □□□ □□□ □□□ □□□□ □□□ □□□□□ □ □ □□□□□. □□ □□□
□□□ □□□ □□□□□. □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□
□□ OSI □□□ □□□ □□□□□ □□□ □ □□□□. □□□ □□□□ □□□ □□□□□ □□□□ □□□
□□ □□□□. □□□ □□□ □□ □□□ □□ OSI □□□ □□ □□□ □□□ □□□□□ CSMA/CD□ □□
□□□ □□□□ □□□□ □□□□□ □□□□ □□□.

□□

□□□ □□□□□□□□ □□

□□□ □□ □□ | □□ 2 | OSI □□

□□□□ □□□□□ □□ □□□□ □ □□□ □□□□ □□□□ □ □□□ □□□□□ □□□□□ □□□. □
□□□□ □□ □□ □ □□ □□ □□□□ □□□?

□

□□□

□□□□□

□□

tracert □□□ □□ □□□□□ □□ □□□□□ □□ □□□ □□□□ □□□□ □□ □□□□□. □□□ □□
□□□□ IP □□□ □□□ □□, □□□ □ □□ □□ □□□ □□□□□. tracert □□□ □□□ □□□□ □□
□□ □□□ □□□□ □□□□ □ □□□ □□□□□ □□□□ □ □□□ □ □□□□. □ □□□ □□□ □□
tracert □□□ □□ □□□□ □□ □□ □□□ □ □□ □□□ □□□□ □□□.

□□

Windows □□ □□□ □□ □□□□ □□ - GeeksforGeeks

□□ Cisco □□□□ □□□□□ □□□ □ 9□□ □□□ □□

□□□□ □□□□ □□□ □ □□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□□□ □□□ □
□□ □□□□□ □□ □ □□ □□ □□□□ □□□?

□□□□

□□ □□

□□ SNMP

□□ VLAN

□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□□□ □□ □□□□ □□□ □□□ □□
□□ □□ □ □□□□□□□. □□□ □□□ □□ □□□□□ □□□ □ □□ □□□ □□□□, □□□□□ □□
□□□□ □□□□□, □□□ □□□ □□□□ □ □□□ □ □□□□. □□□ □□□ □□, □□, □□ □□ □□□
□ □□ □□ □□ □□□□□ □□□□ □□□□□. □□□ □□□ □□ □□ □□□□ □□□□ □□□□□ □
□□□□□ □□□□ □□□□ □□□□ □□ □□□ □ □□□□.

□□

□□ □□ □□□ □□□ □□ | Law Insider

□□ Wi-Fi □□□□□ □□□□□? □□□□ □ □□

□□□□ □□□□□ □□□ □ □□□ □□□□ □□ □□ □□□□. □□□□ □□□□ NIC
□ □□ □□□□ □□□ □□ □□ □□□□□. □□□□ □□□□ □□□ □□□□□□ □□□□ □□□ □□
□□ □□□□ □□□□. □□□□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□ □ □□□□□?

□□□ ARP □□□□□ □□□□ IP □□□ □□□□□.

□□□ □□□□ □□□□ □□□□ □□□□□.

□□□ CAM □□□□□ □□□□ MAC □□□ □□□□□.

□ □□□□ □□□□ □□□□ □□□□□.

□ □□□□□□ □□□□ □□ □□□ □□□□ □□□□□. □ □□□□ □□□ □□□ □□□□ □□□□□.

□ □□□□□□ □□□ □□ □□ □□□□ □ □□□□ □□□□ □□ □ □□ □□□□ □□□□ □□□□ □

□□ □□□□□□ □□□ □ □□□□. □ □□□ □□□□ IP □□ MAC □□□ □□ □□□□ □□□ □□□

□□ □□□□ □□□□ □□□□. □□ □□□□ □□□□□ □□□□□ □□□□□ □□□□ □□□□ □□

□□□□ □□□□ □□□□ □□□ □□□ □□□□□□.

□□

PC□□ □□□□ □□□ □□□ □□ □□□ □□□□□?

□□□ □□ □□□□ □□□ - Comparitech

□ □□□□ □□□ □□□□ □□□ □□ □□

□□□□ □□□□ □□□ □□□ □□□ □□□ □ □□ VLAN□ □□□ □□□□. □ □□□□□ □□ □ □□
□□ □□□□?

□□□

□□ □□

□□ □□

□□ □□

□□□

□□□□ □□ □□ □ □□□ □□ □□□ □□□ □□□□ □□□□, □□□□ □□ □□ □□ □ □□ □□□

□□□□ □□□ □□□□□.1 □□□ □□□ □□□ □□□ □ □□ VLAN□ □□□□□□ □□□□ □□□□

□□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□ □□□□ □

□□□□ □□□□ □□□□□□ □□□□ □□ □□□□ □□□□□ □□□□ □□□□ □ □□□□. □□□

□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□□ □□ □□ □□□ CIA 3□□□ □

□ □□ □ □□□□□.234

□□

□□□□ □□: VLAN □□ □□□ □□ □□□□ □□□

CIA 3□□: □□, □□ □□ □ □ | CSO □□□

□□ - NIST SP 1800-25 □□

CIA 3□□ - □□□, □□□, □□□□ □□ □□

□□□, □□□ □ □□□ - DevQA.io

□□□□ □□□□ □□□ □□□ □□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□□□□. □□□□

□□□ □ □□□ □□ □□□□ □□□□□□. □□□□ □□□□ □□ □□□ □□ □ □□ □□□□?

□□□ □□□

□□□□□

□□□□

□□□□

IPsec 是网络层的安全协议，它通过加密和认证来保护网络通信。IPsec 可以在网络层提供端到端的安全，确保数据在传输过程中不被窃取或篡改。IPsec 通常用于保护敏感数据，如金融交易、医疗记录等。IPsec 的实现方式有多种，如隧道模式、传输模式等。IPsec 的配置和管理相对复杂，需要专业的网络工程师进行配置。

IP

IPsec 是网络层的安全协议，它通过加密和认证来保护网络通信。

IPsec 可以在网络层提供端到端的安全，确保数据在传输过程中不被窃取或篡改。

IPsec 通常用于保护敏感数据，如金融交易、医疗记录等。

IDS

IPsec

IPS

VPN

IPsec 是网络层的安全协议，它通过加密和认证来保护网络通信。IPsec 可以在网络层提供端到端的安全，确保数据在传输过程中不被窃取或篡改。IPsec 通常用于保护敏感数据，如金融交易、医疗记录等。IPsec 的实现方式有多种，如隧道模式、传输模式等。IPsec 的配置和管理相对复杂，需要专业的网络工程师进行配置。

IP

IPsec 是网络层的安全协议，它通过加密和认证来保护网络通信。

IPsec 可以在网络层提供端到端的安全，确保数据在传输过程中不被窃取或篡改。

IPsec 通常用于保护敏感数据，如金融交易、医疗记录等。

IPsec 0

IPsec 2

IPsec 5

IPsec 7

IPsec 是网络层的安全协议，它通过加密和认证来保护网络通信。IPsec 可以在网络层提供端到端的安全，确保数据在传输过程中不被窃取或篡改。IPsec 通常用于保护敏感数据，如金融交易、医疗记录等。IPsec 的实现方式有多种，如隧道模式、传输模式等。IPsec 的配置和管理相对复杂，需要专业的网络工程师进行配置。

IP

Cisco IOS 是网络设备的操作系统，它提供了丰富的配置和管理功能。

Cisco IOS 是网络设备的操作系统，它提供了丰富的配置和管理功能。

Cisco 是网络设备的制造商，它提供了各种网络设备和解决方案。

5GHz 是无线网络的频率，它提供了高速的无线网络连接。

5GHz

1,300Mbps

20/40/80MHz

□□□□ □□□□□ □□ □ □□ □□□ □□□□ □□□?

802.11a

802.11ac

802.11b

802.11n

□□□□□□ □□□ □□ □□ □□□ □□ □□□ □□□□□□. □□ □□□□□ □□□ □□□□ □□□ □
□□□ □□□ □□□□□. □□□□□ □ □□□ □□□□ □□ □□ □ □□ □□□□ □□□□ □□ □ □□
□□ □□□□ □□□?

□□□□□□□

□

□□

nslookup

□□□ □□□□ □□□□ □□□ □□□□□ □□□ □□□ □□ □ □□□□□. □□ □□□□□
NAT □□□ □□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□ □ □
□□□. □□□ □□□□ TCP□ SYN □ ACK □□□ □□□ □□□ □□□□□ □□□□ □□□ □□□ □□
TCP □□□ □□□ □□ □□□□.

□□□ □□□ □□□ □□□□ □□ □□□□□ □□ □ □□ □□□□ □□□□ □□ traceroute □□□ □□
□□ □□□. traceroute □□□ □□□ □□ □□□□ IP □□□ □□□ □□□ □□□□ □□□ □□□ □□□
□ □□□ □□□□ □ □□ □□□ □□□ □□□□□. □□□□□ □□ □□□ traceroute □□□ □□□ □□
□□ □□□□ □ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □ □□□□2.

ping □□□ □ □□ □□ □□□□ □□ □□□ □□□□□ □□□ □□□ □□ □□□ □□□ □□□□ □□□
□ □□□ □□□ □□□ □□□□□ □□□□ □□□□. route □□□ □□□ □□□ □□□□ □□□□□ □□
□ □□□ □□ □□□ □□□□ □□□□. nslookup □□□ □□□ □□□ IP □□□ □□□□□ □ □□□ □
□□□□ □ □□ □□ □□□ □□□□ □□□□ □□□□.

□□

□□□ □□□ □□□ □□ □□□□ □□ | Auvik

WAAS□□ □□□ □□□ □□ □ □□ □□ - Cisco □□□□ □□□ □□ □ SNMP□ □□□□ □□□□ □□
□□□ □□□□ □□□□ □□□ □□ □□ □ □□□□ □□□□□□ □□□□□. □□□□ □□□□ □□ □
□ □ □□ □□□□□?

□□□□ □□□□□ □□□ MIB□ □□□□□.

□□□□ □□□□□ □□□□ □□□□□ Syslog□ □□□□□.

□□ □□□□ □□□□ □□□□ □□□□ □□□□□□□□.

SMB□ □□□□ □□□□ □□□□ □□□□□ □□□□□.

SNMP(Simple Network Management Protocol)□ □□□□ □□□ □□□□ □□□□ □□□□ □□, □□ □
□□□ □□ □□□ □□□ □ □□□ □□ □□□□□□□. SNMP□ MIB(Management Information Bases)□
□□□□□, □□ □□□□ □□□□□□□ □□□ □ □□ □□ □□□ □□□□ □□ □□□□□1.

□□□□ □□□ □ □ □□□□ MIB□ □□ □□□□ □□ □ □□□, □□ □□□□ □□□□ □ □□□□□
□□ □□□□ □□□□□ □□□□ □□ □ □□□ □□□□□. □□ □□ □□□□ □□□□ □□□ □□ □□

□ □□□□ □□□□ □□□□□□ □□ □ □□□□. □□ □□□□□ □□□□ □□□□ □□□
□ □□□□□ □□□ MIB□ □□□□ □ □□□□ MIB□ □□□□ SNMP □□□□ □□□□ □□□ □ □□
□ □□ □□□2.

□□ □□□ □ □□□ □□□ □□□□. □□□□ □□□□ □□□□ □□□□ syslog□ □□□□ SNMP □□
□□ □□□ □□□ □□□□. syslog□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □□ □□□□□
□ □□□□□. □□ □□□□ □□□□ □□□□ □□□□ □□□□□□ □□ □□□ □□ □□□
□. □□ □□□□ □□□□ □□ □□ □□□□ □□□□ □ □□□□ □□ □□□ □□□□ □□□□□ □□□
□ □□□□ □□□ □□□□ □□□□. SMB□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□
□□□□. SMB□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□□□□ SNMP □□□□ □□□
□ □□ □□□□□.

□□

Grafana & Prometheus SNMP: □□ □□□□ □□□□ □□□

SNMP□ □□□ □□□□□ □□ Windows □□□ □□ - ScienceLogic

□□ □ □□ □□ □□□ mGRE □□ □ □□□ □□□□□ □□□ □□□□□□□?

□□□ □ □□ □□□□ □□□ □□□□ □□ □□ □□□□ □□ □ □□□ □□ □□□□ □□ SDWAN □□
□□ □□□ □□□ □□ □□□ □□ □□ □□ □□ □□ □□□□ □□ □□□□ □□□ □□ mGRE(Multipoint
GRE)□ □ □□□□ □□ □□□ □□ □ □□□ □□□ □□ □□, □□ □□□□□□ □□ □□ □□□□□□
□□□ □ □□ □□□ □□□ GRE(Generic Routing Encapsulation) □□□□□. mGRE□ DMVPN(Dynamic
Multipoint VPN)□ □□ □□□ VPN □□□□□ □□ □ □□□ □□□□□□. DMVPN□ mGRE, NHRP(Next
Hop Resolution Protocol), IPsec□ □□□□ □□□ □□ □□□ □□ □□□□ □□□ VPN □□□ □□□

Cisco □□□□□1.

□□□□ □□ □ □□□ □□ □□□□ □□□ mGRE □□ □ □□□ □□□□□ □□□ □□□□ □ □□□
□. □□□ □ □□□ □□ □□ □□ □□ □ □□□ □□□□ □□ □□□□ □ □□ □□□□ □□□□□ □□
□ □□ □□□□□. □□ mGRE□ □□□ □□□ □□□ □□□ □ □□□ □□□□ □□ □□□□ □□□ □
□□□ □□□ □ □□□□.

□□ □□□ mGRE □□ □ □□□ □□□□□ □□ □□□ □□ □□□ □□□□. □□□ □ □□ □□□□ □
□□□ □□□□ □□□ □□□□□ IPsec□ □□□□ □□□. IPsec□ mGRE□□ □□□ □□ □□□ GRE □
□□ □□□ □ □□ □□□ □□□□□□□. SDWAN □□□□ □□□ □□□ □□ □□ □□ □□□ mGRE □
□ DMVPN□ □□ □□□ □□□ □□□□□ □□□□ □□□ □ □□□□. □□□ □□ □□□□□ □□ □□
□□ □□□□ □□□□□ mGRE□ □□ □□, □□□ □□ QoS□ □□ □□□ □□□ □□□□ □□□ □ □
□□□.

□□

Cisco Dynamic Multipoint VPN □□ - DMVPN, mGRE, NHRP

MGRE □□ □□ - Cisco □□□□□

DMVPN(□□ □□□□□ VPN), NHRP, mGRE□ □□□□ □□□ □□□□□? - Cisco □□□□ □□□□□

□□□□□ □□ □□□□□□ □□□ □ □□□ □□□□□. □□ □□□□ □□□□□ □□ PC□□ □□□ □
□□ □ □□□□. □□ □□ □□□□ □□□□□ □□□□□ ping□ □□□□ □□□□ □□ □□□□ □□□
□.

Ping □□□ □□□ www.google.com□ □□ □ □□□□. □□□ □□□□ □□ □□□□□.

□□□□□ □□□ □ □□ □□□ □□□□□?

□□ □□□□□ □□□□□□ Ping 127. 0. 0. 1□ □□□□□.
 □□ □□□□ □□□□□ □□□□□□.
 □□ □□ □□ □□□ □□ Ping□ □□□□□.
 □□□ DNS □□□□ □□□ □□□ □□□ □□□□□□.
 □□ □□□ "Ping □□□ □□□ www.google.com□ □□ □ □□□□"□ □□□□ □□□□□ PC□ □□□
 □□ www.google.com□ □□ IP □□□ □□□ □ □□□ □□□□□. □□ □□□ □□□ IP □□□ □□□□
 □ □□□ □□□□ DNS(Domain Name System) □□□□ □□□ □□□ □□□□□. DNS □□□□ □□□□
 □□□ □□ □□ □□ □□ □□ □□□□ □□□ □ □□□□.
 □□□□□ □□□ □ □□ □□□ □□ □□ □□ □□□ ping□□ □□□□. □, PC□ □□□□ □□□ □□□
 □□ □□□ □□□ □ □□□, □□□ □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □ □□
 □ □□□□□ □□□□. □□ □□ □□□□□ □□ □□□ □□□ □ □□□□.
 □□ □□□ IP □□□ □□□□ ipconfig /all□ □□□□ DNS □□ □□□ □□□□.
 □□ □□□ ping□□□ ping <□□ □□ IP □□>□ □□□□ □□□ □□□□□ □□□□ □□□□ □□□
 □□.
 □□ □□□ □□□□□□ nslookup <□□ □□□ □□>□ □□□□ □□ □□□ □□□ IP □□□ □□□□□
 □□□□□.

If the ping or the nslookup commands fail, it means that the internal name server is not working properly, and the engineer should troubleshoot the name server configuration or connectivity. If the ping and the nslookup commands succeed, it means that the internal name server is working properly, but there is a problem with the external name resolution, and the engineer should check the internet firewall logs for blocked DNS traffic, or test the website from outside the company.

Reference

Windows 10 can't resolve hostnames - ping with IP works but not with hostname Ping request could not find host xyz.local. Please check the name and try again DNS problem, nslookup works, ping doesn't Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is:

E1/0: 192.168.8.1/24

S1: 192.168.7.252/30

After router and device configurations are applied, internet access is not possible. Which of the following is the most likely cause?

The Ethernet interface was configured with an incorrect IP address.

The router was configured with an incorrect loopback address.

The router was configured with an incorrect default gateway.

The serial interface was configured with the incorrect subnet mask.

The default gateway is the IP address of the router that connects a network to the internet or another network.

The default gateway is usually configured on the devices that need to access the internet or other networks, such as PCs, servers, or routers. If the router was configured with an incorrect default gateway, it would not be able to forward packets to the correct destination, and internet access would not be possible.

The other options are not the most likely causes of the issue. The Ethernet interface is the physical port that connects a device to a network using a cable. If the Ethernet interface was configured with an incorrect IP address, it would cause a problem with the local network connectivity, not the internet access. The loopback

address is a special IP address that refers to the device itself, usually used for testing or troubleshooting purposes. If the router was configured with an incorrect loopback address, it would not affect the internet access, as the loopback address is not used for routing packets to other networks. The serial interface is another type of physical port that connects a device to a network using a serial cable, often used for WAN connections. If the serial interface was configured with the incorrect subnet mask, it would cause a problem with the WAN connectivity, not the internet access, as the subnet mask is used to determine the network and host portions of an IP address.

Reference

What is a Default Gateway? | HowStuffWorks

What is an Ethernet Interface? - Definition from Techopedia

What is a Loopback Address? - Definition from Techopedia

What is a Serial Interface? - Definition from Techopedia

□□□□ □□ □□□□□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□□□□. □□ □□□□□ □□
□□□ □□□ □□□ □□□□□ □□ □ □□ □□ □□□□□?

□ □ □ □

33

□ □ □ □ □

□ □ □ □

□□□ □□□□ □□□□ □□□□ □□□□ ID□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □
□□□ □□□□□ □□□. □□□□□ □□□□□ □□□ □□ □ □□ □□□□□?

□□□(DDoS)

ARP ☐☐☐VLAN ☐ ☐ DHCP

VLAN 1000 00000000 0 00 VLAN00 0000 0000 00 0 00 0000 00 000
00. VLAN 000 00 0000 00 000 0000, 000 0000 000000, 000000 00 0
00 000 0 0000. VLAN 000 0 00 000 0000 000 0 0000. 00 00 00 0 000
0001.

00 00 0000 0000 VLAN 00 VLAN 00 0 00 VLAN 000 00 0000 000 000
 0. 0000 VLAN 000 0000 000 0000 00 0000 0000 VLAN000. 0000 000
 000 0000 VLAN 000 VLAN 00 00 0000 0000 0000 000 0000 00000.
 0000 0000 VLAN 0 00 000 0000 00 VLAN 0 00 000 00 0000 0000. 0
 0 00 0000 00 VLAN 0000 00 VLAN 00000 00000.

□□□ □□□□ □□□□ DTP(Dynamic Trunking Protocol) □□□ □□□ □□□□ □□□□□ □□
 □□□□. DTP□ □□□□ □□□□ □□□□ □□□ □ □□□ □□ Cisco □□□□□□□. □□□□ □□□
 □□ □□ □□ □□ □□ □□□□ □□□ □□□ □□ DTP □□□ □□□□ □□□□ □□□□ □□□□□.
 □□□ □□□□ □□□□ □□ VLAN□ □□□□ □ □□□□.

VLAN 000 0000 00 000 0000 00000 00 0000 ID0 000 00 000 0000 0
000 00 000 0000 00000 000. 0, 00000 000 0000 000 0000 00 000
0 0000 VLAN0 00 VLAN 10 00 VLAN00 00000. 000 00 0000 000 000 00
VLAN0 000 VLAN0 00 0000 0 00 000 00 0000 0000 0000 00 00 000 0

□□ □ □□□□. □□□□□ □□ □□□ □□□□ DTP□ □□□□□□ switchport nonegotiate □□□ □□
□□ □□□ □□□ □□□ □□□□ □□□.
□□

VLAN □□ - NetworkLessons.com

□□□□ VLAN□□□□ VLAN □□ - Cisco □□□□

□□:

CompTIA Network+ N10-008 □□ □□ □□, □□□ 5.0: □□□□ □□, □□ □□ 5.1: □□□ □□ □□□ □
□□ □□, 231□□□ CompTIA Network+ □□ □□□ □□ □□□, 8□(□□ N10-008), 18□: □□□□ □□,
□□: □□□ □□, 7372□□□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□ □□□
□□ □□ □□□□□□. □□□ □□□ OSI □□□ □□ □□ □ □□ □□□□ □□□□□?

1□

3□

4□

7□

NEW QUESTION: 294

□□□□□ □□□□□ □□□ □□□ □□□□ □□ □□ AP□ □□ □□ □□ □□□□□□□.

WAP□ □□□□□ □□□□ □□□ □□ □□ □□□□ □□□ □□□ □□ □ □□ □□□ □□□□ □□ □
□ □□□□?

A. □□□□ □□□

B. □□ □□□□□ □□

C. □□ □□

D. □□ SNMP

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 295

□□ □□□ VPN □□□□□□□ □□□ DHCP □□□ □□□□□.

IP address:	10.0.0.1
Subnet mask:	255.255.255.0
Gateway:	10.0.0.254

□□□□ □□□□□ □□ □□□ □ □□□ □□□□□ □□□ □□ □□□□ 300□ □□□, □ □ 252□□ □
□ □□ VPN□ □□□ □ □□□□. □□□ □□ □□□□ □□ □□ VPN□ □□□ □ □□□□. □□ □□□□
□□□□ □□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □ □□□□?

A. □□□□□ □□□□□.

B. DHCP □□□ □□□□□□.

C. □□□ VPN □□□□□□□ □□□□□

D. □ □□□ □□

Answer: A ([LEAVE A REPLY](#))

□□

DHCP □□□□ □□ □□□ □□□ □□□□□□ IP □□ □□□ □ □□ □□□□ □□ □□ □□□□□□ □
□□ □ □□ IP □□□ □□□□□. □□□□: CompTIA Network+ □□ □□ □□□, 3□: IP □□ □□.

NEW QUESTION: 296

Which of the following is a valid IPv4 address? (Choose two.)
A. 192.168.1.1
B. 192.168.1.255
C. 192.168.1.0
D. 192.168.1.256

- A. 192.168.1.1
- B. 192.168.1.255
- C. 192.168.1.0
- D. 192.168.1.256

Answer: A (LEAVE A REPLY)

NEW QUESTION: 297

Which of the following is a valid IPv4 address? (Choose two.)
A. 192.168.1.1
B. 192.168.1.255
C. 192.168.1.0
D. 192.168.1.256

```
16:35:58.756583 IP (tos 0x0, ttl 64, id 56522, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:58.835371 IP (tos 0x0, ttl 64, id 56523, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:35:59.652312 IP (tos 0x0, ttl 64, id 56524, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
16:36:00.765212 IP (tos 0x0, ttl 64, id 56525, offset 0, flags [DF], proto UDP (17), length 57)
192.168.1.15.44232 > 192.168.1.252.53: 50327 + A? comptia.com. (29)
```

Which of the following is a valid IPv4 address? (Choose two.)

- A. 192.168.1.1
- B. 192.168.1.255
- C. 192.168.1.0
- D. 192.168.1.256

Answer: B (LEAVE A REPLY)

Which of the following is a valid IPv4 address? (Choose two.)

Which of the following is a valid IPv4 address? (Choose two.)
A. 192.168.1.1
B. 192.168.1.255
C. 192.168.1.0
D. 192.168.1.256

NEW QUESTION: 298

Which of the following is a valid IPv4 address? (Choose two.)
A. 192.168.1.1
B. 192.168.1.255
C. 192.168.1.0
D. 192.168.1.256

- A. 192.168.1.1
- B. 192.168.1.255

- C. AP □□
- D. □□ □□
- E. SSID □□
- F. AP □□ □□

Answer: A,C ([LEAVE A REPLY](#))

□□
 □□□ □□□□ □□□□□. WAP □□□ □□□ □□□□ □□□. □□□ □□ □□□□ □□□ □□□ □□
 □ □□ □□□.

NEW QUESTION: 299

□□ □□□□□ A □□□□ □□□□□ □ □□ □□□□ □□□□□ □□□ □ □□□□□. □□□ □□□□
 □□ □□ □ □□ □□ □□□□ □□□?

- A. □□
- B. MX
- C. □□□
- D. □□□ □□ □□□□(SOA)

Answer: ([SHOW ANSWER](#))

□□
 TTL(Time To Live)□ A □□□□ □□□□□ □ □□ □□□□ □□□□□ □□□□ □ □□ □□□ □□□□
 □□ □□□□ □□□. TTL□ DNS □□□□ □□□□ □□ □□□ □□ □□ DNS □□□ □□□□□□ DNS
 □□□□ □□□□ □□ □□□ □□□□ □□□□. TTL□ □□ □□□ □□ DNS □□□ □□□□□□ □□□
 □□ □□ IP □□□ □□□□ □□□ A □□□□ □□ □□□□ □□□ □□□ □ □□□□. TTL□ □□□ DNS
 □□□ □□□□□□ □□□ □ □□ □□□□□□ □□□□□ □□ IP □□□ □□□□ □ A □□□□ □□□
 □□. □□:

<https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/>

NEW QUESTION: 300

□□ □ □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □ □□□
 □?

- A. F□
- B. RJ45
- C. LC
- D. RJ11

Answer: ([SHOW ANSWER](#))

F□ □□□□ □□□ □□□ □□ □□□ □□□□ □ □□□□□ □□□□ □□ □□□ □□□□□. □□ □□
 □ □□□ □□□□□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□□. F□ □□□□ □□□□□ □□
 □□, □□□ □□ □ □□ □□□ □□□ □□□□ □□□ □□□□□□.

NEW QUESTION: 301

□□□□ □□□□ □□ □□□□□ □□ □□□ □□□□ □□□□. □□□□ □□□ □□□□ □□ □□□ □
 □□□□.

Tracing route to 10.10.0.22 over 30 hops:

1	14ms	20ms	15ms	192.168.1.253
2	10ms	15ms	12ms	172.16.0.21
3	5ms	10ms	10ms	10.10.5.3
4	10ms	15ms	12ms	10.12.2.1
5	5ms	10ms	10ms	10.10.5.3
6	10ms	15ms	12ms	10.12.2.1
7	5ms	10ms	10ms	10.10.5.3
8	10ms	15ms	12ms	10.12.2.1

□□ □□□ □□□ □□□□□?

A. □□□ □□

B. □□□ □□□

C. □□ □□

D. □□ □□

Answer: A ([LEAVE A REPLY](#))

□□

□□ □□□ □□□ □□□□□. □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□
□□ □□□ □□□□□. □□□ □□□ □□ □□□□□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □
□□□□□ □□ □□□ □□□□□ □□ □□□ □ □□□□. □□□ □□□ traceroute □□□ □□□□ □□
□ □□□, □ □□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□. □□□□ traceroute □□□ □
□□ □ □□□ 10.12.2.1□ 10.12.2.2 □□□ □□□ □□□□ □□□ □□□□, □□ □□□ □□□ □□□□
□. □□: CompTIA Network+ N10-008 □□ □□ □□□, 181□□□; □□ CompTIA Network+ □□ □□□(□
□ N10-008), 7-9□□□.

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:
KrDump)

NEW QUESTION: 302

□□□□□ □□□ □ □□ □□□ □□ IDS□ □□□□□□□. IDS□ □□□ □□□□□□ □□□□ □□□□
□ □□ □□□□□□□. □□ □□□ □□□□ □□ □□□ □□ □□ □□ □□ □□□□ □□□?

A. □□□□ □

B. □□□ □□

C. UTM □□□□□□

D. □□□ □□

Answer: C ([LEAVE A REPLY](#))

UTM □□□□□□□ Unified Threat Management □□□□□□□ □□□□, □□ □□ □□□ □□□ □□□
□□ □□□ □□□□□. UTM □□□□□□□ □□□, IDS/IPS, □□□□ □□, VPN, □ □□□ □ □□ □□
□□□□ □□□ □ □□□□. □□□□□ □□□□ □□ □□□□□ IDS □□ UTM □□□□□□□ □□□□ □□ □

□□ □□□ □ □□□□. UTM □□□□□□□ □□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ □□
□ □ □□ □□□□□. □□: <https://www.comptia.org/blog/what-is-utm>

NEW QUESTION: 303

□□ OSI □□ □□ □ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□ □□□□□?

- A. □□
- B. □□□ □□
- C. □□□□
- D. □□

Answer: (SHOW ANSWER)

□□

□□ □□□ OSI □□□ □ □□ □□□□, □□□□□ □□ □□□□ □□ □ □□□ □□□□□. TCP, UDP, DCCP□ □□ □□ □□□□□ □□□□ □□□ □□□□□□. □□ □□□ □□ □□ □ □□□ □□□□ □□ □□□□□ □□□ □□□ □□□□□ □□ □□□□. □□ □□□ □□, □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□.

NEW QUESTION: 304

□□ □ SOHO □□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?

- A. RG6
- B. 6□□
- C. RJ11
- D. □□□□ □□□

Answer: A (LEAVE A REPLY)

RG6□ □□□ TV□ □□□ □□□□ □□□□□ □□□□ □□ □□□□ □ □□□□□. □□□ □□□ □□ □□□ □□□□□ □□ □□□ □□ □ □□□□ □□□ □□□ □□□□ □□□□□. SOHO □□□ □□□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□ □□□ □□□/□ □□□ □□□ □□□□. □□□ RG6□ SOHO □□□□ □□□ □□□ □□ □□□ □□ □□□□□. □□□□: [CompTIA Network+ □ □□ □□], RG6 □□□□□? | Techwalla

NEW QUESTION: 305

□□□ □□□□□□□□□ □□□ □ □□□□ □□□□□ □□□. □□□□ □□ □□□ □□□□ □□ □□ □ □□ □□ □□□□ □□□?

- A. □□ □□□
- B. OSPF □□□
- C. □□ □□□
- D. NIC □ □□
- E. □□□ □□

Answer: A (LEAVE A REPLY)

□□ □□□□ □□□□□□□□□ □□ □□□ □□□□ □□□□□ □□ □□□□□□. □□ □□□□ □□□ □□ □□□ □□□□□ VLAN□ □□□□ □□□ □ □□□, □□ □□ □□ □□ □□ □□ □□□□ □□□□

<https://www.comptia.org/blog/what-is-a-virtual-switch>

□□□□ □□□□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□□. □□□□ □□□ □□□ □
□□□□ □□□. □□ □□□ □□□□□.
□□ □ □□ □□□ □□□ □□□ □□□ □□□□□□□?

- Answer: ([SHOW ANSWER](#))**

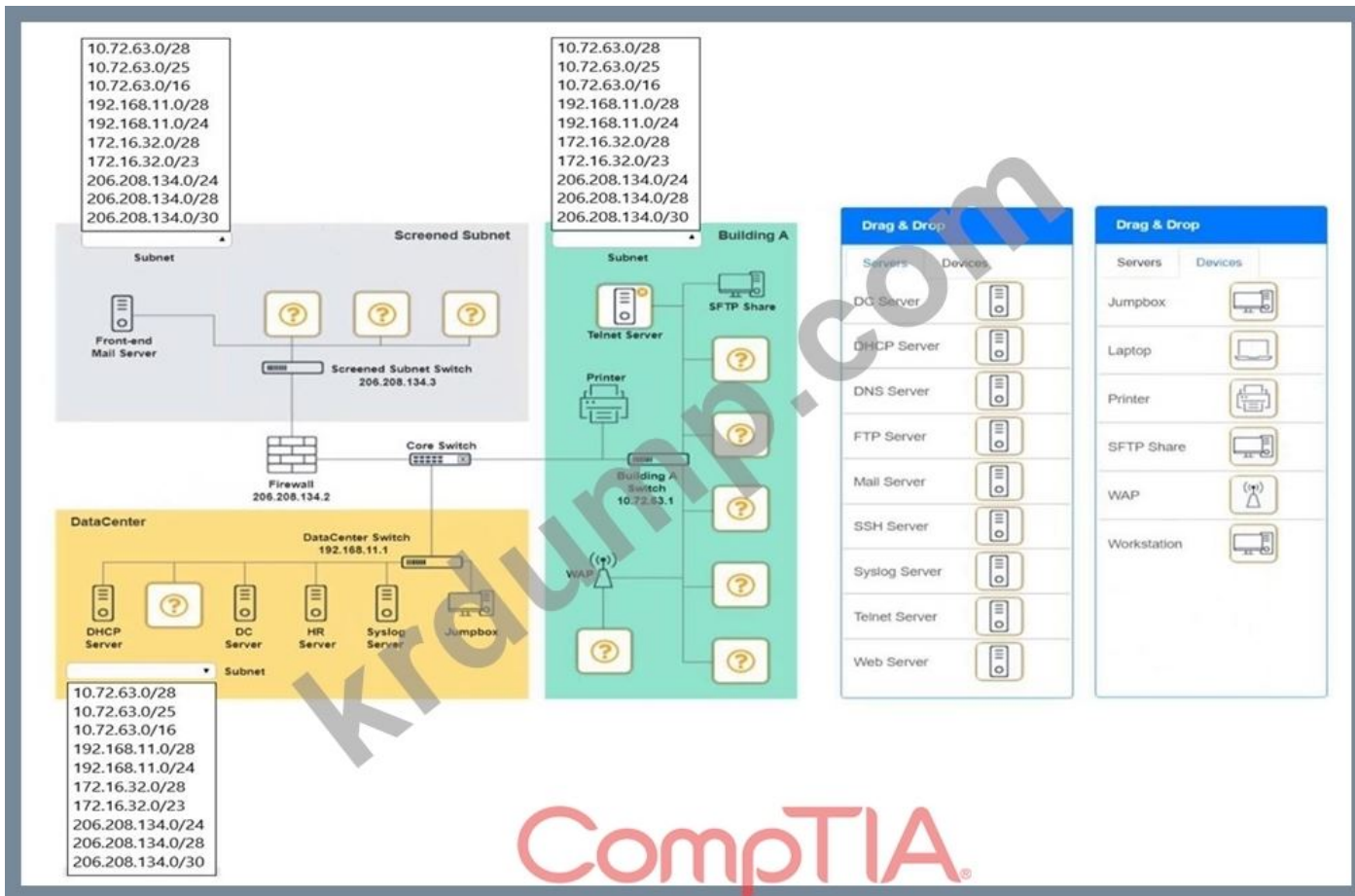
□□□□+ N10-008 □□: 2.1 □□□ □□□□□□ □□□□ □□□ □□ □□□ □□□□□.

□□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□□ □□□□ □□□ □□ □□□□.

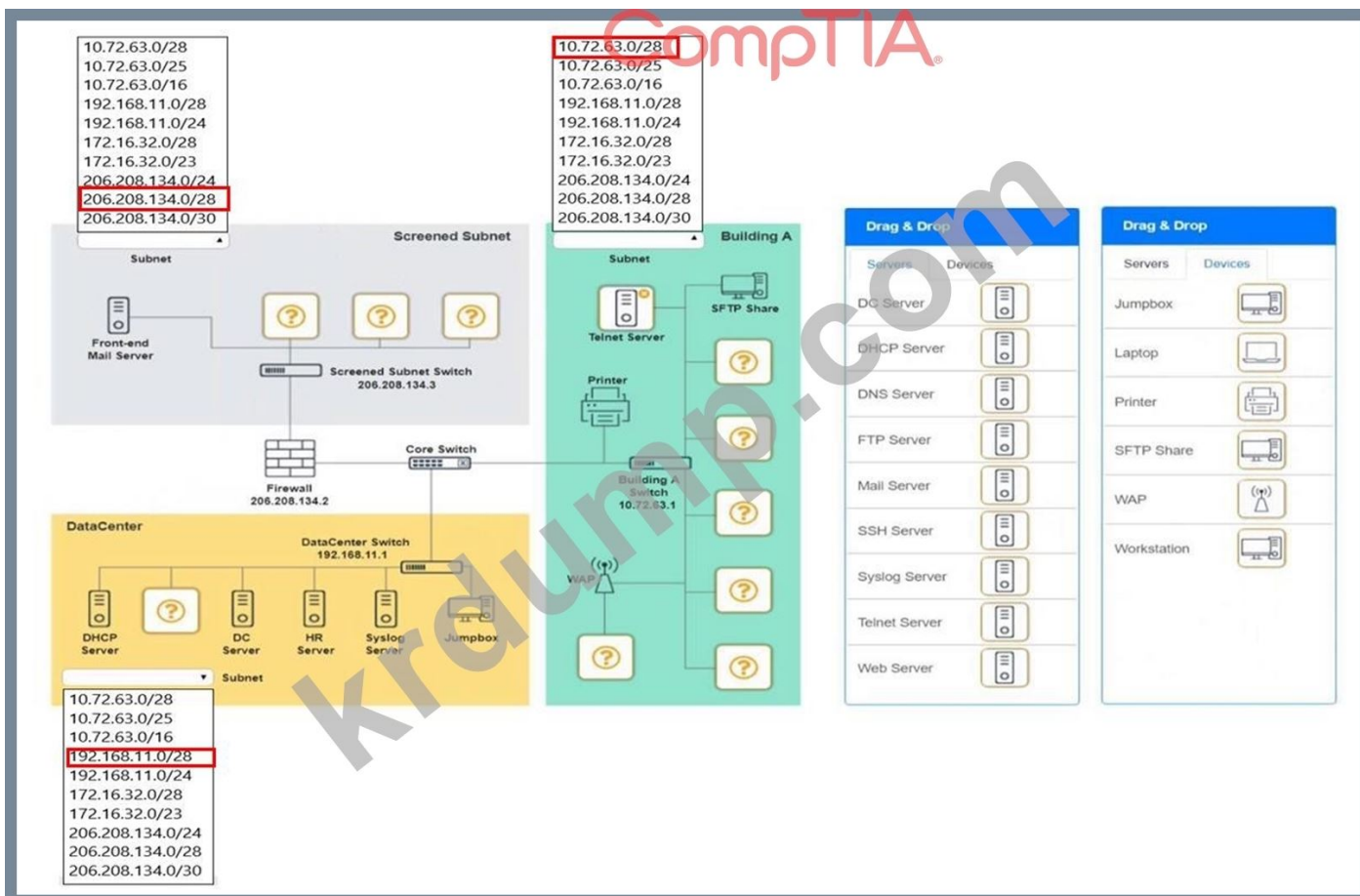
□□ □□:

□□□□□

```
00: 00000 00 00 000 000000 00 000 000 000 0 000 00000 0000 0
00 0000000.IP 0000 0000 0000 00000 00000 00 53 00000 00000 00 000 000
000.00 A 000000 00 00 000 0000000 00 000 000 000 0 000 000000 0
0000 0000 0000000.500 00 000 00000 00000 0000 0000000.00 0000 00000
0000000.Telnet 0000 00 000 000000 0000000.000000 0000 000000 00 00 0
00 0000000 00 0000 0000 0000 0 0000 000000 00000 0000 0000000.00
80/443 00000 00000 0000 0000000.00 20/21 00000 00000 0000 0000000.00 00
0 0000 0000 0000 00000.0000 00 0 0000 0 0000 00 000 00000 00 0000 00000.
00 0000 0000 0000 0 00 0000 00 0 00 00 00 0000.
00000 00000000 00 0000 000000 '00 000' 0000 000000.
```



Answer:



NEW QUESTION: 308

AP 98(30m) Cat 6 □□□□ □□□□ □□□ □□□□ □□□□□. □□□□ 3□ □□ □□ □□□ □□
 □□□ □□□□□. 3□□ □□ □□□ □□□□ □□□ □□ □□□□ □□□□□□ □□ □□ □□□ □□□
 □□. □□ □ □□ □□□□ □□ □□ □□□□□?

- A. ☐ ☐
- B. ☐ ☐
- C. ☐ ☐ ☐ ☐
- D. ☐ ☐

Answer: ([SHOW ANSWER](#))

১০০০ ০০ ০০ ০০০ ০০০০ ০০০০০০ ০০০ ০০০ ০০০০ ০০০ ০০০ ০০ ০ ০০০০ ০০
 ০০০. ০০০ ০০ ০০, ০০ ০০০, ০০ ০০ ০০ ০০০ ০০ ০০০০ ০০০ ০০০ ০ ০০০০. ০০
 ০ ০০০০, ০০, ০০০ ০০ ০০ ০০০ ০০ ০০০ ০০ ০০০ ০ ০০০০. ০ ০০০০০০ 3০
 ০০ ০০০ AP ০০০ ০০০০ ০০০০ Cat 6 ০০০০ ০০০ ০০০ ০০ ০০০০০. ০০০০ ০০ ০
 ০০ ০০০ ০০০ ০০ ০০০০ ০০০০ ০০০০০ ০০০০০.
 ০০০০ ০০ ০০০০ ০০০০০ ০০ ০০০০০ ০০০০ ০০ ০০০০০০ ০ ০০ ০০০০ ০০০০০০.

NEW QUESTION: 309

□□ □□ IP □□ 6□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □□ □□□ □
 □ □□ □□□ □□ □□ □□□ □□□. □□□ □□ □□ □□□ □□□□ □□ □□□□ 0□ □□□, □□
 □ □□ □□ 2^□□□ □□ - 2□□□(-2□ □□□□ □□□ □□□□□□ □□□ □□□□ □□□□). 6□ □□
 □ □□ □□ □□□ □□ □□ □□ □□□ □□□ □□□□□. □ □□□ □□ □□□ □□□ □□□□.

- A. 255.255.255.128**

□□□: 11111111.11111111.11111111.10000000

□□□ □□:7

□□□ □□: $2^7 - 2 = 126 - 2 = 124$

☐ ☐☐☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐

- B. 255.255.255.192**

□□□: 11111111.11111111.11111111.11000000

□□□ □□: 6

□□□ □□: $2^6 - 2 = 64 - 2 = 62$

☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐

- C. 255.255.255.224**

□□□: 11111111.11111111.11111111.11100000

□□□ □□: 5

□□□ □□: $2^5 - 2 = 32 - 2 = 30$

[illegible]

- D. 255.255.255.240**

□□□: 11111111.11111111.11111111.11110000

:4

□□□ □□: $2^4 - 2 = 16 - 2 = 14$

Which of the following is the correct formula for calculating the number of subnets?

Answer: C (LEAVE A REPLY)

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID.

$2^n = 2^6$ where n is the number of bits used for the network ID. $2^6 = (2^2 - 1) \times 2^2 + 1 = 3$. Therefore, there are 3 subnets. The first subnet is 192.168.1.0/27, the second is 192.168.1.0, and the third is 192.168.1.0. The first subnet is 192.168.1.0/27, the second is 192.168.1.0, and the third is 192.168.1.0. The first subnet is 192.168.1.0/27, the second is 192.168.1.0, and the third is 192.168.1.0.

11

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID.

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID.

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID.

1: CompTIA Network+ 110-008 1.41 2: IPv4 110-008 CompTIA Network+: 1.41 3: IPv4 110-008 CompTIA Network+: 1.44

NEW QUESTION: 310

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID.

- A. $2^n = 2^6$
- B. $2^n = 2^2$
- C. $2^n = 2^2 - 1$
- D. $2^n = 2^2 + 1$

Answer: A (LEAVE A REPLY)

Which of the following is the correct formula for calculating the number of subnets?

Which of the following is the correct formula for calculating the number of subnets? 6 bits are used for IP addressing, 2 bits are used for the network ID and 2 bits are used for the host ID. (OSI 7 layers model) The first layer is the physical layer, the second is the data link layer, the third is the network layer, the fourth is the transport layer, the fifth is the session layer, the sixth is the presentation layer, and the seventh is the application layer.

NEW QUESTION: 311

A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.0.1
- D. 255.255.255.0

Answer: B (LEAVE A REPLY)

127.0.0.1 is the loopback address, it is used to test the functionality of a network card by sending traffic to the card and then verifying that it is received properly. This address is used because it is guaranteed to always

point to the local host, regardless of the network configuration. The IP address range for loopback addresses is 127.0.0.0/8.

NEW QUESTION: 312

□□□□ LACP □□□ □□□ □□□□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□ □□ □ □□
□□□□?

- A.** □□□□□ □□
B. □□ □□
C. □□
D. arp □□

Answer: A (LEAVE A REPLY)

IEEE 802.3ad□ □□ □□ □□□ LACP□ □□ □□ □□(LAG)□ □□ □□ □□□ □□□□□. □□ □□ □
□□ □□□□ □□ □□□ □□□ □□□□□□ □□□□ LAG, □□ □□ □□ □□□□□ □□ □□□ □□
□ □□□ □□□□□.

NEW QUESTION: 313

□□□□ □□ □□□□□ □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□ □□ □□□. □□ □
□□ □□□ □□ □□ □ □□□□□□?

- A.** □□ □□ □□
- B.** □□ □□□ □□
- C.** □□ □□ □□
- D.** □□ □□□ □□ □□

Answer: C (LEAVE A REPLY)

□□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□, □□□□ □□ □□□ □
□, □□□, □□□□ □□□ □□□□□. □□□□ □□ □□ □□□ □□□ □□□□□ □□ □□□□ □□□ □
□□□ □□ □□ □□□ □□□□□ □ □□□□. □□:

* □□□□+ N10-008 □□: 1.6 □□□□□ □□□□ □□□□ □□□ □□ □□ □□ □□□ □□□□□.

NEW QUESTION: 314

□□□□□ □□□ □□□□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□. □□ □□ □□□ □□ □□□□ □□□ □□□□ □□ LAN □ □□ □□ IP □□□□ □□□□□ □□□. □□ □ □□ □□ □□□ □ □□ □□□ □□□□ □ □□□ □□□□ □ □□□ □□□?

- A.** □□□□ □□□ □□
- B.** □□□ □□
- C.** □□□□ □□ □□ □□
- D.** Zero Trust □□ □□

Answer: A (LEAVE A REPLY)

A screened subnet is a network topology that uses two firewalls to isolate a segment of the network from both the internal LAN and the internet. The screened subnet, also known as a demilitarized zone (DMZ), hosts the internet-facing servers that need to be accessible from outside the network, such as web servers, mail servers, or DNS servers. The first firewall, also known as the external firewall, filters the traffic between the internet and

the DMZ, allowing only the necessary ports and protocols to pass through. The second firewall, also known as the internal firewall, filters the traffic between the DMZ and the internal LAN, allowing only authorized and secure connections to access the internal resources. This way, the screened subnet provides a layer of protection for both the internet-facing hosts and the internal LAN from potential attacks¹².

The other options are not defense strategies that help meet the design requirement of partitioning off the internet-facing hosts from the internal LAN and internal server IP ranges. Deploying a honeypot is a deception technique that lures attackers to a fake system or network that mimics the real one, in order to monitor their activities and collect information about their methods and motives. However, a honeypot does not isolate or protect the internet-facing hosts from the rest of the network³. Utilizing network access control is a security method that enforces policies on who or what can access the network resources, based on factors such as identity, role, device type, location, or time. However, network access control does not create a separate segment for the internet-facing hosts from the internal LAN. Enforcing a Zero Trust model is a security paradigm that assumes no trust for any entity inside or outside the network, and requires continuous verification and validation of every request and transaction. However, a Zero Trust model does not necessarily imply a specific network topology or architecture for separating the internet-facing hosts from the internal LAN.

NEW QUESTION: 315

□□ □□□ □□□□:

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which of the following would cause performance degradation between PC A and PC B'?

- A. Incorrect pinout
- B. Interference
- C. Decibel loss
- D. Attenuation

Answer: (SHOW ANSWER)

NEW QUESTION: 316

□□□ □□□□ PoE □□ WAP □ □□ □□□□. □□□ □□□□□ □, □□□ □ □□□ □□□ □□□ □□ □□□□□□□□. □□□ WAP□ □□ □□□ □, □□□□□ □□ □□□ □□□□□□ □□□ □□□□□□ □. □□□ □□□□□ □□□ □□, □□ CRC □□□ □□□□□□□□. □□□□ □□□□□ □□□ □□□ □ □□ □□, UTP □□□□ □□□□□□ □□ □□□□□□□. □□ □ CRC □□□ □□ □□□ □□ □□□ □□ □□□?

- A. □□□□ □□□ □□□□□.
- B. PoE□ UTP □□□□
- C. □□□ □□
- D. □□□ □□□ □□□

Answer: C (LEAVE A REPLY)

□□

"□□□□ □□□□□ □□□□ □□ □□ □□ □□□ □□□ □ EMIO □□□ □□□. □□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □ □□□□. □□□□ □□□ EMIO □□□ □□ □ □□□ □□□□. □□ □□□ □□ □(UTP) □□□□ EMIO □□□ □□, □ □□□ □□ □□□ □□□□ EMIO □ □□□□. □□ □□□ □□□ □□ □□□ □□□□□ EMIO □□□ □□ □ □□ □□□ □□□□□."

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□

N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□ □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 317

A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Choose two.)

- A. ARP table
- B. DHCP leases
- C. IP route table
- D. DNS cache
- E. MAC address table
- F. STP topology

Answer: A,B (LEAVE A REPLY)

A DHCP lease is a temporary assignment of an IP address to a device on the network.

MAC address table maps MAC addresses to switchports where the owners of individual MAC addresses are attached.

ARP table maps IP addresses of directly attached neighbors to their MAC addresses.

NEW QUESTION: 318

□□□□□

□□□□ □□ □□□□□ □□□□ □□□ □□□□□. □□□□□ □□□ □□□ 3□□ □□□ 1□□ □□□ □□. □□□□□ □□ □□□□□ □□□□ □□□.

SSID□ S3cr3t □□ □□□□ CorpNet□□ □□□□□ □□□!

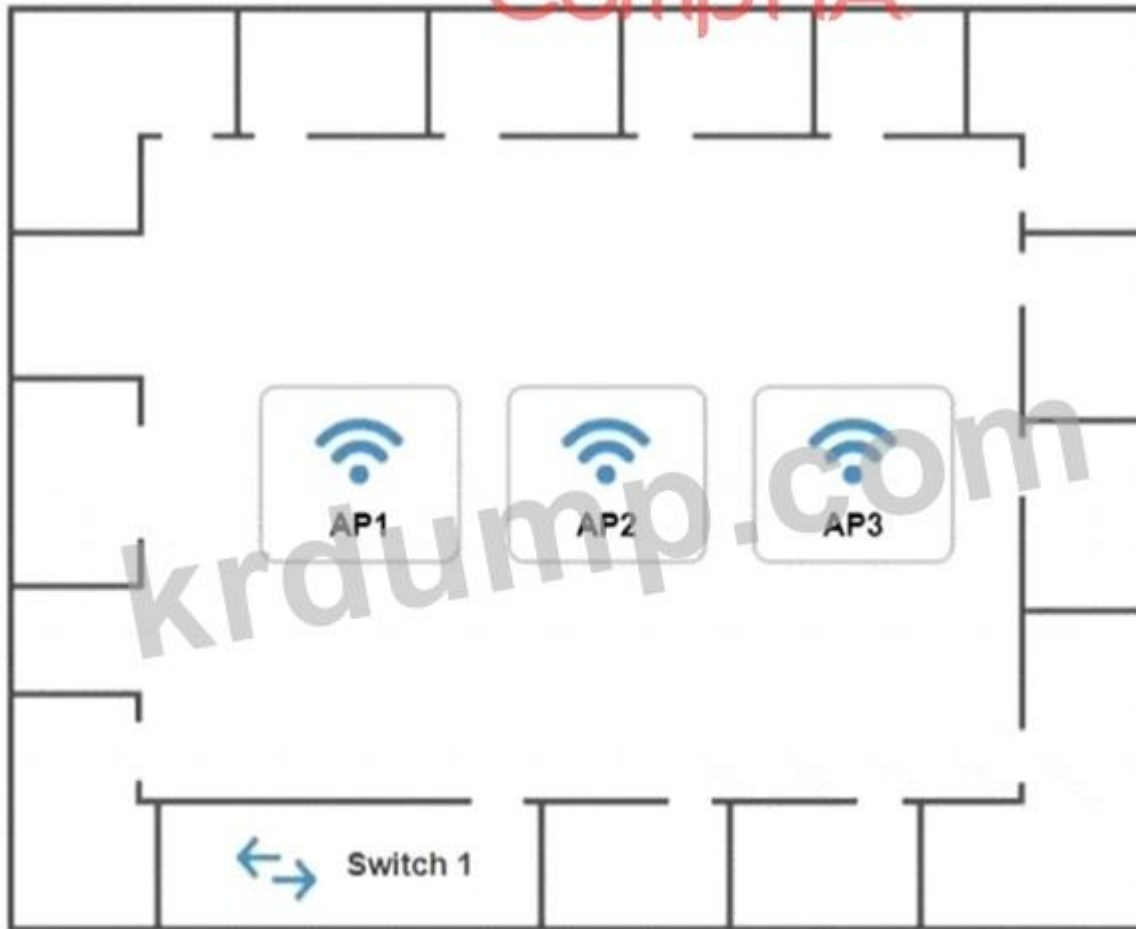
□□ □□□ □□ □□□□□ □□□□.

□□□ □□□□ □□□□ □□ □□□□ □□ 30□□ □□□ □□□□ □□□. □□□ □□□□ □□ □□□

TKIP □□□□□□ □□□□□ □□□□ □□□. □□ □□ □□□ □□□□ □□ □□□ □□□ □, □□□ □ □□□ □□□□□ □□□ □□□□ □□□ □□□□□.

□□□□ □□□□□□ □□ □□□ □□□□□ '□□ □□□' □□□ □□□□□.

CompTIA



192.168.1.2
Speed: Auto
Duplex: Auto

AP1 Configuration

CompTIA



https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B
G

Channel

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP2 Configuration



https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast



Yes



No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed



Auto



100



1000

Duplex



Auto



Half



Full

Security Configuration

Security Settings



None



WEP



WPA



WPA2



WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration



https://ap3.setup.do

Basic Configuration

Access Point Name

IP Address /

Gateway

SSID

SSID Broadcast ☒ Yes ☐ No

Wireless

Mode

B
G

Channel

1
2
3
4
5
6
7
8
9
10
11

Wired

Speed ☐ Auto ☒ 100 ☐ 1000

Duplex ☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

Answer:

□□ □□□ □□□□□.

□□:

□ □□ □□□ □□□□□ □□□ □□□ □□□.

The screenshot shows the 'AP1 Configuration' web interface. The browser address bar displays 'https://ap1.setup.do'. The 'Basic Configuration' section includes fields for 'Access Point Name' (AP1), 'IP Address' (192.168.1.32), 'Gateway' (192.168.1.1), 'SSID' (CorpNet), and 'SSID Broadcast' (Yes). The 'Wireless' section shows 'Mode' (B) and 'Channel' (3). The 'Wired' section shows 'Speed' (100) and 'Duplex' (Full).

□□□ □□□ □□□□□, □□□, □□□□□□, □□ □□ □□ □□□ □□□ □□□ □□□

The screenshot shows the 'Security Configuration' web interface. The 'Security Settings' section has radio buttons for 'None', 'WEP', 'WPA', 'WPA2', and 'WPA2 - Enterprise' (selected). The 'Key or Passphrase' field contains the text 'S3cr3t!'.

□□□ □□□ □□□□□ □□ □□ □□

AP1 Configuration

https://ap1.setup.do

IP Address	192.168.1.32	/	27
Gateway	192.168.1.1		
SSID	CorpNet		
SSID Broadcast	☒ Yes ☐ No		

Wireless		Wired	
Mode	B	Speed	☐ Auto ☒ 100 ☐ 1000
Channel	3	Duplex	☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

□□□ □□□ □□□□□, □□□, □□□□□□, □□ □□ □□ □□□ □□□ □□□ □□□

Security Configuration

Security Settings ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase S3cr3t

□□□ □□□ □□□□□ □□ □□ □□

AP1 Configuration

←

→

↺

https://ap1.setup.do

IP Address

192.168.1.3

/

27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes

☐ No

Wireless

Mode

G

Channel

3

Wired

Speed

☒ Auto

☐ 100

☐ 1000

Duplex

☒ Auto

☐ Half

☐ Full

Security Configuration

Security Settings

☐ None

☐ WEP

☒ WPA

☐ WPA2

☐ WPA2 - Enterprise

Key or Passphrase

S3cr3t!

Reset to Default

Save

Close

□2□□ □□□ □□□□.

□□□ □□ AP2

□□□ □□□ □□□□□ □□ □□ □□

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

192.168.1.96 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

9

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

□□□ □□□ □□□□□, □□□, □□□□□□, □□ □□ □□ □□□ □□□ □□□ □□□

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

□□□ □□□ □□□□□ □□ □□ □□

AP3 Configuration

CompTIA

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

Wireless

Mode: G

Channel: 9

Wired

Speed: ☒ Auto ☐ 100 ☐ 1000

Duplex: ☒ Auto ☐ Half ☐ Full

Security Configuration

Security Settings: ☐ None ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

Reset to Default Save Close

NEW QUESTION: 319

□□□ □□□□□□□□ □□□ □ □□□□ □□□□□ □□□. □□□□ □□ □□□ □□□□ □□ □□ □
 □□ □□ □□□□ □□□?

- A. OSPF □□□
- B. NIC □ □□
- C. □□ □□□
- D. □□ □□□
- E. □□□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 320

A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

- A. Disable DHCP on the computer being removed.

- B. Place the switch port in a private VLAN.
- C. Apply a firewall rule to block the computer's IP address.
- D. Remove the employee's network access.

Answer: (SHOW ANSWER)

The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions.

The other options are not as effective or necessary as removing the employee's network access. They are:

- * Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
- * Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the network through another port or device.
- * Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.

Reference

- 1: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media
- 2: Network+ (Plus) Certification | CompTIA IT Certifications
- 3: 10 Ways to Secure Office Workstations - Computer Security

NEW QUESTION: 321

WAN □□□□ □□□ □□□□ 8□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□. □□ □ □□ □□□□ □ □□ □□□□□?

- A. □□□□ □□ □□□
- B. VLAN □□
- C. □□□ □□□
- D. □□ □□ □□

Answer: D (LEAVE A REPLY)

□□

□□ □□□ □□□□□ □□ □□□ □□□□ □□ □ □□□ □□ □□□ □□ □□□□□ □□□□□.

□□□ □ □□ □□□ □□ □□□ □□□□ WAN □□□ □□□ □ □ □□ □□□ □□□ □□□ □□□□ □□□.

□□□□: Network+ □□ □□□ □□ 2.1: □□□□ □□□□ □□□□ □□□□□.

NEW QUESTION: 322

IT □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□ □□□ □□□ □□□□□. □□□□ □□ □□□ □□ □ □□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□?

- A. □□□ □□

- B. nslookup
- C. □□ □□
- D. □□□□□ □□
- E. □□□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 323

□□□□ □□□□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□□. □□□□ □□□ □□□ □
□□□□ □□□. □□ □□□ □□□□□.

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

□□ □ □□ □□□ □□□ □□□ □□□□□□□□?

- A. □□□□□ □□□
- B. □□ □□ □
- C. CRC
- D. □□□
- E. □□□□□

Answer: C (LEAVE A REPLY)

CRC□ Cyclic Redundancy Check□ □□□, □□ □□□□ □□□ □□□ □□□□ □□ □□ □
□ □□□□□. □□ □□□□□□□ CRC □□□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□
□ □ □□□ □□□□□. □□:
□□□□+ N10-008 □□: 2.1 □□□ □□□□□□ □□□□ □□□ □□ □□□ □□□□□.

NEW QUESTION: 324

□ □□□ □□□ 1,000ml(1,609km) □□□ □□□ SAN□ □□□□ □□□ □□□□ □□□□ □□□□. a. □
□ □ □□ □□□ □□□ □□□□□ □□ □□ □□□□□□□?

- A. iSCSI
- B. FCoE
- C. □□□
- D. FC

Answer: (SHOW ANSWER)

□□□ □□□□

"□□□ □□ □□□ □□□ □□□□□(iSCSI)□ TCP/IP □□ □□□□ SCSI □□□□□ □□□□ □□□ □ □□□ □□ □□ □ □□ □□□□□ □□□□ □□ □□□□□□ □□□ □ □□□ □□□." □□□ □□

"iSCSI(IP Small Computer System Interface)

- □□□ □□□(<10Gbps)□ □□□□ □□□ □□ □□
- □□□□□ □□ □□ □□□□ □□□□ □□□ □□□□□.

NEW QUESTION: 325

□□□□ □□□□ □□□□ □□□ □ □□□ □□□ □□ □□□□ □□□□. □□□□ IP □□□ DHCP □□ □□ □□□□□□, □□ □□□□ □□ □□□□ □□ □□□ ping□ □ □□□□. □□ □ □□ □□ □ □□ □ □□ □□ □ □□□□□?

- A. VLAN□ □□□□ □□□□.
- B. DNS □□
- C. DHCP □□ □□
- D. □□□□□□ □□□□ □□□□.

Answer: ([SHOW ANSWER](#))

VLAN□ □□□ □□□ □□□□□□ □□□ □□□□□ □□□□ □□ □□ □□ □□□□□□□□. VLAN□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□□ □□, □□ □ □□□ □□□ □ □□□□.

DHCP □□□ □□□□ □□□□ MAC □□□ □□ □□□ □□ IP □□□ □□□ □ □□ □□□□□□. □□ □ □ □□□ □□□□□ □□□ □□□□□□□□ □□□ □□ DHCP □□□□□ □□□ IP □□□ □□□□□ □ □□□□.

□□□□ □□□□ □□□ □□□□□□ □□ □□□□ □□□ □ □□ □□□□□. □□□□ □□□□□ □□ □□□□ TCP/IP □□□□□ □□□□ □□ □□□ □□□ □ □□ □□ □□□□ □□□□□ □□(NIC)□ □□□ □.

□□ □□□ □□ □□□□□□ □□ □□□ □□□□ □□ □□ □□□□□ □□□□□□□□□□. □□ □□□ □□ □□□ □□, □□□ □□□□ □□ □ □□□ □□ □□□□□ □□ □□ □□□ □□□ □ □□□□.

□□□□ □□□ □ □□□□□ □□□□ □□□ □ □□□ □□ IP □□□□□ □□□ □□□□□. □□□□ □ □□□ □□□ □□□ □□□ □□□□ □□□□, □□ □□□ □□ □□□ IP □□ □□□ □□□□□. □□□ □□□ □ □□ □□□ □□□ □□□ □□ □□ □□□ □ □□□□.

ping□ □□ □□□ □□□□□ □ □□ □□ □□□□ □□ □□□□ □□□□ □□ □□□□□.

ping □□□ □□□□ □□, □□□ □□, □□□ □□ □□ □□ □□ □□ □□□ □□□ □□□ □ □□ □□.

□□□ □□□, □□□□ □□□□ □□□ □□□□ □□ □□ □□□□ ping□ □□ □ □□ □□□ □□□ □ □□□□. □, □ □□ □□ 2□□ □□□ □□□ □□ □□□□. □□ MAC □□□ VLAN□ □□ □□□□□. □ □□□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □ □□□ □ □□□ □□□□. □□ □□□ IP □□□ □□□□□□ □□ □□□□ 3□□ □□□ □□□ □□□ □□□ □□□□ □ □□□. DNS □□□ IP □□□ □□□□ □□□ □□□ □□□□ □□□□ ping □□□ □□□ □□□ □□□ □□. DHCP □□ □□□ □□□□ □□□ □□□ □□□□. IP □□□ □□□□ DHCP □□□ □□ □□□□□. □□□ □□□□□□ □□ □□□□□ □□□ □□□□□ □□ □□□□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□. □□:

CompTIA Network+ N10-008 □□ □□□, 2□: □□□□ □□ □ □□, 2.2□: □□□□ □□ □□ □ □□, □□ □□: □□ □□, 76-77□.

CompTIA Network+ N10-008 □□ □□□, 3□: □□□□ □□, □□ 3.3: □□□□ □□ □□, □□ □□: DHCP, 144-146□.

CompTIA Network+ N10-008 □□ □□□, 4□: □□□□ □□, □□ 4.2: □□□□ □□□ □ □□, □□ □□: VLAN, 202-204□.

Messer □□□ CompTIA N10-008 □□□□+ □□ □□, □□ 1.5: □□□□ □□ □□ □□□, □□ □□: □□ □□, 16-17□.

Messer □□□ CompTIA N10-008 □□□□+ □□ □□, □□ 2.2: □□□□ □□, □□ □□: □□ □□, p. 28.

Messer □□□ CompTIA N10-008 □□□□+ □□ □□, □□ 2.6: □□□□ □□ □□, □□ □□: DHCP, p. 38.

Messer □□□ CompTIA N10-008 □□□□+ □□ □□, □□ 2.7: □□□□ □□ □□, □□ □□: □□□□, p. 39.

Messer □□□ CompTIA N10-008 Network+ □□ □□, □□ 3.5: □□□□ □□□, □□ □□: VLAN, p. 58.

NEW QUESTION: 326

□□□□ □□□□ □□ □□□ □□□□ □□□□. □□□□ □□ □□ □□□□ □□□□□ □□□□□ □□ □ □□□ □□□□□ □□ □□□□ □□□□□ □□□ □□□□ □ □□□□. □□□□ □□□ □□□ □□ □ □□ □□□ □□□□.

32□□□□ □□□□ comptia.com[172.67.217.56]□ ping□ □□□ □□□□.

172.67.217.56□□ □□: TTL□ □□ □□ □□□□□□□.

172.67.217.56□□ □□: TTL□ □□ □□ □□□□□□□.

172.67.217.56□□ □□: TTL□ □□ □□ □□□□□□□.

172.67.217.56□□ □□: TTL□ □□ □□ □□□□□□□.

□□ □ □ □□□ □□□ □□ □ □□□□ □□ □□□□□?

A. VLAN □□□ □□□□□□□.

B. □□ □□□ □□

C. DNS □□

D. □□□□ □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 327

□□□□ □□ □□□□ □□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □□□ □.

- □□□□ □□ □□□ □□□□ □□□□ □ □□□ □□ □□□.

□□ □□.

- □□ □□□ □□□□ □□ □□□□□ □□□□ □□□□.

□□ □□.

□□□□ □□ □□□□ □□□□ □□□ □ □□ □ □□ □□□ □□□□ □□□? (□ □□□ □□□□□.)

A. □□□ □ VPN

B. □ □□ VPN

C. ☐ ☐ VPN

D. □□□□□□□ VPN

E. ☐☐☐ ☐☐ VPN

F. ☐☐☐☐☐-☐☐☐ VPN

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 328

□□□ □□□□ □□ 80□ □□ 443□□ □ □□□ □□□□ □□□□ □□ □□□ □□□□□.

☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐.

□□ 443□ □□□. □□□ □□□□ □□□ □□□□ □□ □ □□□ □□□ □□□□□ □□□□ □□□. □□

□ □□□□ □□ □ □□□ □□ □□□?

A. □□□ □□ □□□ □□□□□.

B. □□ 80□ □□□□□ □□□ □□□□□.

C. □□□ □□□□ □□ □□□ □□□□□.

D. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

Answer: A (LEAVE A REPLY)

□□□ □□ □□□ □□□ □□, □□ □ □□□ □□ □□ □□□ □□□ □□□□. □□□ □□□□ □□□□

□□, □□, □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □ □□ □□□□ □□□ □□□

□□ □□□ □□□□ □ □□□ □ □ □□□□. □□□ □□ □□□ □□□□ □□□ □□□□ □ □□□□ □

□ 80 □□□□ □□□ □□□ □□□ □□□□□ □□□□ □□ □□□□ □□□ □□□ □ □□□□.

NEW QUESTION: 329

□□ □ □□□□□□□ □□ □□□□ □□□□ □□□ □□□□ □□ □□ □□ □□□□□?

A. ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐

B. □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□ □□

C. □□□□ □□□□ □□ □□□ □□□ □□□□□ □□□ □□□□

D. □□□ □□□□□ □□ IoT □□□□ □□□□ □□□ □□□□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 330

Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

A. EIGRP

B. OSPF

C. BGP

D. RIP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 331

□□□□□ □□□□□ □□ □□□ □□□□ □ □□□ □□□ □□□□□□. □□□□□□□ □□□ □□□

□□ □□□□□ □□ USB □□□□ □□□□□□□□. □□ □ □□ □□ □□□ □□□ □□□□ □□ □□□

□?

- A. □□□□ □□ □□□□ □□ □□□□ □□□ □ □□□□.
- B. □□□□ DHCP □□ □□□□ □□□ □□ □□□□.
- C. □ □□□ □□□□ □□ □□□ □□□□□□□□ □□ □□□□□□□□.
- D. □□□□□□□□ □□□ □□□ □□ IP□ □□□□□□□□.

Answer: D ([LEAVE A REPLY](#))

□□

□□□□□□□□ □□□ □□□ □□ IP□ □□□□□□□, □□ □□□□ □□□□ □□□□ □□□□ □ □□ □ □□ □□ □□□□□□. □□ IP □□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □□ IP □□□□ □. □□ IP □□□ □□□ □□□□ □□ □□□□□□□ □□ □□□□□□ □□□□□ □□ □□□ □□□ □ □□□□. □□□ □□□ □□□□□ □□ □ □□□ □□□ □□ IP □□□ □□□ □□ □□ IP □□ □□□ □□ □ □□□□. IP □□ □□□ □ □□□ □□□ □□□ IP □□□ □□□□□ □ □ □□□□ □□□□ □□ □ □□ □□□ □□□□□. IP □□ □□□ □□ □□□□ □□□□ □□□□ □□ IP □□□ □□□□ □□ □□ □□□□ □□□□□ □□ □ □□□□. □□□□: [CompTIA Network+ □□ □□ □□], IP □□ □□□□? | HowStuffWorks

N10-008 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□
N10-008 □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□ □□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 332

□□□□ □□□□ □□ □□□□□ □□ □□□ □□□□ □□□□. □□□□ □□□ □□□□ □□ □□□ □ □□□□.

□□ □ □□ □□□ □□□ □□□□□?

- A. □□□ □□
- B. □□□ □□□
- C. □□ □□
- D. □□ □□

Answer: ([SHOW ANSWER](#))

□□

□□ □□□ □□□ □□□ □□□□□. □□□ □□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□. □□□ □□□ □□ □□□□□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □ □□□□□ □□ □□□ □□□□□ □□ □□□ □ □□□□. □□□ □□□ traceroute □□□ □□□□ □□ □ □□□□, □ □□□ □□□ □□□□ □□□□□ □□□ □□□ □□□□□. □□□□ traceroute □□□ □ □□ □ □□□ 10.12.2.1□ 10.12.2.2 □□□ □□□ □□□□ □□□ □□□□□, □□ □□□ □□□ □□□□ □. □□: CompTIA Network+ N10-008 □□ □□ □□□, 181□□□; □□ CompTIA Network+ □□ □□□(□ □ N10-008), 7-9□□□.

NEW QUESTION: 333

□□□□□ □□ □□ □□□□ □□□□ □□□□□ □□ □□□ □□□□□□□ □□ □□ □□
□ □□□□ □□□ □□□□. Afield □□□□ □□ □□□□ □□□□□□.
□ □□□□ □□□□, □□ □ □□ □□□□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□?

- A. □□
- B. □□
- C. □□
- D. □□

Answer: B ([LEAVE A REPLY](#))

□□□ □□ □□ □□□□ □□□□. □□ □□□ □□ □□□ □□, □□ □ □□□ □□□ □ □□□□. □□
□□□ □□□□ □□□□ □□□ □□ □□□ □□□□ □ □□□□. □□□ □□□ □□ □□ □□□
40%~60%□□□. □□□□ □□□ □□□□ □□ □□□ 70%□ □□ □□ □□□□ □□□ □□□ □□□□
□□□ □□ □ □□□□. □□□ □□□□ □□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□ □
□ □□□ □□□□ □□□□.

NEW QUESTION: 334

A technician is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes. Which of the following should the technician configure for this tool?

- A. LACP
- B. Flow control
- C. Port mirroring
- D. Jumbo frames

Answer: D ([LEAVE A REPLY](#))

Jumbo frames are Ethernet frames that can carry more than the standard 1,500 bytes of payload data. Jumbo frames can support payloads of up to 9,000 bytes, depending on the network device and configuration. Jumbo frames can improve network performance by reducing the overhead of packet headers and increasing the efficiency of data transmission. Jumbo frames can also reduce the CPU utilization of the sender and receiver devices, as they require fewer interrupts and processing cycles. However, jumbo frames also have some drawbacks, such as increased latency, fragmentation, and compatibility issues. Therefore, jumbo frames should be used with caution and only in networks that support them end-to-end.

A technician who is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes should enable jumbo frames for this tool, as this would allow the tool to capture and analyze more data per frame and provide more accurate and detailed results. However, the technician should also ensure that the network devices and interfaces that the tool is connected to also support jumbo frames, and that the MTU (maximum transmission unit) is set to the same value across the network path.

Reference

What are Jumbo Frames?

How to Enable Jumbo Frames

CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION: 335

□□ □□ □□ □ □□□□ □□□□□ □□□□ □□□ □□□□ □□ □□ □□□□□?

- A.** □ □ □ □ □
- B.** □ □ □ □ □
- C.** □ □ □ □
- D.** □ □ □ □ □ □ □ □ □ □

Answer: C (LEAVE A REPLY)

22

□□ □□□ □□□□ □□ □, □□□□ □□□ □□ □, □□□□ □□ □□ □□ □ □□ □□□ □□□ □□□ □ □□□□ □□□ □□□□ □□□□□. □□□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□□. □ □□ □□□□□ □□□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□.

NEW QUESTION: 336

□□ □□□ □□ □ □□ □□ □□□ □□□□□ □□□ □□□□ □□□□ □□□□□□□ □□□□ □□□□
□□□□ □ □□□□□?

- A. BGP**
B. OSPF
C. EIGRP
D. FHRP

Answer: (SHOW ANSWER)

FHRP First Hop Redundancy Protocol, enables multiple routers to share a single virtual IP address and MAC address. FHRP enables multiple routers to share a single virtual IP address and MAC address. FHRP enables multiple routers to share a single virtual IP address and MAC address. FHRP enables multiple routers to share a single virtual IP address and MAC address.

□□: 1: CompTIA Network+ N10-008 □□ □□□ - 13□: □□□ □□□□32: □ □□ □ □□ □□□□(FHRP)
□□4

NEW QUESTION: 337

"Frederick" IPv6 2001:5689:23:ABCD:6A

"Fred"□□ □□□□. □□ DNS □□ □ □□ □□ □□□ □□□□□?

"□□□"□ □ □ □□□?

- A.** ☐☐
B. SRV
C. ☐☐☐
D. NS
E. ☐☐☐
F. MX

Answer: A (LEAVE A REPLY)

NEW QUESTION: 338

□□ □□□□ □□□□ □□ □ □□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□ □□, □□ □□□
□ □□□□ □□□ □□□ □□□□. □□□□ □□□□ □□□□ □ □□ □□ □□□□ □□ □ □□□□□□□?

- A. 10000 0000 00
- B. 0 00 0 0000 00 00
- C. 00 000000 CRC 00
- D. 00 NetFlow 000

Answer: (SHOW ANSWER)

00

0000 0000 0000 0 00 00 0000 0 00 0 0000 00 000000. 0000 00 0000 0000 0000 0000 0 0000 0000 0 0000 00 0000 0000 0000 0000. 0 00 0 0000 00 0000 0000 0000 00 0 0000 00 0000 0 00 00 0000 0000 0 00 0000 0000 0 0000 0 0000 0 0000. 0000 0000 0 00 0 0000 00 0000 0000 0000 0000 00, 00 000000 0000 00 00 00 0000 0000 00 000000 0000 0 00000.

0000 0000 00 00 0000 0000, 00 0 0000 00000000 0000 0000 0000. 0000 0 00000 00 0000 00000 0000 0000 0000, 0 0000 00000 0 0000 0000 0000.

00 000000 CRC 0000 0000 00 00 00(CRC)0 00 00 00000 00 0000 0000 0000 0 00000 000000. 00 000000 CRC 0000 0000 0000 00000 00000 0000 00 0 0000, 0000, 0000 00 00000000 0000 0000 0000 0 00000. 00 000000 CRC 0000 00000 0 00 0000 0000 00 00000 00 0 0 00000 00 0000 0000 0000 0000 0000 00000 00000.

00 NetFlow 00000 00000 0000 0000 00000000 00000 NetFlow 000000 00 00000 0 0000 00000000. 00 NetFlow 00000 00000 00000 00 00000 0, 00 0 0000 00 0 0 0 IP 00, 00 0 000000 00 0000 0000 0 00000. 00 NetFlow 00000 00000 00 00, 0 0 0000 00000 0 0000 0 0 0000 00000000 00 00000 0000 000000 00000.

00 00000 00 00000 00000 00 00 00000 00 00 0000 00000 00 0000 00000 0 00 0000 CRC 0000 00000 00 00 NetFlow0 00000 0000 000000? CompTIA Network+ 00 0 00 00 0000, 80(00 N10-008)

NEW QUESTION: 339

00 0 DHCP 00000 0000000 00 0000 0000 0000 00 000000?

- A. 00
- B. 000
- C. 200 000
- D. 00

Answer: B (LEAVE A REPLY)

DHCP 0000 000000 00000000 00 00 DHCP 0000 00000 0000 00 00000000.

00000 00000 SD-WAN 00000000 DHCP 0000 00000 00000 00 DHCP 00000000 00 DHCP 00 00 0000 0000 00000 0 00000. 00 00 00 00000 00 DHCP 00000 00 IP 0000 0000 0 00000. 0000 000000 DHCP 00000 00000 00 000000000 00 0 DHCP 00000 000000.

NEW QUESTION: 340

Which IEEE 802.11 standard is designed to support both 2.4GHz and 5GHz channels and is capable of supporting up to 100Mbps? (1 point)

- A. 802.11ac
- B. 802.11ax
- C. 802.11g
- D. 802.11n

Answer: B (LEAVE A REPLY)

802.11 ax is designed to support both 2.4GHz and 5GHz channels and is capable of supporting up to 100Mbps. It is designed to support both 2.4GHz and 5GHz channels and is capable of supporting up to 100Mbps. It is designed to support both 2.4GHz and 5GHz channels and is capable of supporting up to 100Mbps. It is designed to support both 2.4GHz and 5GHz channels and is capable of supporting up to 100Mbps.

11

Which of the following is a feature of 802.11 ax? (1 point)

CompTIA Network+ N10-008 Cram 5000 is a comprehensive study guide for the CompTIA Network+ N10-008 exam. It contains all the questions and answers from the exam, along with detailed explanations. It is available in PDF format and can be downloaded from the following link: [https://www.cram.com/comp-tia-network-plus-n10-008-cram-5000](#).

NEW QUESTION: 341

Which of the following is a feature of 802.11 ax? (1 point)

- A. 100Mbps
- B. 100Mbps
- C. CRC
- D. 100Mbps

Answer: (SHOW ANSWER)

NEW QUESTION: 342

Which of the following is a feature of 802.11 ax? (1 point)

- A. 100Mbps
- B. 100Mbps
- C. 100Mbps
- D. 100Mbps

Answer: (SHOW ANSWER)

NEW QUESTION: 343

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:

CompTIA

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

- ```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

- ```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

- ```

10.10.
10.10.
56 (TFTR): 10.10.
4 (NTP): 10.10.

```

**Answer: C (LEAVE A REPLY)**

□□

□□ □□□ □□ □□ □□□ □□□□ □□□□, □□ □□ AP□ □□□□□ □□□ □□□□□ □□□□ □□ □□□□ □□□□□. □□ □□□ □□ □□□ □□, □□ □□ □ □□ □□□ □□□ □ □□□□. AP □□ □□, EIRP □ RSSI□ □□ □□□□□ □□□ □□ □□ □ □□□□ □□□ □□□□ □□□□.

### NEW QUESTION: 346

□□□□ □□ □□□□ □□□□ □□□ □□□ □ □□□ □□□ □□ □□□□□ □□□□□□□□. □□ □□ □□□ □□ □□□ □□ □□ □□ □□ □□□□ □□□□□□□□. □□□ □□□ □□□ □□□□ □□□□ □□□□□□ □□ □□ □□□ □□□ □□ □□□□□□. □□ □□ □□□□ □□ □□□□□ □□ □□□□ □□□□□ □□□□□ □□ □□□ □□ □□□ □□□□□ □□□ □□□ □□ □□ □□□ □□□□. □□ □□ □□ □□ □□□□□□?

- A. □□ □□□ □□ □□□ □□ □□□□ □□□□.
- B. □□□□ □□ □□□ □□ □□ □□□□□ □□□□.
- C. □□□ □□□ □□ □□□ □□□□ □□□□□□.
- D. □□ □□ □□□□ 5GHz □□□□□ □□□ □□□□ □□□□.

**Answer: C (LEAVE A REPLY)**

□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□ □□□□ □□□□□□. □□□ □□□□ □□□□□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□ □□ □□□□ □□□□ □□□□. □□ □□□ □□□□ □□□□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□□. □□□ □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□□.1 □□: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

**N10-008** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□  
**N10-008** □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□ □□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.  
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

### NEW QUESTION: 347

#### SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

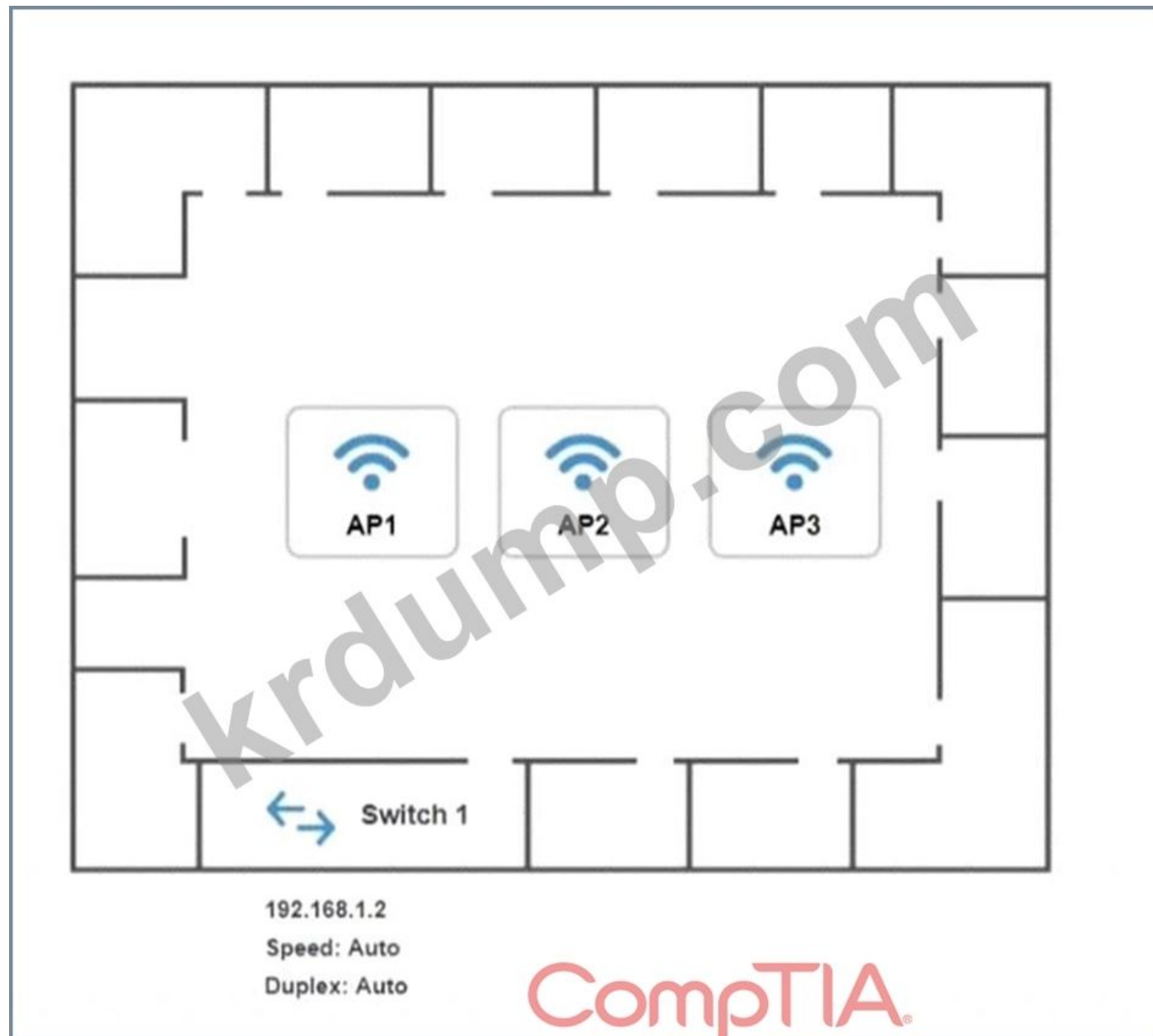
The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTIONS Click on the wireless

devices and review their information and adjust the settings of the access points to meet the given requirements.

□□□□ □□□□□□ □□ □□□ □□□□□ '□□ □□□' □□□ □□□□□.



## AP1 Configuration



https://ap1.setup.do

### Basic Configuration

Access Point Name

IP Address  /

Gateway

SSID

SSID Broadcast ☒ Yes ☐ No

### Wireless

Mode

Channel

### Wired

Speed ☐ Auto ☒ 100 ☐ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### Security Configuration

Security Settings ☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

CompTIA

## AP2 Configuration

CompTIA



https://ap2.setup.do

### Basic Configuration

Access Point Name

AP2

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

### Wireless

Mode

B  
G

Channel

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11

### Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

### Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

AP3 Configuration

https://ap3.setup.do

Basic Configuration

Access Point Name

AP3

IP Address

/

Gateway

192.168.1.1

SSID

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B

G

Channel

1

2

3

4

5

6

7

8

9

10

11

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

Security Configuration

Security Settings

☒ None ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA2 - Enterprise

Key or Passphrase

Reset to Default

Save

Close

Answer:

□□ □□□ □□□□□.  
□□  
□ □□ □□□ □□□□□ □□□ □□□ □□□.

AP1 Configuration

https://ap1.setup.do

Basic Configuration

Access Point Name

AP1

IP Address

192.168.1.32

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

☒ Yes ☐ No

Wireless

Mode

B

Channel

3

Wired

Speed

☐ Auto ☒ 100 ☐ 1000

Duplex

☐ Auto ☐ Half ☒ Full

□□□ □□□ □□□□□, □□□, □□□□□□, □□ □□ □□ □□□ □□□ □□□ □□□

Security Configuration

Security Settings

☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase

S3cr3tl

□□□ □□□ □□□□□ □□ □□ □□

✕

# CompTIA

□□□ □□ AP2

☐ ☐ ☐   ☐ ☐ ☐   ☐ ☐ ☐ ☐ ☐   ☐ ☐   ☐ ☐   ☐ ☐

AP2 Configuration

https://ap2.setup.do

Basic Configuration

Access Point Name

AP2

IP Address

192.168.1.64 / 27

Gateway

192.168.1.1

SSID

CorpNet

SSID Broadcast

Yes

No

Wireless

Mode

B

Channel

6

Wired

Speed

Auto

100

1000

Duplex

Auto

Half

Full

Security Configuration

Reset to Default

Save

Close

000 000 00000, 000, 000000, 00 00 00 000 000 0000 000

Security Configuration

Security Settings

None

WEP

WPA

WPA2

WPA2 - Enterprise

Key or Passphrase

S3cr3t!

0300 000 000 00.  
 000 00 AP3  
 000 000 000000 00 00 00

**AP3 Configuration**

https://ap3.setup.do

**Basic Configuration**

Access Point Name: AP3

IP Address: 192.168.1.96 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ☒ Yes ☐ No

**Wireless**

Mode: B

Channel: 9

**Wired**

Speed: ☐ Auto ☒ 100 ☐ 1000

Duplex: ☐ Auto ☐ Half ☒ Full

**Security Configuration**

Reset to Default Save Close

Which of the following is a valid IPv4 address?

**Security Configuration**

Security Settings: ☐ None ☐ WEP ☐ WPA ☐ WPA2 ☒ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

**NEW QUESTION: 348**

A network technician is configuring a switch. Which of the following is a valid IPv4 address?

- A. 192.168.1.1
- B. 192.168.1.1.1
- C. 192.168.1.1.1.1
- D. 192.168.1.1.1.1.1

**Answer: A (LEAVE A REPLY)**

The correct answer is A. 192.168.1.1 is a valid IPv4 address. The other options are invalid because they contain more than four octets. A network technician is configuring a switch. Which of the following is a valid IPv4 address?



**NEW QUESTION: 350**

□□□□ □□□□ □□ □□□□ □□□ □ □□ □□□□□□□ □□□□ □ □□□ □□ □□□□ □□□□  
□□□□. □□ □ □□ □□ □□□ □□□ □□□ □□□□ □□□□□?

- A.** SSO
- B.** LDAP
- C.** EAP
- D.** □□ □□ □□ +

**Answer: (SHOW ANSWER)**

\* SSO Single Sign-On, which allows users to log in to multiple applications with a single set of credentials.

\* SS0□ □□□□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□.

\* SSO □ □ □ □ □ □ □ □ □ □ ID □ □ □ □ □ (IAM) □ □ □ □ □ □ □ □ □ □.

\* LDAP, EAP, TACACS+ □ □□ □ □□ □□□□□□ □□□□ □ □□ □□ □□□ □□□ □□ □□  
□□. □□□ □□, □□ □□, □□(AAA) □□ □□□□ □□ □□□□□□□3.

\* LDAP□ Lightweight Directory Access Protocol□ □□□, □□□, □□ □ □□□ □□ □□□ □□□□ □□  
□□ □□□□ □□ □□□□ □□□□ □□□□□□□□3.

\* EAP□ Extensible Authentication Protocol□ □□□, □□□□, □□□, □□, □□ □□ □ □□□ □□ □□□□ □□□□ □□□□□□□□□3.

\* TACACS+ □ Terminal Access Controller Access-Control System Plus □ □□□, □□□□ □□□ □□□□□  
□□ □□□ AAA □□□□ □□□□ □□□□□□□.

□ □ □ □ :

\* SSO ☐ ☐ ☐ ☐ ☐? | Single Sign-On ☐ ☐ ☐ ☐

\* Single Sign-On - CompTIA Network+ ☐ (N10-008): ☐ ☐ ☐

\* Network+ (Plus) ☐☐ | CompTIA IT ☐☐

**NEW QUESTION: 351**

□ □ □ □ □

☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐

☐ ☐☐☐.

11

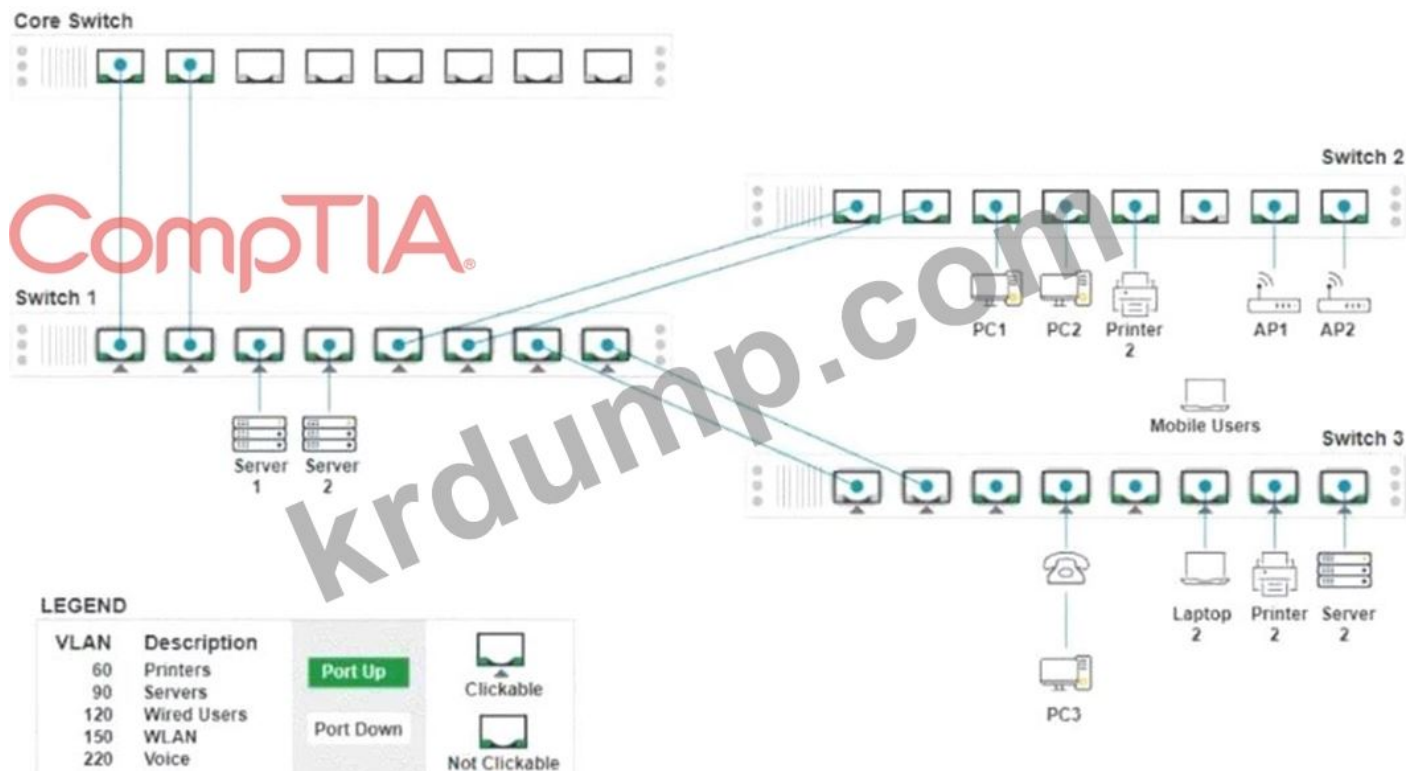
\* □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□.

\* □□□□ □□ □□ □□□ □□ □□□□

\* □□□ □□ □□□□ □□□ □□□□□.

\* □□ □□□□ □□□□ □□ □□□ □□□ □□□□.

□□□□ □□□□□□ □□ □□□ □□□□□□ '□□ □□□' □□□ □□□□□□.



## Switch 3 - Port 8 Configuration

### Status

Port ☒ Enabled

LACP ☐ Disabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1  
VLAN 60  
VLAN 90  
VLAN 120  
VLAN 150  
VLAN 220

Reset to Default

Save

Close

CompTIA

## Switch 3 - Port 7 Configuration



### Status

Port ☒ Enabled

LACP ☐ Disabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 6 Configuration

**Status**

Port ☒ Enabled

LACP ☐ Disabled

**Wired**

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

**VLAN Configuration**

+ Add VLAN

VLAN150

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default Save Close

Switch 3 - Port 4 Configuration

**Status**

Port ☒ Enabled

LACP ☐ Disabled

**Wired**

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

**VLAN Configuration**

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default Save Close

### Switch 3 - Port 1 Configuration

#### Status

Port ☒ Enabled

LACP ☐ Disabled

#### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

#### VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1  
VLAN 60  
VLAN 90  
VLAN 120  
VLAN 150  
VLAN 220

Reset to Default

Save

Close

## Switch 1 - Port 7 Configuration



### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

ComptIA

## Switch 1 - Port 8 Configuration

### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

## Switch 1 - Port 6 Configuration

### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

 Add VLAN

VLAN60

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

Reset to Default

Save

Close

## Switch 1 - Port 2 Configuration

### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

## Switch 1 - Port 1 Configuration



### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default

Save

Close

## Switch 1 - Port 5 Configuration

CompTIA

### Status

Port ☒ Enabled

LACP ☒ Enabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

+ Add VLAN

VLAN60

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

Reset to Default

Save

Close

## Switch 1 - Port 4 Configuration

### Status

Port ☒ Enabled

LACP ☐ Disabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

 Add VLAN

VLAN90

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1  
VLAN 60  
VLAN 90  
VLAN 120  
VLAN 150  
VLAN 220

Reset to Default

Save

Close

## Switch 1 - Port 3 Configuration

### Status

Port ☒ Enabled

LACP ☐ Disabled

### Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

### VLAN Configuration

+ Add VLAN

VLAN90

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1  
VLAN 60  
VLAN 90  
VLAN 120  
VLAN 150  
VLAN 220

Reset to Default

Save

Close



**Answer: C ([LEAVE A REPLY](#))**

SaaS Software as a Service, cloud-based software that is hosted on a cloud provider's infrastructure. SaaS is a type of cloud computing that allows users to access applications and data over the Internet. SaaS is often used for email, CRM, and other business applications. IaaS Infrastructure as a Service, cloud-based infrastructure that is hosted on a cloud provider's infrastructure. IaaS is often used for hosting applications and data. VPN Virtual Private Network, a secure connection over a public network, such as the Internet. VPNs are often used to connect remote users to a private network.

**NEW QUESTION: 353**

Which of the following is a type of data loss prevention (DLP) technology?

- A. DLP
- B. AUP
- C. Data Loss Prevention
- D. BYOD

**Answer: D ([LEAVE A REPLY](#))**

**NEW QUESTION: 354**

Which of the following is a type of cloud-based storage service?

- A. Amazon S3
- B. Google Drive
- C. Microsoft OneDrive
- D. Dropbox

**Answer: B ([LEAVE A REPLY](#))**

Google Drive is a cloud-based storage service that allows users to store and share files and folders. It is part of the Google ecosystem and is accessible from any device with an internet connection. Google Drive offers 15 GB of free storage space, which can be increased by purchasing additional storage. It also offers features such as file sharing, collaboration, and search. Amazon S3 is a cloud-based storage service that is designed for scalability and performance. It is used for storing and retrieving data, such as images, videos, and documents. Microsoft OneDrive is a cloud-based storage service that is integrated with the Microsoft Office suite. It allows users to store and share files and folders, and it is accessible from any device with an internet connection. Dropbox is a cloud-based storage service that is known for its simplicity and ease of use. It allows users to store and share files and folders, and it is accessible from any device with an internet connection.

**NEW QUESTION: 355**

Which of the following protocols is used to dynamically learn MAC addresses? (Choose two.)

- A. MDIX
- B. 802.1Q
- C. STP
- D. RSTP
- E. LACP
- F. LACP

Answer: (SHOW ANSWER)

802.1Q is a VLAN protocol. It is used to dynamically learn MAC addresses. STP is a protocol used to prevent loops in a network. RSTP is a protocol used to prevent loops in a network. LACP is a protocol used to dynamically learn MAC addresses.

NEW QUESTION: 356

Which of the following is the correct IP address for the host?

| IP address | Subnet mask | Default gateway |
|------------|-------------|-----------------|
| 10.1.2.23  | 10.1.2.0/27 | 10.1.2.1        |

Which of the following is the correct IP address for the host? (Choose one.)

- A. 10.1.2.0
- B. 10.1.2.1
- C. 10.1.2.23
- D. 10.1.2.255
- E. 10.1.2.31

Answer: D (LEAVE A REPLY)

Which of the following is the correct IP address for the host? (Choose one.)

10.1.2.255 is the broadcast address for the network 10.1.2.0/27. It is not a valid host address. 10.1.2.1 is the default gateway for the network. It is not a valid host address. 10.1.2.23 is a valid host address. 10.1.2.0 is the network address for the network. It is not a valid host address. 10.1.2.31 is the broadcast address for the network 10.1.2.0/27. It is not a valid host address.

Source: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION: 357

IT is a process that involves the use of technology to improve the efficiency of a business.

- IT is a process that involves the use of technology to improve the efficiency of a business.
- IT is a process that involves the use of technology to improve the efficiency of a business.

- □□□□□□ □□□□ □□□□ □□ □□□□ □□□□□.

- □□ □□ □□□ □□ □□ □□□ □□□□□.

□□ □ □□ □□□ □□□ □□□□ □□□ □□□ □□□ □ □□□□?

- A. □□□
- B. TCP□□
- C. □□□
- D. nmap

Answer: D ([LEAVE A REPLY](#))

#### NEW QUESTION: 358

□ □□□ □□ □□ □ □□□□ □ □□ □□ □□□ □□□ □□□□□ □□□. □□□□□ □□□□ □□□ □□□□ □□□ □□□. □□ □ □□ □□□ □□□□ □□□?

- A. □□-□□
- B. □□□
- C. □□□
- D. □□

Answer: C ([LEAVE A REPLY](#))

#### NEW QUESTION: 359

□□□□ □□□□ □□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□. □□ □□ □ □□□ □□□□□□.

□□ □ □□□ □□□ □□ □□□□ □□□□ □□□□ □□□□. □ □□ □□□ □□□ 2.4GHz □□□ □□□□ 11□ □□□ □□□ □□□

- A. □□ 3
- B. □□ 9
- C. □□ 10
- D. □□ 11

Answer: D ([LEAVE A REPLY](#))

□□

□□□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□ □□□□□.

□□□ □□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □ □□□□. □ □□ □□□ □□□ 2.4GHz □□□ □□□□ 11□ □□□ □□□ □□□

1, 6, 11□ □□□ □□□□. □□ □□□ □□ 1□ 6□ □□□□ □□□□, □□□ □□□ □□ □□ □□□ □□ □ □□ □□ 11□ □□□□ □□□.12 □□□□1: □ □□ 1, 6, 11□□? | MetaGeek 2: □□□□□ □□ □□□

Wi-Fi □□□ □□□□ □□ - Lifewire

#### NEW QUESTION: 360

□□□□□□ □□□□ □□□□ □□ □□ □□ CRC □□□ □□□□□. □□□□ □□ □□ □□ □□□ □ □□ OSI □□□ □□□ □□□□□?

- A. □□□ 1
- B. □□□ 2

- C.** ☐ ☐ ☐ 3  
**D.** ☐ ☐ ☐ 4  
**E.** ☐ ☐ ☐ 5  
**F.** ☐ ☐ ☐ 6  
**G.** ☐ ☐ ☐ 7

**Answer: ([SHOW ANSWER](#))**

CRC 0000 00 00 00000 0000 0 00000 00 00 00 000000. CRC 0000 000000 00  
0 00 0000, 0000, 00 00 0000 00 0000 00 0000 00 000000. 00000 00000 0000  
00 00 0000 00000 0000 0000 OSI 0000 00 100 00 0000 0000 00000 00 00000.  
00: CompTIA Network+ 00 00 00 00 2.0(00 00: N10-006), 0000 4.0 00000 00 00 0 0  
0, 00 4.1 0000 00000000 00000 00 00 00000 000000.

**NEW QUESTION: 361**

□□ □ □□□ □□ □□□□□□ □□□□ □ □□ □□ □□□ □□ □□ □□□□□?

- A.** □□ □□□ □□
- B.** □□ □□
- C.** □□ □□ □□
- D.** □□□ □□ □□

**Answer: ([SHOW ANSWER](#))**

**N10-008** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□

**N10-008** □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□  
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

**NEW QUESTION: 362**

A customer wants to log in to a vendor's server using a web browser on a laptop. Which of the following would require the LEAST configuration to allow encrypted access to the server?

- A. Secure Sockets Layer**  
**B. Site-to-site VPN**  
**C. Remote desktop gateway**  
**D. Client-to-site VPN**

**Answer: (SHOW ANSWER)**

Secure Sockets Layer (SSL) would require the least configuration to allow encrypted access to the server. SSL provides secure communication between a client and a server, such as a web browser and a web server, by using encryption to protect the data transmitted between them. A SSL certificate is installed on the server, and the web browser uses SSL to encrypt data before sending it to the server. The encryption is transparent to the

user and requires no additional configuration or setup beyond ensuring that the SSL certificate is installed and recognized by the web browser.

#### NEW QUESTION: 363

Which of the following is a feature of the Cisco IOS QoS? (Choose two.)

- A. QoS is a feature of the Cisco IOS.
- B. QoS is a feature of the Cisco IOS.
- C. QoS is a feature of the Cisco IOS.
- D. QoS is a feature of the Cisco IOS.

Answer: C ([LEAVE A REPLY](#))

#### NEW QUESTION: 364

Which of the following is a feature of the Cisco IOS? (Choose two.)

- A. MPLS
- B. mGRE
- C. EIGRP
- D. VRRP

Answer: A ([LEAVE A REPLY](#))

Which of the following is a feature of the Cisco IOS?

Which of the following is a feature of the Cisco IOS? (Choose two.)

#### NEW QUESTION: 365

Which of the following is a feature of the Cisco IOS? (Choose two.)

- A. QoS is a feature of the Cisco IOS.
- B. QoS is a feature of the Cisco IOS.
- C. QoS is a feature of the Cisco IOS.
- D. QoS is a feature of the Cisco IOS.

Answer: ([SHOW ANSWER](#))

Independent Basic Service Set (IBSS) is a type of wireless network that does not require a central access point. IBSS is a type of wireless network that does not require a central access point. IBSS is a type of wireless network that does not require a central access point. IBSS is a type of wireless network that does not require a central access point.

#### NEW QUESTION: 366

□□ □ □□ 40Gbps□ □□□ □ □□ □□□□ □□□ □□□□□?

- A. SFP+
- B. QSFP+
- C. QSFP
- D. SFP

Answer: B ([LEAVE A REPLY](#))

SFP = 1Gbps

SFP+ = 10Gbps

SFP = 4xSFP = 4Gbps

SFP+ = 4xSFP = 40Gbps

#### NEW QUESTION: 367

□ □□□ □□□□□(CEO)□ □□ □□□ □□□□ □□ □□□ □ □□□□ □□□□□. CEO□ SIM □□□ □□□□ □□□□□ □□ □□□ □□ □□ □□□ □□ □ □□□ □□□. □□ □ CEO□ □□□□ □□□ □ □□ □□□ □□□□□?

- A. WDMA
- B. □□□ □□ □□(SLA)
- C. GSM
- D. CDMA

Answer: C ([LEAVE A REPLY](#))

#### NEW QUESTION: 368

□□□□ □□□□□ SLAAC□ □□□ □□□□□□ □□□ □□ □□□□ □□□□ □□□. □□ □ □□□□ □ □□□□□ □□ □□ □□□ □□□□□?

- A. □□□□□□□□ □ □□□ □□□ □ □□□ ARP□ □□ □□□□ □□□□□.
- B. □□□□ ND□ □□□ □□□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□.
- C. □□□□ □□□ □□□□ □□□□□□□□ □□ □□□□ □□□□ □□□□□.
- D. □□□□□□□□ □ □□□ □□□ □ □□□ DHCP □□□□ □□ □□□ □□□ □□□□□.

Answer: B ([LEAVE A REPLY](#))

#### NEW QUESTION: 369

□□□ □□□□ □□ □□□□□ □□□□□□□□. □□□□□□ □□□ □□□ □□□ □□□□□ □□ □□ □ □□□ □□□□ □□□□. □□ □ □□ □□ □□□□□ □□□?

- A. □□ □□□
- B. □□ □□
- C. □□□
- D. 2□□ □□

Answer: ([SHOW ANSWER](#))

\* □□□□ □□ □□ □□□□□ □□□□ □□□□ □□ □ □□ □□□□ □□□□ □□□□□.

□□□ □□□□□ □□□□ □□□□ □□□ □□□ □□□□ □□□□□ □□□□□ □□ □□□ □ □□□□ □.



FCoE □□□ □□□ □□□□□ □□□□ □□□□ LAN□□ SAN□ □□ SCSI □□□ □□□□ □□□□ □□□□□□□. NetBEUI□ □□□□□□□ □□□□ LAN□ □□ NetBIOS □□□ □□□□ □□□□ □□□□ □□□□.

**NEW QUESTION: 372**

□□□ Cat 8 □□□□ □□□ □, □□□ □□ □□□□ □□□ □□ □□□□ □ □□ □□□ □□□□□□. □  
□□□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□?

- A.** □□□□ □□ □ □□ □□□ □□ □□□□ □□ □□□ □□□□□.
- B.** □□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□□□.
- C.** RX/TX □□□□ □□ □□ □□□□□.
- D.** □□ 100Mbps □□□ □□□ □ □□ □□□□ □□ □□□□ □□□□□.

**Answer: (SHOW ANSWER)**

11

Cat 8 □□□□ □□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□ □□□  
 □□□ □□□□□. □□□□ □□ □□ □□□□ □ □□□□ □□□ □□ □□□ □□□□ □□□  
 □□□ □ □□ □□□□□. □□□□ □□□ □□□ □□□□ □□□□□ RX/TX □□□□ □□ □□ □□□□  
 □ □□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □ □□□ □□□ □□□□ □□□□.

□ □ □ □ :

CompTIA Network+ N10-008 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ 191 ☐ ☐ ☐

CompTIA Network+ N10-008 □□ □□□, □□□ □□□, 362□□□

CAT8 RJ45 Keystone  : r/HomeNetworking2

Cat8 Shielded Keystone Jacks3□ □□□□ □□

**NEW QUESTION: 373**

□□ □ □□□ □□□ □□□□ □□□□ □□□□□ □□ □□ □□□□ □□ □□□□□ □□□□ □□ □  
□□□□?

- A.** □ □ □ □
- B.** □ □ □ □
- C.** □ □ □ □ □ □
- D.** □ □ □ □ □ □

**Answer: C (LEAVE A REPLY)**

00 0000 000000 0000 0000 0000 000000 00 00 0000 00 0000  
 0000. 00 0000 000000 0000 000000 00000 00 00 0000 000000 0000, 00  
 00 0000 0 0000 000000. 00 0000 000000 0000 0 00 00, 0000 00 00, 00000  
 00 0 00, 0000 00 00, 00000 00000000, ID 0 0000 0000 00 0000 0000 0000 0000  
 0 00000 0000 000000 0000 00 000000 00 0000 000000123.

11

□□ □□□□□ □□□□? | □□ □□□ | CompTIA3

000 00: 00 000000 (00) 000 00000 | 000 00 | CompTIA2 CompTIA Network+ 00 00

N10-008 □□ □□ 17 - ExamCompass1

**NEW QUESTION: 374**

00 0000 0000 000 0000 0 00 SSID 00 0 0 000 00 0000000 000 00 0  
 000. 00 00 0000 0000, 0 00 00 000 0000 0 AP 0000 00 000 RSSI 000  
 0000. AP 00 00 000 0000 00 SSID 00000000000. 00 00 00 AP 00 0 00  
 0 00000.

□□ □ □□ □□ □□□ □□□□ □□ □□□ □□□□ □ □□ SSID□ □□ □ □ □□ □□□?

- A.** WPA2 Enterprise □□ □□ □□  
**B.** □ AP□ □□ □□□ □□□ □□  
**C.** □ AP□ □□ □□ □□ □□ □□  
**D.** □ AP □□ 802.11ac □□ □□□ □□□□□ □□

**Answer: D (LEAVE A REPLY)**

SSID AP 802.11ac 5GHz  
 . 802.11ac 5GHz  
 . 802.11ac , 2.4GHz  
 AP1 2.4GHz  
 AP2 5GHz  
 802.11a  
 802.11b 802.11a SSID AP  
 802.11ac SSID:  
 CompTIA Network+ N10-008 , 75%; CompTIA Network+ (N10-008), 2-18%.

**NEW QUESTION: 375**

WAN □□□□ □□□ □□□□ 8□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□. □□ □ □□  
□□□□ □ □□ □□□□□?

- A.** □□□ □□□
- B.** □□□□ □□ □□□
- C.** □□ □□ □□
- D.** VLAN □□

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 376**

□□ □ □□ □□□ □□ □□□ ISP □ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □  
TCP □□□□ □□□□ □□□ □□□□□ □□□ □□□ □□□□□?

- A.** ☐☐☐ ☐☐☐
- B.** ☐☐ ☐☐
- C.** ☐☐ ☐☐
- D.** ☐☐ ☐☐☐☐ ☐☐

**Answer: (SHOW ANSWER)**

□□□ □□□□ □□□□□ □□□ □□□ □□□□ ISP□ □□□ □□□ □□□ □□ □□□ □□□  
□□□□ □□□ □ TCP □□□□ □□□□ □□□ □□ □□□ □□ □□□□□. □□□ □□□□ □□□ □□  
□ □□□□ □□□ □□□□ □□ □□ □□ □□□□ □□ □□□ □□□ □□□□ □□□ □□□□□. □□  
□□ TCP □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□. □□□ □□□□ □□□ □□, □□, □□  
□□ □□ □□□ □□ □□□ □□□□□ □□□ □□ □□□□. □□: □□□ □□ □ □□□ □□ | □□ □□ |  
Pearson IT □□, CompTIA Network+ □□ □□ □□

**N10-008** □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ N10-008 □□! DumpTop □ □□  
**N10-008** □□ □□□ □□□□□□, DumpTop N10-008 □□ □□□ □□□□□□□□ □□□ □□□□□  
□□. □□□□ □□□ □□□□ □□ DumpTop N10-008 □□□ □□□□□.  
<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount:  
**KrDump**)

#### NEW QUESTION: 377

□□□ □ □□□ □□ ISP□ □□□□□□. □□□ □ □□□□.

- A. □□□□.
- B. □□□□□ □□□ □□.
- C. □□.
- D. □□□□ □□□.

**Answer: A (LEAVE A REPLY)**

□□ □□□ IT □□□ □□□□ □□□□□ □□□□ □□□ □□□□. □□ □□□□□ □ □□ □□□□□□  
□□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□, □□ □□□ □□ □□ □□ □□□□ □□ □  
□□ □□□□(□□□□□ ISP □□ □□□ □□□)□ "□□ □□"□□□. □□ □□□□□ ISP□ □□□ □ □  
□ □□□□□ □□ □□□□ □ □□ □□□ □□□ □ □□ ISP□ □□□□ □□□□□ □□ □□□ □□□ □  
□□ □□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□ □□ □ □□ □ □□ □□□ □□□□□.

#### NEW QUESTION: 378

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

Which of the following is the cause of the connection issue?

- A. Routing loop
- B. Asymmetrical routing
- C. Broadcast storm
- D. Switching loop

**Answer: A (LEAVE A REPLY)**

The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to

the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. Reference: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

**NEW QUESTION: 379**

□□ □ □□□ □□□ □□□ □□□□ □□□□ □□□□□ □ □□□□ □□ □□□□□?

- A.** CVE
- B.** □□ □□□
- C.** □□□□
- D.** □□□
- E.** □□ □□

**Answer:** ([SHOW ANSWER](#))

[illegible]

**NEW QUESTION: 380**

A Wi-Fi network was recently deployed in a new, multilevel building. 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?

- A. Perform a site survey.**
- B. Review the AP placement**
- C. Monitor channel utilization.**
- D. Test cable attenuation.**

**Answer: A (LEAVE A REPLY)**

Incorrect antenna placement could cause or exacerbate attenuation and interference problems. Use a site survey and heat map to determine the optimum position for APs and (if available) the direction in which to point adjustable antennas.

**NEW QUESTION: 381**

□□□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□  
 □□□□□□. □□ □ □□ □□ □□□ □□□□ □□□?

- A.** □□□□ □□□ □□□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □□ □□□ □□□□□.
- B.** □□□ □□□ □□ □□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□□.
- C.** □□□ □□□□ □□□ SLA□ □□□□ □□ □□□ IT □□ □□ □□□□□.
- D.** □□□ □□□□□ □□□ □□ □□ □□ □□ □□□ □□□□□.

**Answer: B (LEAVE A REPLY)**

## NEW QUESTION: 382

Which of the following ports are used by default for secure remote access protocols? (Select two)

- A. 22
- B. 23
- C. 69
- D. 443
- E. 587
- F. 8080

Answer: B,C (LEAVE A REPLY)

- \* Port 23 is used by Telnet, a protocol that sends data in plain text. Telnet port 22 is used by SSH, a secure protocol.
- \* Port 69 is used by TFTP, a protocol that sends data in plain text.
- \* TFTP, SFTP, and FTPS are protocols that send data in plain text. SFTP and FTPS use port 22 and 990 respectively.

\* Port 443 is used by HTTPS, a secure protocol that encrypts the data using SSL/TLS certificates. HTTPS should be preferred over HTTP, which uses port 80 and sends data in plain text.

\* Port 587 is used by SMTP, a protocol that sends email messages. SMTP can be secured by using STARTTLS, which initiates encryption after the initial handshake. Alternatively, port 465 can be used for SMTPS, which encrypts the data from the start.

\* Port 8080 is used by HTTP proxy, a protocol that allows clients to access web servers through an intermediary. HTTP proxy can be secured by using HTTPS proxy, which uses port 443 and encrypts the data.

References:

\* CompTIA Network+ N10-008 Study Guide, Chapter 2: Network Protocols and Services, pages 62-63, 66-67, 69-70, 72-73, 75-76.

\* Professor Messer's CompTIA N10-008 Network+ Course Notes, Section 2.1: Common TCP and UDP Ports, pages 16-17.

\* Professor Messer's CompTIA N10-008 Network+ Training Course, Video 2.1: Common TCP and UDP Ports, 6.

### NEW QUESTION: 383

Which of the following protocols are used by default for secure remote access protocols? (Select two)

- A. STP
- B. 802.1Q
- C. STP
- D. 802.1Q

Answer: A (LEAVE A REPLY)

Which of the following protocols are used by default for secure remote access protocols? (Select two)

[illegible]

<https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html>

□□□□ □ □□□ □□□ □□□□□. □□□ □□□ □□□□ □ □□□ □□□ □□□□ □□□□ □□ □□  
□□□. □□□□ □□□□□ □□ □□□□ □□□ □ □□□□. □□ □ □□ □□ □□□□ □ □□ □□ □□  
□ □□□ □ □□□□?

- A.** □ □ □ □ □ □  
**B.** □ □ □ □ □  
**C.** LACP  
**D.** 802.1Q

11

□□ □□□□ 1500□□□ □□□ □□□□ □□□□ □□□ □ □□ □□□ □□□□□□. □□ □□□□ □□  
□ □□ □□□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □□ □□□ □□□□ □  
□□ □ □□□□. □□□□ □□□ □□□□ □ □□ □□□□ □□□□ □ □□ □□ □□□ □□□ □ □□□  
□

The following configuration is applied to a DHCP server connected to a VPN concentrator:

```
IP address: 10.0.0.1
Subnet mask: 255.255.255.0
Gateway: 10.0.0.254
```

There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any Issues. The remaining sales representatives cannot connect to the VPN over the course of the day. Which of the following can be done to resolve the issue without utilizing additional resources?

- A. Decrease the lease duration**  
**B. Reboot the DHCP server**  
**C. Install a new VPN concentrator**  
**D. Configure a new router**

### Explanation

DHCP 0000 00 0000 0000 00000000 IP 00 0000 0 00 00000 00 00 00000000 0  
00 0 000 IP 0000 000000. 00000: CompTIA Network+ 00 00 0000, 30: IP 00 00.

**NEW QUESTION: 386**

Which of the following is a valid IP address for a host on a network? (Select two.)

A. 192.168.1.1

B. 10.10.10.10

C. 172.16.1.1

D. 192.168.1.10

|                       |            |                       |         |
|-----------------------|------------|-----------------------|---------|
| Total Rx (bps)        | 23,041,464 | Total Tx (bps)        | 621,032 |
| Unicast Rx (Pkts/sec) | 102,465    | Unicast Tx (Pkts/sec) | 66      |
| B/Mcast Rx (Pkts/sec) | 21,456.465 | B/Mcast Tx (Pkts/sec) | 7       |
| Utilization Rx        | 2.3%       | Utilization Tx        | 0.06%   |

Which of the following is a valid IP address for a host on a network? (Select two.)

- A. 192.168.1.1
- B. 10.10.10.10
- C. 172.16.1.1
- D. 192.168.1.10

Answer: D (LEAVE A REPLY)

**NEW QUESTION: 387**

Which of the following is a valid IP address for a host on a network? (Select two.)

A. 192.168.1.1

B. 10.10.10.10

C. 172.16.1.1

D. 192.168.1.10

- A. 192.168.1.1
- B. 10.10.10.10
- C. 172.16.1.1
- D. 192.168.1.10

Answer: (SHOW ANSWER)

Which of the following is a valid IP address for a host on a network? (Select two.)

A. 192.168.1.1

B. 10.10.10.10

C. 172.16.1.1

D. 192.168.1.10

RBAC is a model of access control that is based on the principle of least privilege.

RBAC is a model of access control that is based on the principle of least privilege.

Which of the following is a valid IP address for a host on a network? (Select two.)

A. 192.168.1.1

B. 10.10.10.10

C. 172.16.1.1

D. 192.168.1.10

□□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□ □□ □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□ □□ □□□□. □□□□ □□ □□□ ACL □ NAC□ □□□□ □□ □□□ □□□□ □ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□□□ □ □□□ □□ □ □□□□. RDP □□□ □□□□ □□□□□ □□ □□□□ □□ □□□□□ □□ □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□□.

□□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□□□. □□: CompTIA Network+ Study Guide, Fourth Edition, Chapter 7, section 7.4.

#### NEW QUESTION: 388

IT □□□□ □□□ WAP□ □□□□ □□□□. □□□□ WAP□ □□□□ □□□□□ □□□□ □□ □ □□ □□ □□□□ □□□□?

- A. □□□□ □□ □□
- B. □□ □ □□ □□ □□□□□ □□
- C. TKIP □□□ □□□□
- D. AES □□□

Answer: ([SHOW ANSWER](#))

#### NEW QUESTION: 389

□□□□ MDF□ □□ □□□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□ □□ □□□□□□. □□ □□ MDF□ □□□ □□□ □□ □ □□□□□□ □□ □□□□ □□ □□ □□ □□□ □□□□□?

- A. □□
- B. □□
- C. □□
- D. □□

Answer: ([SHOW ANSWER](#))

"□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□ □□□□ □□□□. □□□ □ □□□ □□□□ □□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□ □□ □□ □□□□."

#### NEW QUESTION: 390

RJ45 □□□ □□ □□□□□ □□□ ST □□□ □□ □□□□ □□□ □□□ □ □□□ □□ □□ □ □□□□ □□?

- A. □□□ □□□
- B. □□
- C. MDIX
- D. □□ □□□

Answer: A ([LEAVE A REPLY](#))

RJ45 □□□ □□ □□□□□ □□□ ST □□□ □□ □□□□ □□□ □□□ □ □□□ □□□ □□□ □□□ □□□. □□□ □□□□ □□ □ □□□□ □□ □□□ □□□ □□□ □□ □□□ □□□□ □□□□□. RJ45 □□□ □□ □ □□ □□□□ □□□□ ST □□□ □□□ □□□□ □□□□□. □□□ □□□□ □□□□ □ □□□ □□□□ □□ □□□□ □□ □□□□ □□□ □ □□□□. □□: CompTIA Network+ N10-008 □□ □□ □□□, 54□□□; □□ CompTIA Network+ □□ □□□(□□ N10-008), 2-5□□□.

### NEW QUESTION: 391

Two buildings are 410 feet (125m) apart. A technician is connecting two 10GBASE-T Cat 5e patch panels. What is the most likely cause of the connection issue?

- A. The patch panels are not Cat 5e.
- B. The patch panels are not Cat 6.
- C. The patch panels are not Cat 7.
- D. The patch panels are not Cat 6a.

Answer: (SHOW ANSWER)

The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

**N10-008** A technician is connecting two 10GBASE-T Cat 5e patch panels. What is the most likely cause of the connection issue?

**N10-008** A technician is connecting two 10GBASE-T Cat 5e patch panels. What is the most likely cause of the connection issue?

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

### NEW QUESTION: 392

During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users to groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied?

- A. Job rotation
- B. Role separation
- C. Privileged user accounts
- D. Container administration

Answer: B (LEAVE A REPLY)

### NEW QUESTION: 393

A technician is configuring a network. Which of the following is the most secure method of connecting to the network?

- A. WLAN
- B. Ethernet
- C. SIEM

#### D. Syslog ☐☐

**Answer: A (LEAVE A REPLY)**

WLAN □□□□□ □□ LAN(WLAN)□□ □□ □□ □□□ □□□(WAP)□ □□□□ □□□□ □□□□□.

WLAN □□□□□ □□□ WAP□ □□ □□, □□ □ □□□ □□□ □□□□ □□□ □ □□ □□□ □□□ □

□□□. WLAN □□□□□ □□ WLAN□ □□ □□ □□, □□ □ □□□ □□(QoS)□ □□□ □ □□□□.

□□□□: Network+ □□ □□□ □□ 3.1: □□ □□□□ □□□ □□□ □□ □□□ □□□□□.

**NEW QUESTION: 394**

□□□□ □□□□ □□□□ □□□□ □□□□□□ □□□□□□ □□□.

☐☐☐☐ ☐ ☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

☐☐☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐☐

- A.** □□ □□  
**B.** □□□ □□□  
**C.** VLAN □□ □□  
**D.** □□□□ □□ □□□

**Answer: C (LEAVE A REPLY)**

0000 000 000 0000 0000000 0000 00 0000 VLAN(Virtual Local Area Networks) 0  
 00 000 0 0000. VLAN 00 000 000000 00 000 000 00 "00" 00 00 000  
 00000 000 00000. 0 000 00 VLAN 0000 0000000 0000 00000 0000 00  
 000 00 000 0000 00 00000 0 0 0000. 00 00 0000 00, 00 0 0000 00  
 00 0000 00000 00 0 0000000 0000 0 0000.

VLAN 1000000000000000, 000 00 0000 000 VLAN 000 00000, 0 000 000  
000 VLAN 00000 000.

□□□□ □□ □□ VLAN□ □□ □□□ □ □□□ VLAN □□□□ □□□□ □ □□ □□□□.

VLAN□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□  
□□□□ □□□ □ □□□□.

**NEW QUESTION: 395**

□□ OSI □□ □□ □ IP □□□ □□□□ □□□ □□□□□?

- A.** □□□□
- B.** □□
- C.** □□□□□□
- D.** □□ □□□□
- E.** □□□ □□

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 396**

Which of the following is the first step a network administrator should take in the troubleshooting methodology?

- A. Establish a plan of action.**
- B. Document findings and outcomes.**
- C. Test the theory to determine cause.**

D. Identify the problem.

**Answer: D** ([LEAVE A REPLY](#))

Explanation

According to the network troubleshooting methodology, the first step a network administrator should take is to identify the problem. This involves gathering information from the users, the network devices, and the symptoms of the issue. Identifying the problem helps to narrow down the scope and the possible causes of the network issue.

References

1: Network troubleshooting methodology | CompTIA Network+ N10-008 ...

2: Chapter 21. A Network Troubleshooting Methodology - CompTIA Network+ ...

3: Network Troubleshooting Methodology - N10-008 CompTIA Network+ : 5.1

#### NEW QUESTION: 397

□□□□ □□□□□ □ □□□□ □□□□□ □□□ □□□□□. □□□□ □□□□ □□□□□ □□ □□□□  
□ □□□□□ □□ □□□□□□. □□□ □ □□□□□ □□□□□ OS □□□ □□□□□.  
□□□□ □□ □ □□ □□□ □□□□□□ □□ □□□□ □□□?

- A. □□□ □□□
- B. □□□□ □□ □□
- C. SNMP □□
- D. □□□□□□□

**Answer: D** ([LEAVE A REPLY](#))

#### NEW QUESTION: 398

□□□□ □□□□ □□ □□□□□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□. □  
□ □□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□□□. □□□□ □□□ □□□ □□□  
□□□□ □□□□ □□ □□□□ □□□□□□.

| Metric       | Value         |
|--------------|---------------|
| Bytes input  | 441,164,698   |
| Bytes output | 2,625,115,257 |
| Runts        | 0             |
| CRCs         | 5,489         |
| Collisions   | 1             |
| MDIX         | On            |
| Speed        | 1,000         |
| Duplex       | Full          |

□□□□ □□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□ □□□?

- A. Cat 5 □□ □□□□ Cat 6 □□□□ □□□□□.
- B. □□□ □□□ □□□ □□□□□ □□□□ □□□□□.
- C. □□□□□ □□□ □□□□□□.
- D. □□□□ NetFlow □□□□ □□□□ □□□ □□□□□.
- E. □□□□□□□ MDIX□ □□□□□□ □□□ □□□□□□.

**Answer: A** ([LEAVE A REPLY](#))

Which of the following is a common cause of network congestion? (Select all that apply.)  
A. Too many devices connected to the network.  
B. A single bottleneck in the network.  
C. A network that is not properly configured.  
D. A network that is not properly maintained.  
E. A network that is not properly monitored.  
1000BASE-TX is a standard for Cat 5 Ethernet (Cat 6 is also a standard for 1000BASE-TX). Which of the following is a common cause of network congestion?  
A. Too many devices connected to the network.  
B. A single bottleneck in the network.  
C. A network that is not properly configured.  
D. A network that is not properly maintained.  
E. A network that is not properly monitored.

#### NEW QUESTION: 399

Which of the following is a common cause of network congestion? (Select all that apply.)  
A. Too many devices connected to the network.  
B. A single bottleneck in the network.  
C. A network that is not properly configured.  
D. A network that is not properly maintained.  
E. A network that is not properly monitored.

- A. IDS is a common cause of network congestion.
- B. IDS is a common cause of network congestion.
- C. IDS is a common cause of network congestion.
- D. IDS is a common cause of network congestion.
- E. IDS is a common cause of network congestion.

Answer: E ([LEAVE A REPLY](#))

#### NEW QUESTION: 400

Which of the following is a common cause of network congestion? (Select all that apply.)

- A. DDoS (DDoS)
- B. DDoS
- C. DDoS
- D. MAC address

Answer: ([SHOW ANSWER](#))

Which of the following is a common cause of network congestion? (Select all that apply.)

#### NEW QUESTION: 401

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 switch port's performance:



**NEW QUESTION: 403**

Which DNS record type is used to map an IP address to a domain name?

A. A

B. NS

C. AAAA

D. PTR

**Answer: D (LEAVE A REPLY)**

Explanation:

CNAME(Canonical Name) records are used to map a domain name to another domain name. For example, if you have a domain named blog.example.com and you want to map it to example.com, you would create a CNAME record for blog.example.com that points to example.com. CNAME records are used to map domain names to IP addresses. IP addresses are used to map domain names to IP addresses. IP addresses are used to map domain names to IP addresses.

**N10-008** dumps are available for free at DumpTop. N10-008 dumps are available for free at DumpTop.

**N10-008** dumps are available for free at DumpTop. N10-008 dumps are available for free at DumpTop.

<https://www.dumptop.com/CompTIA/N10-008-dump.html> (1075 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)