



Exam Code: 920-806

Exam Name: Nortel Advanced Data Networking
Technology

Vendor: Nortel

Version: DEMO

Part: A

1: An employee wants to set up a wireless network at home, so that the employee can work from anywhere in the house. They know that using the default security settings on the WLAN would leave their network open to attack. They would like to avoid eavesdropping passive network attacks. Which security procedure best provides authentication, encryption, and authorization?

- A.Enable 128-bit Wired Equivalent Privacy (WEP).
- B.Enable Temporal key integrity protocol (TKIP).
- C.Disable broadcast of the Service Set Identifier (SSID).
- D.Limit logins to a single MAC address.

Correct Answers: B

2: An engineer downloaded confidential email while working from a hotspot. The hotspot requires that the user login, but does not have data encryption. The email program uses POP3 to transfer email and does not use encryption. Another patron at the hotspot was running packet capture software on the WLAN and received all of the engineer email in plain text.

Which security measure, if taken by the engineer, would be ineffective?

- A.Use a VNP to connect into corporate and check email, the VPN would encrypt the traffic.
- B.Connect only to access points that use an encryption protocol to encrypt data.
- C.Select only an email program that encrypts the messages using a secure protocol such as SSL.
- D.Select an email program that uses HTTP to transfer the email.

Correct Answers: D

3: A small cafe has decided that it would like to provide a free wireless hotspot to attract new customers. When they first installed the wireless access point (AP), they discovered that the signal strength was very poor. They think this may be related to another nearby hotspot. The AP that was installed supports 802.11g and 802.11b. What should they do to improve the signal strength?

- A.Install a new 802.11a AP.
- B.Change their AP to 802.11g only.
- C.Change their AP to 802.11b only.
- D.Change the channel on the AP to remove the hotspot overlap.

Correct Answers: D

4: A customer would like to increase the bandwidth between two locations connected over the WAN. They would like to have multiple paths that use a single entry in the route table if possible. Which solution allows for this?

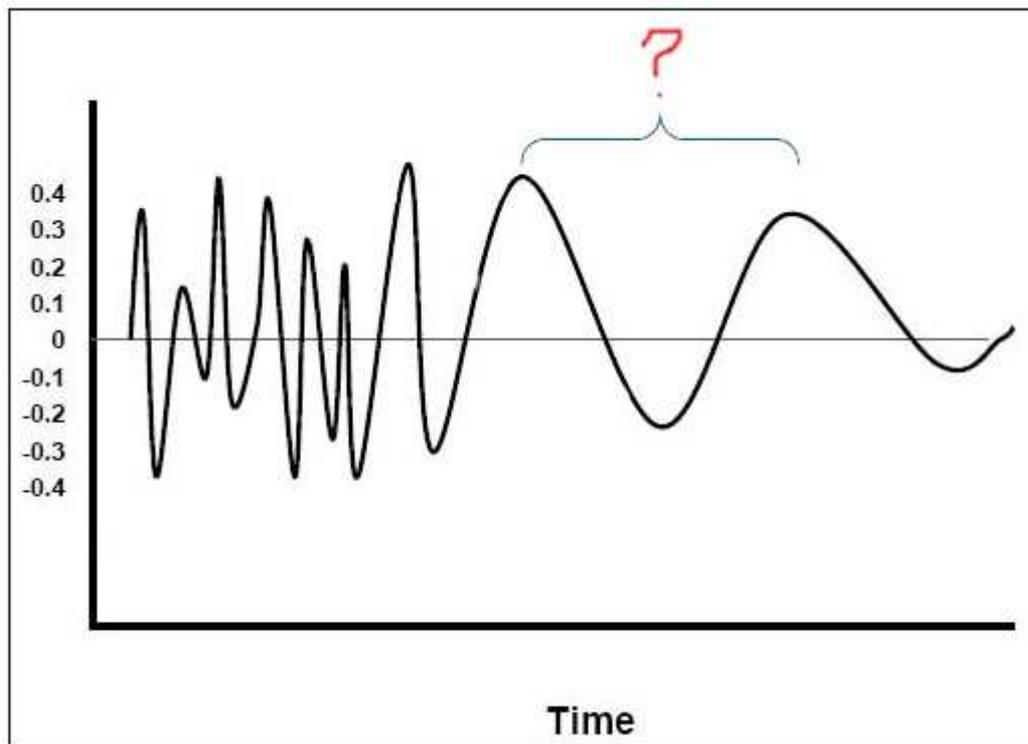
- A.multiline circuit
- B.multilink trunking
- C.Virtual Link Aggregation Control Protocol (VLACP)
- D.Virtual Router Redundancy Protocol (VRRP)

Correct Answers: A

5: Click on the Exhibit button.

Using the exhibit, what do you call the measure of the amount of time the wave takes from the

moment it hits peak intensity to the moment it hits peak intensity again?



- A.cycle
- B.amplitude
- C.frequency
- D.wavelength

Correct Answers: D

6: Line-of-sight is one of the boundaries of Radio Frequency (RF) waves. They are also affected by obstacles that can cause the waves to bend, bounce, or become distorted. Which type of electromagnetic wave is a radio wave?

- A.direct wave
- B.ground wave
- C.space wave
- D.fluid wave

Correct Answers: A

7: A customer has enabled Single Host Single Authentication Extensible Authentication Protocol over LAN (EAPoL) on ports on their Ethernet switch. Not all PCs have the ability to authenticate against the RADIUS server. They would like to allow these users to access limited network resources, and they do not want to use MAC authentication against the non-EAP customers. Which EAPoL feature should they use to allow non-EAP-enabled customers to send data on an EAP-enabled port when there are no authorized hosts?

- A.Multi-host single authentication (MHSA)
- B.Guest VLAN
- C.Multi-host multiple authentication (MHMA)

D.Non-EAP hosts (NEAP)

Correct Answers: B

8: An enterprise is developing an e-commerce application that requires secure communications between the web client and the e-commerce server. They will use SSL. Which encryption key is used by SSL?

A.public key encryption

B.private key encryption

C.secret key encryption

D.public and secret key encryption

Correct Answers: D

9: A customer requires secure network communications with network devices. Which protocol should be disabled on the network devices to ensure secure communication?

A.Telnet

B.Secure web (HTTPS)

C.Secure Shell (SSH or SSHv2)

D.Simple Network Management Protocol (SNMP) v3

Correct Answers: A

10: A customer is requesting help with deciding what authentication protocol they should use with their Extensible Authentication Protocol over LAN (EAPoL) configuration.

Their environment contains the following:

switches that support EAP-MD5, EAP-TLS, and PEAP-MSCHAPv2

corporate workstations that run Microsoft Windows 2000

corporate servers that run Microsoft Windows 2003

The solution should have the following characteristics:

user credentials should be username and password

machine credentials should be hostname and password

authenticator credentials should be digital certificates

a single sign-on solution

machine authentication should occur transparently using a random password assigned to the computer in the domain

user authentication should occur transparently using the user credentials when the user logs into the computer

user authentication should occur transparently using the user

Which Extensible Authentication Protocol (EAP) authentication protocol should they select?

A.EAP-MD5

B.EAP-TLS

C.PEAP-MSCHAPv2

D.no supported authentication protocol supports all the requirements

Correct Answers: C