CCNA4 v 4.0 Exam chapter 6 Teleworking

1. Which two statements about DSL are true? (Choose two.)

users are on a shared medium
uses RF signal transmission
local loop can be up to 3.5 miles (5.5km)
physical and data link layers are defined by DOCSIS
user connections are aggregated at a DSLAM located at the CO

2. Which two Layer 1 requirements are outlined in the Data-over-Cable Service Interface Specification (DOCSIS)? (Choose two.)

channel widths
access method
maximum data rate
modulation techniques
compression techniques

3. Which two statements are valid solutions for a cable ISP to reduce congestion for users? (Choose two.)

use higher RF frequencies
allocate an additional channel
subdivide the network to reduce users on each segment
reduce the length of the local loop to 5.5 kilometers or less
use filters and splitters at the customer site to separate voice from data traffic

4. A technician has been asked to configure a broadband connection for a teleworker. The technician has been instructed that all uploads and downloads for the connection must use existing phone lines. Which broadband technology should be used?

cable
DSL
ISDN
POTS

5. After conducting research to learn about common remote connection options for teleworkers, a network administrator has decided to implement remote access over broadband to establish VPN connections over the public Internet. What is the result of this solution?

A reliable connection is established at greater speeds than what is offered from dialup over POTS. Security is increased, but username and password information are sent in plain text.
The connection has increased security and reliable connectivity. Users need a remote VPN router or VPN client software.
Security and reliability are increased at a substantial loss in throughput, which is considered acceptable when supporting a single user environment.
Reliability and security are increased without the need for additional equipment, when compared to dialup connections using POTS.

6. What are the three main functions of a secure VPN? (Choose three.)

accounting
authentication
authorization
data availability
data confidentiality
data integrity

7. Which two methods could an administrator use to authenticate users on a remote access VPN? (Choose two.)

digital certificates
ESP
hashing algorithms
smart cards
WPA

8. Data confidentiality through a VPN is achieved through which two methods? (Choose two.)

digital certificates
encryption
encapsulation
hashing
passwords

9. Data confidentiality through a VPN can be enhanced through the use of which three encryption protocols? (Choose three.)

AES
DES
AH
hash
MPLS
RSA

10. Which is an example of symmetric-key encryption?

Diffie-Hellman
digital certificate

pre-shared key
RSA signature

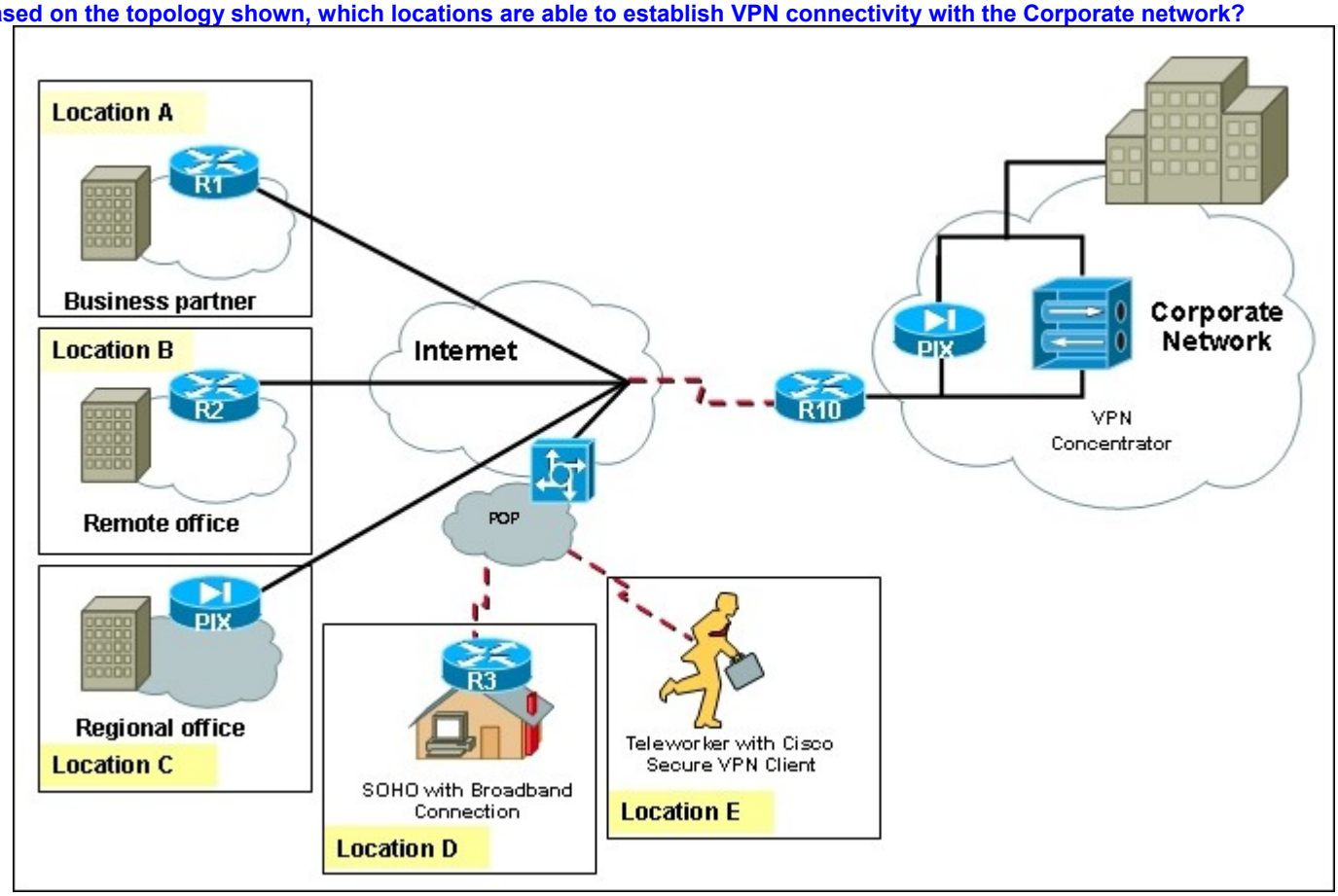
11. Which statement describes cable?
Delivering services over a cable network requires downstream frequencies in the 50 to 860 MHz range, and upstream frequencies in the 5 to 42 MHz range.
The cable subscriber must purchase a cable modem termination system (CMTS)
Each cable subscriber has dedicated upstream and downstream bandwidth.
Cable subscribers may expect up to 27 Mbps of bandwidth on the upload path.

12. A company is using WiMAX to provide access for teleworkers. What home equipment must the company provide at the teleworker's site?
a WiMAX tower
a one-way multicast satellite
a WiMAX receiver
an access point connected to the company WLAN

13. Which two features can be associated with the Worldwide Interoperability for Microwave Access (WiMAX) telecommunication technology? (Choose two.)
supports municipal wireless networks utilizing mesh technologies
covers areas as large as 7,500 square kilometers
supports point-to-point links, but not full mobile cellular-type access
connects directly to the Internet through high-bandwidth connections
operates at lower speeds than Wi-Fi, but supports many more users

14. While monitoring traffic on a cable network, a technician notes that data is being transmitted at 38 MHz. Which statement describes the situation observed by the technician?
Data is being transmitted from the subscriber to the headend.
Data is flowing downstream.
Cable television transmissions are interfering with voice and data transmissions.
The system is experiencing congestion in the lower frequency ranges.

15. Refer to the exhibit. All users have a legitimate purpose and the necessary persissions to access the Corporate network. Based on the topology shown, which locations are able to establish VPN connectivity with the Corporate network?



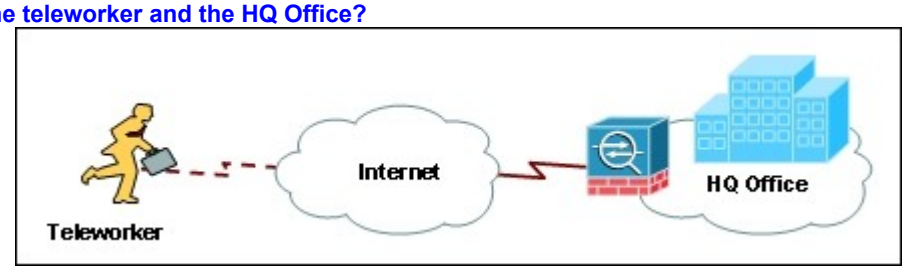
Locations C, D, and E can support VPN connectivity. Locations A and B require an additional PIX Firewall appliance installed on the edge of the network.
Locations C and E can support VPN connectivity. Locations A, B, and D require an additional PIX Firewall appliance installed on the edge of the network.
Locations A, B, D, and E can support VPN connectivity. Location C requires an additional router on the edge of the network.
All locations can support VPN connectivity.

16. What two protocols provide data authentication and integrity for IPsec? (Choose two.)
AH

L2TP
ESP
GRE
PPTP

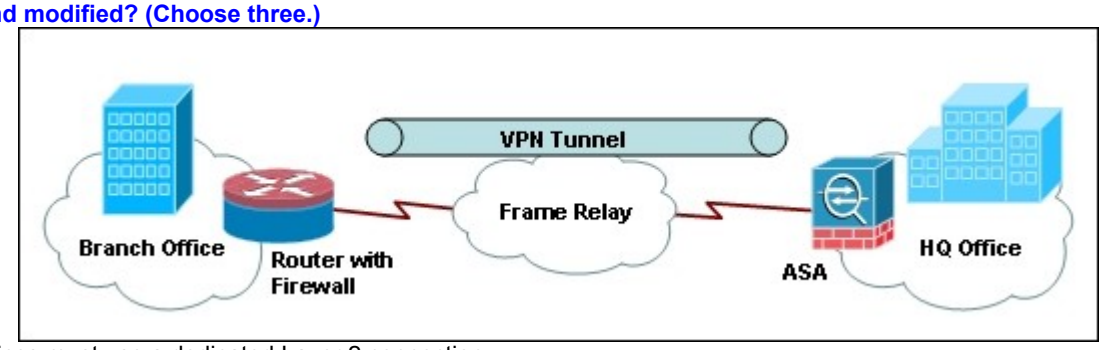
17. Which two protocols can be used to encapsulate traffic that is traversing a VPN tunnel? (Choose two.)
ATM
CHAP
IPsec
IPX
MPLS
PPTP

18. Refer to the exhibit. A teleworker is connected over the Internet to the HQ Office. What type of secure connection can be established between the teleworker and the HQ Office?



a GRE tunnel
a site-to-site VPN
a remote-access VPN
the user must be at the office location to establish a secure connection

19. Refer to the exhibit. A VPN tunnel has been established between the HQ Office and the Branch Office over the public Internet. Which three mechanisms are required by the devices on each end of the VPN tunnel to protect the data from being intercepted and modified? (Choose three.)



The devices must use a dedicated Layer 2 connection.
The devices must have the VPN client software installed.
The two parties must inspect the traffic against the same ACLs.
The two parties must establish a secret key used by encryption and hash algorithms.
The two parties must agree on the encryption algorithm to be used over the VPN tunnel.
The devices must be authenticated before the communication path is considered secure.