[Updated Constantly]

HERE

CCNA 4 (v5.0.3 + v6.0) Chapter 7 Exam Answers Full

1. **What is an example of an M2M connection in the IoT?**
   - A user sends an email over the Internet to a friend.
   - **Sensors in a warehouse communicate with each other and send data to a server block in the cloud.***
   - Redundant servers communicate with each other to determine which server should be active or standby.
   - An automated alarm system in a campus sends fire alarm messages to all students and staff.

   The Internet of Things (IoT) connects devices that traditionally are not connected to the Internet, such as sensors and actuators. A machine-to-machine (M2M) connection is unique to the IoT in that devices are connected together and communicate with each other. These devices can send data to a server block in the cloud for analysis and further operation change.

2. **What is the term for the extension of the existing Internet structure to billions of connected devices?**
   - M2M
   - digitization
   - **IoT***
   - SCADA

   The Internet of Things (IoT) refers to the interconnection of billions of things, or “smart dust.” SCADA refers to a type of IoT system applied to the industrial Internet. Digitization has several meanings. It can refer to the process of converting analog to digital, or it can refer to the process by which an organization modernizes by planning and ultimately building, a sophisticated and forward-thinking IT network ecosystem that will allow for greater connectivity, productivity, and security. Finally, M2M refers to communication from machine to machine.

3. **Which statement describes the Cisco IoT System?**
   - It is a switch operating system to integrate many Layer 2 security features.
   - It is an advanced routing protocol for cloud computing.
   - **It is an infrastructure to manage large scale systems of very different endpoints and platforms.***
   - It is a router operating system combining IOS and Linux for fog computing.

   Cisco developed the Cisco IoT System to help organizations and industries adopt IoT solutions. The IoT system provides an infrastructure to manage large scale systems of very different endpoints and platforms, and the huge amount of data that they create. Cisco IOx combines IOS and Linux to support fog computing.

4. **Which three network models are described in the fog computing pillar of the Cisco IoT System? (Choose three.)**

- **fog computing***
- **client/server***
- P2P
- **cloud computing***
- peer-to-peer
- enterprise WAN

The network models describe how data flows within a network. The network models described in the Fog computing pillar of the Cisco IoT System include:
Client/Server model – Client devices request services of servers. Servers are often located locally and managed by the organization.
Cloud computing model – a newer model where servers and services are dispersed globally in distributed data centers. Data is synchronized across multiple servers.
Fog computing – This model identifies a distributed computing infrastructure closer to the network edge. It enables edge devices to run applications locally and make immediate decisions.

5. **Which IoT pillar extends cloud connectivity closer to the network edge?**
   - network connectivity pillar
   - **fog computing pillar***
   - management and automation pillar
   - application enablement platform pillar

   By running distributed computing infrastructure closer to the network edge, fog computing enables edge devices to run applications locally and make immediate decisions.

6. **Which cybersecurity solution is described in the security pillar of the Cisco IoT System to address the security of power plants and factory process lines?**
   - IoT network security
   - cloud computing security
   - **operational technology specific security***
   - IoT physical security

   The Cisco IoT security pillar offers scalable cybersecurity solutions that include the following:
   Operational Technology specific security – the hardware and software that keeps the power plants running and manages factory process lines
   IoT Network security – network and perimeter security devices such as switches, routers, and ASA Firewall devices
   IoT Physical Security – include Cisco Video Surveillance IP Cameras that enable surveillance in a wide variety of environments

7. **Which cloud computing opportunity would provide the use of network hardware such as routers and switches for a particular company?**
   - **infrastructure as a service (IaaS)***
   - software as a service (SaaS)
   - browser as a service (BaaS)
   - wireless as a service (WaaS)

   This item is based on information contained in the presentation.
   Routers, switches, and firewalls are infrastructure devices that can be provided in the cloud.

8. **What technology allows users to access data anywhere and at any time?**
   - **Cloud computing***
   - virtualization
   - micromarketing
   - data analytics

   Cloud computing allows organizations to eliminate the need for on-site IT equipment, maintenance, and management. Cloud computing allows organizations to expand their services or capabilities while avoiding the increased costs of energy and space.

9. **The exhibit is not required to answer the question. The exhibit shows a fog covering trees on the side of a mountain.What statement describes Fog computing?**

   - It requires Cloud computing services to support non-IP enabled sensors and controllers.
   - It supports larger networks than Cloud computing does.
   - **It creates a distributed computing infrastructure that provides services close to the network edge.***
   - It utilizes a centralized computing infrastructure that stores and manipulates big data in one very secure data center.

   Three of the defining characteristics of Fog computing are as follows:
   its proximity to end-users
   its distributed computing infrastructure that keeps it closer to the network edge
   its enhanced security since data is not released into the Cloud

10. **Which Cloud computing service would be best for a new organization that cannot afford physical servers and networking equipment and must purchase network services on-demand?**
    - ITaaS
    - SaaS
    - PaaS
    - **IaaS***

    Infrastructure as a service (IaaS) provides an environment where users have an on-demand infrastructure that they can install any platform as needed.

11. **Which cloud model provides services for a specific organization or entity?**
    - a public cloud
    - a hybrid cloud
    - **a private cloud***

- a community cloud

Private clouds are used to provide services and applications to a specific organization and may be set up within the private network of the organization or managed by an outside organization.

12. **How does virtualization help with disaster recovery within a data center?**
    - improvement of business practices
    - supply of consistent air flow
    - **support of live migration***
    - guarantee of power

    Live migration allows moving of one virtual server to another virtual server that could be in a different location that is some distance from the original data center.

13. **What is a difference between the functions of Cloud computing and virtualization?**
    - **Cloud computing separates the application from the hardware whereas virtualization separates the OS from the underlying hardware.***
    - Cloud computing requires hypervisor technology whereas virtualization is a fault tolerance technology.
    - Cloud computing utilizes data center technology whereas virtualization is not used in data centers.
    - Cloud computing provides services on web-based access whereas virtualization provides services on data access through virtualized Internet connections.

    Cloud computing separates the application from the hardware. Virtualization separates the OS from the underlying hardware. Virtualization is a typical component within cloud computing. Virtualization is also widely used in data centers. Although the implementation of virtualization facilitates an easy server fault tolerance setup, it is not a fault tolerance technology by design. The Internet connection from a data center or service provider needs redundant physical WAN connections to ISPs.

14. **Which two business and technical challenges does implementing virtualization within a data center help businesses to overcome? (Choose two.)**
    - **physical footprint***
    - server hardware needs
    - virus and spyware attacks
    - **power and air conditioning***
    - operating system license requirements

    Traditionally, one server was built within one machine with one operating system. This server required power, a cool environment, and a method of backup. Virtualized servers require more robust hardware than a standard machine because a computer or server that is in a virtual machine commonly shares hardware with one or more servers and operating systems. By placing multiple servers within the same physical case, space is saved. Virtualized systems still need the proper licenses for operating systems or applications or both and still need the proper security applications and settings applied.

15. **When preparing an IoT implementation, what type of network will devices be connected to in order to share the same infrastructure and facilitate communications, analytics, and management?**
    - **converged***

- video
- telephone
- VoIP

16. **Which type of Hypervisor is implemented when a user with a laptop running the Mac OS installs a Windows virtual OS instance?**
    - virtual machine
    - bare metal
    - **type 2***
    - type 1

    Type 2 hypervisors, also know as hosted hypervisors, are installed on top of an existing operating system, such as Mac OS, Windows, or Linux.

17. **Which statement describes the concept of cloud computing?**
    - separation of operating system from hardware
    - separation of management plane from control plane
    - **separation of application from hardware***
    - separation of control plane from data plane

    Cloud computing is used to separate the application or service from hardware. Virtualization separates the operating system from the hardware.

18. **Which is a characteristic of a Type 2 hypervisor?**
    - best suited for enterprise environments
    - installs directly on hardware
    - **does not require management console software***
    - has direct access to server hardware resources

    Type 2 hypervisors are hosted on an underlaying operating system and are best suited for consumer applications and those experimenting with virtualization. Unlike Type 1 hypervisors, Type 2 hypervisors do not require a management console and do not have direct access to hardware.

19. **Which is a characteristic of a Type 1 hypervisor?**
    - does not require management console software
    - **installed directly on a server***
    - installed on an existing operating system
    - best suited for consumers and not for an enterprise environment

    Type 1 hypervisors are installed directly on a server and are known as “bare metal” solutions giving direct access to hardware resources. They also require a management console and are best suited for enterprise environments.

20. **How is the control plane modified to operate with network virtualization?**
    - Control plane redundancy is added to each network device.
    - The control plane on each device is interconnected to a dedicated high-speed network.
    - A hypervisor is installed in each device to allow multiple instances of the control plane.
    - **The control plane function is consolidated into a centralized controller.***

    In network virtualization design, the control plane function is removed from each network device and is performed by a centralized controller. The centralized controller communicates control plane functions to each network device and each device focuses on forwarding data.

21. **Which technology virtualizes the network control plane and moves it to a centralized controller?**
    - IaaS
    - **SDN***
    - fog computing
    - cloud computing

    Networking devices operate in two planes: the data plane and the control plane. The control plane maintains Layer 2 and Layer 3 forwarding mechanisms using the CPU. The data plane forwards traffic flows. SDN virtualizes the control plane and moves it to a centralized network controller.

22. **Which two layers of the OSI model are associated with SDN network control plane functions that make forwarding decisions? (Choose two.)**
    - Layer 1
    - **Layer 2***
    - **Layer 3***
    - Layer 4
    - Layer 5

    The SDN control plane uses the Layer 2 ARP table and the Layer 3 routing table to make decisions about forwarding traffic.

23. **What pre-populates the FIB on Cisco devices that use CEF to process packets?**
    - the adjacency table
    - **the routing table***
    - the DSP
    - the ARP table

    CEF uses the FIB and adjacency table to make fast forwarding decisions without control plane processing. The adjacency table is pre-populated by the ARP table and the FIB is pre-populated by the routing table.

24. **Which type of hypervisor would most likely be used in a data center?**
    - **Type 1***
    - Hadoop
    - Nexus
    - Type 2

    The two type of hypervisors are Type 1 and Type 2. Type 1 hypervisors are usually used on enterprise servers. Enterprise servers rather than virtualized PCs are more likely to be in a data center.

25. **What component is considered the brains of the ACI architecture and translates application policies?**
    - the Application Network Profile endpoints
    - the Nexus 9000 switch
    - the hypervisor
    - **the Application Policy Infrastructure Controller***

    The ACI architecture consists of three core components: the Application Network Profile, the Application Policy Infrastructure Controller, which serves as the brains of the ACI architecture, and the Cisco Nexus 9000 switch.

26. **Fill in the blank.**
In an IoT implementation, devices will be connected to a
network to share the same infrastructure and to facilitate communications, analytics, and management.
Correct Answer: converged

Currently, many things are connected using a loose collection of independent use-specific networks. In an IoT implementation, devices will be connected to a converged network to share the same infrastructure and to facilitate communications, analytics, and management.

27. **Fill in the blank.**
In a scenario where a user with a laptop running the Mac OS installs a Windows virtual OS instance, the user is implementing a Type
hypervisor.
Correct Answer: 2

Type 2 hypervisors, also know as hosted hypervisors, are installed on top of an existing operating system, such as Mac OS, Windows, or Linux.

Older Version

28. **A network design engineer is planning the implementation of a cost-effective method to interconnect multiple networks securely over the Internet. Which type of technology is required?**
- a GRE IP tunnel
- a leased line
- **a VPN gateway***
- a dedicated ISP

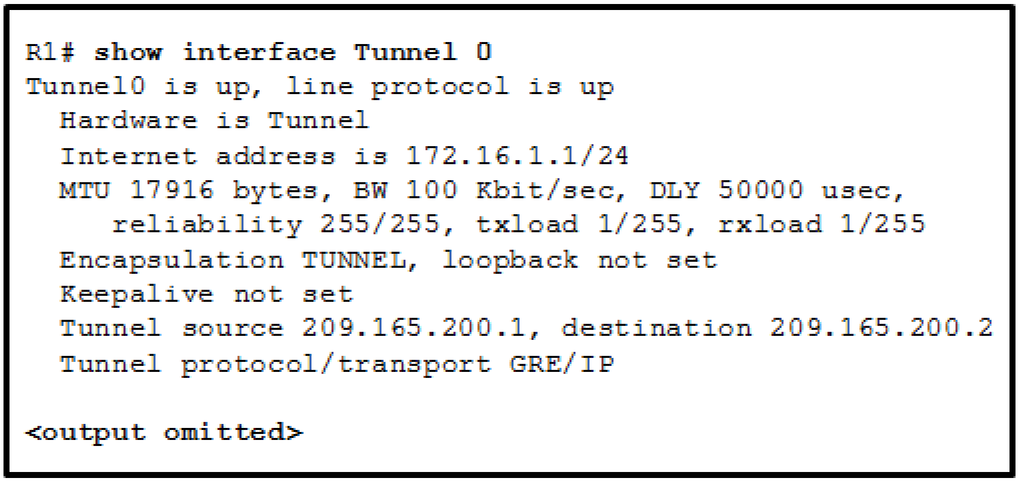
29. **What is one benefit of using VPNs for remote access?**
- lower protocol overhead
- ease of troubleshooting
- **potential for reduced connectivity costs***
- increased quality of service

30. **How is “tunneling” accomplished in a VPN?**
- **New headers from one or more VPN protocols encapsulate the original packets.***
- All packets between two hosts are assigned to a single physical medium to ensure that the packets are kept private.
- Packets are disguised to look like other types of traffic so that they will be ignored by potential attackers.
- A dedicated circuit is established between the source and destination devices for the duration of the connection.

31. **Two corporations have just completed a merger. The network engineer has been asked to connect the two corporate networks without the expense of leased lines. Which solution would be the most cost effective method of providing a proper and secure connection between the two corporate networks?**
- Cisco AnyConnect Secure Mobility Client with SSL
- Cisco Secure Mobility Clientless SSL VPN
- Frame Relay

- remote access VPN using IPsec
- site-to-site VPN*

32. **Which two scenarios are examples of remote access VPNs? (Choose two.)**
    - A toy manufacturer has a permanent VPN connection to one of its parts suppliers.
    - All users at a large branch office can access company resources through a single VPN connection.
    - A mobile sales agent is connecting to the company network via the Internet connection at a hotel.*
    - A small branch office with three employees has a Cisco ASA that is used to create a VPN connection to the HQ.
    - An employee who is working from home uses VPN client software on a laptop in order to connect to the company network.*
33. **Which statement describes a feature of site-to-site VPNs?**
    - The VPN connection is not statically defined.
    - VPN client software is installed on each host.
    - Internal hosts send normal, unencapsulated packets.*
    - Individual hosts can enable and disable the VPN connection.
34. **What is the purpose of the generic routing encapsulation tunneling protocol?**
    - to provide packet level encryption of IP traffic between remote sites
    - to manage the transportation of IP multicast and multiprotocol traffic between remote sites*
    - to support basic unencrypted IP tunneling using multivendor routers between remote sites
    - to provide fixed flow-control mechanisms with IP tunneling between remote sites
35. **Which remote access implementation scenario will support the use of generic routing encapsulation tunneling?**
    - a mobile user who connects to a router at a central site
    - a branch office that connects securely to a central site
    - a mobile user who connects to a SOHO site
    - a central site that connects to a SOHO site without encryption*
36. **Refer to the exhibit. A tunnel was implemented between routers R1 and R2. Which two conclusions can be drawn from the R1 command output? (Choose two.)**



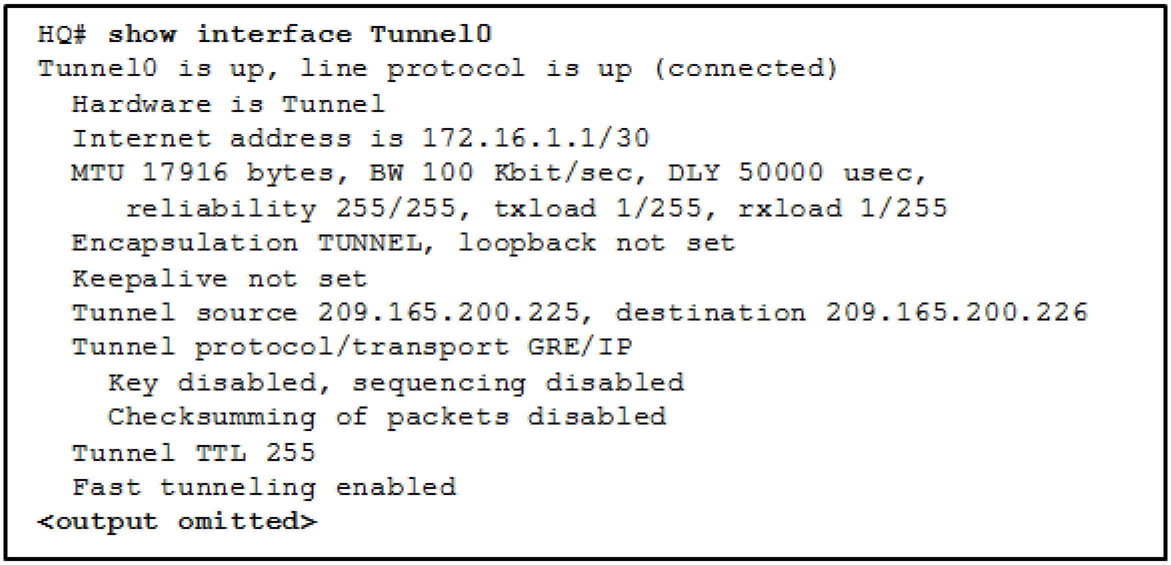
```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.200.1, destination 209.165.200.2
  Tunnel protocol/transport GRE/IP

<output omitted>
```

- This tunnel mode is not the default tunnel interface mode for Cisco IOS software.

- This tunnel mode provides encryption.
- **The data that is sent across this tunnel is not secure.***
- This tunnel mode does not support IP multicast tunneling.
- **A GRE tunnel is being used.***

37. **Refer to the exhibit. Which IP address would be configured on the tunnel interface of the destination router?**



```
HQ# show interface Tunnel0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.200.225, destination 209.165.200.226
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
<output omitted>
```

- 172.16.1.1
- **172.16.1.2***
- 209.165.200.225
- 209.165.200.226

38. **Which statement correctly describes IPsec?**

- **IPsec works at Layer 3, but can protect traffic from Layer 4 through Layer 7.***
- IPsec uses algorithms that were developed specifically for that protocol.
- IPsec implements its own method of authentication.
- IPsec is a Cisco proprietary standard.

39. **Which function of IPsec security services allows the receiver to verify that the data was transmitted without being changed or altered in any way?**

- anti-replay protection
- authentication
- **data integrity***
- confidentiality

40. **Which statement describes a characteristic of IPsec VPNs?**

- IPsec is a framework of Cisco proprietary protocols.
- IPsec can secure traffic at Layers 1 through 3.
- IPsec encryption causes problems with routing.
- **IPsec works with all Layer 2 protocols.***

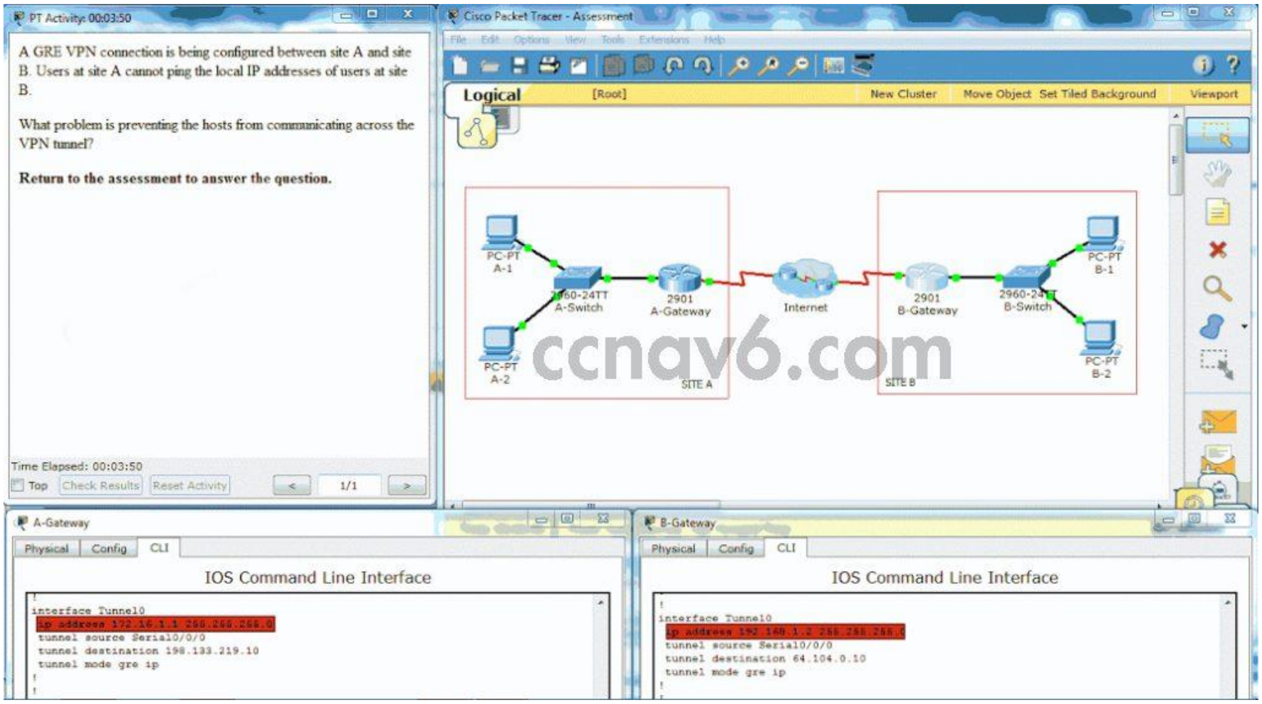
41. **What is an IPsec protocol that provides data confidentiality and authentication for IP packets?**

- AH
- **ESP***
- RSA
- IKE

42. **What two encryption algorithms are used in IPsec VPNs? (Choose two.)**
    - DH
    - PSK
    - IKE
    - **AES ***
    - **3DES***
43. **Which algorithm is an asymmetrical key cryptosystem?**
    - **RSA***
    - AES
    - 3DES
    - DES
44. **Which two algorithms use Hash-based Message Authentication Code for message authentication? (Choose two.)**
    - 3DES
    - DES
    - AES
    - **MD5 ***
    - **SHA***
45. **Which three statements describe the building blocks that make up the IPsec protocol framework? (Choose three.)**
    - **IPsec uses encryption algorithms and keys to provide secure transfer of data.***
    - IPsec uses Diffie-Hellman algorithms to encrypt data that is transferred through the VPN.
    - IPsec uses 3DES algorithms to provide the highest level of security for data that is transferred through a VPN.
    - **IPsec uses secret key cryptography to encrypt messages that are sent through a VPN.***
    - IPsec uses Diffie-Hellman as a hash algorithm to ensure integrity of data that is transmitted through a VPN.
    - **IPsec uses ESP to provide confidential transfer of data by encrypting IP packets.***
46. **A network design engineer is planning the implementation of an IPsec VPN. Which hashing algorithm would provide the strongest level of message integrity?**
    - SHA-1
    - MD5
    - AES
    - **512-bit SHA***
47. **What is the purpose of utilizing Diffie-Hellman (DH) algorithms as part of the IPsec standard?**
    - DH algorithms allow unlimited parties to establish a shared public key that is used by encryption and hash algorithms.
    - **DH algorithms allow two parties to establish a shared secret key that is used by encryption and hash algorithms.***
    - DH algorithms allow unlimited parties to establish a shared secret key that is used by encryption and hash algorithms.
    - DH algorithms allow two parties to establish a shared public key that is used by encryption and hash algorithms.
48. **What is the purpose of a message hash in a VPN connection?**
    - It ensures that the data cannot be read in plain text.

- **It ensures that the data has not changed while in transit.***
- It ensures that the data is coming from the correct source.
- It ensures that the data cannot be duplicated and replayed to the destination.

49. **Which Cisco VPN solution provides limited access to internal network resources by utilizing a Cisco ASA and provides browser-based access only?**
    - **clientless SSL VPN***
    - client-based SSL VPN
    - SSL
    - IPsec
50. **What key question would help determine whether an organization should use an SSL VPN or an IPsec VPN for the remote access solution of the organization?**
    - Is a Cisco router used at the destination of the remote access tunnel?
    - What applications or network resources do the users need for access?
    - Are both encryption and authentication required?
    - **Do users need to be able to connect without requiring special VPN software?***
51. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. What problem is preventing the hosts from communicating across the VPN tunnel?**



PT Activity: 00:03:50

A GRE VPN connection is being configured between site A and site B. Users at site A cannot ping the local IP addresses of users at site B.

What problem is preventing the hosts from communicating across the VPN tunnel?

Return to the assessment to answer the question.

Time Elapsed: 00:03:50

A-Gateway

IOS Command Line Interface

```
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Serial0/0/0
 tunnel destination 198.133.219.10
 tunnel mode gre ip
!
!
```

B-Gateway

IOS Command Line Interface

```
!
interface Tunnel0
 ip address 192.168.1.2 255.255.255.0
 tunnel source Serial0/0/0
 tunnel destination 64.104.0.10
 tunnel mode gre ip
!
```

- The EIGRP configuration is incorrect.
- The tunnel destinations addresses are incorrect.
- **The tunnel IP addresses are incorrect.***
- The tunnel source interfaces are incorrect

52. **Which critical function that is provided by IPsec ensures that data has not been changed in transit between the source and destination?**
    - **integrity***
    - anti-replay protection
    - confidentiality
    - authentication

53. **Which service of IPsec verifies that secure connections are formed with the intended sources of data?**
    - encryption
    - **authentication***
    - confidentiality
    - data integrity
54. **Fill in the blank.**
    "__**GRE**__" is a site-to-site tunnel protocol developed by Cisco to allow multiprotocol and IP multicast traffic between two or more sites.
55. **What is an advantage of using the Cisco Secure Mobility Clientless SSL VPN?**
    - Security is provided by prohibiting network access through a browser.
    - Any device can connect to the network without authentication.
    - **Clients do not require special software.***
    - Clients use SSH to access network resources.
56. **How can the use of VPNs in the workplace contribute to lower operating costs?**
    - VPNs prevents connectivity to SOHO users.
    - **VPNs can be used across broadband connections rather than dedicated WAN links.***
    - VPNs require a subscription from a specific Internet service provider that specializes in secure connections.
    - High-speed broadband technology can be replaced with leased lines.
57. **Which two characteristics describe IPsec VPNs? (Choose two.)**
    - Key lengths range from 40 bits to 256 bits.
    - IPsec authentication is one-way or two-way.
    - **Specific PC client configuration is required to connect to the VPN.***
    - IPsec is specifically designed for web-enabled applications.
    - **IPsec authenticates by using shared secrets or digital certificates.***