**[Updated Constantly]**

**HERE**

## CCNA 4 (v5.0.3 + v6.0) Chapter 3 Exam Answers Full

1. **Which broadband wireless technology is based on the 802.11 standard?**
   - WiMAX
   - UMTS
   - **municipal Wi-Fi***
   - CDMA

   The IEEE 802.11 standard is also known as Wi-Fi. Municipal Wi-Fi is a variant of the 802.11 standard.

2. **What is the approximate distance limitation for providing a satisfactory ADSL service from the central office to a customer?**
   - **3.39 miles or 5.46 kilometers***
   - 2.11 miles or 3.39 kilometers
   - 11.18 miles or 18 kilometers
   - 6.21 miles or 10 kilometers

   For customers to receive satisfactory ADSL service, the local loop, or distance from the central office, must be less than 5.46 kilometers.

3. **What is a component of an ADSL connection that is located at the customer site?**
   - CO
   - DSLAM
   - **CPE***
   - SOHO

   Customer premises equipment (CPE) is the equipment, such as a router or modem, that is located at the customer site and connects the internal network to the carrier network.

4. **What is the function of the DSLAM in a broadband DSL network?**
   - separates POTS traffic from ADSL traffic
   - separates voice from data signals
   - **multiplexes individual customer DSL connections into a single upstream link***
   - communicates directly with customer cable modems to provide Internet services to customers

   On a DSL network the DSLAM is used to multiplex connections from DSL subscribers into a single high-capacity link. The DSLAM is located at the central office of the provider.

5. **Which broadband technology would be best for a small office that requires fast upstream connections?**
   - **fiber-to-the-home***
   - WiMax
   - DSL

- cable

Fiber-to-the-home provides fast downstream and upstream connections. DSL, cable, and WiMax provide relatively slow upstream connections.

6. **What are two WAN connection enhancements that are achieved by implementing PPPoE? (Choose two.)**
   - An Ethernet link supports a number of data link protocols.
   - DSL CHAP features are included in PPPoE.
   - Encapsulating Ethernet frames within PPP frames is an efficient use of bandwidth.
   - **CHAP enables customer authentication and accounting.***
   - **PPP enables the ISP to assign an IP address to the customer WAN interface.***

   Encapsulating a PPP frame within an Ethernet frames enables IP address assignment by ISPs that are using DSL technology, as well as the ability to use CHAP for authentication and accounting. Traditional DSL does not support CHAP authentication. A traditional Ethernet link supports only Ethernet-based data link protocols.

7. **When PPPoE is configured on a customer router, which two commands must have the same value for the configuration to work? (Choose two.)**
   - **dialer pool 2***
   - interface dialer 2
   - ppp chap password 2
   - interface gigabitethernet 0/2
   - **pppoe-client dial-pool-number 2***
   - ppp chap hostname 2

   The dialer pool number configured on both the dialer and Ethernet interfaces must match. The interface numbers and the username and the password do not have to match

8. **Why is the MTU for a PPPoE DSL configuration reduced from 1500 bytes to 1492?**
   - to establish a secure tunnel with less overhead
   - to enable CHAP authentication
   - **to accommodate the PPPoE headers***
   - to reduce congestion on the DSL link

   The default maximum data field of an Ethernet frame is 1500 bytes. However, in PPPoE the Ethernet frame payload includes a PPP frame which has also has a header. This reduces the available data MTU to 1492 bytes.

9. **What are two characteristics of a PPPoE configuration on a Cisco customer router? (Choose two.)**
   - The customer router CHAP username and password are independent of what is configured on the ISP router.
   - An MTU size of 1492 bytes is configured on the Ethernet interface.
   - **The Ethernet interface does not have an IP address.***
   - **The PPP configuration is on the dialer interface.***
   - The dialer pool command is applied to the Ethernet interface to link it to the dialer interface.

   PPP, CHAP, an IP address, the dialer pool number, and the MTU size are all configured on the dialer interface. The customer router CHAP username and password must match what

is configured the ISP router. The pppoe-client command, not the dialer pool command, is applied to the Ethernet interface to link it to the dialer interface.

10. **Where is PPPoE configured on a Cisco router?**
   - on any physical interface
   - **on the dialer interface***
   - on an Ethernet interface
   - on a serial interface

   The PPPoE configuration is applied to the dialer interface, not to the Ethernet interface. The dialer interface is linked to the Ethernet interface with the dialer-pool and pppoe-client commands.

11. **How can the use of VPNs in the workplace contribute to lower operating costs?**
   - High-speed broadband technology can be replaced with leased lines.
   - **VPNs can be used across broadband connections rather than dedicated WAN links.***
   - VPNs prevents connectivity to SOHO users.
   - VPNs require a subscription from a specific Internet service provider that specializes in secure connections.

   VPN technology can be used with broadband connectivity or more expensive leased lines. VPNs provide connectivity between offices, users, and SOHO environments. VPNs do not require a specific ISP to be used.

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

   Packets in a VPN are encapsulated with the headers from one or more VPN protocols before being sent across the third party network. This is referred to as "tunneling". These outer headers can be used to route the packets, authenticate the source, and prevent unauthorized users from reading the contents of the packets.

13. **Which two statements describe a remote access VPN? (Choose two.)**
   - **It may require VPN client software on hosts.***
   - It requires hosts to send TCP/IP traffic through a VPN gateway.
   - It connects entire networks to each other.
   - **It is used to connect individual hosts securely to a company network over the Internet.***
   - It requires static configuration of the VPN tunnel.

   Remote access VPNs can be used to support the needs of telecommuters and mobile users by allowing them to connect securely to company networks over the Internet. To connect hosts to the VPN server on the corporate network, the remote access VPN tunnel is dynamically built by client software that runs on the hosts.

14. **Which is a requirement of a site-to-site VPN?**
   - It requires hosts to use VPN client software to encapsulate traffic.

- It requires the placement of a VPN server at the edge of the company network.
- It requires a client/server architecture.
- **It requires a VPN gateway at each end of the tunnel to encrypt and decrypt traffic.***

Site-to-site VPNs are static and are used to connect entire networks. Hosts have no knowledge of the VPN and send TCP/IP traffic to VPN gateways. The VPN gateway is responsible for encapsulating the traffic and forwarding it through the VPN tunnel to a peer gateway at the other end which decapsulates the traffic.

15. **What functionality does mGRE provide to the DMVPN technology?**
- **It allows the creation of dynamically allocated tunnels through a permanent tunnel source at the hub and dynamically allocated tunnel destinations at the spokes.***
- It provides secure transport of private information over public networks, such as the Internet.
- It is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.
- It creates a distributed mapping database of public IP addresses for all VPN tunnel spokes.

DMVPN is built on three protocols, NHRP, IPsec, and mGRE. NHRP is the distributed address mapping protocol for VPN tunnels. IPsec encrypts communications on VPN tunnels. The mGRE protocol allows the dynamic creation of multiple spoke tunnels from one permanent VPN hub.

16. **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 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.***
- **A mobile sales agent is connecting to the company network via the Internet connection at a hotel.***

Remote access VPNs connect individual users to another network via a VPN client that is installed on the user device. Site-to-site VPNs are "always on" connections that use VPN gateways to connect two sites together. Users at each site can access the network on the other site without having to use any special clients or configurations on their individual devices.

17. **Refer to the exhibit. What solution can provide a VPN between site A and site B to support encapsulation of any Layer 3 protocol between the internal networks at each site?**
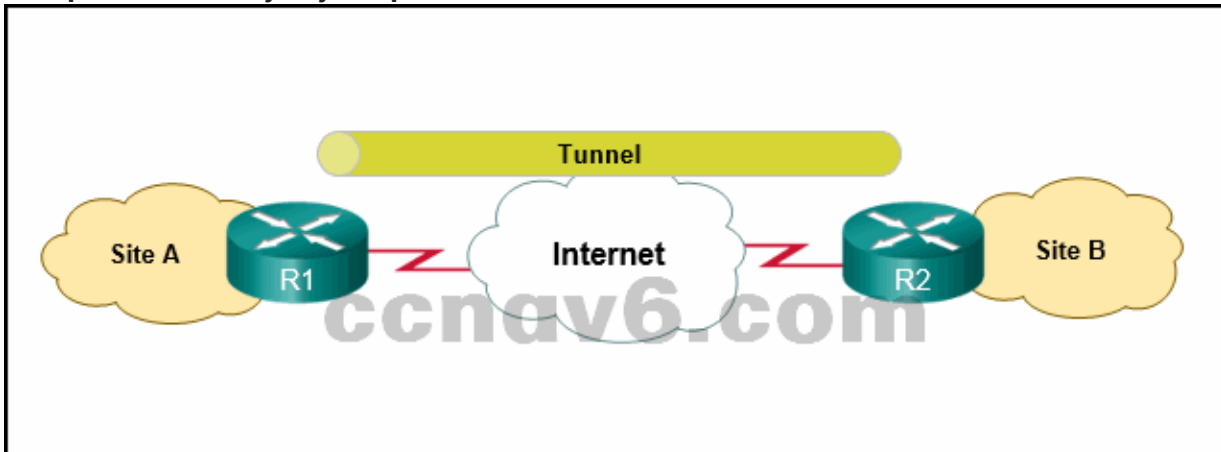


- a remote access tunnel
- **a GRE tunnel***
- an IPsec tunnel
- Cisco SSL VPN

A Generic Routing Encapsulation (GRE) tunnel is a non-secure, site-to-site VPN tunneling solution that is capable of encapsulating any Layer 3 protocol between multiple sites across over an IP internetwork.

18. **Which three statements are characteristics of generic routing encapsulation (GRE)? (Choose three.)**
- **GRE does not have strong security mechanisms.***
- The GRE header alone adds at least 24 bytes of overhead.
- **GRE is stateless.***
- **GRE encapsulation supports any OSI Layer 3 protocol.***
- GRE is the most secure tunneling protocol.
- GRE provides flow control by default.

GRE uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol. GRE itself is stateless; it does not include any flow-control mechanisms by default. GRE does not have strong security mechanisms.

19. **Refer to the exhibit. Which IP address is configured on the physical interface of the CORP router?**

```
CORP# show interface Tunnel1
Tunnel1 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 10.1.1.1/30
  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 209.165.202.133, destination 209.165.202.134
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
<output omitted>
```

   - 10.1.1.1
   - **209.165.202.133***
   - 209.165.202.134
   - 10.1.1.2

   The tunnel source and tunnel destination addresses reference the IP addresses of the physical interfaces on the local and remote routers respectively.

20. **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>
```

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

   The IP address that is assigned to the tunnel interface on the local router is 172.16.1.1 with a prefix mask of /30. The only other address, 172.16.1.2, would be the destination tunnel

interface IP address. Although 209.165.200.226 is listed as a destination address in the output, this is the address of the physical interface at the destination, not the tunnel interface.

21. **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>
```

  ▪ **The data that is sent across this tunnel is not secure.***
  ▪ This tunnel mode is not the default tunnel interface mode for Cisco IOS software.
  ▪ This tunnel mode provides encryption.
  ▪ **A GRE tunnel is being used.***
  ▪ This tunnel mode does not support IP multicast tunneling.

  According to the R1 output, a GRE tunnel mode was specified as the tunnel interface mode. GRE is the default tunnel interface mode for Cisco IOS software. GRE does not provide encryption or any other security mechanisms. Therefore, data that is sent across a GRE tunnel is not secure. GRE supports IP multicast tunneling.

22. **What is used by BGP to determine the best path to a destination?**
  ▪ cost
  ▪ administrative distance
  ▪ hop count
  ▪ **attributes***

  BGP uses attributes, such as AS-path, to determine the best path to a destination.

23. **What command specifies a BGP neighbor that has an IP address of 5.5.5.5/24 and that is in AS 500?**
  ▪ **(config-router)# neighbor 5.5.5.5 remote-as 500***
  ▪ (config-router)# network 5.0.0.0 0.0.0.255
  ▪ (config-router)# router bgp 500
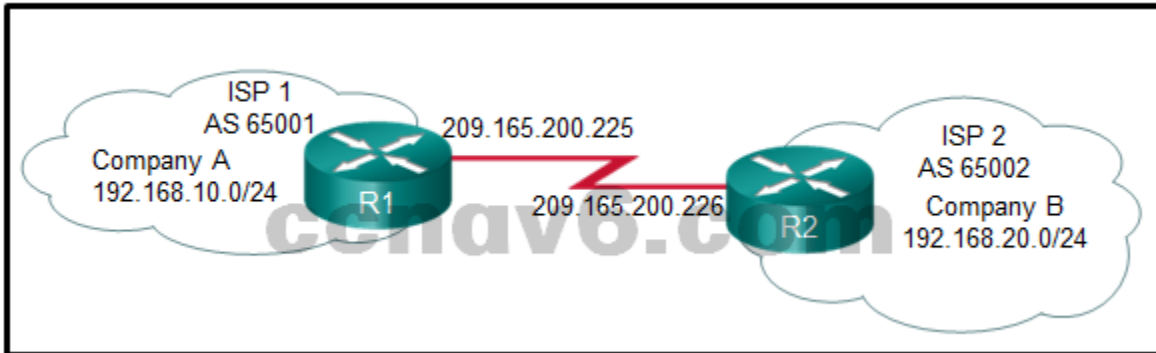  ▪ (config-router)# neighbor 500 remote-as 5.5.5.5

  The neighbor command is used to specify an EBGP neighbor router and peer with it. The command requires that the AS number of the neighbor be included as part of the command.

24. **True or False? Multiple BGP processes can run on a router.**
  true
  **false***

Because a BGP router can only belong to a single autonomous system, it can only run a single BGP process.

25. **Refer to the exhibit. Which two configurations will allow router R1 to establish a neighbor relationship with router R2? (Choose two.)**



- R1(config)# router bgp 65001
  R1(config-router)# network 192.168.20.0R2(config)# router bgp 65002
  R2(config-router)# network 192.168.10.0
  R2(config-router)# neighbor 209.165.200.226 remote-as 65002
- **R2(config)# router bgp 65002**
  **R2(config-router)# network 192.168.20.0**
  **R2(config-router)# neighbor 209.165.200.225 remote-as 65001***
- R1(config)# router bgp 65002
  R1(config-router)# network 192.168.20.0
  R1(config-router)# neighbor 209.165.200.225 remote-as 65001
- **R1(config)# router bgp 65001**
  **R1(config-router)# network 192.168.10.0**
  **R1(config-router)# neighbor 209.165.200.226 remote-as 65002***
- R2(config)# router bgp 65002
  R2(config-router)# network 192.168.10.0

To configure EBGP, the router bgp command is followed by the AS number in which the router resides. Conversely, the neighbor command contains the AS number to which the remote router belongs.

26. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**
   **What is the code displayed on the web page?**
- Welldone!
- BGP is configured!
- **BGP is running!***
- Configuration is correct!

The basic EBGP configuration includes the following tasks:
Step 1: Enable BGP routing.
Step 2: Configure the BGP neighbors or neighbor.
Step 3: Advertise the network or networks originating from the AS.

Older Version

27. **At which layer of the OSI model does multiplexing take place?**
   - **Layer 1 \***
   - Layer 2
   - Layer 3
   - Layer 4

28. **Which command can be used to view the cable type that is attached to a serial interface?**
   - Router(config)# show interfaces
   - **Router(config)# show controllers\***
   - Router(config)# show ip interface
   - Router(config)# show ip interface brief

29. **Which field marks the beginning and end of an HDLC frame?**
   - Data
   - FCS
   - Control
   - **Flag\***

30. **Which serial 0/0/0 interface state will be shown if no serial cable is attached to the router, but everything else has been correctly configured and turned on?**
   - Serial 0/0/0 is up, line protocol is up
   - Serial 0/0/0 is up, line protocol is down
   - **Serial 0/0/0 is down, line protocol is down\***
   - Serial 0/0/0 is up (looped)
   - Serial 0/0/0 is up (disabled)
   - Serial 0/0/0 is administratively down, line protocol is down

31. **Which is an advantage of using PPP on a serial link instead of HDLC?**
   - **option for authentication\***
   - higher speed transmission
   - fixed-size frames
   - option for session establishment

32. **What are three components of PPP? (Choose three.)**
   - authentication
   - **LCP\***
   - multilink
   - **NCP\***
   - compression
   - **HDLC-like framing\***

33. **How does PPP interface with different network layer protocols?**
   - **by using separate NCPs\***
   - by negotiating with the network layer handler
   - by encoding the information field in the PPP frame
   - by specifying the protocol during link establishment through LCP

34. **Which address is used in the Address field of a PPP frame?**
   - a single byte of binary 00000000
   - a single byte of binary 10101010
   - **a single byte of binary 11111111\***
   - the IP address of the serial interface

35. **Which three physical layer interfaces support PPP? (Choose three.)**

- FastEthernet
- GigabitEthernet
- POTS
- **asynchronous serial ***
- **synchronous serial ***
- **HSSI***

36. **Which three are types of LCP frames used with PPP? (Choose three.)**
    - link-negotiation frames
    - link-acknowledgment frames
    - **link-maintenance frames***
    - **link-termination frames***
    - link-control frames
    - **link-establishment frames***

37. **Which protocol will terminate the PPP link after the exchange of data is complete?**
    - NCP
    - **LCP***
    - IPCP
    - IPXCP

38. **During a PPP session establishment phase, which two messages are sent by the requested party if the options are not acceptable? (Choose two.)**
    - **Configure-Nak***
    - Code-Reject
    - Protocol-Reject
    - **Configure-Reject***
    - Discard-Request

39. **Which three statements are true about PPP? (Choose three.)**
    - **PPP can use synchronous and asynchronous circuits.***
    - PPP can only be used between two Cisco devices.
    - PPP carries packets from several network layer protocols in LCPs.
    - **PPP uses LCPs to establish, configure, and test the data link connection.***
    - **PPP uses LCPs to agree on format options such as authentication, compression, and error detection.***

40. **Which PPP option can detect links that are in a looped-back condition?**
    - **Magic Number***
    - MRU
    - Callback
    - ACCM

41. **When configuring Multilink PPP, where is the IP address for the multilink bundle configured?**
    - on a physical serial interface
    - on a subinterface
    - **on a multilink interface***
    - on a physical Ethernet interface

42. **Refer to the exhibit. Which statement describes the status of the PPP connection?**

```
Serial1 is up, line protocol is up
  Hardware is HD64570
  Internet address is 200.200.200.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:04, output 00:00:04, output hang never
  Last clearing of "show interface" counters 00:08:59
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
```

- Only the link-establishment phase completed successfully.
- Only the network-layer phase completed successfully.
- Neither the link-establishment phase nor the network-layer phase completed successfully.
- **Both the link-establishment and network-layer phase completed successfully.***

43. **Refer to the exhibit. A network administrator is configuring the PPP link between the two routers. However, the PPP link cannot be established. Based on the partial output of the show running-config command, what is the cause of the problem?**

```
ISP(config)# show running-config
<output omitted>

username BORDER password 0 Cisco
!
interface Serial0/0/0
  ip address 209.165.200.225 255.255.255.252
  encapsulation ppp
  ppp authentication chap

BORDER(config)# show running-config
<output omitted>

username ISP password 0 cisco
!
interface Serial0/0/0
  ip address 209.165.200.226 255.255.255.252
  encapsulation ppp
  ppp authentication chap
```

- The usernames do not match.
- **The passwords do not match.***
- The passwords should be longer than 8 characters.
- The interface IP addresses are in different subnets.

44. **In which situation would the use of PAP be preferable to the use of CHAP?**

- when router resources are limited
- when multilink PPP is used
- **when plain text passwords are needed to simulate login at the remote host\***
- when a network administrator prefers it because of ease of configuration

45. **A network administrator is evaluating authentication protocols for a PPP link. Which three factors might lead to the selection of CHAP over PAP as the authentication protocol? (Choose three.)**
    - establishes identities with a two-way handshake
    - **uses a three-way authentication periodically during the session to reconfirm identities\***
    - control by the remote host of the frequency and timing of login events
    - **transmits login information in encrypted format \***
    - **uses an unpredictable variable challenge value to prevent playback attacks\***
    - makes authorized network administrator intervention a requirement to establish each session

46. **Refer to the exhibit. Based on the debug command output that is shown, which statement is true of the operation of PPP.**

```
<output omitted>
*Jun 30 08:01:41.367: Se0/0/0 LCP: State is Open
*Jun 30 08:01:41.367: Se0/0/0 PPP: Phase is AUTHENTICATING, by both
*Jun 30 08:01:41.367: Se0/0/0 CHAP: O CHALLENGE id 252 len 23 from "R1"
*Jun 30 08:01:41.367: Se0/0/0 CHAP: I CHALLENGE id 247 len 23 from "R2"
*Jun 30 08:01:41.371: Se0/0/0 CHAP: Using hostname from unknown source
*Jun 30 08:01:41.371: Se0/0/0 CHAP: Using password from AAA
*Jun 30 08:01:41.371: Se0/0/0 CHAP: O RESPONSE id 247 len 23 from "R1"
*Jun 30 08:01:41.375: Se0/0/0 CHAP: I RESPONSE id 252 len 23 from "R2"
*Jun 30 08:01:41.375: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
*Jun 30 08:01:41.375: Se0/0/0 PPP: Phase is AUTHENTICATING, Unauthenticated User
*Jun 30 08:01:41.375: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
*Jun 30 08:01:41.375: Se0/0/0 PPP: Phase is AUTHENTICATING, Authenticated User
*Jun 30 08:01:41.379: Se0/0/0 CHAP: I SUCCESS id 247 len 4
*Jun 30 08:01:41.379: Se0/0/0 CHAP: O SUCCESS id 252 len 4
*Jun 30 08:01:41.379: Se0/0/0 PPP: Phase is UP
*Jun 30 08:01:41.379: Se0/0/0 PPP: Process pending ncp packets
*Jun 30 08:01:41.383: Se0/0/0 CDPCP: O CONFREQ [Closed] id 1 len 4
*Jun 30 08:01:41.383: Se0/0/0 CDPCP: I CONFREQ [REQsent] id 1 len 4
*Jun 30 08:01:41.383: Se0/0/0 CDPCP: O CONFACK [REQsent] id 1 len 4
*Jun 30 08:01:41.387: Se0/0/0 CDPCP: I CONFACK [ACKsent] id 1 len 4
*Jun 30 08:01:41.387: Se0/0/0 CDPCP: State is Open
```

- CHAP authentication failed because of an unknown hostname.
- **A PPP session was successfully established.\***
- Both PAP and CHAP authentication were attempted.
- The debug output is from router R2.

47. **Match the PPP option with the correct description. (Not all options are used.)**

Match the PPP option with the correct description. (Not all options are used.)

| | |
|---|---|
| Maximum Receive Unit | Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link. |
| Authentication Protocol | Provides load balancing over the router interfaces. |
| Multilink | The maximum size of the PPP frame. |
| Compression | Helps to ensure a reliable, loop-free data link layer. |
| | The two choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). |

Place the options in the following order: **Compression -> Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link.**
**Multilink -> Provides load balancing over the router interfaces.**
**Maximum Receive Unit -> The maximum size of the PPP frame**
**– not scored –**
**Authentication Protocol -> The two choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)**

48. **Match the steps to the PPP CHAP authentication process sequence. (Not all options are used.)**

Match the steps to the PPP CHAP authentication process sequence. (Not all options are used.)

| | |
|---|---|
| Step 1 | calculate the MD5 hash |
| Step 2 | calculate the ID and random number |
| Step 3 | send the challenge ID, hash, and username |
| Step 4 | use LCP to negotiate the type of authentication |
| Step 5 | negotiate the Layer 3 protocol |
| Step 6 | calculate the hash based on received information |
| | compare the received hash with the calculated hash |

**Place the options in the following order:**
**Step 3 -> calculate the MD5 hash***
**Step 2 -> calculate the ID and random number***
**Step 4 -> send challenge ID, hash, and username***
**Step 1 -> use LCP to negotiate the type of authentication***
**– not scored –**
**Step 5 -> calculate the hash based on received information***
**Step 6 -> compare the received hash with the calculated hash**

49. **Match the phases of establishing a PPP session in the correct order. (Not all options are used.)**

Match the phases of establishing a PPP session in the correct order. (Not all options are used.)

| phase 1 | | negotiate with the network layer to configure L3 protocol |
| phase 2 | | verify authentication between NCP and the network layer protocol |
| phase 3 | | establish the link and negotiate configuration options |
| | | determine the quality of the link |

**Place the options in the following order:**
**Phase 3** -> negotiate with the network layer to configure L3 protocol
− not scored −
**Phase 1** -> establish the link and negotiate configuration options
**Phase 2** -> determine the quality of the link

50. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. Why is the serial link between router R1 and router R2 not operational?**



- The encapsulation in both routers does not match.
- The passwords are different in both routers.
- **In each case the expected username is not the same as the remote router hostname.***
- The authentication type is not the same in both routers.

51. **What PPP information will be displayed if a network engineer issues the show ppp multilink command on Cisco router?**
- the IP addresses of the link interfaces
- **the serial interfaces participating in the multilink***
- the queuing type on the link
- the link LCP and NCP status

52. **Refer to the exhibit. What type of Layer 2 encapsulation will be used for connection D on the basis of this configuration on a newly installed router:**
**RtrA(config)#** interface serial0/0/0

**RtrA(config-if)#** ip address 128.107.0.2 255.255.255.252
**RtrA(config-if)#** no shutdown
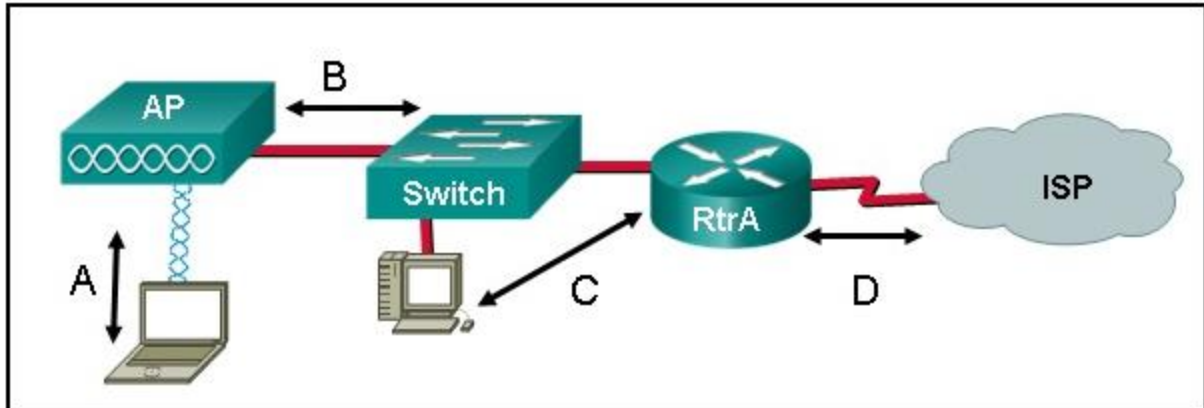


- Ethernet
- Frame Relay
- **HDLC***
- PPP

53. **A network engineer is monitoring an essential, but poor quality, PPP WAN link that periodically shuts down. An examination of the interface configurations shows that the ppp quality 90 command has been issued. What action could the engineer take to reduce the frequency with which the link shuts down?**
    - **Issue the command ppp quality 70.***
    - Issue the command ppp quality 100.
    - Set the DCE interface to a lower clock rate.
    - Use the bandwidth command to increase the bandwidth of the link.

54. **A network engineer is troubleshooting the loss of MPEG video viewing quality as MPEG video files cross a PPP WAN link. What could be causing this loss of quality?**
    - Link Quality Monitoring was not configured correctly on each interface.
    - **The compress command was used when PPP was configured on the interfaces.***
    - The clock rates configured on each serial interface do not match.
    - PAP authentication was misconfigured on the link interfaces.