Latest Version: 6.0

Question: 1

What are two benefits of 802.3ad link aggregation? (Choose two)

A. It increases bandwidth
B. It ensures symmetrical paths
C. It simplifies interface configuration.
D. It creates physical layer redundancy.

Answer: A, D

Explanation:
Aggregating multiple links between physical interfaces creates a single logical point-to-point trunk link or a LAG. The LAG balances traffic across the member links within an aggregated Ethernet bundle and effectively increases the uplink bandwidth. Another advantage of link aggregation is increased availability, because the LAG is composed of multiple member links. If one member link fails, the LAG continues to carry traffic over the remaining links.
https://www.juniper.net/documentation/us/en/software/junos/interfaces-ethernetswitches/topics/topic-map/switches-interface-aggregated.html

Question: 2

Click the Exhibit button.

```
user@router> show bgp neighbor 192.168.200.2
Peer: 192.168.200.2+179 AS 11685 Local: 192.168.200.1+49469 AS 7029
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference AddressFamily PeerAS LocalAS Rib-group Refresh>
  Address families configured: inet-unicast inet-vpn-unicast l2vpn-signaling
  Holdtime: 90 Preference: 170 Local AS: 7029 Local System AS: 0
  Number of flaps: 0
  Peer ID: 10.8.241.31      Local ID: 10.8.241.30       Active Holdtime: 90
  Keepalive Interval:30          Group index: 0    Peer index: 0
  BFD: disabled, down
  Local Interface: xe-0/2/3.0
  NLRI for restart configured on peer: inet-unicast inet-vpn-unicast l2vpn
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 11685)
  Peer does not support Addpath
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              0
    Received prefixes:            0
    Accepted prefixes:            0
    Suppressed due to damping:    0
    Advertised prefixes:          0
  Last traffic (seconds): Received 17   Sent 17   Checked 17
  Input messages:  Total 2      Updates 1       Refreshes 0     Octets 42
  Output messages: Total 3      Updates 0       Refreshes 0     Octets 136
  Output Queue[0]: 0
```

Your router is configured to peer with your ISP's router using BGP. You can only control your BGP configuration.
Which address families are negotiated between the two BGP peers shown in the exhibit?

A. inet-unicast inet-vpn-unicast 12vpn-signaling
B. inet-unicast
C. inet-vpn-unicast
D. inet-unicast inet-vpn-unicast 12vpn

Answer: B

Question: 3

Which statement is true about IP-IP tunnels?

A. Intermediate devices must have a route to the destination address of the traffic being tunneled.
B. Intermediate devices must have a route to both the tunnel source address and the tunnel destination address.

C. Intermediate devices must have a route to the tunnel destination address but do not require a route to the tunnel source address.
D. Intermediate devices must have a route to the tunnel source address but do not require a route to the tunnel destination address

Answer: B

Explanation:
Routing is based on destination, not source; Only the route for the destination tunnel endpoint is necessary for each packet.
If you're thinking about a lab environment with a single intermediary device, it's incidental that it will have a route for both tunnel endpoint IPs. Only the relevant destination will be considered with each packet it processes.

Question: 4

You have a conference room with an open network port that is used by employees to connect to the network. You are concerned about rogue switches being connected to this port
Which two features should you enable on your switch to limit access to this port? (Choose two.)

A. DHCP snooping
B. dynamic ARP inspection
C. MAC limiting
D. 802.1X

Answer: A, B

Question: 5

Which two port security features use the DHCP snooping database for additional port security? (Choose two.)

A. dynamic ARP inspection
B. MACsec
C. IP Source guard
D. MAC learning

Answer: A, C