

## Exam Questions JN0-664

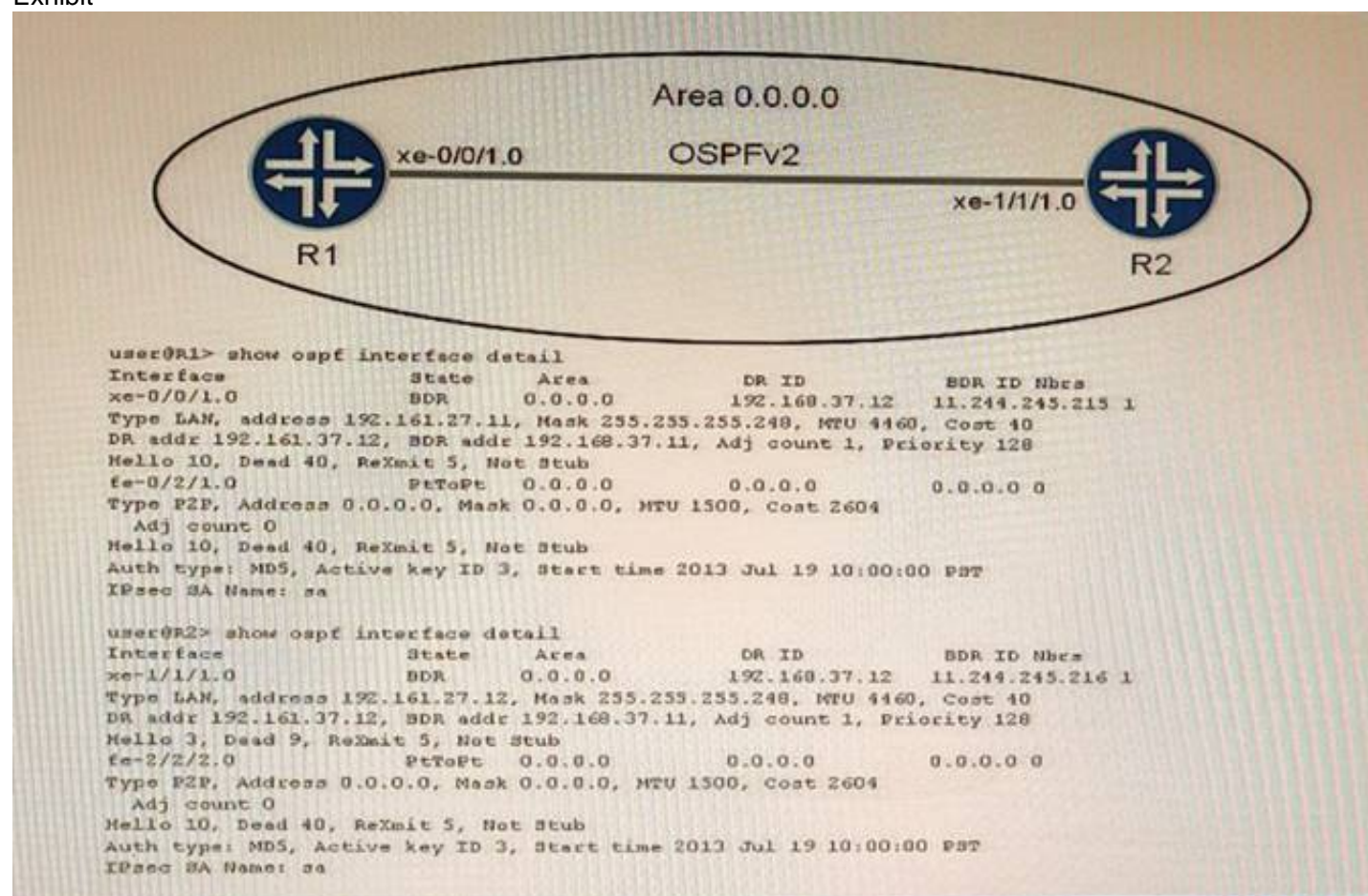
Service Provider - Professional (JNCIP-SP)

<https://www.2passeasy.com/dumps/JN0-664/>



## NEW QUESTION 1

Exhibit



Which two statements are true about the OSPF adjacency displayed in the exhibit? (Choose two.)

- A. There is a mismatch in the hello interval parameter between routers R1 and R2
- B. There is a mismatch in the dead interval parameter between routers R1 and R2.
- C. There is a mismatch in the OSPF hold timer parameter between routers R1 and R2.
- D. There is a mismatch in the poll interval parameter between routers R1 and R2.

**Answer:** AB

### Explanation:

The hello interval is the time interval between two consecutive hello packets sent by an OSPF router on an interface. The dead interval is the time interval after which a neighbor is declared down if no hello packets are received from it. These parameters must match between two OSPF routers for them to form an adjacency. In the exhibit, router R1 has a hello interval of 10 seconds and a dead interval of 40 seconds, while router R2 has a hello interval of 30 seconds and a dead interval of 120 seconds. This causes a mismatch and prevents them from becoming neighbors.

## NEW QUESTION 2

Exhibit.



**Exhibit**

```

user@R1# show interfaces
ge-1/2/3 {
  unit 0 {
    description to-R2;
    family inet {
      address 10.1.1.1/30;
    }
    family iso;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.16.1/32;
    }
    family iso {
      address 49.0001.1921.6801.6001.00;
    }
  }
}
user@R1# show protocols
isis {
  interface ge-1/2/3.0 {
    level 2 disable;
  }
}
...
user@R2# show interfaces
ge-1/2/3 {
  unit 0 {
    description to-R1;
    family inet {
      address 10.1.1.2/30;
    }
    family iso;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 192.168.16.2/32;
    }
    family iso {
      address 49.0001.1921.6801.6002.00;
    }
  }
}
user@R2# show protocols
isis {
  interface ge-1/2/3.0 {
    level 1 disable;
  }
  interface lo0.0 {
    level 1 disable;
  }
}

```

Referring to the exhibit, what must be changed to establish a Level 1 adjacency between routers R1 and R2?

- A. Change the level 1 disable parameter under the R1 protocols isis interface lo0.0 hierarchy to the level 2 disable parameter.
- B. Remove the level 1 disable parameter under the R2 protocols isis interface lo0.0 configuration hierarchy.
- C. Change the level 1 disable parameter under the R2 protocols isis interface ge-1/2/3.0 hierarchy to the level 2 disable parameter.
- D. Add IP addresses to the interface ge-1/2/3 unit 0 family iso hierarchy on both R1 and R2.

**Answer: B**

**Explanation:**

IS-IS routers can form Level 1 or Level 2 adjacencies depending on their configuration and network topology. Level 1 routers are intra-area routers that share the same area address with their neighbors. Level 2 routers are inter-area routers that can connect different areas. Level 1-2 routers are both intra-area and inter-area routers that can form adjacencies with any other router.

In the exhibit, R1 and R2 are in different areas (49.0001 and 49.0002), so they cannot form a Level 1 adjacency. However, they can form a Level 2 adjacency if they are both configured as Level 1-2 routers. R1 is already configured as a Level 1-2 router, but R2 is configured as a Level 1 router only, because of the level 1 disable command under the lo0.0 interface. This command disables Level 2 routing on the loopback interface, which is used as the router ID for IS-IS. Therefore, to establish a Level 1 adjacency between R1 and R2, the level 1 disable command under the R2 protocols isis interface lo0.0 hierarchy must be removed. This will enable Level 2 routing on R2 and allow it to form a Level 2 adjacency with R1.

### NEW QUESTION 3

Which two statements are correct about VPLS tunnels? (Choose two.)

- A. LDP-signaled VPLS tunnels only support control bit 0.
- B. LDP-signaled VPLS tunnels use auto-discovery to provision sites
- C. BGP-signaled VPLS tunnels can use either RSVP or LDP between the PE routers.
- D. BGP-signaled VPLS tunnels require manual provisioning of sites.

**Answer:** BC

#### Explanation:

VPLS is a Layer 2 VPN technology that allows multiple sites to connect over a shared IP/MPLS network as if they were on the same LAN. VPLS tunnels can be signaled using either Label Distribution Protocol (LDP) or Border Gateway Protocol (BGP). LDP-signaled VPLS tunnels use auto-discovery to provision sites, meaning that PE routers can automatically discover other PE routers that belong to the same VPLS instance

### NEW QUESTION 4

Which statement is true regarding BGP FlowSpec?

- A. It uses a remote triggered black hole to protect a network from a denial-of-service attack.
- B. It uses dynamically created routing policies to protect a network from denial-of-service attacks
- C. It is used to protect a network from denial-of-service attacks dynamically
- D. It verifies that the source IP of the incoming packet has a resolvable route in the routing table

**Answer:** B

#### Explanation:

BGP FlowSpec is a feature that extends the Border Gateway Protocol (BGP) to enable routers to exchange traffic flow specifications, allowing for more precise control of network traffic. The BGP FlowSpec feature enables routers to advertise and receive information about specific flows in the network, such as those originating from a particular source or destined for a particular destination. Routers can then use this information to construct traffic filters that allow or deny packets of a certain type, rate limit flows, or perform other actions<sup>1</sup>. BGP FlowSpec can also help in filtering traffic and taking action against distributed denial of service (DDoS) attacks by dropping the DDoS traffic or diverting it to an analyzer<sup>2</sup>. BGP FlowSpec rules are internally converted to equivalent Cisco Common Classification Policy Language (C3PL) representing corresponding match and action parameters<sup>2</sup>. Therefore, BGP FlowSpec uses dynamically created routing policies to protect a network from denial-of-service attacks.

References: 1: <https://www.networkingsignal.com/what-is-bgp-flowspec/> 2: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/xr-16/irg-xe-16-book/bgp-flowspec-route-reflector-support.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xr-16/irg-xe-16-book/bgp-flowspec-route-reflector-support.html)

### NEW QUESTION 5

Which two statements about IS-IS are correct? (Choose two.)

- A. PSNPs are flooded periodically.
- B. PSNPs contain only descriptions of LSPs.
- C. CSNPs are flooded periodically
- D. CSNPs contain only descriptions of LSPs.

**Answer:** BC

#### Explanation:

IS-IS is an interior gateway protocol that uses link-state routing to exchange routing information among routers within a single autonomous system. IS-IS uses two types of packets to synchronize link-state databases among routers: Link State Packets (LSPs) and Partial Sequence Number Packets (PSNPs). LSPs contain information about the state and cost of links in the network, and are flooded periodically throughout the network. PSNPs are used to acknowledge receipt of LSPs and request retransmission of missing or corrupted LSPs. PSNPs contain only descriptions of LSPs, such as their sequence numbers and checksums<sup>3</sup>. IS-IS also uses another type of packet called Complete Sequence Number Packets (CSNPs), which are used to summarize the entire link-state database at regular intervals or when a new adjacency is formed. CSNPs are flooded periodically throughout the network and contain only descriptions of LSPs<sup>4</sup>. Therefore, PSNPs contain only descriptions of LSPs and CSNPs are flooded periodically. References: 3: <https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/routing-policy-is-is-partial-sequence-number-packet-psnp.html> 4: <https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/routing-policy-is-is-complete-sequence-number-packet-csnp.html>

### NEW QUESTION 6

You want to ensure that L1 IS-IS routers have only the most specific routes available from L2 IS-IS routers. Which action accomplishes this task?

- A. Configure the ignore-attached-bit parameter on all L2 routers.
- B. Configure all routers to allow wide metrics.
- C. Configure all routers to be L1.
- D. Configure the ignore-attached-bit parameter on all L1 routers

**Answer:** D

#### Explanation:

The attached bit is a flag in an IS-IS LSP that indicates whether a router is connected to another area or level (L2) of the network. By default, L2 routers set this bit when they advertise their LSPs to L1 routers, and L1 routers use this bit to select a default route to reach other areas or levels through L2 routers. However, this may result in suboptimal routing if there are multiple L2 routers with different paths to other areas or levels. To ensure that L1 routers have only the most specific routes available from L2 routers, you can configure the ignore-attached-bit parameter on all L1 routers. This makes L1 routers ignore the attached bit and install all interarea routes learned from L2 routers in their routing tables.



### NEW QUESTION 7

Which two EVPN route types are used to advertise a multihomed Ethernet segment? (Choose two )

- A. Type 1
- B. Type 3
- C. Type 4
- D. Type 2

**Answer:** AC

#### Explanation:

EVPN is a solution that provides Ethernet multipoint services over MPLS networks. EVPN uses BGP to distribute endpoint provisioning information and set up pseudowires between PE devices. EVPN uses different route types to convey different information in the control plane. The following are the main EVPN route types:

? Type 1 - Ethernet Auto-Discovery Route: This route type is used for network-wide messaging and discovery of other PE devices that are part of the same EVPN instance. It also carries information about the redundancy mode and load balancing algorithm of the PE devices.

? Type 2 - MAC/IP Advertisement Route: This route type is used for MAC and IP address learning and advertisement between PE devices. It also carries information about the Ethernet segment identifier (ESI) and the label for forwarding traffic to the MAC or IP address.

? Type 3 - Inclusive Multicast Ethernet Tag Route: This route type is used for broadcast, unknown unicast, and multicast (BUM) traffic forwarding. It also carries information about the multicast group and the label for forwarding BUM traffic.

? Type 4 - Ethernet Segment Route: This route type is used for multihoming scenarios, where a CE device is connected to more than one PE device. It also carries information about the ESI and the designated forwarder (DF) election process.

### NEW QUESTION 8

An interface is configured with a behavior aggregate classifier and a multifield classifier How will the packet be processed when received on this interface?

- A. The packet will be discarded.
- B. The packet will be processed by the BA classifier first, then the MF classifier.
- C. The packet will be forwarded with no classification changes.
- D. The packet will be processed by the MF classifier first, then the BA classifier.

**Answer:** C

#### Explanation:

behavior aggregate (BA) classifiers and multifield (MF) classifiers are two types of classifiers that are used to assign packets to a forwarding class and a loss priority based on different criteria. The forwarding class determines the output queue for a packet. The loss priority is used by a scheduler to control packet discard during periods of congestion.

A BA classifier maps packets to a forwarding class and a loss priority based on a fixed- length field in the packet header, such as DSCP, IP precedence, MPLS EXP, or IEEE 802.1p CoS bits. A BA classifier is computationally efficient and suitable for core devices that handle high traffic volumes. A BA classifier is useful if the traffic comes from a trusted source and the CoS value in the packet header is trusted.

An MF classifier maps packets to a forwarding class and a loss priority based on multiple fields in the packet header, such as source address, destination address, protocol type, port number, or VLAN ID. An MF classifier is more flexible and granular than a BA classifier and can match packets based on complex filter rules. An MF classifier is suitable for edge devices that need to classify traffic from untrusted sources or rewrite packet headers.

You can configure both a BA classifier and an MF classifier on an interface. If you do this, the BA classification is performed first and then the MF classification. If the two classification results conflict, the MF classification result overrides the BA classification result.

Based on this information, we can infer the following statements:

? The packet will be discarded. This is not correct because the packet will not be discarded by the classifiers unless it matches a filter rule that specifies discard as an action. The classifiers only assign packets to a forwarding class and a loss priority based on their match criteria.

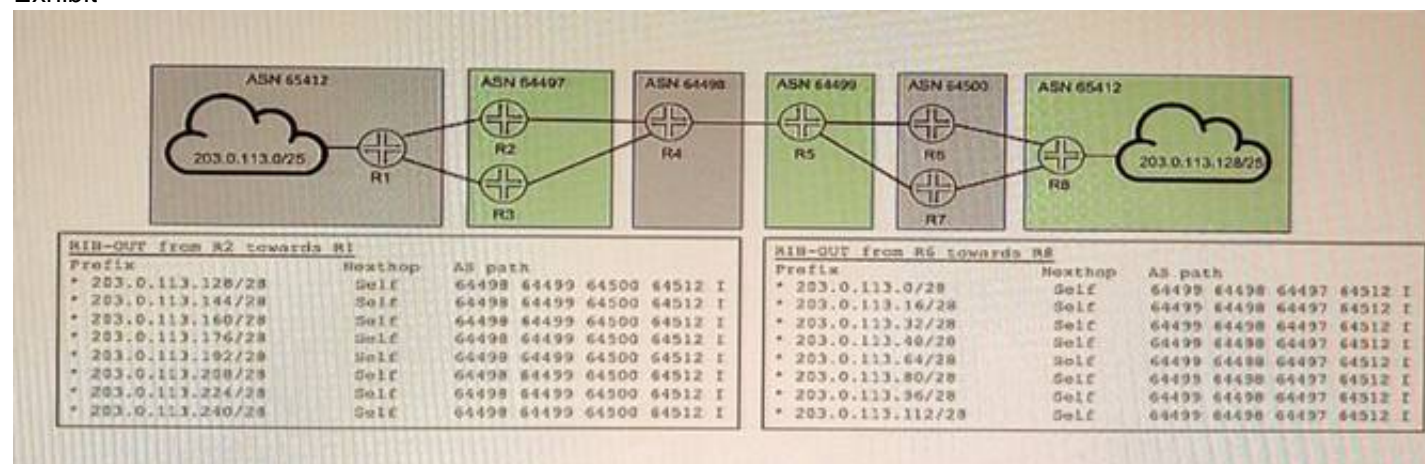
? The packet will be processed by the BA classifier first, then the MF classifier. This is correct because if both a BA classifier and an MF classifier are configured on an interface, the BA classification is performed first and then the MF classification. If they conflict, the MF classification result overrides the BA classification result.

? The packet will be forwarded with no classification changes. This is not correct because the packet will be classified by both the BA classifier and the MF classifier if they are configured on an interface. The final classification result will determine which output queue and which discard policy will be applied to the packet.

? The packet will be processed by the MF classifier first, then the BA classifier. This is not correct because if both a BA classifier and an MF classifier are configured on an interface, the BA classification is performed first and then the MF classification. If they conflict, the MF classification result overrides the BA classification result.

### NEW QUESTION 9

Exhibit



R1 and R8 are not receiving each other's routes

Referring to the exhibit, what are three configuration commands that would solve this problem? (Choose three.)

- A. Configure loops and advertise-peer-as on routers in AS 64497 and AS 64450.
- B. Configure loops on routers in AS 65412 and advertise-peer-as on routers in AS 64498.
- C. Configure as-override on advertisement from AS 64500 toward AS 64512.

- D. Configure remove-private on advertisements from AS 64497 toward AS 64498
- E. Configure remove-private on advertisements from AS 64500 toward AS 64499

**Answer:** BDE

**Explanation:**

The problem in this scenario is that R1 and R8 are not receiving each other's routes because of private AS numbers in the AS path. Private AS numbers are not globally unique and are not advertised to external BGP peers. To solve this problem, you need to do the following:

? Configure loops on routers in AS 65412 and advertise-peer-as on routers in AS 64498. This allows R5 and R6 to advertise their own AS number (65412) instead of their peer's AS number (64498) when sending updates to R7 and R8. This prevents a loop detection issue that would cause R7 and R8 to reject the routes from R5 and R62.

? Configure remove-private on advertisements from AS 64497 toward AS 64498 and from AS 64500 toward AS 64499. This removes any private AS numbers from the AS path before sending updates to external BGP peers. This allows R2 and R3 to receive the routes from R1 and R4, respectively3.

**NEW QUESTION 10**

What is the correct order of packet flow through configurable components in the Junos OS CoS features?

- A. Multifield Classifier -> Behavior Aggregate Classifier -> Input Policer -> Forwarding Policy Options -> Fabric Scheduler -> Output Policer -> Rewrite Marker -> Scheduler/Shaper/RED
- B. Behavior Aggregate Classifier -> Multifield Classifier -> Input Policer -> Forwarding Policy Options -> Fabric Scheduler -> Output Policer -> Scheduler/Shaper/RED -> Rewrite Marker
- C. Behavior Aggregate Classifier -> Input Policer -> Multifield Classifier -> Forwarding Policy Options -> Fabric Scheduler -> Output Policer -> Scheduler/Shaper/RED -> Rewrite Marker
- D. Behavior Aggregate Classifier -> Multifield Classifier -> Input Policer -> Forwarding Policy Options -> Fabric Scheduler -> Scheduler/Shaper/RED -> Output Policer -> Rewrite Marker

**Answer:** C

**Explanation:**

The correct order of packet flow through configurable components in the Junos OS CoS features is as follows:

? Behavior Aggregate Classifier: This component uses a single field in a packet header to classify traffic into different forwarding classes and loss priorities based on predefined or user-defined values.

? Input Policer: This component applies rate-limiting and marking actions to incoming traffic based on the forwarding class and loss priority assigned by the classifier.

? Multifield Classifier: This component uses multiple fields in a packet header to classify traffic into different forwarding classes and loss priorities based on user-defined values and filters.

? Forwarding Policy Options: This component applies actions such as load balancing, filtering, or routing to traffic based on the forwarding class and loss priority assigned by the classifier.

? Fabric Scheduler: This component schedules traffic across the switch fabric based on the forwarding class and loss priority assigned by the classifier.

? Output Policer: This component applies rate-limiting and marking actions to outgoing traffic based on the forwarding class and loss priority assigned by the classifier.

? Scheduler/Shaper/RED: This component schedules, shapes, and drops traffic at the egress interface based on the forwarding class and loss priority assigned by the classifier.

? Rewrite Marker: This component rewrites the code-point bits of packets leaving an interface based on the forwarding class and loss priority assigned by the classifier.

**NEW QUESTION 10**

Exhibit



```

user@PE1# show routing-instances
VPN-A {
  instance-type vrf;
  interface ge-0/0/1.0;
  vrf-target target:64512:1234;
  protocols {
    bgp {
      group CE {
        type external;
        family inet {
          unicast;
        }
        neighbor 10.0.0.1 {
          peer-as 64512;
          as-override;
        }
      }
    }
  }
}

```

Which two statements about the configuration shown in the exhibit are correct? (Choose two.)

- A. This VPN connects customer sites that use different AS numbers.
- B. This VPN connects customer sites that use the same AS number
- C. A Layer 2 VPN is configured.
- D. A Layer 3 VPN is configured.

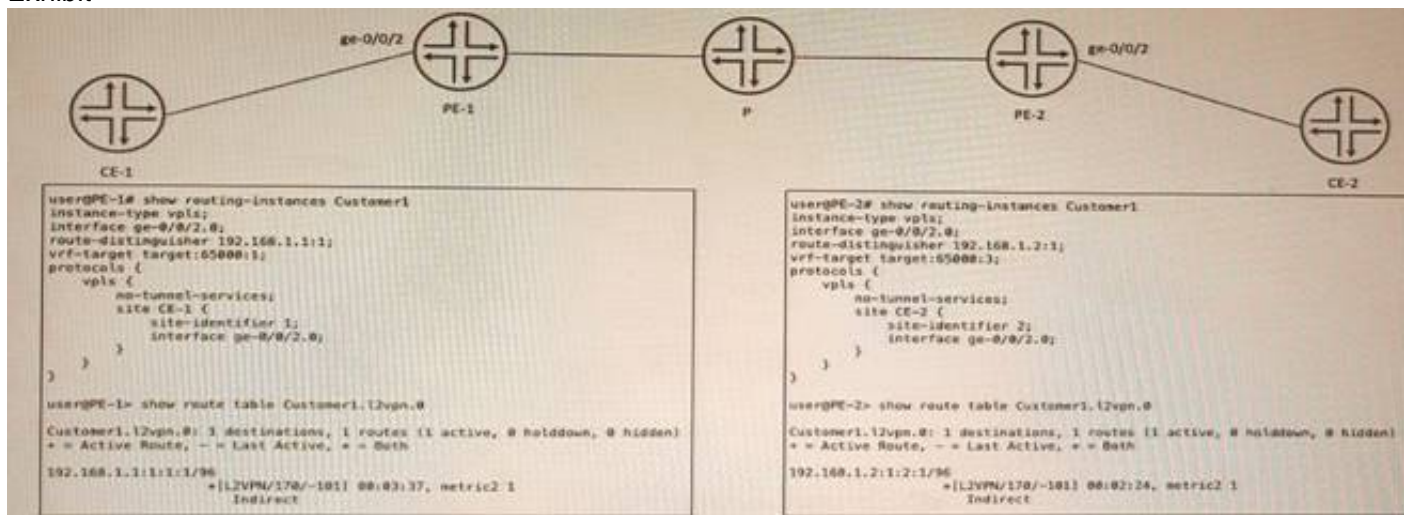
**Answer:** AD

**Explanation:**

The configuration shown in the exhibit is for a Layer 3 VPN that connects customer sites that use different AS numbers. A Layer 3 VPN is a type of VPN that uses MPLS labels to forward packets across a provider network and BGP to exchange routing information between PE routers and CE routers. A Layer 3 VPN allows customers to use different routing protocols and AS numbers at their sites, as long as they can peer with BGP at the PE-CE interface. In this example, CE-1 is using AS 65530 and CE-2 is using AS 65531, but they can still communicate through the VPN because they have BGP sessions with PE-1 and PE-2, respectively.

**NEW QUESTION 15**

Exhibit



CE-1 and CE-2 are part of a VPLS called Customer1. No connectivity exists between CE-1 and CE-2. In the process of troubleshooting, you notice PE-1 is not learning any routes for this VPLS from PE-2, and PE-2 is not learning any routes for this VPLS from PE-1.

- A. The route target must match on PE-1 and PE-2.
- B. The route distinguisher must match on PE-1 and PE-2.
- C. The instance type should be changed to l2vpn.
- D. The no-tunnel-services statement should be deleted on both PEs.



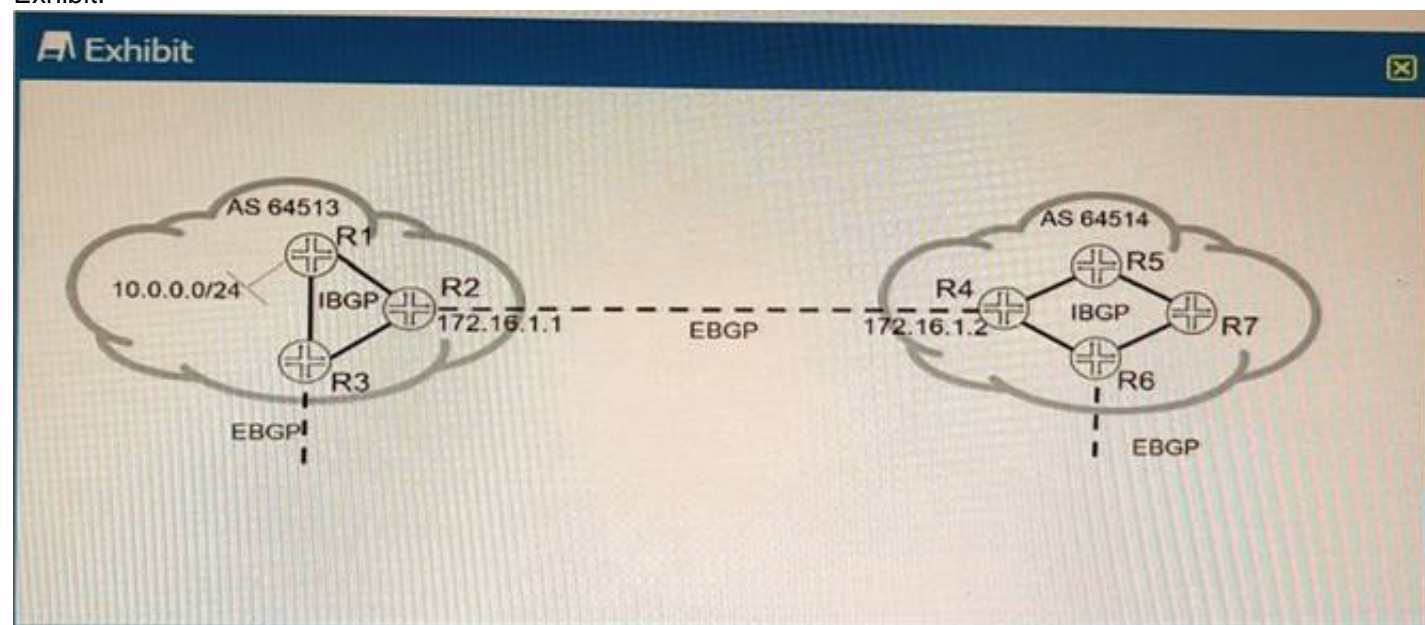
Answer: A

**Explanation:**

VPLS is a technology that provides Layer 2 VPN services over an MPLS network. VPLS uses BGP as its control protocol to exchange VPN membership information between PE routers. The route target is a BGP extended community attribute that identifies which VPN a route belongs to. The route target must match on PE routers that participate in the same VPLS instance, otherwise they will not accept or advertise routes for that VPLS.

**NEW QUESTION 20**

Exhibit.



Referring to the exhibit; the 10.0.0.0/24 EBGP route is received on R5; however, the route is being hidden. What are two solutions that will solve this problem? (Choose two.)

- A. On R4, create a policy to change the BGP next hop to itself and apply it to IBGP as an export policy
- B. Add the external interface prefix to the IGP routing tables
- C. Add the internal interface prefix to the BGP routing tables.
- D. On R4, create a policy to change the BGP next hop to 172.16.1.1 and apply it to IBGP as an export policy

Answer: AB

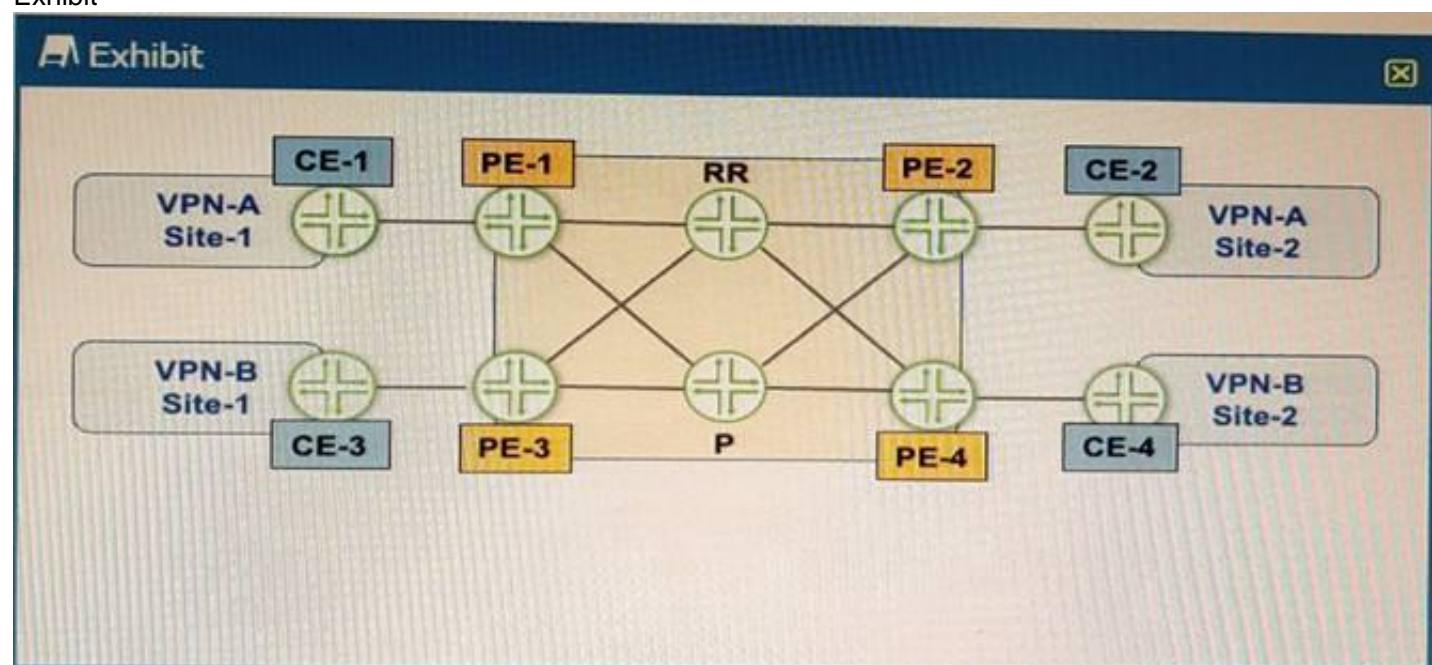
**Explanation:**

the default behavior for iBGP is to propagate EBGP-learned prefixes without changing the next-hop. This can cause issues if the next-hop is not reachable via the IGP. One solution is to use the next-hop self command on R4, which will change the next-hop attribute to its own loopback address. This way, R5 can reach the next-hop via the IGP and install the route in its routing table.

Another solution is to add the external interface prefix (120.0.4.16/30) to the IGP routing tables of R4 and R5. This will also make the next-hop reachable via the IGP and allow R5 to use the route. According to 2, this is a possible workaround for a pure IP network, but it may not work well for an MPLS network.

**NEW QUESTION 25**

Exhibit



Referring to the exhibit, PE-1 and PE-2 are getting route updates for VPN-B when neither of them service that VPN. Which two actions would optimize this process? (Choose two.)

- A. Configure the family route-target statement on the PEs.
- B. Configure the family route-target statement on the RR
- C. Configure the resolution rib bgp . 13vpn . 0 resolution-ribs ine
- D. 0 Statement on the PEs.
- E. Configure the resolution rib bgp.13vpn.0 resolution-ribs ine
- F. 0 Statement on the RR

Answer: BD

**Explanation:**

BGP route target filtering is a technique that reduces the number of routers that receive VPN routes and route updates, helping to limit the amount of overhead associated with running a VPN. BGP route target filtering is based on the exchange of the route-target address family, which contains information about the VPN



membership of each PE device. Based on this information, a PE device can decide whether to accept or reject VPN routes from another PE device. BGP route target filtering can be configured on PE devices or on route reflectors (RRs). Configuring BGP route target filtering on RRs is more efficient and scalable, as it reduces the number of BGP sessions and updates between PE devices. To configure BGP route target filtering on RRs, the following steps are required:

- ? Configure the family route-target statement under the BGP group or neighbor configuration on the RRs. This enables the exchange of the route-target address family between the RRs and their clients (PE devices).
- ? Configure the resolution rib bgp.l3vpn.0 resolution-ribs inet.0 statement under the routing-options configuration on the RRs. This enables the RRs to resolve next hops for VPN routes using the inet.0 routing table.
- ? Configure an export policy for BGP route target filtering under the routing-options configuration on the RRs. This policy controls which route targets are advertised to each PE device based on their VPN membership.

### NEW QUESTION 29

Which two statements are correct about the customer interface in an LDP-signaled pseudowire? (Choose two)

- A. When the encapsulation is vlan-ccc or extended-vlan-ccc, the configured VLAN tag is not included in the control plane LDP advertisement
- B. When the encapsulation is ethernet-ccc, only frames without a VLAN tag are accepted in the data plane
- C. When the encapsulation is vLan-ccc or extended-vlan-ccc, the configured VLAN tag is included in the control plane LDP advertisement
- D. When the encapsulation is ethemet-ccc, tagged and untagged frames are both accepted in the data plane.

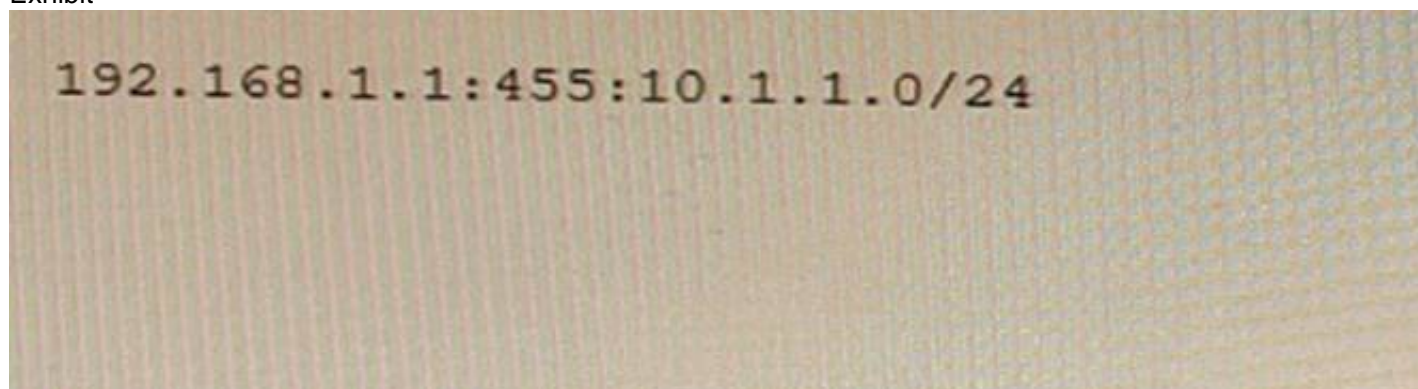
**Answer:** CD

### Explanation:

The customer interface in an LDP-signaled pseudowire is the interface on the PE router that connects to the CE device. An LDP-signaled pseudowire is a type of Layer 2 circuit that uses LDP to establish a point-to-point connection between two PE routers over an MPLS network. The customer interface can have different encapsulation types depending on the type of traffic that is carried over the pseudowire. The encapsulation types are ethernet-ccc, vlan-ccc, extended-vlan-ccc, atm-ccc, frame-relay-ccc, ppp-ccc, cisco-hdlc-ccc, and tcc-ccc. Depending on the encapsulation type, the customer interface can accept or reject tagged or untagged frames in the data plane, and include or exclude VLAN tags in the control plane LDP advertisement. The following table summarizes the behavior of different encapsulation types:

### NEW QUESTION 33

Exhibit



You are examining an L3VPN route that includes the information shown in the exhibit Which statement is correct in this scenario?

- A. The information shows a Type 1 route distinguisher.
- B. The information shows a Type 0 route distinguisher
- C. The information shows a Type 2 route distinguisher.
- D. The information shows a route target

**Answer:** B

### Explanation:

The information shows a Type 0 route distinguisher, which is one of the three types of route distinguishers defined by RFC 4364. A route distinguisher is a 64-bit value that is prepended to an IPv4 address to create a VPN-IPv4 address, which is unique within a VPN routing and forwarding (VRF) table. A Type 0 route distinguisher has two fields: an administrator subfield (2 bytes) and an assigned number subfield (6 bytes). The administrator subfield can be an AS number or an IP address, and the assigned number subfield can be any value assigned by the administrator. In this example, the administrator subfield is 65530 (an AS number) and the assigned number subfield is 1.

### NEW QUESTION 35

Which two statements are correct about IS-IS interfaces? (Choose two.)

- A. If a broadcast interface is in both L1 and L2, one combined hello message is sent for both levels.
- B. If a point-to-point interface is in both L1 and L2, separate hello messages are sent for each level.
- C. If a point-to-point interface is in both L1 and L2, one combined hello message is sent for both levels.
- D. If a broadcast interface is in both L1 and L2, separate hello messages are sent for each level

**Answer:** BD

### Explanation:

IS-IS supports two levels of routing: Level 1 (intra-area) and Level 2 (interarea). An IS-IS router can be either Level 1 only, Level 2 only, or both Level 1 and Level 2. A router that is both Level 1 and Level 2 is called a Level 1-2 router. A Level 1-2 router sends separate hello messages for each level on both point-to-point and broadcast interfaces<sup>1</sup>. A point-to-point interface provides a connection between a single source and a single destination. A broadcast interface behaves as if the router is connected to a LAN.

### NEW QUESTION 37

Exhibit

```

user@router> show l2vpn connections
Layer-2 VPN connections:
Legend for connection status (St)
EI -- encapsulation invalid          NC -- interface encapsulation not
CCC/TCC/VPLS                        WE -- interface and instance encaps not same
EM -- encapsulation mismatch        NP -- interface hardware not present
VC-Dn -- Virtual circuit down       -> -- only outbound connection is up
CM -- control-word mismatch         <- -- only inbound connection is up
CN -- circuit not provisioned        Up -- operational
OR -- out of range                  Dn -- down
OL -- no outgoing label             CF -- call admission control failure
LD -- local site signaled down       SC -- local and remote site ID collision
RD -- remote site signaled down      LM -- local site ID not minimum designated
LN -- local site not designated      RM -- remote site ID not minimum designated
RN -- remote site not designated     IL -- no incoming label
XX -- unknown connection status      MI -- Mesh-Group ID not available
MM -- MTU mismatch                  ST -- Standby connection
BK -- Backup connection             PB -- Profile busy
PF -- Profile parse failure          SN -- Static Neighbor
RS -- remote site standby            RB -- Remote site not best-site
LB -- Local site not best-site       HS -- Hot-standby Connection
VM -- VLAN ID mismatch
Legend for interface status
Up -- operational
Dn -- down
Instance: vpn-A
Edge protection: Not-Primary
Local site: CE1-2 (2)
connection-site Type St      Time last up          # Up trans
1               rmt  Up      Apr 11 14:35:27 2020          1
Remote PE: 172.17.20.1, Negotiated control-word: Yes (Null)
Incoming label: 21, Outgoing label: 22
Local interface: ge-0/0/6.610, Status: Up, Encapsulation: VLAN
Flow Label Transmit: No, Flow Label Receive: No

```

Which two statements about the output shown in the exhibit are correct? (Choose two.)

- A. The PE is attached to a single local site.
- B. The connection has not flapped since it was initiated.
- C. There has been a VLAN ID mismatch.
- D. The PE router has the capability to pop flow labels

**Answer:** AD

#### Explanation:

According to 1 and 2, BGP Layer 2 VPNs use BGP to distribute endpoint provisioning information and set up pseudowires between PE devices. BGP uses the Layer 2 VPN (L2VPN) Routing Information Base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 virtual forwarding instance (VFI) is configured. The prefix and path information is stored in the L2VPN database, which allows BGP to make decisions about the best path. In the output shown in the exhibit, we can see some information about the L2VPN RIB and the pseudowire state. Based on this information, we can infer the following statements:

- ? The PE is attached to a single local site. This is correct because the output shows only one local site ID (1) under the L2VPN RIB section. A local site ID is a unique identifier for a site within a VPLS domain. If there were multiple local sites attached to the PE, we would see multiple local site IDs with different prefixes.
- ? The connection has not flapped since it was initiated. This is correct because the output shows that the uptime of the pseudowire is equal to its total uptime (1w6d). This means that the pseudowire has been up for one week and six days without any interruption or flap.
- ? There has been a VLAN ID mismatch. This is not correct because the output shows that the remote and local VLAN IDs are both 0 under the pseudowire state section. A VLAN ID mismatch occurs when the remote and local VLAN IDs are different, which can cause traffic loss or misdelivery. If there was a VLAN ID mismatch, we would see different values for the remote and local VLAN IDs.
- ? The PE router has the capability to pop flow labels. This is correct because the output shows that the flow label pop bit is set under the pseudowire state section. The flow label pop bit indicates that the PE router can pop (remove) the MPLS flow label from the packet before forwarding it to the CE device. The flow label is an optional MPLS label that can be used for load balancing or traffic engineering purposes.

#### NEW QUESTION 39

Exhibit

```

user@router> show route advertising-protocol bgp 10.0.0.43 extensive 10.0.0.188
inet.0: 23 destinations, 41 routes (23 active, 0 holddown, 0 hidden)
+ 10.0.0.188/32 (2 entries, 1 announced)
  BGP group underlay type External
    AS path: [65189] 65170 65188 I

```

Referring to the exhibit, what do the brackets [ ] in the AS path identify?

- A. They identify the local AS number associated with the AS path if configured on the router, or if AS path prepending is configured
- B. They identify an AS set, which are groups of AS numbers in which the order does not matter
- C. They identify that the autonomous system number is incomplete and awaiting more information from the BGP protocol.
- D. They identify that a BGP confederation is being used to ensure that there are no routing loops.

**Answer:** B

#### Explanation:

The brackets [ ] in the AS path identify an AS set, which are groups of AS numbers in which the order does not matter. An AS set is used when BGP aggregates



routes from different ASs into a single prefix. For example, if BGP aggregates routes 10.0.0.0/16 and 10.1.0.0/16 from AS 100 and AS 200, respectively, into a single prefix 10.0.0.0/15, then the AS path for this prefix will be [100 200]. An AS set reduces the length of the AS path and prevents routing loops.

#### NEW QUESTION 43

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual JN0-664 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the JN0-664 Product From:

<https://www.2passeasy.com/dumps/JN0-664/>

## Money Back Guarantee

### JN0-664 Practice Exam Features:

- \* JN0-664 Questions and Answers Updated Frequently
- \* JN0-664 Practice Questions Verified by Expert Senior Certified Staff
- \* JN0-664 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* JN0-664 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year