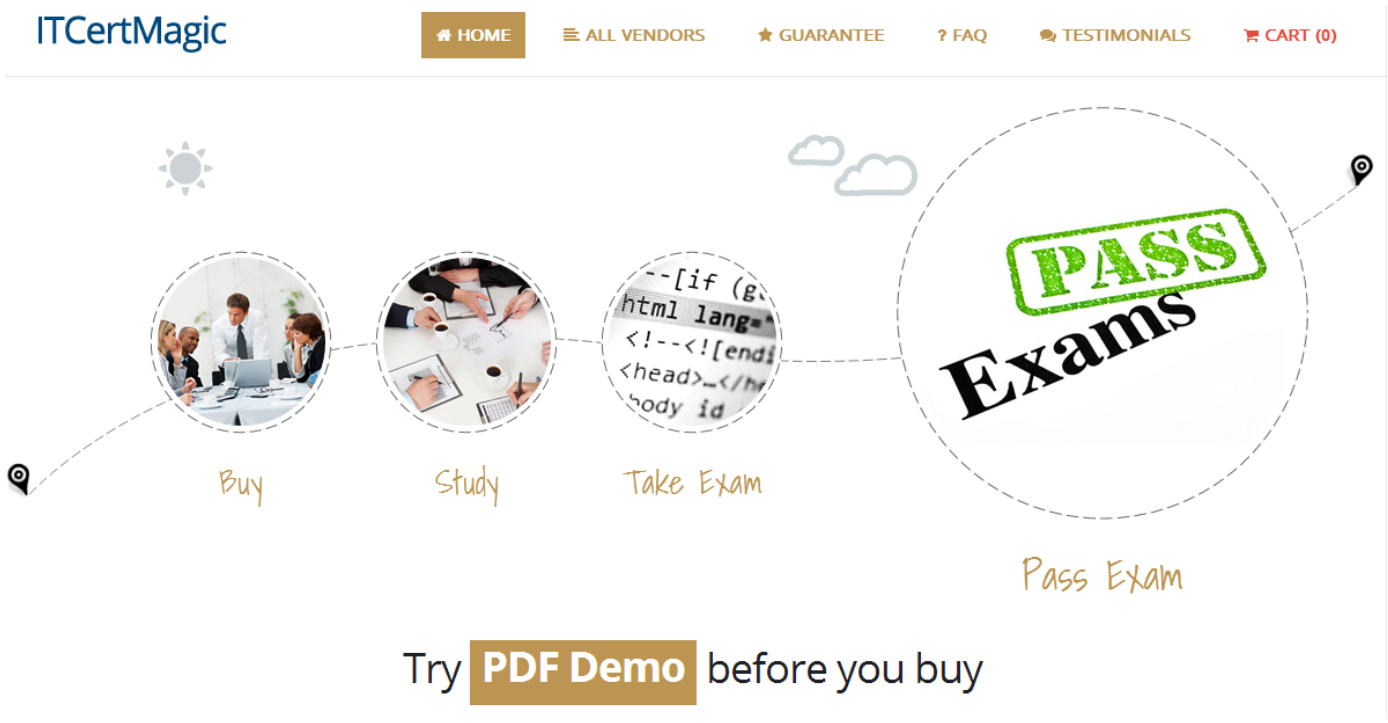
ITCertMagic



http://www.itcertmagic.com/

Pass-Guaranteed Certification Exam Questions | Exam Dumps - ITCertMagic

Exam : **300-410J**

Title : Implementing Cisco Enterprise Advanced Routing and Services (300-410日本語版)

Vendor : Cisco

Version : DEMO

QUESTION NO: 1
IPv6 RA ガードに関する正しい記述はどれですか?
A. IPv6 トラフィックがトンネリングされる環境では保護されません。
B. スイッチ ポート インターフェイスではイングレス方向に設定できません。
C. IPv6 RA ガードによってドロップされたパケットはスパニングできません。
D. TCAM がプログラムされている場合、ハードウェアではサポートされません。
Answer: A
Explanation:
Restrictions for IPv6 RA Guard
+ The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
+ This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
+ This feature can be configured on a switch port interface in the ingress direction.
+ This feature supports host mode and router mode.
+ This feature is supported only in the ingress direction; it is not supported in the egress direction.
+ This feature is not supported on EtherChannel and EtherChannel port members.
+ This feature is not supported on trunk ports with merge mode.
+ This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
+ Packets dropped by the IPv6 RA Guard feature can be spanned.
+ If the platform ipv6 acl icmp optimize neighbor-discovery command is configured, the IPv6 RA
Guard feature cannot be configured and an error message will be displayed. This command adds
default global Internet Control Message Protocol (ICMP) entries that will override the RA guard
ICMP entries.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-
xe-3s-book/ip6-ra-guard.html

QUESTION NO: 2
エリア2を使用するOSPFネットワークに新しいサイトが追加されました。エリア2はこのOSPFネットワークのエリア1にのみ接続されています。エリア1は、エリア1をバックボーンエリア0に接続するために使用されます。このシナリオでは、エリア0からエリア2にあるネットワークへの完全な接続が期待できますか？
A. はい、デフォルトでは完全な接続が確保されます。
B. いいえ、エリア 2 のルートをエリア 0 に再分配する必要があります。
C. いいえ、エリア 2 とエリア 0 を論理的に接続するには仮想リンクが必要です。
D. はい、ただしエリア2はスタブエリアとして構成する必要があります。
Answer: C

QUESTION NO: 3
MPLS転送を行うために、どのタイプのルーターでどの2つの機能が必要ですか？(2つ選択してください。)
A. PEルーターとコアルーター上のMPLS
B. PEルーターとコアルーターでのLDP
C. CEルーターとコアルーター上のMPLS
D. PEルーターとCEルーター上のLDP
E. PEルーターとCEルーター上のCEF
Answer: AB

QUESTION NO: 4
図を参照してください。SW101は起動設定をTFTPサーバーに転送できませんでした。スイッチにはACLが設定されておらず、ホストへのpingは正常に実行できます。どの操作でこの問題を解決できますか？

```
SW101#cop nvram:startup-config tftp:
Address or name of remote host []? 10.1.0.1
Destination filename [sw101-confg]?
%Error opening tftp://10.1.0.1/sw101-confg (Permission denied)
SW101#

SW101#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/15 ms
SW101#
```

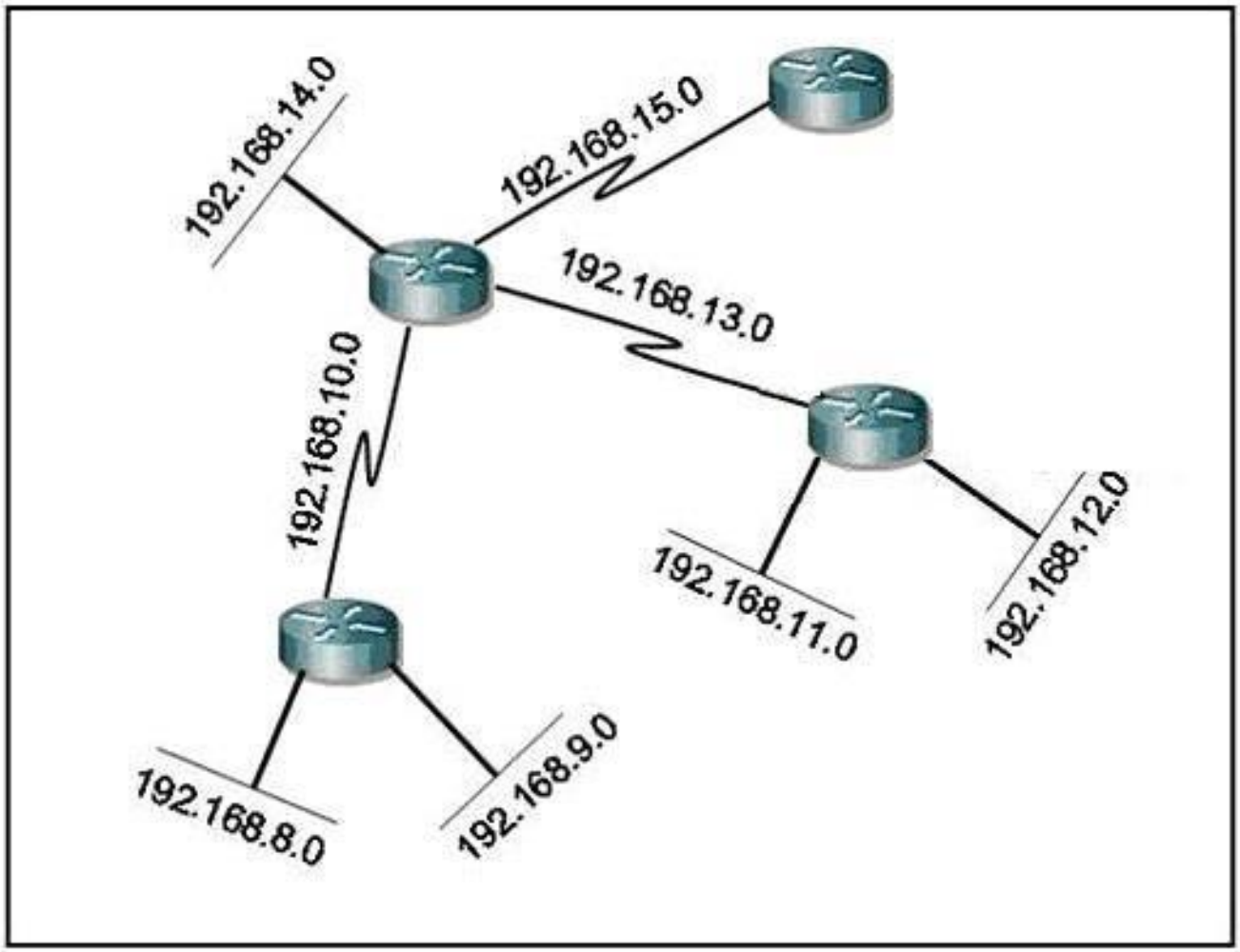
A. TFTPサーバーでUDPポート69を開きます。
B. TFTPサーバーでUDPポート179を開きます。
C. TFTP の双方向通信を可能にするために、中間に FW を設定します。
D. ホスト上で TFTP サーバーを起動します。
Answer: D

QUESTION NO: 5
OSPFシャムリンクの目的は何ですか？
A. MPLS VPNネットワークでPE-CE接続プロトコルとしてOSPFを使用する場合に、エリア間ルーティングを許可する。
B. MPLS VPNネットワークでPE-CE接続プロトコルとしてOSPFを使用する場合に、エリア内ルーティングを許可する。
C. MPLS VPNネットワークでOSPFをPE-CE接続プロトコルとして使用している場合のOSPFバックドアルーティングを修正する
D. MPLS VPNネットワークでOSPFをPE-PE接続プロトコルとして使用している場合に、OSPFバックドアルーティングを修正する
Answer: C

Explanation:
In an MPLS VPN network, OSPF is often used as the routing protocol between the Provider Edge
(PE) and Customer Edge (CE) routers. A problem arises when there is an OSPF backdoor link
between two CE routers in the same OSPF area. This link may be preferred over the MPLS VPN
path, as OSPF inherently prefers intra-area routes over inter-area routes.
A sham-link is configured to create a logical intra-area link between the PE routers, ensuring that
traffic uses the MPLS VPN backbone instead of the backdoor link. This allows the MPLS VPN
backbone to maintain OSPF intra-area routing and avoids the suboptimal routing caused by OSPF's preference for intra-area routes.

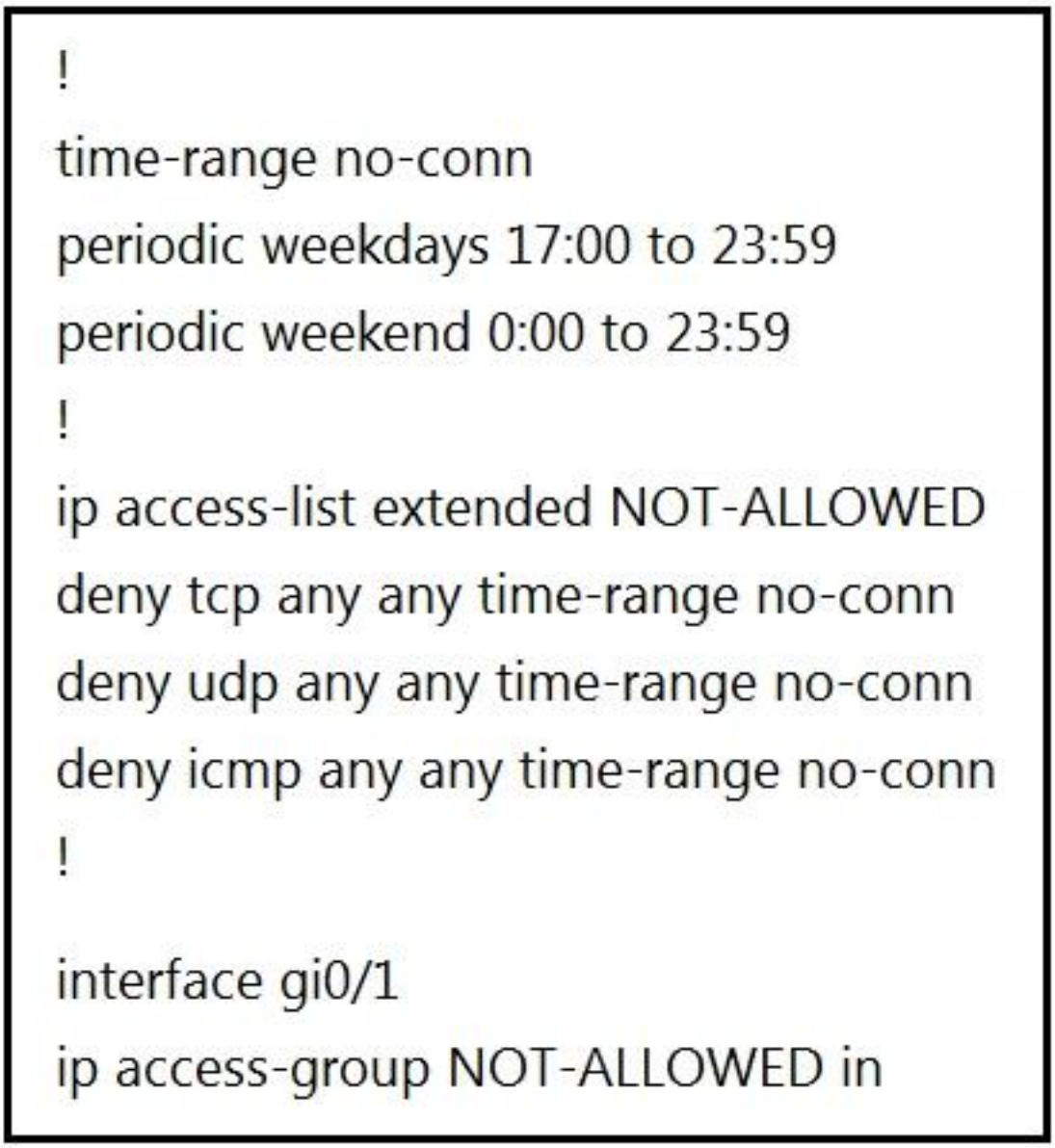
QUESTION NO: 6
DMVPNネットワークにおいて、論理IPアドレスを物理IPアドレスにマッピングするために使用されるプロトコルはどれですか？
A. BGP
B. LLDP
C. EIGRP
D. NHRP
Answer: D
Explanation:
Next Hop Resolution Protocol (NHRP), defined in RFC 2332, is a Layer 2 address resolution protocol and cache, like Address Resolution Protocol (ARP). NHRP is used by a branch router
connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of
the "NBMA next hop"; in this case, the headend router or the destination IP address of another
branch router.
NHRP is used to map tunnel IP addresses to "physical" or "real" IP addresses, used by endpoint
routers. It resolves private addresses (those behind mGRE and optionally IPSEC) to a public address. NHRP is layer 2 resolution protocol and cache, much like Address Resolution Protocol
(ARP) or Reverse ARP (Frame Relay).

QUESTION NO: 7
ネットワーク図が与えられた場合、表示されているネットワークのみを適切に要約するアドレスはどれでしょうか？



A. 192.168.0.0/24
B. 192.168.8.0/20
C. 192.168.8.0/21
D. 192.168.12.0/20
E. 192.168.16.0/21
F. これらのネットワークは要約できません。
Answer: C

QUESTION NO: 8
図を参照してください。ネットワーク管理者は、営業時間外と週末にインターネットへのすべてのトラフィックをブロックしたいと考えています。管理者がインターフェースGi0/1にアクセスリストを適用すると、すべてのトラフィックがブロックされ、インターネットへのアクセスが一切できなくなります。
どの行動で問題が解決しますか？



A. アクセスリストの deny udp any any time-range no-conn コマンドの後に permit ip any any time-range no-conn ステートメントを追加します。
B. アクセスリストの deny icmp any any time-range no-conn コマンドの後に permit ip any any ステートメントを追加します。
C. アクセスリストの deny icmp any any time-range no-conn コマンドの後に permit allowed time-range no-conn ステートメントを追加します。
D. アクセスリストの deny icmp any any time-range no-conn コマンドの後に permit ip any any time-range no-conn ステートメントを追加します。
Answer: B

QUESTION NO: 9
図を参照してください。エンジニアがポリシーベースルーティングを設定し、その設定を適切なインターフェースに適用しました。アクセスリストに一致するトラフィックには、どのように設定が適用されますか？

```
Route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access lists): FILTER_ACL
  Set clauses:
    ip next-hop verify-availability 209.165.202.129 1 track 100 [down]
    ip next-hop verify-availability 209.165.202.131 2 track 200 [up]
  Policy routing matches: 0 packets, 0 bytes
route-map PBR, deny, sequence 20
  Match clauses:
  Set clauses:
    ip next-hop 209.165.201.30
  Policy routing matches: 275364861 packets, 12200235037 bytes
```

A. 209.165.202.131 に送信されます。
B. 209.165.202.129 に送信されます。
C. 削除されます。
D. ルーティングテーブルのルックアップを使用して転送されます。
Answer: A
Explanation:
The first next hop IP is down, so the second one will be used.

QUESTION NO: 10
図を参照してください。192.168.12.1 から R2
へのアクセスを制限するアクションはどれですか？

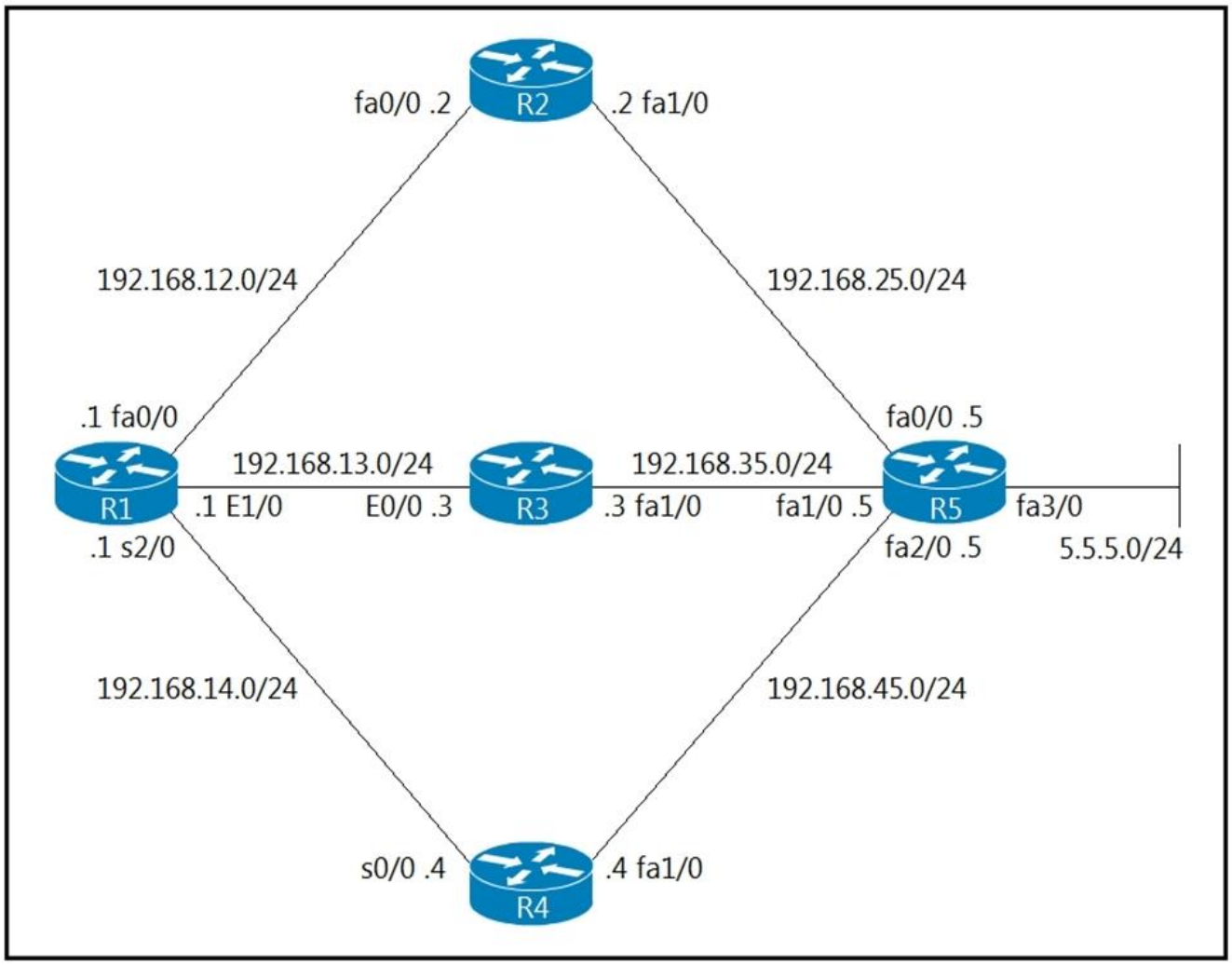
```
R2#show policy-map control-plane
 Control Plane
  Service-policy input: CoPP
    Class-map: SSH (match-all)
      29 packets, 2215 bytes
      5 minute offered rate 0000 bps
      Match: access-group 100

    Class-map: ANY (match-all)
      46 packets, 3878 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group 199
      drop

    Class-map: class-default (match-any)
      41 packets, 5687 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

R2#show access-list 100
Extended IP access list 100
    10 deny tcp any any eq 22 (14 matches)
    20 permit tcp host 192.168.12.1 any eq 22 (29 matches)
R2#show access-list 199
Extended IP access list 199
    10 permit ip any any (51 matches)
```

A. アクセスリスト100内のシーケンス10とシーケンス20を交換します。
B. シーケンス20を変更して、TCPホスト192.168.12.1 eq 22 anyをアクセスリスト100に許可します。
C. アクセスリスト100内のシーケンス20をシーケンス10と交換する
D. シーケンス 10 を変更して、アクセス リスト 100 に対して tcp any eq 22 any を拒否します。
Answer: C

QUESTION NO: 11
ネットワーク内のリンクが共通の光ファイバーで接続されている状況において、保護されたパスに属するLFAを排除する属性はどれですか？
A.インターフェースの失望
B. 共有リスクリンクグループ-非連結
C. ラインカードが互いに素
D. 最小修復パス指標
Answer: B
Explanation:
Shared Risk Link Group (SRLG)-disjoint-Eliminates LFAs that belong to any of the protected path SRLGs. SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may also fail. Therefore, links

in a group share risks.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-3s/asr1000/ire-
xe-3s-asr1000/ire-ipfrr.html

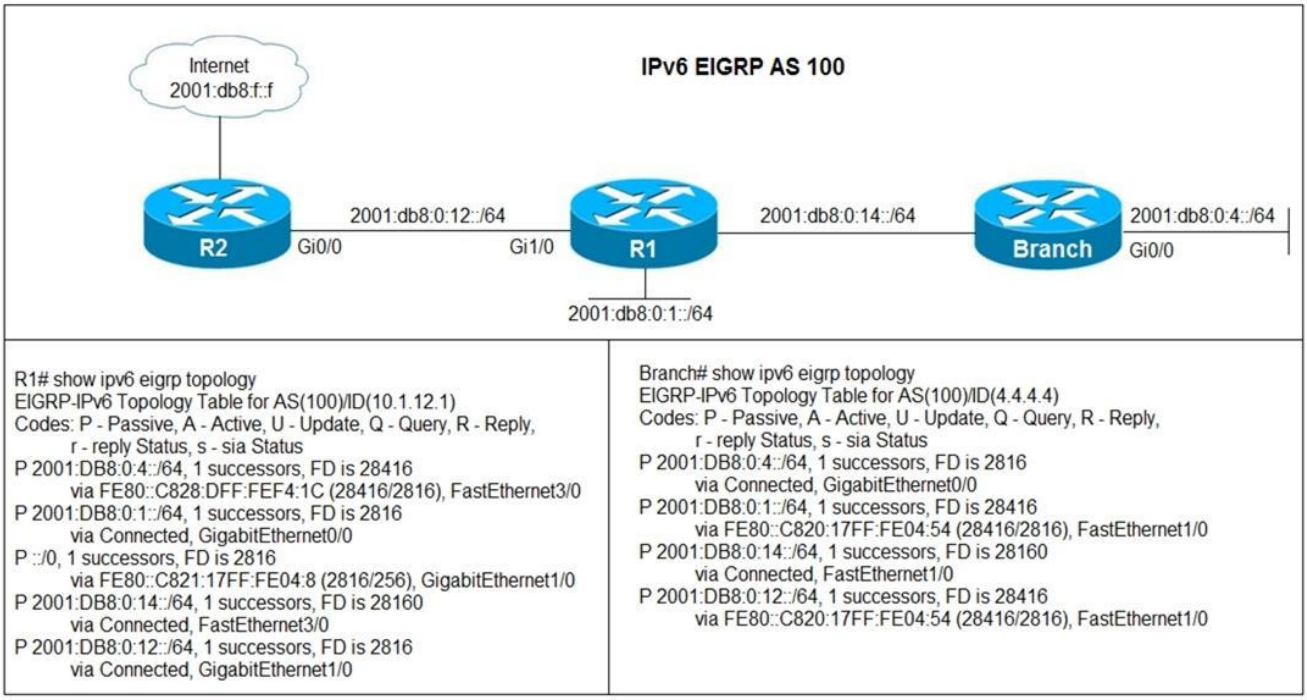
QUESTION NO: 12
添付資料を参照してください。エンジニアがR1のルーティング問題を調査したところ、5.5.5.0/24宛てのトラフィックがすべての経路を通っていないことがわかりました。
どの行動で問題が解決しますか？



A. EIGRP の分散値を増加させます。
B. EIGRP の分散値を減少させます。
C. EIGRPからR3の隣接関係を削除します。
D. EIGRPで192.168.13.0/24の広告を停止します。
Answer: A
Explanation:
EIGRP variante enables unequal cost path balance routing and add those prefixes to the EIGRP
routing table.

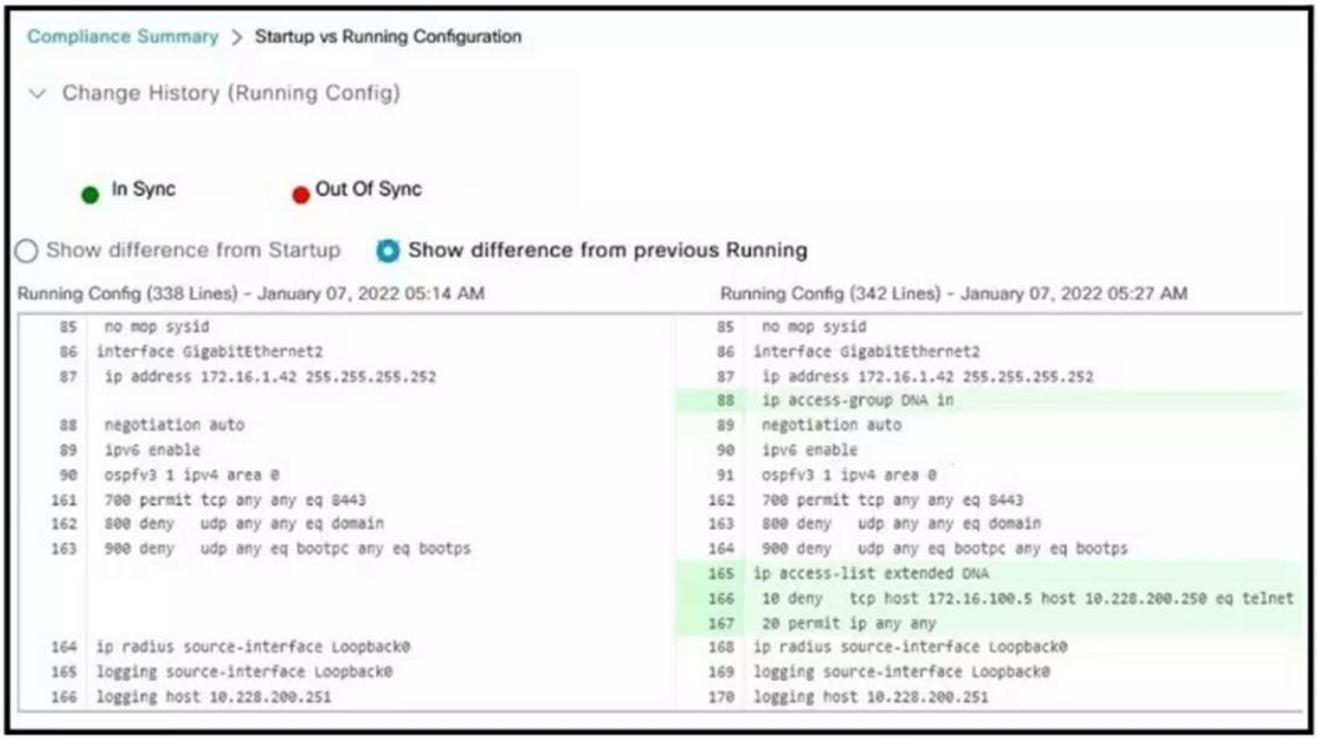
QUESTION NO: 13

図を参照してください。ブランチネットワーク2001:db8:0:4::/64のユーザーから、インターネットにアクセスできないという報告がありました。この問題を解決するために、IPv6ルータのEIGRP 100設定モードでどのコマンドを実行すればよいでしょうか？



A. R1でeigrp stubコマンドを発行します。
B. R1でno eigrp stubコマンドを実行します。
C. R2でeigrp stubコマンドを発行します。
D. R2でno eigrp stubコマンドを実行します。
Answer: B
Explanation:
In the output of R1, we see R1 has a default route to the Internet via G1/0, which is correct but R2
does not have this route. One reasonable answer of this issue is R1 has been configured as a
stub router so it only advertised connected and summary routes. In Branch router output, we also
see routes that are directly connected to R1 only.
Note: In this topology, only Branch router should be configured as stub, not R1 router.

QUESTION NO: 14
図を参照してください。エンジニアがデバイスの設定を更新した後、予期しない動作が発生しました。起動設定を完全に置き換えることで問題を解決するコマンドはどれですか？



A. configure replace nvram:startup-config
B. system:running.config nvram:startup-config をコピーします。
C. configure replace nvram:private-config
D. 実行中の設定をスタートアップ設定にコピーする
Answer: A
Explanation:
configure replace nvram:startup-config replaces the current running configuration with the saved
startup configuration, removing unintended changes and restoring the device to the exact startup-
config state. This is the correct command when a full replacement is required rather than merging
configuration lines.

QUESTION NO: 15
図を参照してください。ルーターR1とR2は、OSPFを介して互いのループバックへのルートを交換します。R2 Lo0からR1
Lo2へのTelnetトラフィックはブロックする必要があります。どの設定でこの問題が解決しますか？

R1

```
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 traffic-filter DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

A.

R1

```
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 access-class DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

B.

R1

```
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 access-class DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

C.

R1

```
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 traffic-filter DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

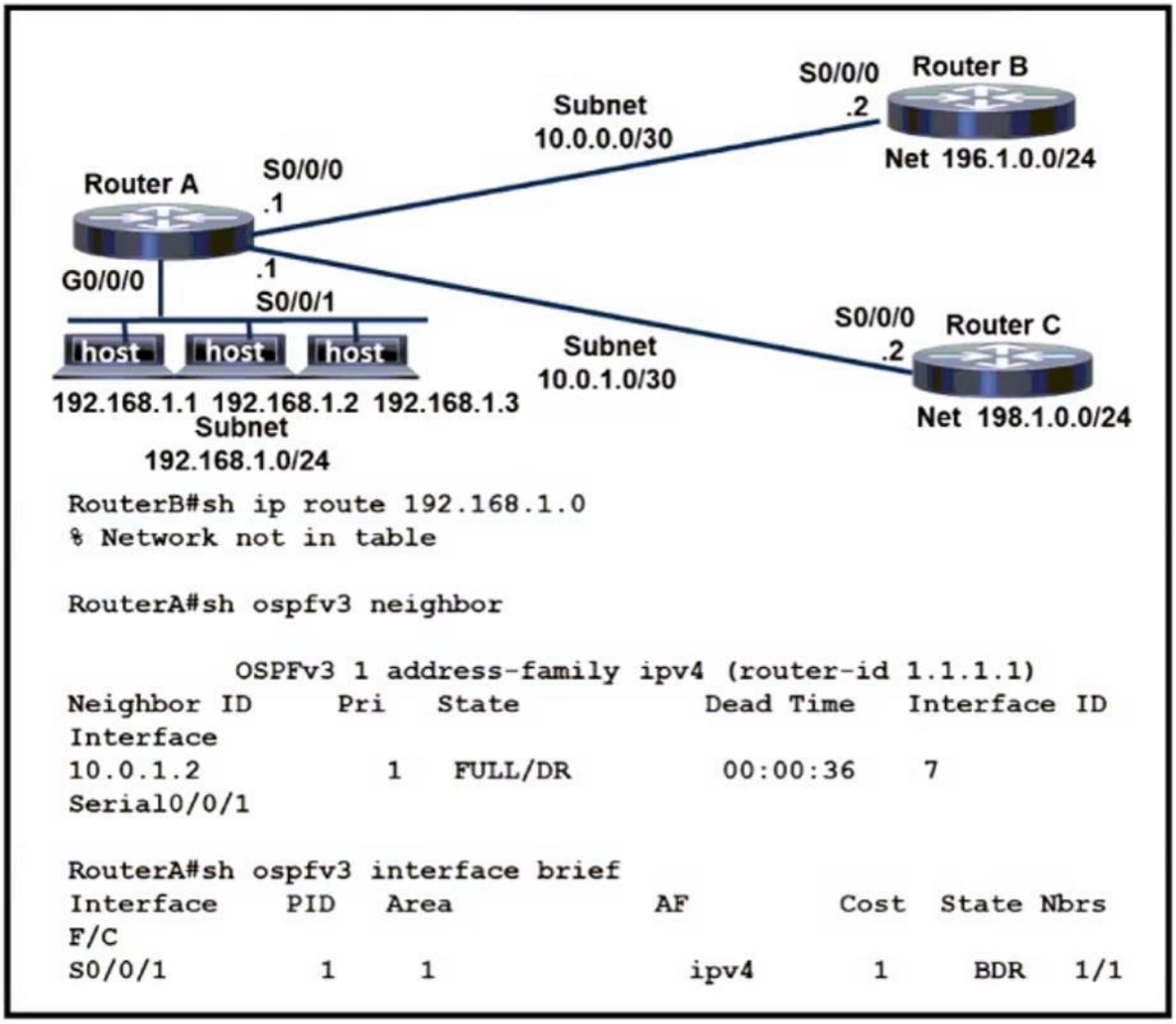
D.

```
R1
 Interface loopback1
  no ip address
  ipv6 address 100A:0:100C::1/64
  ipv6 enable
  ipv6 ospf 1 area 0
  !
 interface Loopback2
  no ip address
  ipv6 address 200A:0:200C::1/64
  ipv6 enable
  ipv6 ospf 1 area 0
 !
 interface GigabitEthernet0/0
  no ip address
  ipv6 address AB01:2011:8:100::/64 eui-64
  ipv6 enable
  ipv6 ospf network point-to-point
  ipv6 ospf 1 area 0
  !
 ipv6 access-list DENY_TELNET_Lo2
  sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
  permit ipv6 any any
```

Answer: C

QUESTION NO: 16

図を参照してください。エンジニアは、OSPF を介してルータ A の LAN ネットワーク 192.168.1.0 をルータ B にアドバタイズする必要があります。エンジニアは、ルータ B は設定されているものの、ルータ A の LAN ネットワークがルータ B のルーティングテーブルに存在しないことに気づきました。ルータ A
のどの設定でこの問題が解決しますか？


S0/0/0
Router B
.2
Subnet
10.0.0.0/30
Net 196.1.0.0/24
Router A
S0/0/0
.1
.1
G0/0/0
S0/0/1
host
host
host
192.168.1.1 192.168.1.2 192.168.1.3
Subnet
192.168.1.0/24
Subnet
10.0.1.0/30
S0/0/0
Router C
.2
Net 198.1.0.0/24
RouterB#sh ip route 192.168.1.0
% Network not in table
RouterA#sh ospfv3 neighbor
OSPFv3 1 address-family ipv4 (router-id 1.1.1.1)
Neighbor ID Pri State Dead Time Interface ID
Interface
10.0.1.2 1 FULL/DR 00:00:36 7
Serial0/0/1
RouterA#sh ospfv3 interface brief
Interface PID Area AF Cost State Nbrs
F/C
S0/0/1 1 1 ipv4 1 BDR 1/1

A.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

B.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

C.

```
interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 area 1 range 192.168.1.0 255.255.255.0
 router-id 1.1.1.1
 exit-address-family
```

D.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

Answer: B

QUESTION NO: 17
BFD を使用する利点は何ですか?
A. レイヤ 1 でローカルリンク障害を検出し、ルーティング テーブルを更新します。
B. レイヤ 2 でローカル リンク障害を検出し、ルーティング プロトコルを更新します。
C. レイヤ 1 およびレイヤ 3 の問題に対して 1 秒未満の障害検出を備えています。
D. レイヤ 1 およびレイヤ 2 の問題に対して 1 秒未満の障害検出を備えています。
Answer: D

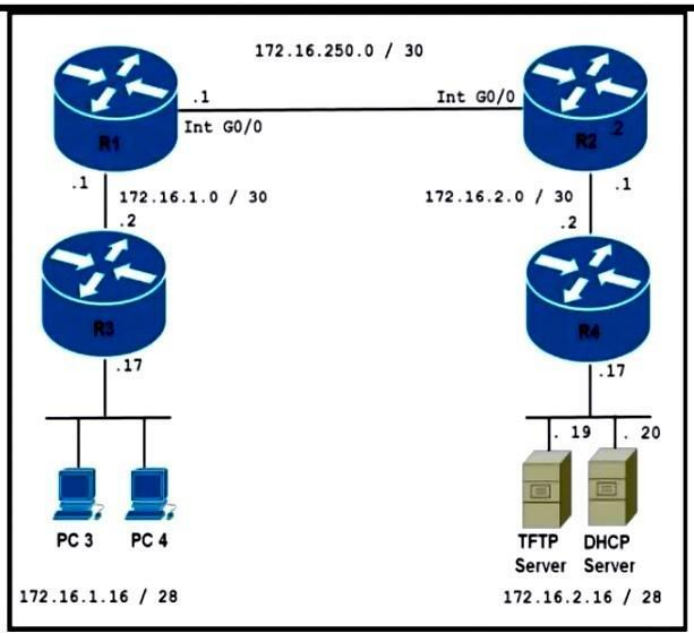
Explanation:
BFD provides rapid, sub-second failure detection independent of the underlying protocol and works across Layer 3, allowing routing protocols to quickly react to both Layer 1 and Layer 3 failures.

QUESTION NO: 18
パケットヘッダー内にACKが含まれているかどうかをチェックするアクセスリストのエントリはどれですか？
A. アクセスリスト 49 permit ip any any eq 21 tcp-ack
B. アクセスリスト 49 permit tcp any any eq 21 tcp-ack
C. アクセスリスト 149 permit tcp any any eq 21 established
D. アクセスリスト 49 permit tcp any any eq 21 established
Answer: C

QUESTION NO: 19
図を参照してください。エンジニアは新しいIOSファイルをルーターR3に転送しようとしていますが、エラーが発生しています。どの設定でファイル転送が成功しますか？

```
R3#sh ip int brie
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0         unassigned      YES NVRAM  administratively
down down
GigabitEthernet0/1         172.16.250.2    YES manual up
up
GigabitEthernet0/2         172.16.250.14   YES manual up
up
GigabitEthernet0/3         172.16.1.17     YES manual up
up
R3#

R3#sh run | begin router eigrp
router eigrp 100
 network 172.16.1.0 0.0.0.3
 network 172.16.1.16 0.0.0.15
!
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0/3
!
line con 0
line aux 0
line vty 0 4
 login
 transport input none
!
```

```
R4#sh run
!
hostname R4
!
ip cef
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.252
 ip access-group 120 in
!
interface GigabitEthernet0/1
 ip address 172.16.2.17 255.255.255.240
!
router eigrp 100
 network 172.16.2.0 0.0.0.3
 network 172.16.2.16 0.0.0.15
 !
access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq tftp
access-list 120 deny   udp any any eq tftp
access-list 120 permit tcp any any
```

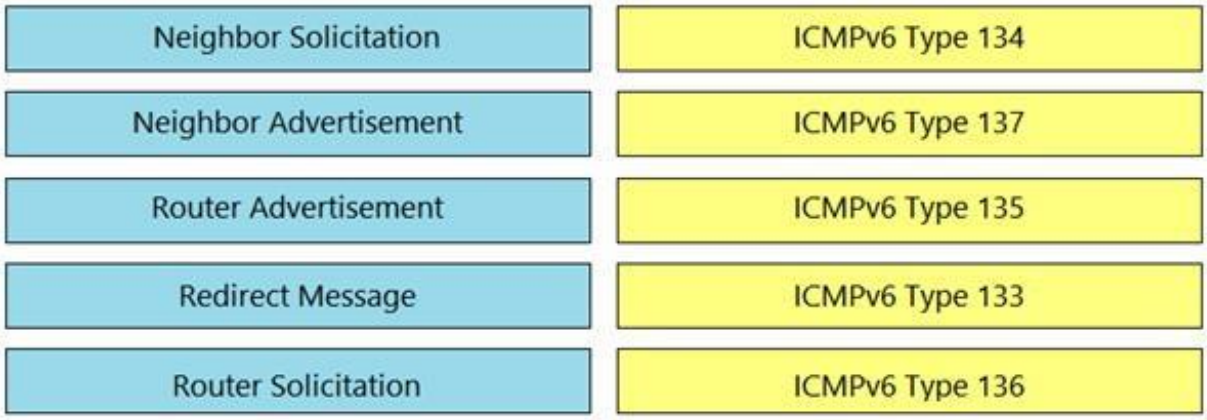


A. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69 R4(config)#no access-list 120 deny udp any any eq tftp R4(config)#access-list 120 permit tcp

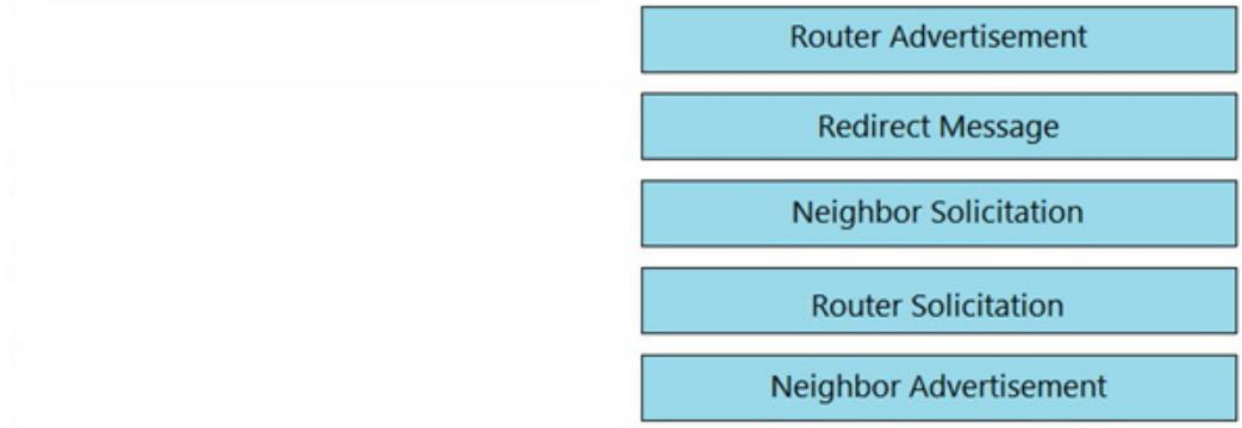
any any
B. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit udp host 172.16.1.17 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp any any
C. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R3(config)#no ip tftp source-interface GigabitEthernet0/3
D. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp host 172.16.1.17 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp any any
Answer: B
Explanation:
The issue arises because the current access list on R4 only permits TFTP traffic between 172.16.1.2 and 172.16.2.19 on UDP port 69. However, R3 is using its GigabitEthernet0/3 interface with IP 172.16.1.17 as the source for TFTP transfers.
To resolve this, update the ACL on R4 to permit TFTP traffic from 172.16.1.17 (R3's source IP) to
172.16.2.19 (TFTP server) on UDP port 69. Additionally, ensure that other TCP traffic is permitted
for the transfer process by maintaining access-list 120 permit tcp any any. This allows the file transfer from R3 to the TFTP server on R4.

QUESTION NO: 20
MPLS LDPルーターIDに関する以下の記述のうち、正しいものはどれですか？
A.
forceキーワードは、ルーターIDを特定のアドレスに変更し、何らかの影響を引き起こします。
B. 最も高いIPアドレスを持つループバックがルーターIDとして選択されます。
C.
設定されていない場合、ループバックが設定されていても、動作中の物理インターフェイスがルータ ID として選択されます。
D. MPLS LDPルーターIDがIGPルーターIDと一致する必要がある場合。
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4m-
book.pdf

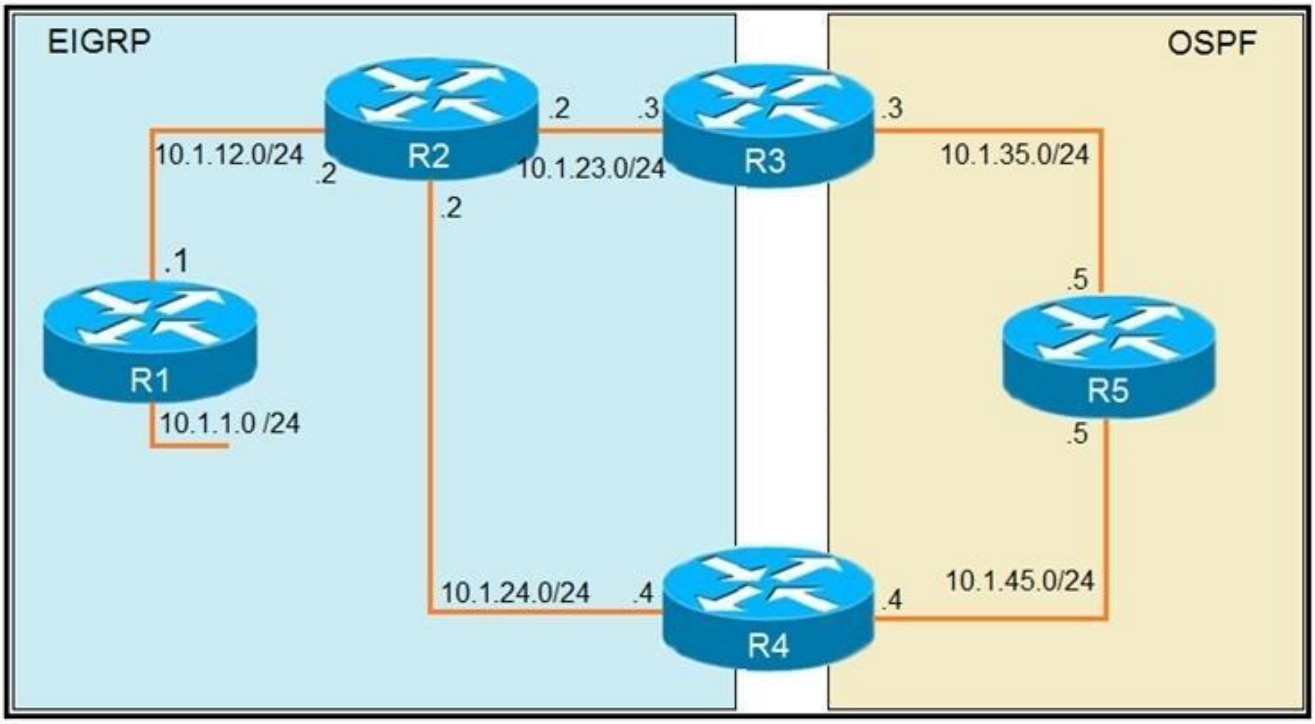
QUESTION NO: 21
ドラッグアンドドロップ問題
左側のICMPv6近隣探索メッセージを、右側の適切なパケットタイプにドラッグアンドドロップしてください。

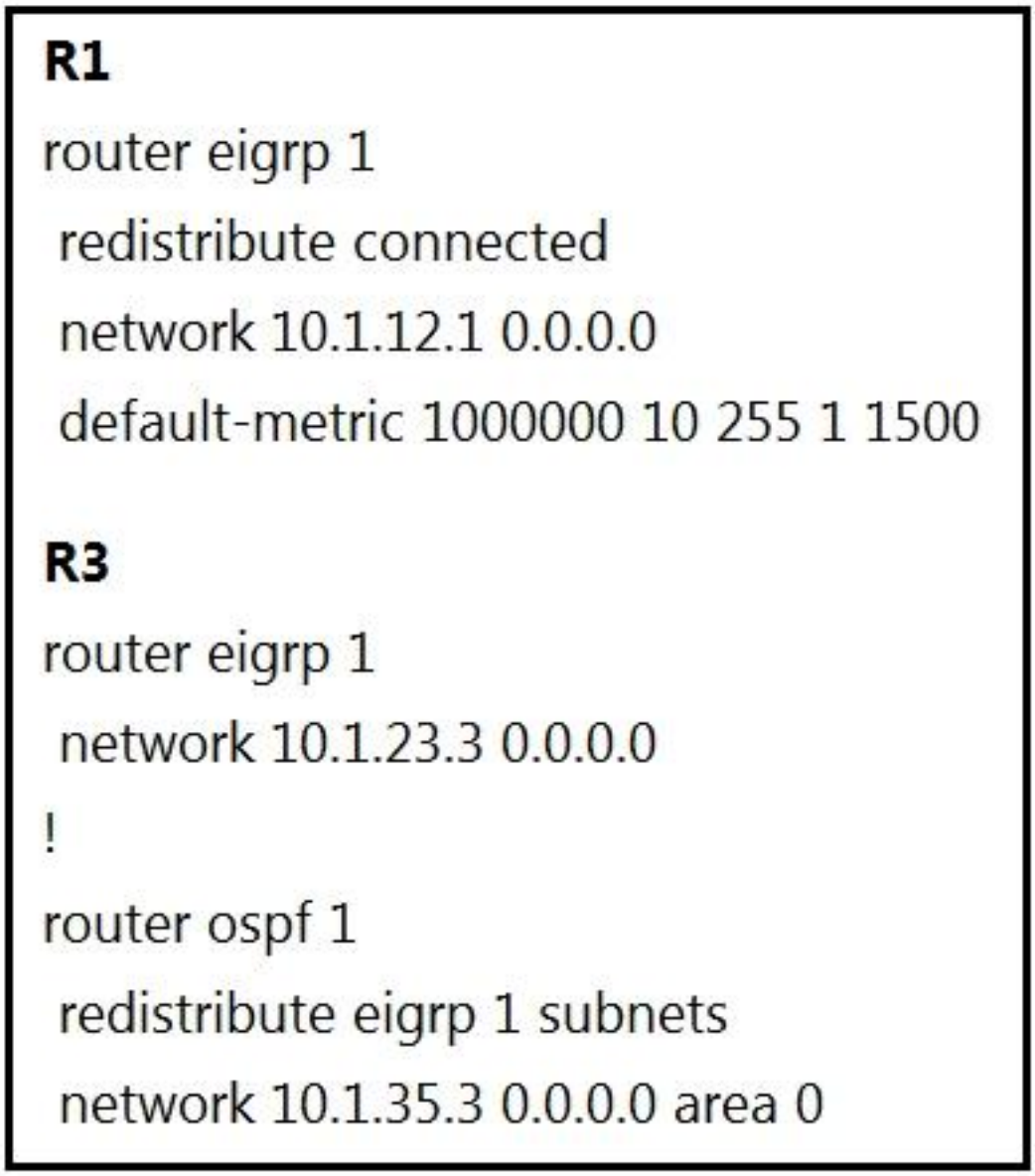


Answer:



QUESTION NO: 22
図を参照してください。ネットワーク管理者は、R5 からネットワーク 10.1.1.0/24 への到達性を確保するために、R3 で EIGRP を OSPF に再配布しますが、R4 が R5 を経由して 10.1.1.0/24
ネットワークに到達する際に最適ではない経路を使用していることに気づきます。
R5から10.1.1.0/24ネットワークへの接続性を維持したまま、問題を解決するには、どの操作を行うべきでしょうか？


EIGRP
OSPF
R1
R2
R3
R4
R5
10.1.12.0/24
10.1.23.0/24
10.1.35.0/24
10.1.1.0 /24
10.1.24.0/24
10.1.45.0/24
.1
.2
.2
.3
.3
.2
.5
.5
.4
.4



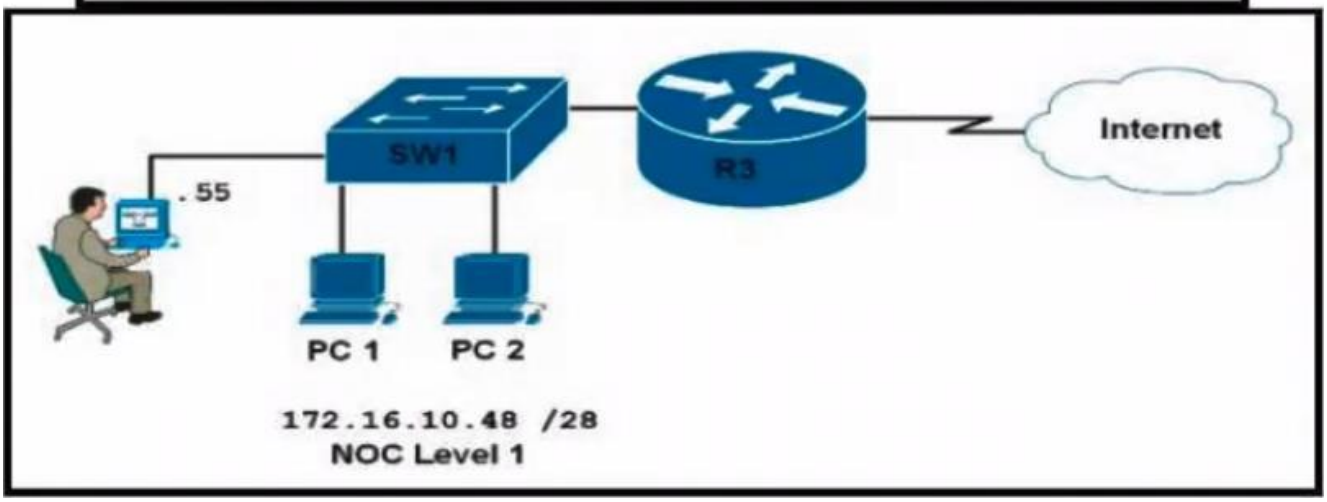
A. 外部 EIGRP の管理距離を 90 に変更します。
B. OSPF において、R5 から R4 への送信配布リストを適用します。
C. R5 の OSPF の管理距離を 200 に変更します。
D. R4でOSPFをEIGRPに再配布する
Answer: A
Explanation:
The subnet 10.1.1.1/24 is redistributed into EIGRP domain so it will have the Administrative Distance (AD) of 170. Therefore R4 also learns about this subnet advertised from R2 with the same AD of 170.
In the other hand, subnet 10.1.1.0/24 is also redistributed into OSPF on R3 so R5 & R4 will learn
about this subnet with AD of 110, which is better than the above AD of 170 so R4 will choose path R4 -> R5 -> R3 -> R2 -> R1.
In order to solve this problem, we can configure an outbound distribute list on R5 to prevent (filter
out) this subnet from advertising to R4. Then R4 only has one way to reach R1, which is R4 -

> R2
- > R1. But this method will remove the backup route so it is not the best solution.
Another solution is to reduce the AD of the external EIGRP to a value smaller than 110. This method reserves the backup route in case of the main route fails -> This is the best solution. To
do this, we can use the following command on R4:
router eigrp 1
distance eigrp 90 91 //Changes the AD to 90 for internal EIGRP routes and changes the AD to 91
for EIGRP external routes
We tested this lab in GNS3 and you can read this lab here. This is the result when we type the
"distance eigrp ..." command above on R4:
R4#show ip route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 6 subnets
D 10.1.12.0 [90/30720] via 10.1.24.2, 00:00:05, FastEthernet0/0 D EX 10.1.1.0 [91/33280] via
10.1.24.2, 00:00:05, FastEthernet0/0 C 10.1.24.0 is directly connected, FastEthernet0/0
D 10.1.23.0 [90/30720] via 10.1.24.2, 00:00:05, FastEthernet0/0 C 10.1.45.0 is directly connected, FastEthernet1/0
O 10.1.35.0 [110/2] via 10.1.45.5, 00:00:11, FastEthernet1/0
Note: We can change the AD of EIGRP routes via the "distance eigrp ..." command but the effect
of this command is local only.

QUESTION NO: 23
LDP セッションの形成にはどのトランスポート層プロトコルが使用されますか?
A. UDP
B.SCTP
C.TCP
D.RDP
Answer: C
Explanation:
LDP uses TCP as a reliable transport for sessions. When multiple LDP sessions are required between two LSRs, there is one TCP session for each LDP session.
Reference: https://tools.ietf.org/html/rfc5036

QUESTION NO: 24
図を参照してください。どの構成であれば、10人のエンジニアからなる運用レベル1チームが、HTTP経由のネットワーク認証情報を使用して、ルーターR3に一度に少なくとも3人ずつログインできますか？

```
R3#sh run | begin ip http server
ip http server
ip http access-class 20
ip http authentication local
no ip http secure-server
ip http max-connections 2
!
access-list 20 permit 172.16.10.48 0.0.0.15
!
end
```



A. R3(config)#ip http authentication enable
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
B. R3(config)#ip http max-connections 3
R3(config)#ip http accounting commands 3 default
C. R3(config)#ip http authentication aaa
R3(config)#ip http max-connections 3
D. R3(config)#ip http authentication aaa
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
Answer: C

QUESTION NO: 25
サービスプロバイダがL3VPN
MPLSアプリケーションを利用するために必要な2つのコンポーネントは何ですか？
(2つ選択してください。)
A. PルータはPEルータに対してMP-iBGPを設定する必要があります
B. PルーターはRSVPで設定する必要があります。
C. PEルータは、他のPEルータとの間でMP-iBGPを設定する必要があります。
D. PEルータは、CEに接続するにはMP-eBGPが設定されている必要があります。

E. PルーターとPEルーターはLDPまたはRSVPで設定する必要があります

Answer: CE

Explanation:

MPLS Network Protocols

+ IGP: OSPF, EIGRP, IS-IS on core facing and core links + RSVP and/or LDP on core and/or core facing links

+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN

Reference: https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmateriell/mpls-lecture.pdf

QUESTION NO: 26

ネットワーク エンジニアは、過剰なトラフィックを示すインターフェイスでの IP SLA 動作を確認する必要があります。

エンジニアはこのアクションを完了するためにどのコマンドを使用する必要がありますか?

A. 周波数を表示

B. トラックを表示

C. 到達可能性を表示

D. しきい値を表示

Answer: B

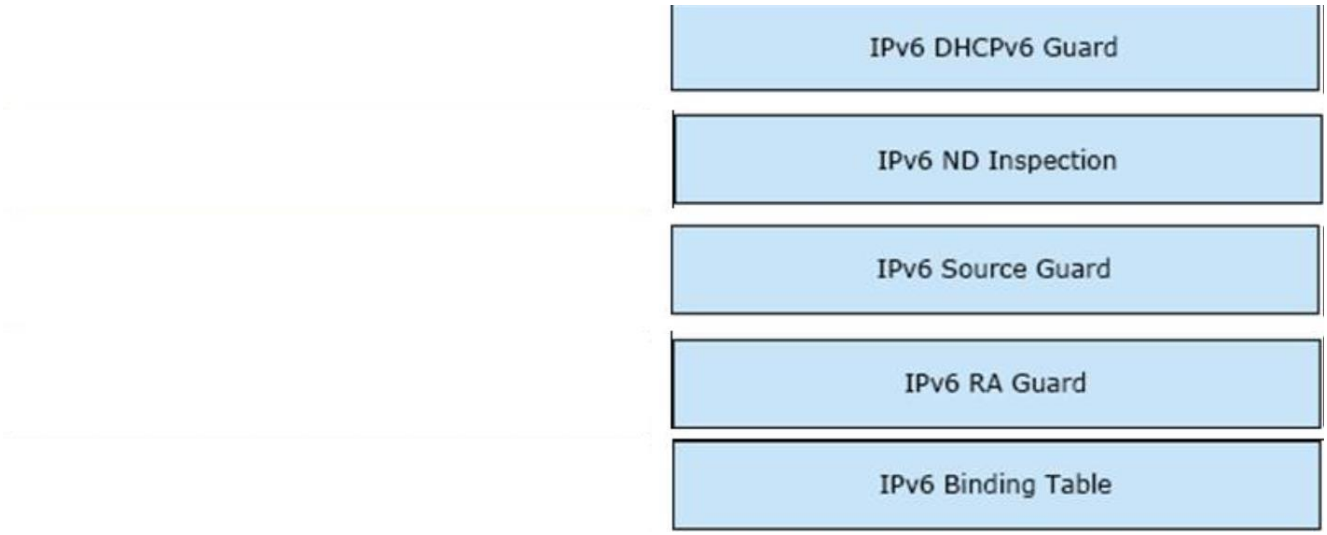
QUESTION NO: 27

ドラッグアンドドロップ問題

左側のIPv6ファーストホップセキュリティ機能を、右側の定義にドラッグアンドドロップしてください。

IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents
IPv6 DHCPv6 Guard	Create a binding table that is based on NS and NA messages
IPv6 Source Guard	Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table
IPv6 ND Inspection	Block a malicious host and permit the router from a legitimate route
IPv6 RA Guard	Create IPv6 neighbors connected to the device from information sources such as NDP snooping

Answer:



Explanation:
The DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from
unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients.
Client messages or messages sent by relay agents from clients to servers are not blocked.
IPv6 ND Inspection creates a binding table that is based on NS (Neighbor Solicitation) and NA
(Neighbor Advertisement) messages. The switch then uses this table to check any future NS/NA
messages. When the IPv6-LLA combination does not match, it drops the message. This only applies to NS/NA messages, it doesn't drop any actual data packets that have a spoofed IPv6 or
MAC address.
IPv6 Source Guard filters inbound traffic on L2 switch ports that are not in the IPv6 binding table.
The binding table stores the following information:
+ IPv6 address
+ MAC address
+ VLAN
+ Interface ID
Source Guard only looks at information found in the binding table, and it doesn't fill the binding
table.
The IPv6 RA Guard feature provides support for allowing the network administrator to block or
reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are
used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these
RAs and filters out RAs that are sent by unauthorized devices.

QUESTION NO: 28

ネットワーク管理者は、172.16 1.99 にある管理者デバイスからルータ CPU
に向かうすべての HTTP および HTTPS トラフィックが 500 kbps に制限されるように
CoPP
を設定しました。この制限を超えるトラフィックはすべてドロップする必要があります。
アクセスリスト 100 許可 IP ホスト 172.16.1.99 任意
！
クラスマップ CM-ADMIN
アクセスグループ 100 に一致
！
ポリシーマップ PM-COPP
クラスCM-ADMIN
警察 500000 適合アクション送信
！
インターフェースE0/0
サービス ポリシー入力 PM-COPP
CoPP が必要なトラフィックをキャプチャできなかったため、CPU 負荷が増加しています
。
問題を解決できる 2 つの構成はどれですか? (2つお選びください。)
A. インターフェース E0/0
サービス ポリシー入力なし PM-COPP
！
コントロールプレーン
サービス ポリシー入力 PM-COPP
B. ポリシーマップ PM-COPP
クラスCM-ADMIN
警察なし 500000 適合アクション送信
警察 500 適合アクション送信
！
コントロールプレーン
サービス ポリシー入力 PM-COPP
C. アクセスリスト 100 なし
アクセスリスト 100 許可 tcp ホスト 172.16.1.99 任意の eq 80
D. アクセスリスト 100 なし
アクセスリスト 100 許可 tcp ホスト 172.16.1.99 任意の eq 80
アクセスリスト 100 許可 tcp ホスト 172.16.1.99 任意の eq 443
E. ポリシーマップ PM-COPP
クラスCM-ADMIN
警察なし 500000 適合アクション送信
警察 500 適合アクション送信
Answer: A

QUESTION NO: 29
内部BGPでは、すべてのピアが論理的に完全にメッシュ接続されている必要があり、すべてのIBGPルータは他のすべてのIBGPルータとピアリングする必要があります。スケーリングの目的で、この要件を回避するために開発されたメカニズムが2つあります。それらは何で

すか？(2つ選択してください。)
A. 連邦
B. IBGPからEBGPへの経路再配布
C. BGPピアフィルタリング
D.ルートリフレクター。
Answer: AD

QUESTION NO: 30
図を参照してください。エンジニアは、ルーターR1へのユーザーのログインに影響を与えたAAA認証の問題をトラブルシューティングする必要があります。設定済みのユーザーが認証できるようにするコマンドはどれですか？

```
*Mar 10 20:13:58.156: AAA/BIND(00000055): Bind i/f
*Mar 10 20:13:58.156: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Mar 10 20:13:58.156: TAC+: Queuing AAA Authentication request 85 for processing
*Mar 10 20:13:58.156: TAC+:(00000055) login timer started 1020 sec timeout
*Mar 10 20:13:58.156: TAC+: processing authentication start request id 85
*Mar 10 20:13:58.156: TAC+: Authentication start packet created for 85()
*Mar 10 20:13:58.156: TAC+: Using server 10.106.60.182
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: socket event 2
*Mar 10 20:13:58.156: TAC+:(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: Would block while reading
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: socket event 1
*Mar 10 20:13:58.156: TAC+:(00000055)/0/READ: read entire 18 bytes response
*Mar 10 20:13:58.156: TAC+:(00000055)/0/225FE2DC: Processing the reply packet
*Mar 10 20:13:58.156: TAC+:: received bad AUTHEN packet: length = 6, expected 43974
*Mar 10 20:13:58.156: TAC+:: Invalid AUTHEN packet (check keys).
```

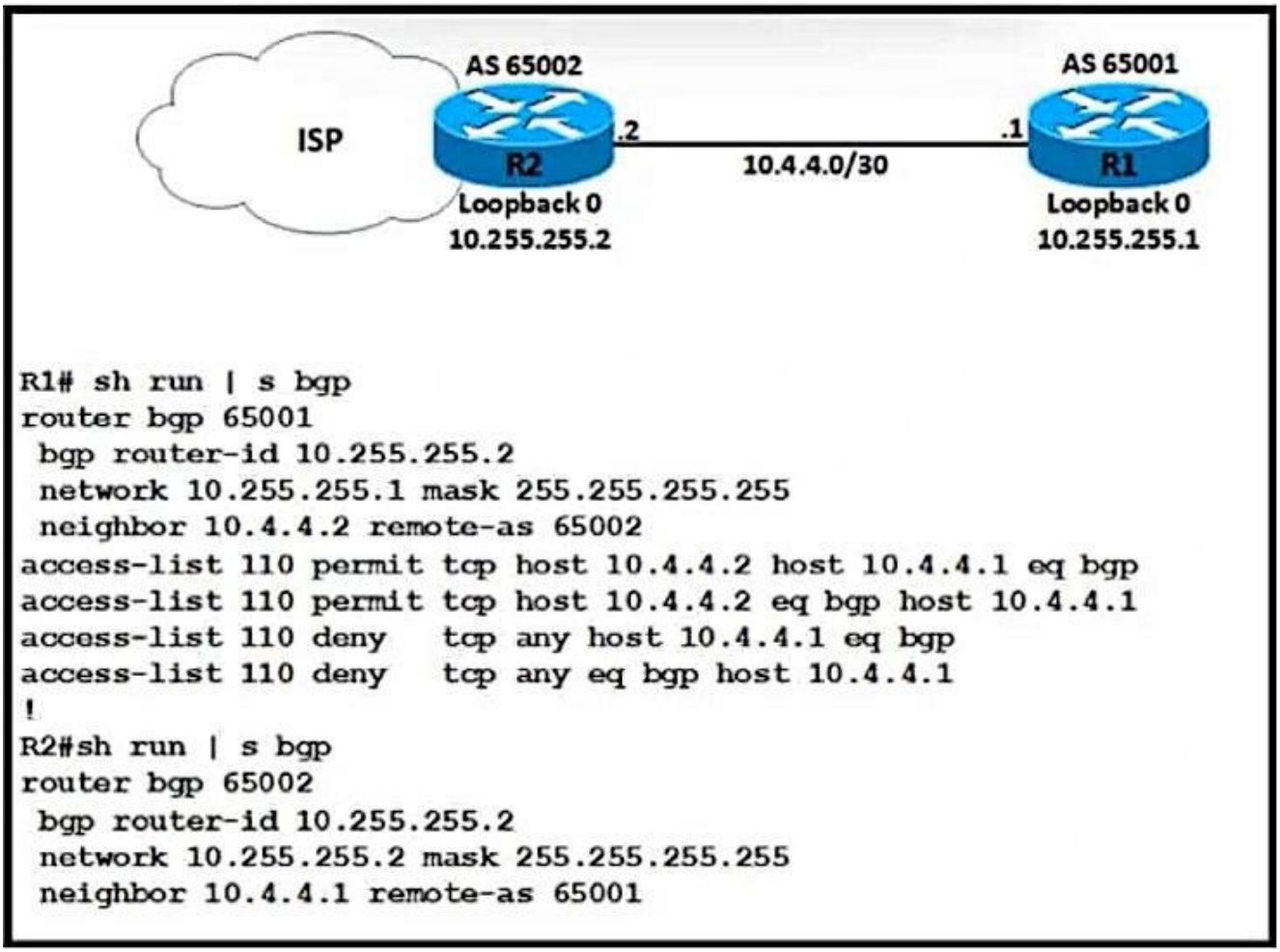
A. aaa 認証ログインデフォルトグループradiusローカル
B. aaa 認証ログインデフォルトグループradius tacacs+
C. aaa 認証ログインデフォルトグループ tacacs+
D. aaa認証ログインデフォルトグループradius
Answer: C
Explanation:
The debug log shows an "Invalid AUTHEN packet (check keys)" error, which indicates a mismatch between the shared key configured on the router and the TACACS+ server. Once the
shared key is corrected on both the TACACS+ server and the router, the appropriate AAA authentication method must be applied.
The correct command is aaa authentication login default group tacacs+, which specifies that the
router should use TACACS+ for authentication. If TACACS+ is the intended authentication

method and the shared key is properly configured, this command ensures that the user can successfully log in to the router using TACACS+.

QUESTION NO: 31
MPLS ラベルの 2 つの特性とは何ですか? (2つお選びください。)
A. ラベル エッジ ルーターは、受信したパケットのラベルを交換します。
B. ラベルは、レイヤ 3 ヘッダーの後のパケットに付加されます。
C.LDP は、信頼性の高い情報配信のために TCP を使用します。
D. MPLS ラベルは、転送等価クラスを識別する短い識別子です。
E. MPLS パケットには最大 2 つのラベルを付加できます。
Answer: CD
Explanation:
A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an
MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label
onto an incoming packet and pop it off an outgoing packet.
MPLS labels are added between the Layer 2 and the Layer 3 header in the packets (-> Therefore
MPLS labels are added before Layer 3 header).
There are no limit on the number of labels in a stack.
A label is a short, four-byte, fixed-length, locally-significant identifier which is used in order to identify a Forwarding Equivalence Class (FEC). The label which is put on a particular packet represents the FEC to which that packet is assigned.
LDP uses TCP as a reliable transport for sessions. Each TCP connection has only one LDP session.
Reference: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html

QUESTION NO: 32
MPLSにおけるダウンストリーム非要求配信方式とは何ですか？
A. ピアが要求した場合にのみ、ラベルをピアに通知します。
B. 特定の LSR にユニキャスト hello メッセージを送信します。
C. 特定の LER にユニキャスト hello メッセージを送信します。
D. ピアからのリクエストなしに、ラベルをピアに通知します。
Answer: D

QUESTION NO: 33
図を参照してください。ネットワークエンジニアは、R1とR2がeBGPピアリングを確立できないことに気づきました。



ログには以下のメッセージが表示されます。

*Dec 21 12:08:59.991: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) NSF delete stale NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x44361063:8) NSF no stale paths state is NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) Resetting ALL counters.
*Dec 21 12:09:09.819: BG-3-NOTIFICATION: sent to neighbor 10.4.4.2 passive 2/3 (BGP identifier wrong) 4 bytes OAFFFF02
*Dec 21 12:09:09.823: BGP-4-MSGDUMP: unsupported or mal-formatted message received from 10.4.4.2:
*Dec 21 12:09:12.443: 8BGP SESSION-5-ADJCHANGE: neighbor 10.4.4.2 IPv4 Unicast topology base removed from session BGP Notification received
*Dec 21 12:09:00.191: BGP: br global 10.4.4.2 Open active delayed 12288ms (35000ms max, 60% jitter)

eBGPピアリングを復元するために、エンジニアはR1にどの設定を適用する必要がありますか？

A.

```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

B.

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny tcp any host 10.4.4.1 eq 179
access-list 110 deny tcp any eq 179 host 10.4.4.1
```

C.

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

D.

```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny   tcp any host 10.4.4.1 eq 179
access-list 110 deny   tcp any eq 179 host 10.4.4.1
```

Answer: D

QUESTION NO: 34
管理者が会社のルーターにセキュリティ対策を実装したいと考えています。ルーターのセキュリティを強化するために使用するオプションを3つ選択してください。(3つ選択してください。)
A. ルーターへのアクセス制御
B. ルーターを経由するすべてのトラフィックを制限する
C. SNMPを制限する
D.未使用のサービスをすべて有効にする
E. すべてのパスワードを暗号化する
F. ログ記録を無効にする
Answer: ACE

QUESTION NO: 35
図を参照してください。隣接するOSPFネイバールータのルーティングテーブルに、スタティックルートが存在しません。どの操作でこの問題を解決できますか？

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

A. プレフィックスリストDMZ-STATICにネクストホップ10.20.20.1を設定します。
B.
静的ルーターの末尾にあるネクストホップインターフェイスを設定して、再配布できるようにします。
C. ルートマップにpermit 20ステートメントを設定して、静的ルートを再配布します。
D.再配布コマンドでsubnetsキーワードを設定します。
Answer: D
Explanation:
When you include the subnets keyword, the OSPF redistributes the routes, which are subnetted.
The process uses 20 as the default metric. This happens when no metric is specified by the use
of the metric-type keyword.