

CCNA 3 Examen Final ENSAv7 Questions et Réponses Français

December 20, 2021 CCNA 3 No Comments

1. Un administrateur réseau a modifié un routeur compatible OSPF pour avoir un paramètre de minuterie Hello de 20 secondes. Quel est le nouveau paramètre d'intervalle Dead par défaut?

- 40 secondes
- 60 secondes
- **80 secondes**
- 100 secondes

2. Quelle table OSPF est identique sur tous les routeurs convergents dans la même zone OSPF?

- neighbor
- contiguïté
- routage
- **topologie**

3. Quel groupe d'API est utilisé par le contrôleur SDN pour communiquer avec les diverses applications ?

- Les API dirigées vers l'ouest
- Les API descendantes
- Les API dirigées vers l'est
- **Les API ascendantes**

4. Quelle est la fonction principale d'un hyperviseur ?

- **Il est utilisé pour créer et gérer plusieurs instances de machine virtuelle sur une machine hôte.**
- C'est un dispositif qui filtre et vérifie les informations d'identification de sécurité.
- Il est utilisé par les FAI pour contrôler les ressources informatiques du cloud.
- Il s'agit d'un logiciel utilisé pour coordonner et préparer les données à des fins d'analyse.
- C'est un dispositif qui synchronise un groupe de capteurs.

5. En quoi la virtualisation est-elle utile à la reprise après sinistre dans un data center ?

- Le provisionnement des serveurs est plus rapide.
- **Tous les équipements n'ont pas être identiques.**
- Moins d'énergie est consommée.
- Il y a toujours du courant.

_Explique : Amélioration de la reprise après sinistre : la virtualisation offre des solutions avancées de continuité des activités. Il fournit une capacité d'abstraction matérielle afin que le site de récupération n'ait plus besoin d'avoir un matériel identique au matériel de l'environnement de production. La plupart des plates-formes de virtualisation de serveurs d'entreprise disposent également d'un logiciel qui peut aider à tester et à automatiser le basculement avant qu'un sinistre ne se produise.

6. Associez les fonctions aux couches correspondantes. (Les options ne sont pas toutes utilisées.)



couche d'accès

- Fournir un accès réseau à l'utilisateur
- Constituer la périphérie du réseau

couche distribution

- Implémenter une politique d'accès réseau
- Définir les limites de routage de couche 3

couche cœur de réseau

- Fournir une connectivité haut débit du réseau fédérateur
- Constituer un associateur de tous les blocs de campus

7. Quel ensemble d'entrées de contrôle d'accès permettrait à tous les utilisateurs du réseau 192.168.10.0/24 d'accéder à un serveur Web situé à l'adresse 172.17.80.1, sans toutefois les autoriser à utiliser le protocole Telnet ?

- access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1
- access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
- access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
- access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23
- **access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80**
- **access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23**
- access-list 103 deny tcp host 192.168.10.0 any eq 23
- access-list 103 permit tcp host 192.168.10.1 eq 80

8. Citez trois raisons d'utiliser des adresses IP privées et la NAT ? (Choisissez trois réponses.)

- Pour créer plusieurs adresses IP publiques
- Pour réduire l'utilisation du processeur sur les routeurs des clients
- **Pour empêcher les périphériques extérieurs connectés à Internet d'accéder à l'adressage de réseau local**
- **Pour économiser les adresses IP publiques enregistrées**
- Pour améliorer les performances du routeur connecté à Internet
- **Pour autoriser l'extension de réseau local sans ajout d'adresses IP publiques supplémentaires**

9. Quelle est la caractéristique d'un réseau OSPF à zone unique?

- Tous les routeurs ont la même table de routage.
- Tous les routeurs ont la même table de voisins.
- **Tous les routeurs sont dans la zone fédérateur.**
- Tous les routeurs partagent une base de données de transfert commune.

10. Quel est le but de l'établissement d'un étalon réseau ?

- Il vérifie la configuration de la sécurité des périphériques réseau.
- Il gère les performances des périphériques réseau.
- **Il crée un point de référence pour des évaluations futures du réseau.**
- Il fournit une moyenne statistique pour les performances réseau.

_Explique : Une ligne de base est utilisée pour établir les performances normales du réseau ou du système. Il peut être utilisé pour comparer les performances futures du réseau ou du système afin de détecter des situations anormales.

11. Quelle déclaration décrit un VPN?

- Les VPN utilisent des connexions physiques dédiées pour transférer des données entre des utilisateurs distants.
- **Les VPN utilisent des connexions virtuelles pour créer un réseau privé via un réseau public.**
- Les VPN utilisent des connexions logiques pour créer des réseaux publics via Internet.
- Les VPN utilisent un logiciel de virtualisation de source ouverte pour créer le tunnel via Internet.

_Explique : Un VPN est un réseau privé créé sur un réseau public. Au lieu d'utiliser des connexions physiques dédiées, un VPN utilise des connexions virtuelles acheminées via un réseau public entre deux périphériques réseau.

12. Reportez-vous à l'illustration. Un administrateur a d'abord configuré une liste ACL étendue comme indiqué par la sortie de la commande show access-lists . L'administrateur a ensuite modifié cette liste d'accès en exécutant les commandes ci-dessous.

```
Router(config)# ip access-list extended 101

Router(config-ext-nacl)# no 20

Router(config-ext-nacl)# 5 permit tcp any any eq 22

Router(config-ext-nacl)# 20 deny udp any any
```

**Quelles deux conclusions peut-on tirer de cette nouvelle configuration?
(Choisissez deux.)**

- Les paquets TFTP seront autorisés.
- Les paquets Telnet seront autorisés.
- **Les paquets ping seront autorisés.**
- Tous les paquets TCP et UDP seront refusés.
- **Les paquets SSH seront autorisés.**

_Explique : Après l'édition, la configuration finale est la suivante :

Router#_ afficher les listes d'accès

Liste d'accès IP étendue 101

5 autoriser tcp tout tout eq ssh

10 refuser tcp tout tout

20 refuser udp tout

30 permis icmp tout tout

Ainsi, seuls les paquets SSH et les paquets ICMP seront autorisés.

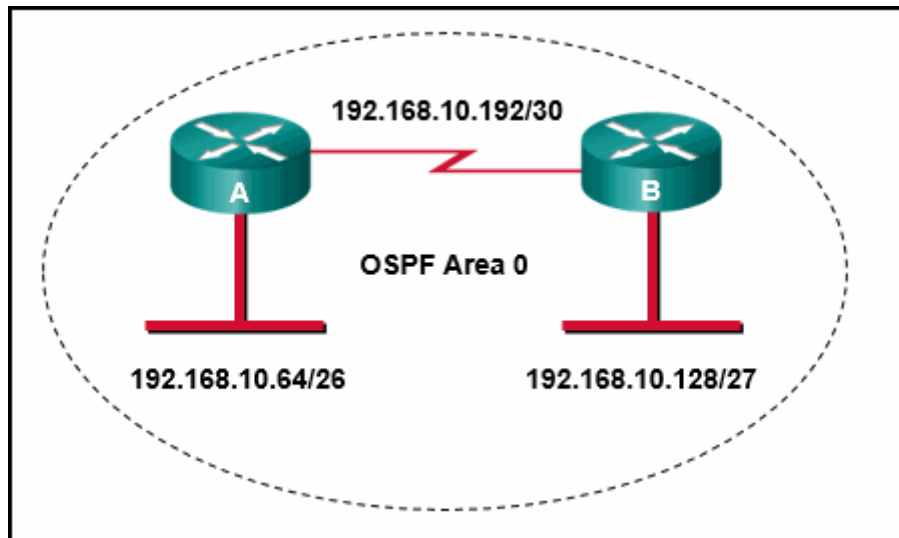
13. Quelle affirmation décrit une caractéristique des listes de contrôle d'accès IPv4 standard ?

- Elles peuvent être configurées de manière à filtrer le trafic en fonction des adresses IP source et des ports source.
- **Elles filtrent le trafic en fonction des adresses IP source uniquement.**
- Elles peuvent être créées avec un numéro, mais pas avec un nom.
- Elles sont configurées en mode de configuration d'interface.

14. Qu'est-ce qu'un WAN ?

- Une infrastructure réseau conçue pour prendre en charge le stockage, la récupération et la réplication de données
- **Une infrastructure réseau qui fournit un accès à d'autres réseaux dans un vaste périmètre**
- Une infrastructure réseau qui s'étend sur un périmètre physique limité, comme une ville
- Une infrastructure réseau qui fournit un accès dans un petit périmètre

15. Reportez-vous à l'illustration. Quelle séquence de commandes doit être utilisée pour configurer le routeur A pour OSPF?



i386046n1v2.gif

- router ospf 1
network 192.168.10.0 area 0
- router ospf 1
network 192.168.10.64 255.255.255.192
network 192.168.10.192 255.255.255.252
- **router ospf 1**
network 192.168.10.64 0.0.0.63 area 0
network 192.168.10.192 0.0.0.3 area 0
- router ospf 1
network 192.168.10.0

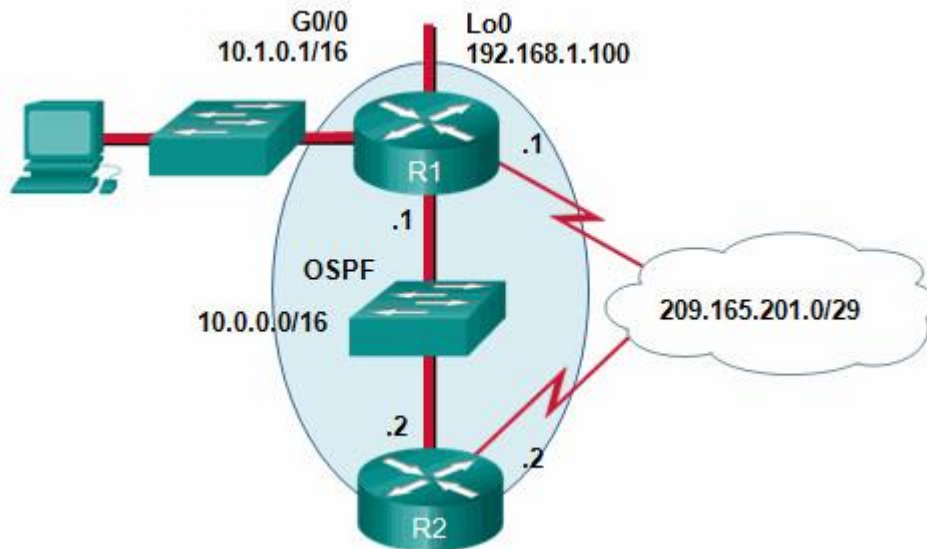
16. Sur quels éléments du routeur l'administrateur réseau doit-il effectuer des modifications pour une récupération de mot de passe ? (Choisissez deux réponses.)

- Mémoire morte (ROM) système
- **Fichier de configuration initiale**
- **Valeur du registre de configuration**
- Fichier de l'image système
- Fichier système NVRAM

17. Quel type de réseau utilise une infrastructure commune pour transporter le trafic voix, de données et vidéo ?

- **Convergé**
- Sans frontières
- Administré
- Commuté

18. Reportez-vous à l'illustration. Si aucun ID de routeur n'a été configuré manuellement, que le routeur R1 utiliserait-il comme ID de routeur OSPF?



- 209.165.201.1
- 10.0.0.1
- 10.1.0.1
- **192.168.1.100**

19. Quel type de paquet OSPF est utilisé par un routeur pour découvrir les routeurs voisins et établir la contiguïté voisine?

- Description de base de données (DD)
- hello==
- Les mises à jour d'état de lien
- LSR (Link-State Request)

20. Quels sont trois avantages du cloud computing ? Citez-en trois.

- Il utilise des logiciels open source pour le traitement distribué des grands ensembles de données.
- Il transforme les données brutes en informations utiles en identifiant les tendances et les relations.
- Il utilise des clients répartis chez les utilisateurs finaux pour réaliser une portion substantielle du prétraitement et du stockage.
- **Il élimine ou réduit le besoin d'équipements IT, de maintenance et de gestion sur site.**
- **Il permet d'accéder aux données de l'entreprise partout, à tout moment.**
- **Il rationalise les opérations IT d'une entreprise en s'abonnant uniquement aux services nécessaires.**

21. Parmi les scénarios suivants, lesquels sont des exemples de VPN d'accès à distance ? (Choisissez deux réponses.)

- Une petite filiale de trois salariés utilise un dispositif Cisco ASA pour créer une connexion VPN au siège social.
- **Un agent commercial itinérant se connecte au réseau de l'entreprise via la connexion Internet d'un hôtel.**
- Tous les utilisateurs d'une filiale importante ont accès aux ressources de l'entreprise via une seule connexion VPN.
- Un fabricant de jouets a une connexion VPN permanente avec l'un de ses fournisseurs de pièces.
- **Un employé travaillant chez lui utilise un logiciel client VPN sur un ordinateur portable pour se connecter au réseau de l'entreprise.**

22. Quelles affirmations caractérisent un virus ? Citez-en deux.

- Un virus se reproduit en exploitant indépendamment des vulnérabilités dans les réseaux.
- **Un virus peut être en sommeil, puis s'activer à une date ou une heure spécifique.**
- Un virus fournit au hacker des données sensibles, comme des mots de passe.
- Un virus comprend une vulnérabilité habilitante, un mécanisme de propagation et une charge utile.
- **Un virus nécessite généralement une intervention de l'utilisateur final.**

_Explication : Le type d'interaction de l'utilisateur final requis pour lancer un virus est généralement l'ouverture d'une application, l'ouverture d'une page Web ou la mise sous tension de l'ordinateur. Une fois activé, un virus peut infecter d'autres fichiers situés sur l'ordinateur ou d'autres ordinateurs sur le même réseau.

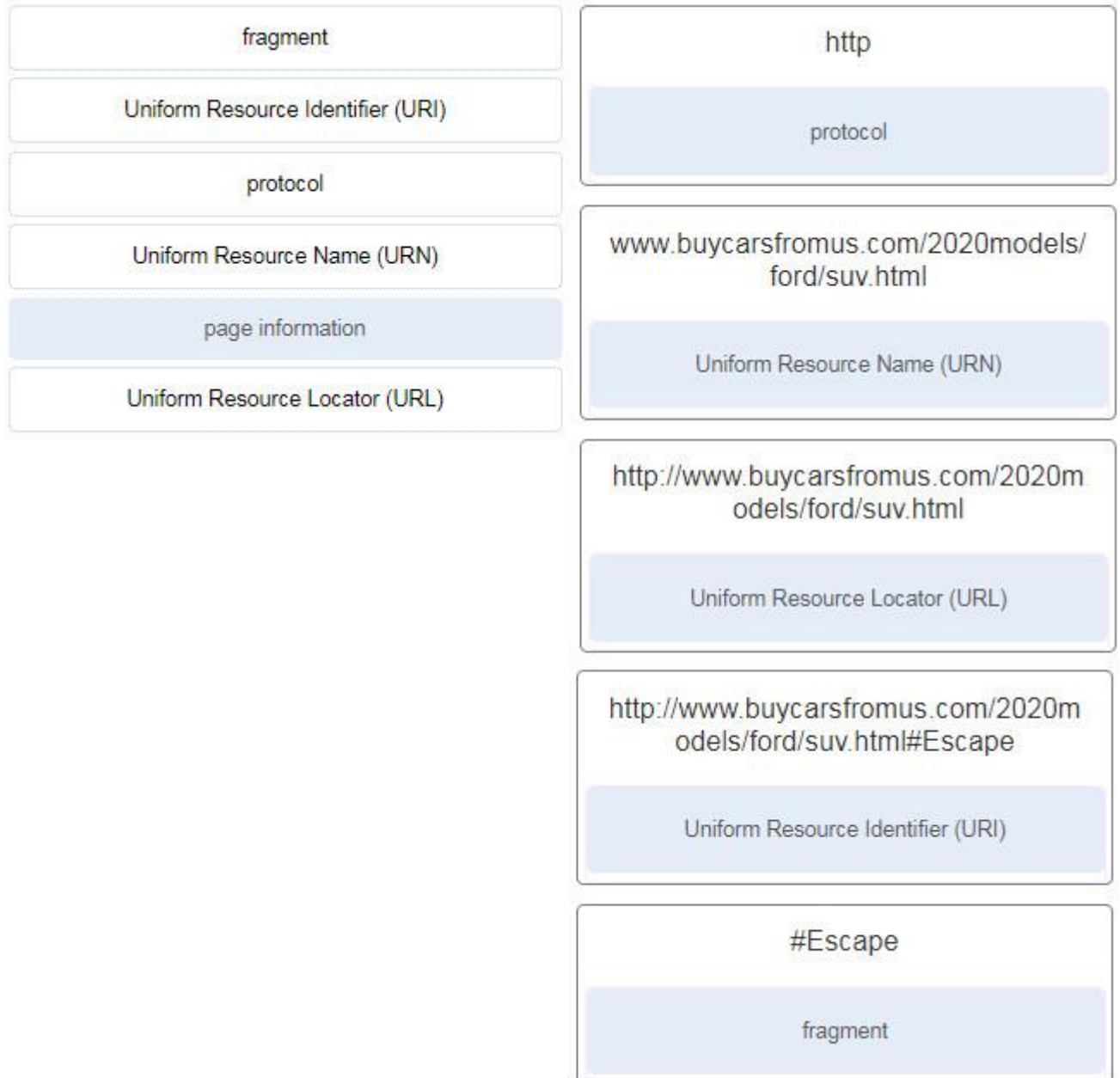
23. Pourquoi la QoS est-elle un élément important dans un réseau convergé qui combine communications vocales, vidéo et de données ?

- Les communications de données sont sensibles à la gigue.
- **Les communications vocales et vidéo sont plus sensibles à la latence.**
- Les communications de données doivent être la première priorité.
- Les appareils anciens ne peuvent pas transmettre de la voix et de la vidéo sans QoS.

24. Faites correspondre le terme avec le lien web du composant

<http://www.buycarsfromus.com/2020models/ford/suv.html#Escape> . (les

options ne doivent pas être toutes utilisées.)



- http — protocole
- www.buycarsfromus.com/2020models/ford/suv.html — Uniform Resource Name (URN)
- http://www.buycarsfromus.com/2020models/ford/suv.html — URL (Uniform Resource Locator)
- http://www.buycarsfromus.com/2020models/ford/suv.html#Escape — Uniform Resource Identifier (URI)
- #Escape — fragment

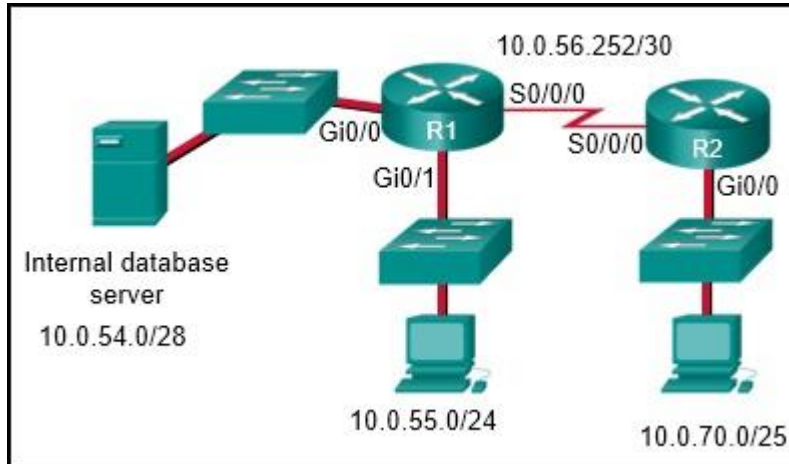
25. À quelle étape du recueil des symptômes l'ingénieur réseau détermine-t-il si le problème se situe sur la couche cœur de réseau, la couche de distribution ou la couche d'accès du réseau ?

- Détermination de la propriété.
- Identification des symptômes.
- Collecte d'informations.

- **Réduction de l'étendue des causes probables.**

- Documentation des symptômes.

26. Reportez-vous à l'illustration. Quelles deux configurations seraient utilisées pour créer et appliquer une liste d'accès standard sur R1, de sorte que seuls les périphériques réseau 10.0.70.0/25 sont autorisés à accéder au serveur de base de données interne? Citez-en deux.



- **R1 (config) # access-list 5 permit 10.0.70.0 0.0.127**
- R1(config)# access-list 5 permit 10.0.54.0 0.0.1.255
- R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip access-group 5 out
- R1(config)# interface Serial0/0/0
R1(config-if)# ip access-group 5 in
- R1(config)# access-list 5 permit any

27. Examinez la liste de contrôle d'accès suivante, qui permet le transfert des fichiers de configuration du téléphone IP depuis un hôte spécifique vers un serveur TFTP :

```
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range
1024 5000

R1(config)# access-list 105 deny ip any any

R1(config)# interface gi0/0

R1(config-if)# ip access-group 105 out
```

Quelle méthode permettrait à l'administrateur réseau de modifier la liste de contrôle d'accès et d'inclure des transferts FTP à partir de n'importe quelle adresse IP source ?

- **R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000**
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any
- R1(config)# interface gi0/0
R1(config-if)# no ip access-group 105 out
R1(config)# no access-list 105

```
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
```

```
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
```

```
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
```

```
R1(config)# access-list 105 deny ip any any
```

```
R1(config)# interface gi0/0
```

```
R1(config-if)# ip access-group 105 out
```

- R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20

```
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
```

- R1(config)# interface gi0/0

```
R1(config-if)# no ip access-group 105 out
```

```
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
```

```
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
```

```
R1(config)# interface gi0/0
```

```
R1(config-if)# ip access-group 105 out
```

28. ABCTech étudie l'utilisation de l'automatisation pour certains de ses produits. Afin de contrôler et de tester ces produits, les programmeurs nécessitent Windows, Linux et MAC OS sur leurs ordinateurs. Quel service ou quelle technologie permettrait de répondre à cette exigence ?

- ACI Cisco
- data center
- SDN (Software Defined Networking)
- **virtualisation**

29. Quel type de VPN utilise une configuration hub-and-spoke pour établir une topologie de maillage complet ?

- VPN MPLS
- GRE sur IPsec
- Interface de tunnel virtuel IPsec
- **VPN multipoint dynamique**

30. Quelle fonctionnalité permet de limiter la taille d'un domaine défaillant sur un réseau d'entreprise ?

- L'achat d'équipement d'entreprise conçu pour un volume de trafic important
- **L'utilisation de la méthode du bloc de commutation du bâtiment**
- L'utilisation d'une conception réseau principale regroupée
- L'installation d'alimentations redondantes

31. Quelle commande serait utilisée dans le cadre de la configuration NAT ou PAT pour afficher des informations sur les paramètres de configuration NAT et le nombre d'adresses dans le pool?

- show version
- show ip cache
- **show ip nat statistics**
- show running-config

32. Reportez-vous à l'exposition. Quel format de données est utilisé pour représenter les données pour les applications d'automatisation de réseau?

```
<message>complete</message>
<username>efriends</username>
<user_info>
<First_name>Emily</First_name>
<Last_name>Friends</Last_name>
</user_info>
```

- HTML
- YAML
- JSON
- **XML**

33. Quelle est la caractéristique de l'API REST ?

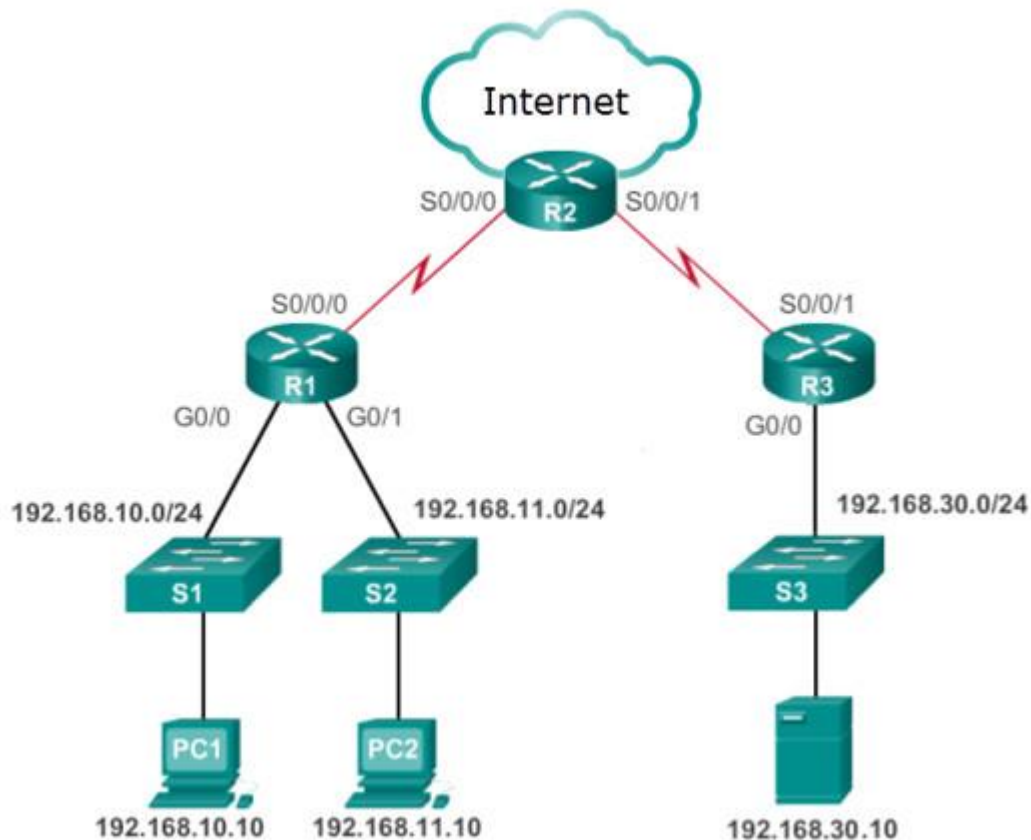
- évolué vers ce qui est devenu SOAP
- **l'API la plus utilisée pour les services web**
- utilisé pour échanger des informations structurées XML sur HTTP ou SMTP
- considérés comme lents, complexes et rigides

34. Dans JSON, qu'est-ce qui se tient entre crochets []?

- **an array**
- paires clé/valeur
- valeurs imbriquées
- un objet

35. Reportez-vous à l'illustration. La société a fourni des téléphones IP aux employés sur le réseau 192.168.10.0/24 et le trafic vocal aura besoin de priorité sur le trafic de données. Quel est le meilleur type et placement ACL à utiliser dans

cette situation?



- **ACL entrante étendue sur R3 G0/0**
- ACL entrante standard sur les lignes R1 vty
- ACL entrante étendue sur R3 G0/0
- ACL entrante standard sur R1 G0/1

36. Un administrateur configure OSPF à zone unique sur un routeur. L'un des réseaux qui doivent être annoncés est 172.20.0.0 255.255.252.0. Quel masque générique l'administrateur utiliserait-il dans l'instruction réseau OSPF?

- 0.0.0.3
- 0.0.63.255
- **0.0.3.255**
- 0.0.0.7

37. Deux grandes entreprises viennent de fusionner. L'ingénieur réseau a pour mission de connecter les réseaux des deux entreprises sans encourir les frais liés aux lignes louées. Quelle solution serait la plus économique pour fournir une connexion propre et sécurisée entre les réseaux des deux entreprises ?

- Frame Relay
- Client Cisco AnyConnect Secure Mobility avec SSL
- VPN à accès distant utilisant IPsec
- **Réseau privé virtuel site à site**
- VPN SSL sans client Cisco Secure Mobility

Explication : Le VPN de site à site est une extension d'un réseau WAN classique qui fournit une interconnexion statique de réseaux entiers. Frame Relay serait un meilleur choix que les lignes louées, mais serait plus coûteux que la mise en œuvre de VPN de site à site. Les autres options font référence aux VPN d'accès à distance

qui sont mieux adaptés pour connecter les utilisateurs au réseau de l'entreprise que pour interconnecter deux réseaux ou plus.

38. Quelle affirmation décrit précisément une caractéristique de WAN? (Quelle affirmation décrit précisément une caractéristique de IPsec)

- IPsec est un cadre de normes développé par Cisco qui s'appuie sur des algorithmes OSI.
- IPsec fonctionne sur la couche de l'application et protège toutes les données de l'application.
- IPsec fonctionne au niveau de la couche de transport et protège les données au niveau de la couche réseau.
- **IPsec est un cadre de normes ouvertes qui repose sur des algorithmes existants.**
- IPsec est un cadre de normes propriétaires qui dépendent d'algorithmes spécifiques à Cisco.

39. Quelle technologie d'accès de WAN public repose sur l'utilisation de lignes téléphoniques en cuivre pour donner un accès aux abonnés qui ont des lignes multiplexées dans une liaison T3 unique ?

- **DSL**
- câble
- RNIS
- liaison commutée

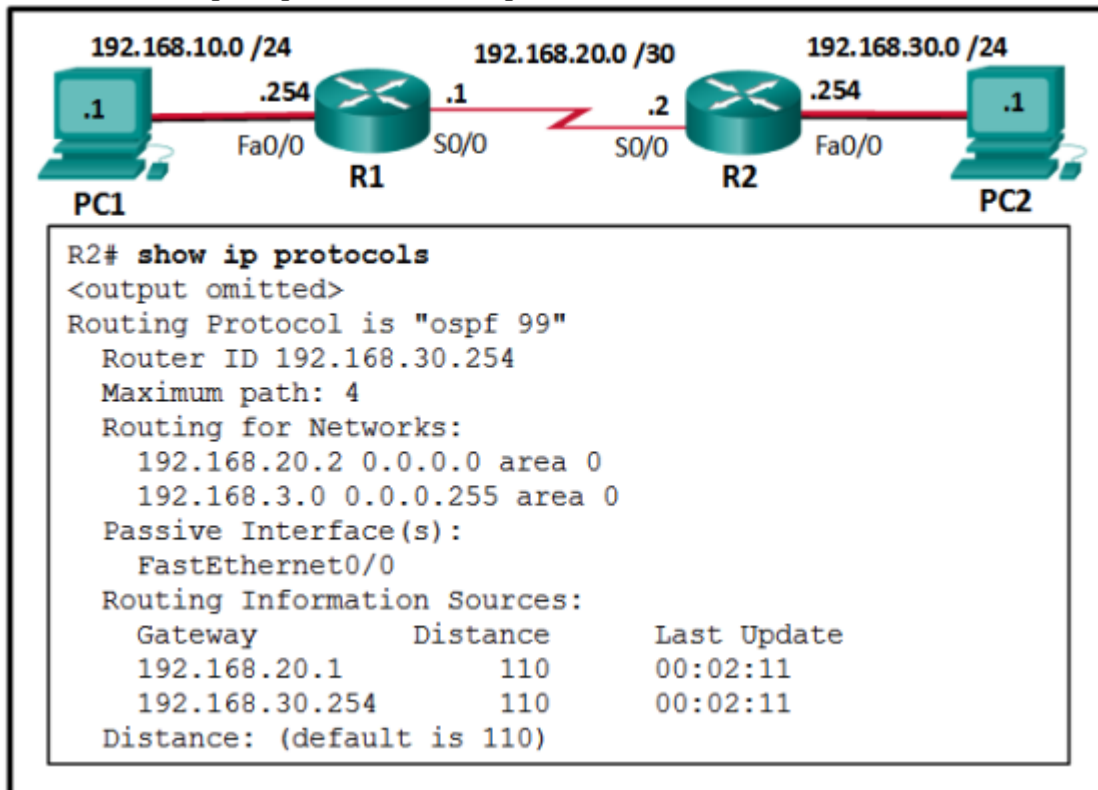
40. Mettez en correspondance chaque composant d'une connexion WAN et sa description. (Les options ne sont pas toutes utilisées.)

customer premises equipment	<p>devices that put data on the local loop</p> <p>data communications equipment</p>
demarcation point	<p>devices and inside wiring located on the enterprise edge and which connect to a carrier link</p> <p>customer premises equipment</p>
data terminal equipment	<p>a point that is established in a building or complex to separate customer equipment from service provider equipment</p> <p>demarcation point</p>
data communications equipment	<p>the point of presence that is the local service provider facility or building that connects the CPE to the provider network</p> <p></p>
	<p>customer devices that pass the data from a customer network or host computer for transmission over the WAN</p> <p>data terminal equipment</p>

- périphériques plaçant des données sur la boucle locale — DCE
- appareils et câblage interne qui se trouvent à la périphérie du réseau de l'entreprise et se connectent à la liaison d'un opérateur — CPE
- point établi dans un bâtiment ou un complexe pour séparer l'équipement du client et celui du fournisseur d'accès — point de démarcation

- point de présence représentant l'installation ou le bâtiment du fournisseur d'accès local qui connecte l'équipement d'abonné au réseau du fournisseur
- périphériques du client qui transfèrent les données à partir du réseau d'un client ou d'un ordinateur hôte pour qu'elles soient transmises via le WAN — équipement terminal de traitement de données

41. Reportez-vous à l'illustration. Un administrateur réseau a configuré OSPFv2 sur les deux routeurs Cisco, mais PC1 ne parvient pas à se connecter à PC2. Quelle est la cause la plus probable de ce problème ?



- L'interface Fa0/0 est configurée en tant qu'interface passive sur le routeur R2.
- L'interface S0/0 est configurée en tant qu'interface passive sur le routeur R2.
- **L'interface Fa0/0 n'a pas été activée pour OSPFv2 sur le routeur R2.=**
- L'interface s0/0 n'a pas été activée pour OSPFv2 sur le routeur R2.

Explication : Si un réseau LAN n'est pas annoncé à l'aide d'OSPFv2, un réseau distant ne sera pas accessible. La sortie affiche une contiguïté réussie entre les routeurs R1 et R2 sur l'interface S0/0 des deux routeurs.

42. Reportez-vous à l'illustration. Un concepteur web appelle pour signaler que le serveur web web-s1.cisco.com n'est pas joignable via un navigateur web. Le technicien en charge utilise des utilitaires de commandes en ligne pour vérifier le problème et commencer le processus de dépannage. Quelles sont les deux choses qui peuvent être déterminées concernant le problème ? (Choisissez deux réponses.)

```
C:\WINNT\system32\cmd.exe
D:\>ping web-s1.cisco.com
Unknown host web-s1.cisco.com.
D:\>ping 192.168.0.10
Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time<10ms TTL=128
Reply from 192.168.0.10: bytes=32 time<10ms TTL=128
Reply from 192.168.0.10: bytes=32 time<10ms TTL=128
Reply from 192.168.0.10: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:\>
```

- Le logiciel de serveur Web sur web-s1.cisco.com présente un problème.
- Un routeur est en panne entre l'hôte source et le serveur web-s1.cisco.com.
- **DNS ne peut pas résoudre l'adresse IP pour le serveur web-s1.cisco.com.**
- La passerelle par défaut entre l'hôte d'origine et le serveur 192.168.0.10 est en panne.
- **Le serveur Web sur 192.168.0.10 est joignable depuis l'hôte d'origine.**

_Explique : Le résultat réussi du ping vers l'adresse IP indique que le réseau est opérationnel et que le serveur Web est en ligne. Cependant, le fait que le ping vers le nom de domaine du serveur échoue indique qu'il y a un problème DNS, à savoir que l'hôte ne peut pas résoudre le nom de domaine en son adresse IP associée.

43. Quel type de trafic est décrit comme prévisible et fluide?

- Données
- **Voix**
- Vidéo

44. Une société élabore une stratégie de sécurité pour sécuriser les communications. Lors de l'échange de messages sensibles entre le siège d'une société et une succursale, une valeur de hachage ne doit être recalculée qu'avec un code prédéfini, garantissant ainsi la validité de la source de données. Sur quel aspect des communications sécurisées cette mesure de sécurité porte-t-elle ?

- L'intégrité des données
- La confidentialité des données
- système de non-répudiation
- **authentification de l'origine**

_Explique : Les communications sécurisées se composent de quatre éléments :
Confidentialité des données – garantit que seuls les utilisateurs autorisés peuvent lire le message

Intégrité des données – garantit que le message n'a pas été altéré

Authentification de l'origine – garantit que le message n'est pas un faux et qu'il provient bien de qui il déclare

Non-répudiation des données – garantit que l'expéditeur ne peut pas répudier ou réfuter la validité d'un message envoyé

45. Un groupe d'utilisateurs sur le même réseau se plaint de l'exécution lente de leurs ordinateurs. Après quelques recherches, le technicien détermine que ces ordinateurs font partie d'un réseau de zombies. Quel type de malware est utilisé pour contrôler ces ordinateurs ?

- logiciel espion
- **réseau de zombies**
- rootkit
- virus

46. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une entrée unique:

```
access-list 101 permit udp 192.168.100.0 0.0.2.255 64.100.40.0 0.0.15 eq telnet .
```

Si un paquet avec une adresse source 192.168.101.45, une adresse de destination 64.100.40.4 et un protocole 23 est reçu sur l'interface, le paquet est-il autorisé ou refusé?

- **refusé**
- Autorisé

47. Quels sont les deux bénéfices de l'utilisation des dérivements SNMP ? (Choisissez deux propositions.)

- **Ils réduisent la charge sur les ressources du réseau et des agents.**
- Ils peuvent passivement écouter les datagrammes NetFlow exportés.
- Ils limitent l'accès aux systèmes de gestion uniquement.
- Ils peuvent fournir des données sur les paquets TCP/IP qui transitent par les appareils Cisco.
- **Ils permettent d'éliminer le besoin d'interrogations périodiques.**

48. Reportez-vous à l'illustration. Les routeurs R1 et R2 sont connectés via une liaison série. Un routeur est configuré en tant que NTP maître et l'autre en tant que NTP client. Quelles informations concernant R2 peuvent être tirées du résultat partiel de la commande show ntp associations detail présenté ? (Choisissez deux réponses.)

```
R2# show ntp associations detail
192.168.1.2 configured, authenticated, our_master, sane, valid,
stratum 3
<output omitted>
```

- L'adresse IP de R2 est 192.168.1.2.
- Les deux routeurs sont configurés pour utiliser NTPv2.
- Le routeur R2 est le maître et R1 est le client.
- **L'adresse IP de R1 est 192.168.1.2.**
- **Le routeur R1 est le maître et R2 est le client.**

Explique : Avec la commande show NTP associations, l'adresse IP du maître NTP est donnée.

49. Quelle étape du processus de routage d'état de liens est décrite par un routeur inondant l'état de liens et les informations de coût sur chaque liaison directement connectée?

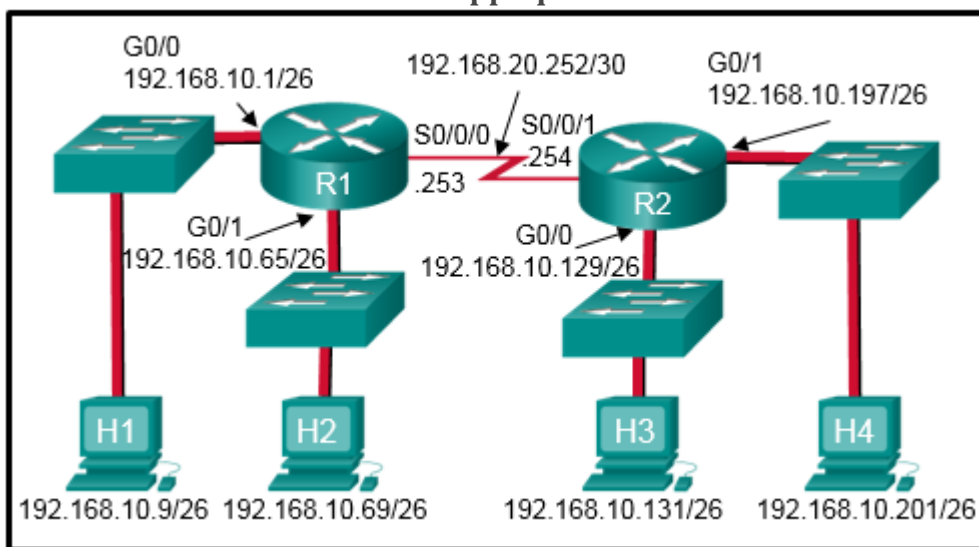
- déclarer un voisin inaccessible
- **échange d'annonces à état de liens**

- création de la table de topologie
- sélection de l'ID du routeur

50. Si un routeur a deux interfaces et achemine à la fois le trafic IPv4 et IPv6, combien de liste ACL pourrait-on créer et appliquer?

- 4
- 6
- **8**
- 12
- 16

51. Reportez-vous à l'illustration. Un administrateur réseau a configuré une liste ACL standard pour autoriser uniquement les deux réseaux LAN connectés à R1 à accéder au réseau qui se connecte à l'interface R2 G0/1, mais pas à l'interface G0/0. Lorsque vous appliquerez les meilleures pratiques, à quel endroit la liste ACL standard devrait-elle être appliquée?



- **R2 G0/0 sortant**
- R1 S0/0/0 entrant
- R1 S0/0/0 sortant
- R2 S0/0/1 sortant
- R2 G0/1 entrant

52. Quel protocole est un protocole de couche 2 neutre par le fournisseur qui annonce l'identité et les capacités du périphérique hôte à d'autres périphériques réseau connectés?

- Protocole NTP
- SNMP
- TFTP
- **LLDP**

53. Quel type de marquage QoS est appliqué aux trames Ethernet ?

- DSCP
- **CoS**
- Priorité IP
- ToS

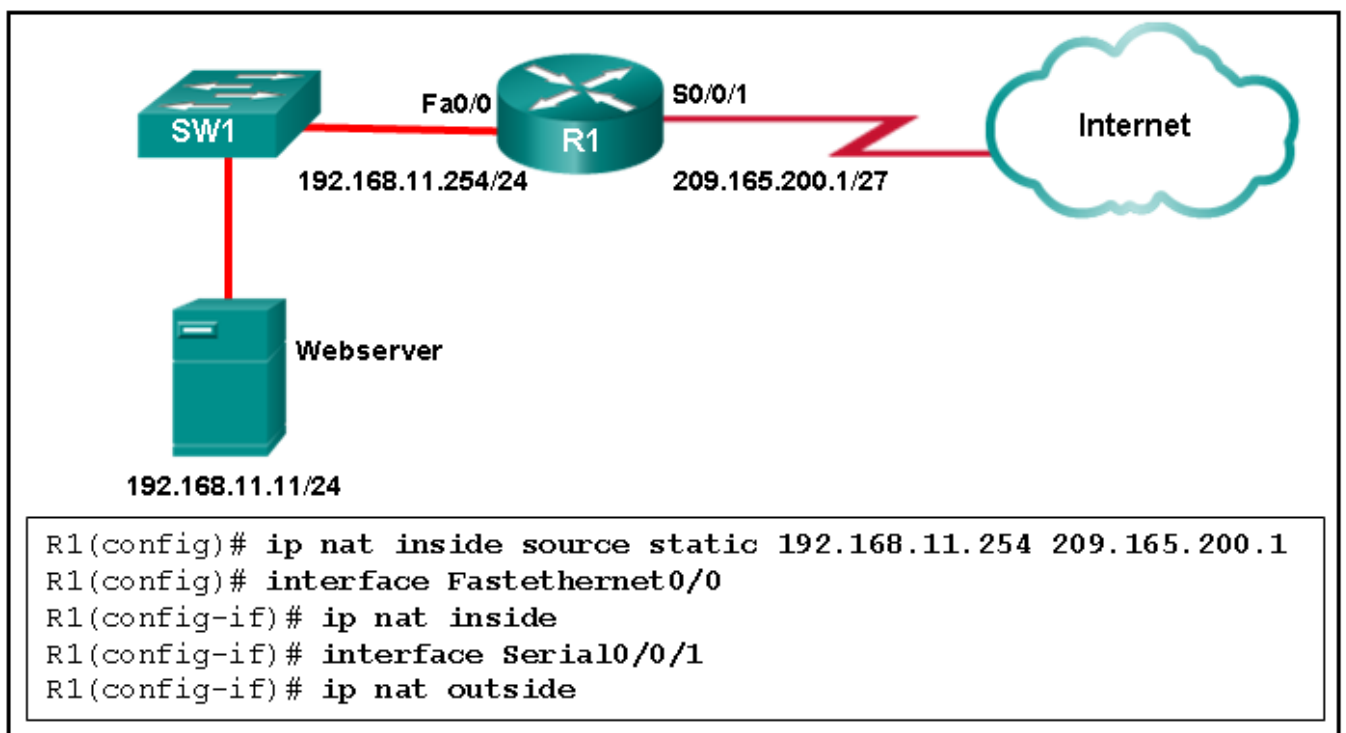
54. Lors de la configuration du réseau d'un petit bureau, l'administrateur réseau décide d'attribuer des adresses IP privées de manière dynamique aux stations de travail et aux terminaux mobiles. Quelle fonctionnalité doit-il activer sur le

routeur de l'entreprise pour permettre aux appareils de bureau d'accéder à Internet ?

- UPnP
- Filtrage MAC
- **NAT**
- QoS

Explication : La traduction d'adresses réseau (NAT) est le processus utilisé pour convertir des adresses privées en adresses routables sur Internet qui permettent aux appareils de bureau d'accéder à Internet.

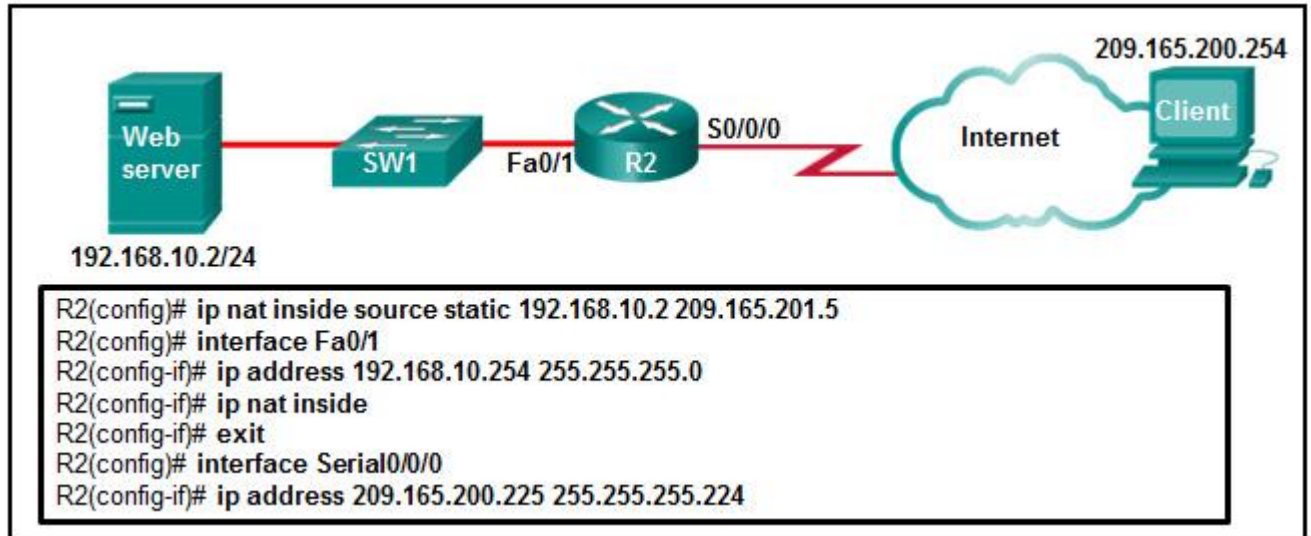
55. Examinez l'illustration. Le routeur R1 est configuré avec la NAT statique. L'adressage est correctement configuré sur le routeur et sur le serveur Web, mais il n'y a pas de connectivité entre le serveur Web et les utilisateurs sur Internet. Quelle est la cause probable de cette absence de connectivité ?



- L'adresse globale interne est incorrecte.
- **La configuration NAT du routeur présente une adresse locale interne incorrecte.**
- L'interface Fa0/0 devrait être configurée avec la commande ip nat outside .
- La configuration NAT de l'interface S0/0/1 est incorrecte.

56. Examinez l'illustration. Un technicien configure R2 de sorte que la NAT statique permette au client d'accéder au serveur Web. Quelle est la cause probable

de l'impossibilité pour le PC client d'accéder au serveur Web ?



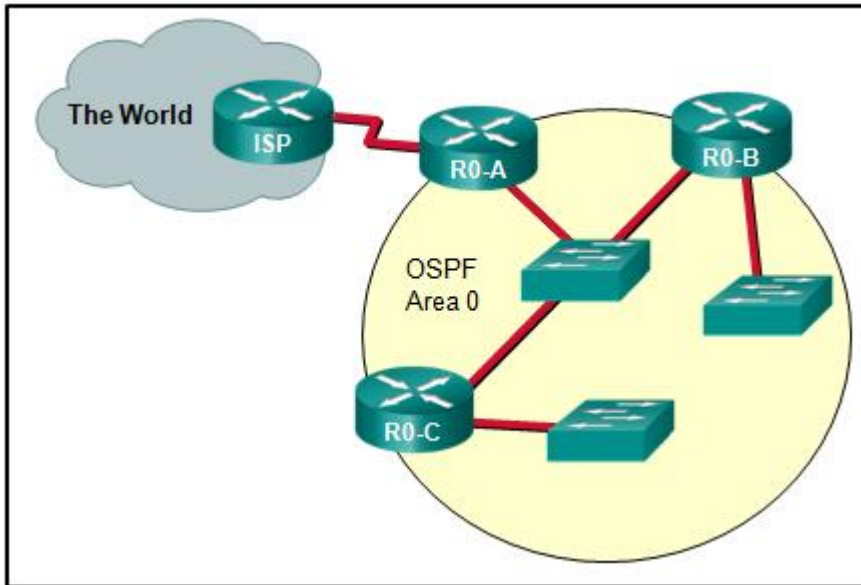
- L'interface Fa0/1 devrait être identifiée en tant qu'interface NAT externe.
- **L'interface S0/0/0 devrait être identifiée en tant qu'interface NAT externe.**
- La configuration ne dispose pas d'une liste de contrôle d'accès valide.
- L'instruction IP NAT est incorrecte.

Explication : L'interface S0/0/0 doit être identifiée comme l'interface NAT externe. La commande pour ce faire serait R2(config-if)# ip nat extérieur.

57. Une entreprise a conclu un contrat avec une entreprise de sécurité réseau pour aider à identifier les vulnérabilités du réseau d'entreprise. L'entreprise envoie une équipe pour effectuer des tests de pénétration sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des fuzzers?

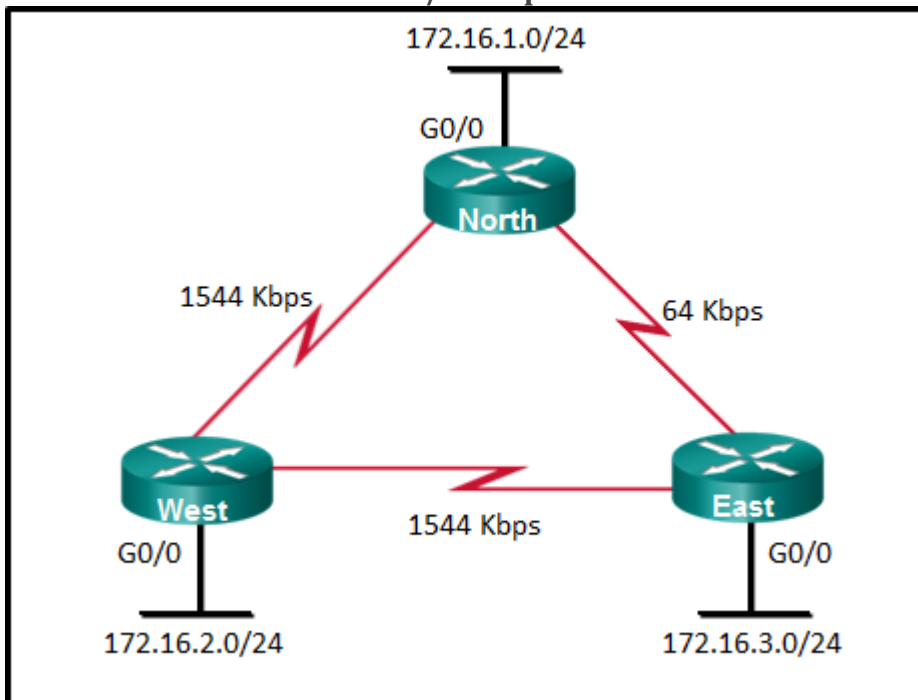
- pour inverser l'ingénierie des fichiers binaires lors de l'écriture d'exploits et lors de l'analyse de logiciels malveillants
- pour détecter les outils installés dans les fichiers et répertoires qui fournissent aux acteurs des menaces un accès à distance et un contrôle sur un ordinateur ou un réseau
- pour détecter toute preuve d'un piratage ou d'un programme malveillant dans un ordinateur ou un réseau
- **pour découvrir les vulnérabilités de sécurité d'un ordinateur**

58. Reportez-vous à l'illustration. Quelle méthode permet d'activer un routeur OSPF afin d'annoncer une route par défaut aux routeurs OSPF voisins ?



- **Utilisez la commande default-information originate sur R0-A.**
- Utilisez la commande redistribute static sur le routeur ISP.
- Utilisez la commande default-information originate sur le routeur ISP.
- Utilisez une route statique renvoyant vers le routeur ISP et redistribuez- la.
- Utilisez la commande redistribute static sur R0-A.

59. Reportez-vous à l'illustration. Quel est le coût de l'OSPF pour atteindre le réseau LAN Ouest 172.16.2.0/24 depuis l'Est?



- 782
- 74
- **65**
- 128

60. Reportez-vous à l'illustration. Quelles trois conclusions peut-on tirer de la sortie affichée? (Choisissez trois réponses.)

```
R3# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.3/28, Area 0, Attached via Network Statement
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0                1         no           nc           Base
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
```

<output omitted>

- Le BDR a trois voisins.
- L'ID du routeur sur le routeur DR est 3.3.3.3
- Il y a eu 9 secondes depuis le dernier paquet hello envoyé.
- Le DR peut être atteint via l'interface GigabitEthernet 0/0.
- Les valeurs d'ID du routeur n'étaient pas les critères utilisés pour sélectionner le DR et le BDR.
- Cette interface utilise la priorité par défaut.

61. Quel type de VPN implique un protocole de tunnel non sécurisé encapsulé par IPSec?

- VPN SSL
- **GRE sur IPsec**
- Interface de tunnel virtuel IPSec
- VPN multipoint dynamique

62. Reportez-vous à l'illustration. Un administrateur réseau souhaite ajouter une entrée ACE à la liste de contrôle d'accès TRAFFIC-CONTROL pour refuser le trafic IP du sous-réseau 172.23.16.0/20. Quelle entrée ACE répond à cette exigence ?

```
Router1# show access-lists
standard IP access list TRAFFIC-CONTROL
  10 permit 172.23.0.0, wildcard bits 0.0.255.255
  20 deny any
```

- 30 deny 172.23.16.0 0.0.15.255
- 5 deny 172.23.16.0 0.0.255.255
- 15 deny 172.23.16.0 0.0.15.255
- **5 deny 172.23.16.0 0.0.15.255**

63. Un administrateur réseau établit une liste de contrôle d'accès standard qui interdira tout trafic venant du réseau 172.16.0.0/16 mais autorisera tous les autres trafics. Quelles sont les deux commandes à utiliser ? (Choisissez deux réponses.)

- Router(config)# access-list 95 172.16.0.0 255.255.255.255
- Router(config)# access-list 95 host 172.16.0.0
- Router(config)# access-list 95 deny any
- Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0

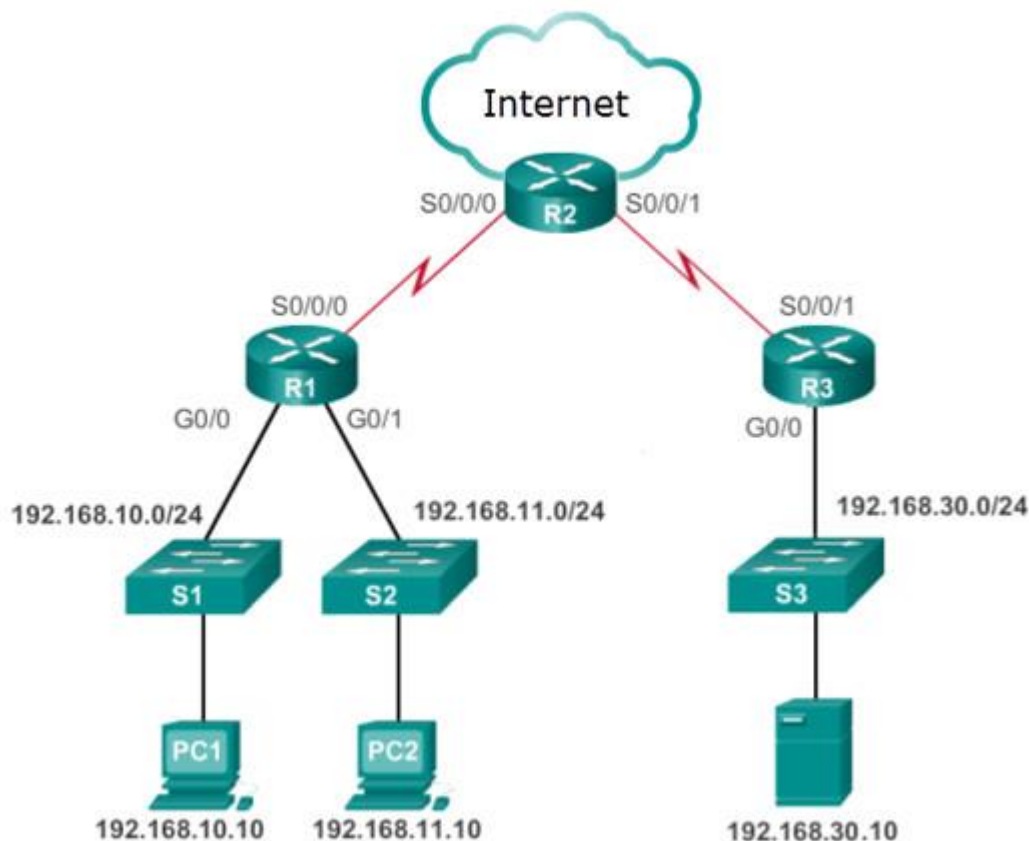
- **Router(config)# access-list 95 permit any**
- **Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255**

_Explique : Pour refuser le trafic du réseau 172.16.0.0/16, la commande `_access-list 95 deny 172.16.0.0 0.0.255.255` est utilisée. Pour autoriser tout autre trafic, l'instruction `_access-list 95 allow any` est ajoutée.

64. Pour le dépannage, quelle approche un administrateur réseau chevronné privilégiera-t-il contrairement à un administrateur réseau moins expérimenté ?

- **une approche moins structurée reposant sur des déductions que permettent l'expérience**
- une approche structurée qui débute avec l'examen de la couche physique avec progression ascendante dans les couches du modèle OSI jusqu'à ce que l'origine du problème soit identifiée
- une approche qui débute avec l'examen des applications des utilisateurs avec progression descendante dans les couches du modèle OSI jusqu'à ce que l'origine du problème soit identifiée
- la comparaison des composants qui fonctionnent et ceux qui ne fonctionnent pas pour déterminer les différences significatives

65. Reportez-vous à l'illustration. L'administrateur réseau a une adresse IP 192.168.11.10 et a besoin d'un accès pour gérer R1. Quel est le meilleur type et placement ACL à utiliser dans cette situation?



- **ACL entrante standard sur les lignes R1 vty**
- ACL étendues entrantes sur R1 G0/0 et G0/1
- ACL entrante standard sur l'interface WAN R2 se connectant à l'internet
- ACL sortante étendue sur R2 S0/0/1

_Explique : les ACL standard autorisent ou refusent les paquets en fonction uniquement de l'adresse IPv4 source. Étant donné que tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situées aussi près que possible de la destination.

Les ACL étendues autorisent ou refusent les paquets en fonction de l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination, etc. Étant donné que le filtrage des ACL étendues est si spécifique, les ACL étendues doivent être situées aussi près que possible de la source du trafic à filtrer. Le trafic indésirable est refusé à proximité du réseau source sans traverser l'infrastructure réseau.

66. Quelle table OSPF est identique sur tous les routeurs convergents dans la même zone OSPF?

- neighbor
- contiguïté
- routage
- **topologie**

67. Deux routeurs compatibles OSPF sont connectés via une liaison point à point. Pendant l'état ExStart, quel routeur sera choisi comme premier à envoyer des paquets DBD?

- le routeur avec l'ID de routeur le plus bas
- le routeur avec l'adresse IP la plus basse sur l'interface de connexion
- le routeur avec l'adresse IP la plus élevée sur l'interface de connexion
- **le routeur avec l'ID de routeur le plus élevé**

_Expliquez : Dans l'état ExStart, les deux routeurs décident quel routeur enverra les paquets DBD en premier. Le routeur avec l'ID de routeur le plus élevé sera le premier routeur à envoyer des paquets DBD pendant l'état d'échange

68. Quelles sont les deux règles de syntaxe utiliser pour écrire un tableau JSON? (Choisissez deux réponses.)

- Un espace doit séparer chaque valeur du tableau.
- **Les valeurs sont placées entre crochets.**
- Le tableau ne peut inclure qu'un seul type de valeur.
- Un point-virgule sépare la clé et la liste des valeurs.
- **Chaque valeur du tableau est séparée par une virgule.**

69. Quel type d'API serait utilisé pour permettre aux vendeurs autorisés d'une organisation d'accéder aux données de vente internes à partir de leurs appareils mobiles?

- ouvrir
- public
- partenaire
- **privé**

70. Quels sont les deux types de connexions VPN ? (Choisissez deux propositions.)

- PPPoE
- **L'accès distant**
- Ligne louée
- **Site à site**
- Frame Relay

_Explique : PPPoE, les lignes louées et Frame Relay sont des types de technologie WAN, pas des types de connexions VPN.

71. Quels énoncés décrivent l'utilisation d'algorithmes asymétriques ? Citez-en deux.

- Les clés publiques et privées peuvent être utilisées de manière interchangeable.
- Si une clé privée est utilisée pour chiffrer les données, une clé du même type doit également être utilisée pour les déchiffrer.
- **Si une clé publique est utilisée pour chiffrer les données, une clé privée doit être utilisée pour les déchiffrer.**
- **Si une clé privée est utilisée pour chiffrer les données, une clé publique doit être utilisée pour les déchiffrer.**
- Si une clé publique est utilisée pour chiffrer les données, une clé du même type doit également être utilisée pour les déchiffrer.

72. Pouvez-vous citer une caractéristique d'un cheval de Troie sur le plan de la sécurité du réseau ?

- D'énormes quantités de données sont envoyées à une interface de périphérique réseau en particulier.
- Trop d'informations sont adressées à un bloc mémoire en particulier, ce qui a pour effet d'affecter d'autres zones de mémoire.
- Un dictionnaire électronique est utilisé pour obtenir un mot de passe qui servira à infiltrer un périphérique réseau essentiel.
- **Un programme malveillant est dissimulé dans un programme exécutable d'apparence légitime.**

Explication : Un cheval de Troie effectue des opérations malveillantes sous couvert d'un programme légitime. Les attaques par déni de service envoient des quantités extrêmes de données à un hôte particulier ou à une interface de périphérique réseau. Les attaques par mot de passe utilisent des dictionnaires électroniques pour tenter d'apprendre les mots de passe. Les attaques par débordement de tampon exploitent les tampons de mémoire en envoyant trop d'informations à un hôte pour rendre le système inutilisable.

73. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une entrée unique:

`access-list 210 permit tcp 172.18.20.0 0.0.31 172.18.20.32 0.0.0.31 eq ftp .`

Si un paquet avec une adresse source 172.18.20.14, une adresse de destination 172.18.20.40 et un protocole 21 est reçu sur l'interface, le paquet est-il autorisé ou refusé?

- **Autorisé**
- refusé

74. Reliez les types de périphérique ou de service WAN à leur description. (Les options ne doivent pas être toutes utilisées.)

CPE	service provider facility that connects the CPE to the provider network
DCE	
DTE	devices and inside wiring that are located on the enterprise edge and connect to a carrier link
local loop	CPE
	a physical connection from the customer to the service provider POP
	local loop
	location where the responsibility for the connection changes from the customer to the service provider
	customer devices that pass the data from a customer network for transmission over the WAN
	DTE
	devices that provide an interface for customers to connect to within the WAN cloud
	DCE

CPE —> périphériques et câblage intérieur situés à la périphérie de l'entreprise et connectés à une liaison opérateur

DCE —> appareils qui fournissent une interface à laquelle les clients peuvent se connecter dans le cloud WAN

DTE —> dispositifs clients qui transmettent les données d'un réseau client pour transmission sur le WAN

boucle locale —> une connexion physique du client au fournisseur de services POP

75. Quel type de trafic est décrit comme étant capable de tolérer un certain temps de latence, de gigue et de perte sans effets perceptibles ?

- **Voix**
- Données
- Vidéo

76. Un administrateur configure OSPF à zone unique sur un routeur. L'un des réseaux qui doivent être annoncés est 192.168.0.0 255.255.252.0. Quel masque générique l'administrateur utiliserait-il dans l'instruction réseau OSPF?

- **0.0.3.255**
- 0.0.0.7
- 0.0.63.255
- 0.0.0.3

77. Un technicien réseau est en train de configurer SNMPv3 et a défini un niveau de sécurité d'authentification. Quel est l'effet de ce paramètre?

- authentifie un paquet à l'aide des algorithmes HMAC MD5 ou HMAC SHA et crypte le paquet avec les algorithmes DES, 3DES ou AES
- **authentifie un paquet en utilisant soit la méthode HMAC avec MD5, soit la méthode SHA**
- authentifie un paquet par une correspondance de chaîne du nom d'utilisateur ou de la chaîne de communauté
- authentifie un paquet en utilisant uniquement l'algorithme SHA

Explication : Pour activer SNMPv3, l'un des trois niveaux de sécurité peut être configuré :

- 1) pas d'authentification
- 2) authentification
- 3) privé

Le niveau de sécurité configuré détermine les algorithmes de sécurité appliqués aux paquets SNMP. Le niveau de sécurité d'authentification utilise HMAC avec MD5 ou SHA.

78. Qu'est-ce qui caractérise un hyperviseur de type 2 ?

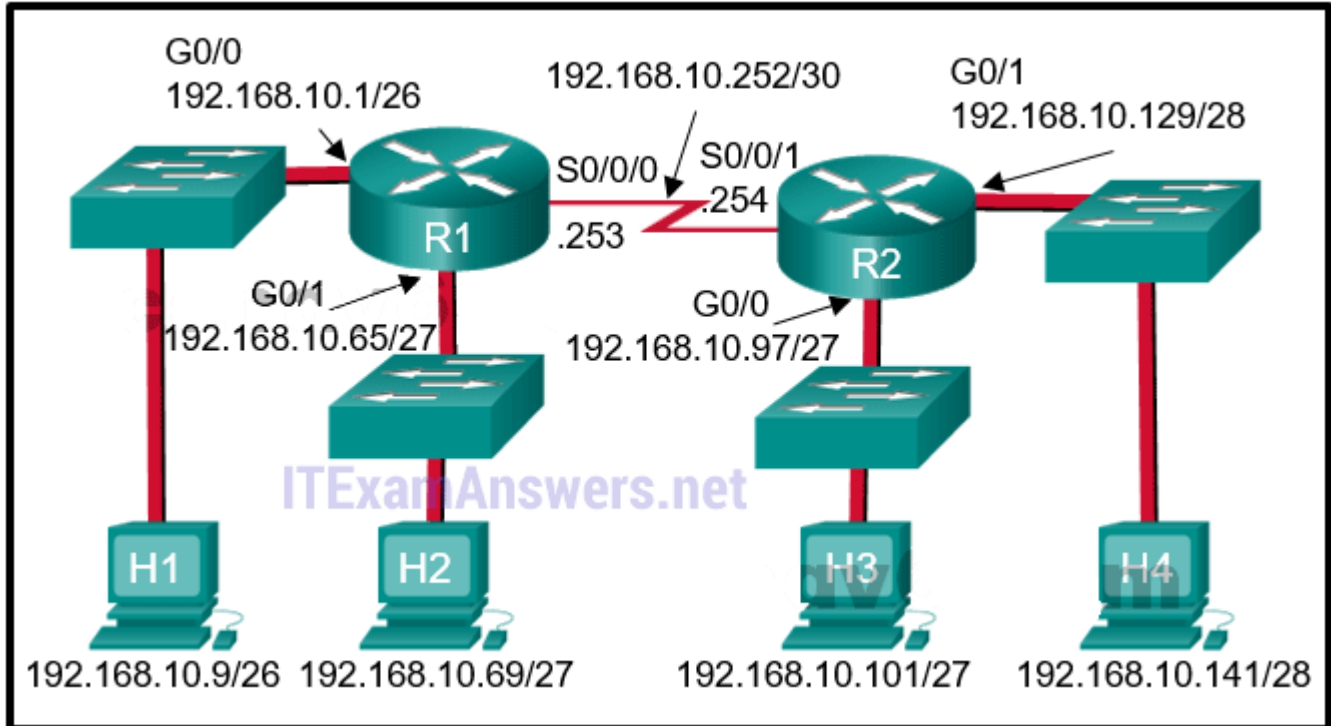
- il convient mieux aux environnements des entreprises
- il est installé directement dans le matériel
- **ne nécessite pas de logiciel de console de gestion**
- il présente un accès direct aux ressources matérielles du serveur

79. Un data center a récemment mis à jour un serveur physique pour héberger plusieurs systèmes d'exploitation sur un seul processeur. Le data center peut désormais fournir un serveur Web distinct à chaque client sans avoir à allouer un serveur réel distinct à chaque client. Quelle est la tendance liée au réseau qui est implémentée par le data center dans cette situation ?

- BYOD
- Garantir l'intégrité des communications
- **virtualisation**

- Collaboration en ligne

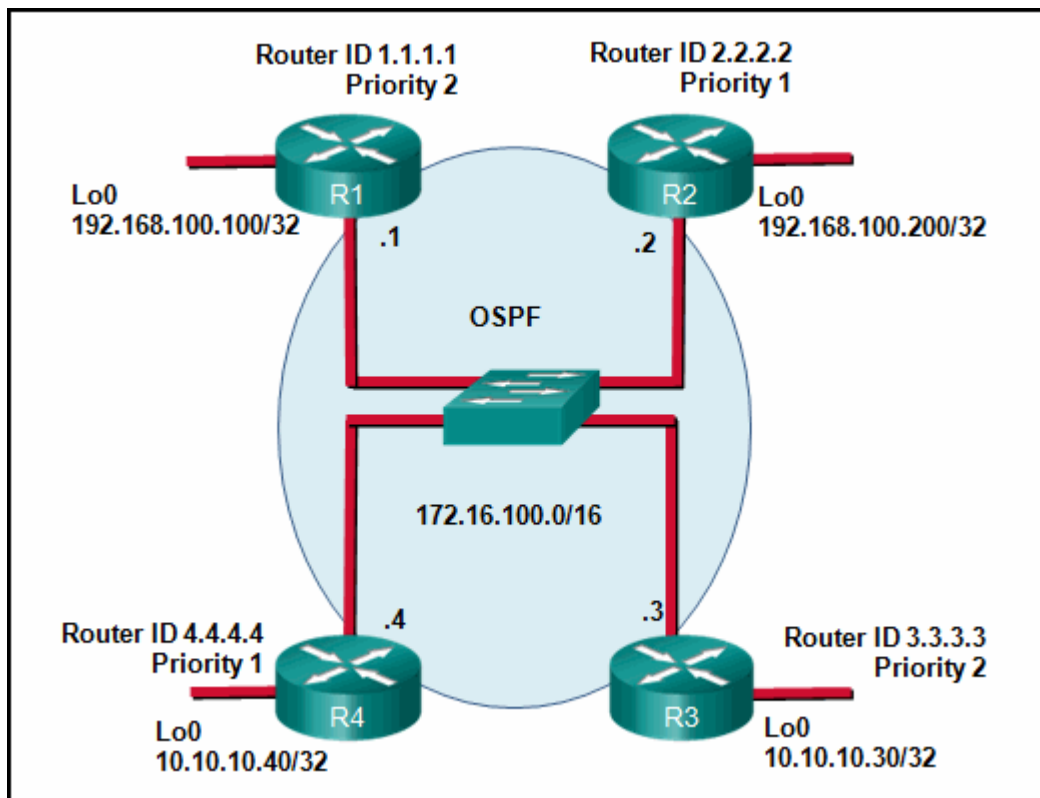
80. Reportez-vous à l'illustration. Si l'administrateur réseau a créé une liste de contrôle d'accès standard qui autorise uniquement les périphériques connectés à l'accès réseau de l'interface G0/0 de R2 à se brancher aux périphériques de l'interface G0/1 de R1, comment la liste de contrôle d'accès doit-elle être appliquée ?



- **en sortie sur l'interface G0/1 de R1**
- en sortie sur l'interface S0/0/1 de R2
- en entrée sur l'interface G0/0 de R2
- en entrée sur l'interface G0/1 de R1

Explication : Étant donné que les listes d'accès standard ne filtrent que sur l'adresse IP source, elles sont généralement placées au plus près du réseau de destination. Dans cet exemple, les paquets source proviendront du réseau R2 G0/0. La destination est le réseau R1 G0/1. Le placement correct d'ACL est sortant sur l'interface R1 G0/1.

81. Reportez-vous à l'illustration. Si le commutateur redémarre et que tous les routeurs doivent rétablir les adjacences OSPF, quels routeurs deviendront les nouveaux DR et BDR ?



- Le routeur R4 deviendra le DR et le routeur R3 deviendra le BDR.
- Le routeur R2 deviendra le DR et le routeur R1 deviendra le BDR.
- **Le routeur R3 deviendra DR et le routeur R2 deviendra BDR.**
- Le routeur R1 deviendra le DR et le routeur R2 deviendra le BDR.

Explique : les élections OSPF d'un DR sont basées sur les éléments suivants par ordre de priorité :

- priorité la plus élevée de 1 à 255 (0 = jamais un DR)
- ID de routeur le plus élevé
- l'adresse IP la plus élevée d'un bouclage ou d'une interface active en l'absence d'ID de routeur configuré manuellement. Les adresses IP de bouclage ont une priorité plus élevée que les autres interfaces.

Dans ce cas, les routeurs R3 et R1 ont la priorité de routeur la plus élevée. Entre les deux, R3 a l'ID de routeur le plus élevé. Par conséquent, R3 deviendra le DR et R1 deviendra le BDR.

82. Un routeur OSPF a trois réseaux directement connectés: 10.0.0.0/16, 10.1.0.0/16 et 10.2.0.0/16. Quelle commande réseau OSPF annoncerait uniquement le réseau 10.1.0.0 aux voisins?

- router(config-router)# network 10.1.0.0 255.255.255.0 area 0
- router(config-router)# network 10.1.0.0 0.0.0.0 area 0
- **router(config-router)# network 10.1.0.0 0.0.255.255 area 0**
- router(config-router)# network 10.1.0.0 0.0.15.255 area 0

83. Toute entreprise a décidé de réduire son empreinte environnementale en réduisant les coûts énergétiques, en déménageant dans une installation plus petite et en favorisant le télétravail. Quel service ou quelle technologie permettrait de répondre à cette exigence ?

- **services de cloud**
- ACI Cisco

- data center
- APIC-EM

84. Quel protocole synchronise avec une horloge maître privée ou avec un serveur accessible au public sur l'internet?

- MPLS
- TFTP
- **Protocole NTP**
- CBWFQ

85. Quelle étape du processus de routage d'état de liaison est décrite par un routeur exécutant un algorithme pour déterminer le meilleur chemin vers chaque destination?

- **exécution de l'algorithme SPF**
- déclarer un voisin inaccessible
- sélection de l'ID du routeur
- création de la table de topologie

86. Le trafic vidéo a ses caractéristiques propres. Citez-en deux. (Choisissez deux propositions.)

- **Le trafic vidéo est imprévisible et fluctuant.**
- Le trafic vidéo consomme moins de ressources de réseau que le trafic vocal.
- Le trafic vidéo nécessite un minimum de 30 kbit/s de bande passante.
- Le trafic vidéo est plus résilient à la perte que le trafic vocal.
- **La latence du trafic vidéo doit être inférieure à 400 ms.**

87. Examinez l'illustration. Un PC à l'adresse 10.1.1.45 ne peut pas accéder à Internet. Quelle est la cause la plus probable du problème ?

```
R1# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 33, occurred 00:00:46 ago
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0
Hits: 42 Misses: 0
CEF Translated packets: 42, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NATPOOL refcount 4
  pool NATPOOL: netmask 255.255.255.224
    start 209.165.201.10 end 209.165.201.11
    type generic, total addresses 2, allocated 2 (100%), misses 0

R1# show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
icmp 209.165.201.10:6  10.1.1.33:6          209.165.200.226:6   209.165.200.226:6
--- 209.165.201.10    10.1.1.33            ---                  ---
icmp 209.165.201.11:3  10.1.1.123:3         209.165.200.226:3   209.165.200.226:3
--- 209.165.201.11    10.1.1.123          ---                  ---
```

- **Le pool NAT est épuisé.**
- La liste de contrôle d'accès ACL 1 n'a pas été correctement configurée.
- Le masque de réseau incorrect a été utilisé sur le pool NAT.
- Les interfaces interne et externe ont été configurées à l'envers.

_Explique : La sortie des statistiques de show ip nat indique qu'il y a 2 adresses au total et que 2 adresses ont été allouées (100 %). Cela indique que le pool NAT n'a plus d'adresses globales pour donner de nouveaux clients. D'après les traductions de show ip nat, les PC aux adresses 10.1.1.33 et 10.1.1.123 ont utilisé les deux adresses disponibles pour envoyer des messages ICMP à un hôte sur le réseau extérieur.

88. Reportez-vous à l'illustration. Quelle(s) adresse(s) représente(nt) l'adresse globale interne ?

```
Router1 (config)# ip nat inside source static 192.168.0.100 209.165.20.25
Router1 (config)# interface serial0/0/0
Router1 (config-if)# ip nat inside
Router1 (config-if)# ip address 10.1.1.2 255.255.255.0
Router1 (config)# interface serial 0/0/2
Router1 (config-if)# ip address 209.165.20.25 255.255.255.0
Router1 (config-if)# ip nat outside
```

- Toute adresse dans le réseau 10.1.1.0
- 192.168.0.100
- **209.165.20.25**
- 10.1.1.2

_9. Un administrateur réseau a été chargé de créer un plan de reprise après sinistre. Dans le cadre de ce plan, l'administrateur recherche un site de sauvegarde pour toutes les données sur les serveurs de l'entreprise. Quel service ou technologie répondrait à cette exigence ?

- **centre de données**
- virtualisation
- serveurs dédiés
- réseau défini par logiciel

_13. Un client a besoin d'une connexion WAN de zone métropolitaine qui fournit une bande passante dédiée à haut débit entre deux sites. Quel type de connexion WAN répondrait le mieux à ce besoin ?

- réseau à commutation de paquets
- **réseau étendu Ethernet**
- réseau à commutation de circuits
- MPLS

_14. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise.

Pourquoi l'équipe utiliserait-elle des débogueurs ?

- pour détecter les outils installés dans les fichiers et les répertoires qui permettent aux pirates d'accéder et de contrôler à distance un ordinateur ou un réseau
- **pour désosser les fichiers binaires lors de l'écriture d'exploits et de l'analyse de logiciels malveillants**
- pour obtenir des systèmes d'exploitation spécialement conçus et préchargés avec des outils optimisés pour le piratage
- pour détecter toute preuve de piratage ou de logiciel malveillant dans un ordinateur ou un réseau

_15. Considérez la sortie suivante pour une ACL qui a été appliquée à un routeur via la commande access-class in. Que peut déterminer un administrateur réseau à partir du résultat affiché ?

```
R1#  
Liste d'accès IP standard 2  
10 permis 192.168.10.0, bits génériques 0.0.0.255 (2 correspondances)  
20 deny any (1 match)
```

- Deux appareils connectés au routeur ont des adresses IP de 192.168.10. x .
- **Deux appareils ont pu utiliser SSH ou Telnet pour accéder au routeur.**
- Le trafic d'un appareil n'était pas autorisé à entrer dans un port de routeur et à être acheminé vers un port de routeur différent.
- Le trafic provenant de deux appareils était autorisé à entrer dans un port de routeur et à être acheminé vers un port de routeur différent.

_Explique : La commande access-class est utilisée uniquement sur les ports VTY. Les ports VTY prennent en charge le trafic Telnet et/ou SSH. Le match permit ACE correspond au nombre de tentatives autorisées à l'aide des ports VTY. Le match deny ACE indique qu'un périphérique d'un réseau autre que 192.168.10.0 n'a pas été autorisé à accéder au routeur via les ports VTY.

_16. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour effacer les entrées dynamiques avant l'expiration du délai ?

- effacer l'ip dhcp
- **traduction ip nat claire**
- effacer les compteurs de liste d'accès
- effacer les statistiques ip pat

_19. Lors de la configuration d'un réseau de petite entreprise, l'administrateur réseau décide d'attribuer dynamiquement des adresses IP privées aux postes de travail et aux appareils mobiles. Quelle fonctionnalité doit être activée sur le routeur de l'entreprise pour que les appareils de bureau accèdent à Internet ?

- UPnP
- Filtrage MAC
- **NAT**
- Qualité de service

_Explique : La traduction d'adresses réseau (NAT) est le processus utilisé pour convertir des adresses privées en adresses routables sur Internet qui permettent aux appareils de bureau d'accéder à Internet.

_22. Quels sont les deux protocoles IPsec utilisés pour assurer l'intégrité des données ?

- **MD5**
- DH
- AES
- **SHA**
- RSA

_Explique : Le cadre IPsec utilise divers protocoles et algorithmes pour assurer la confidentialité des données, l'intégrité des données, l'authentification et l'échange de

clés sécurisé. Deux algorithmes populaires utilisés pour s'assurer que les données ne sont pas interceptées et modifiées (intégrité des données) sont MD5 et SHA. AES est un protocole de cryptage et assure la confidentialité des données. DH (Diffie-Hellman) est un algorithme utilisé pour l'échange de clés. RSA est un algorithme utilisé pour l'authentification.

_23. Si un hôte externe n'a pas le client Cisco AnyConnect préinstallé, comment l'hôte pourrait-il accéder à l'image client ?

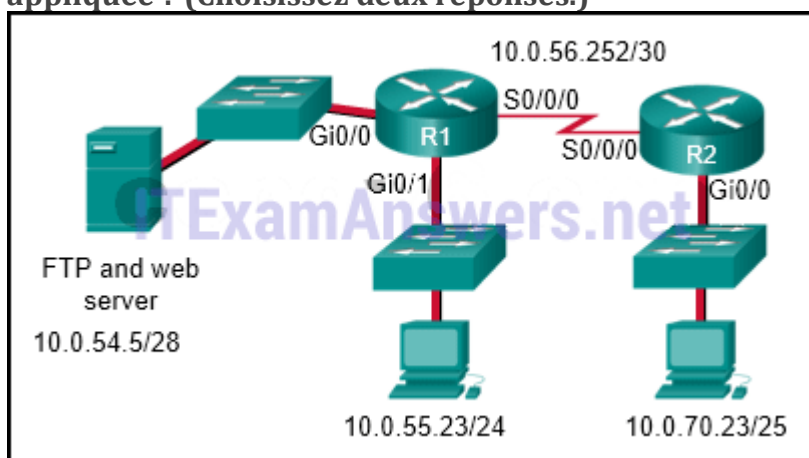
- Le client Cisco AnyConnect est installé par défaut sur la plupart des principaux systèmes d'exploitation.
- **L'hôte initie une connexion VPN sans client à l'aide d'un navigateur Web compatible pour télécharger le client.**
- L'hôte initie une connexion sans client à un serveur TFTP pour télécharger le client.
- L'hôte initie une connexion sans client à un serveur FTP pour télécharger le client.

_Explique : Si un hôte externe n'a pas le client Cisco AnyConnect préinstallé, l'utilisateur distant doit initier une connexion VPN SSL sans client via un navigateur Web conforme, puis télécharger et installer AnyConnect client sur l'hôte distant.

_24. Une entreprise envisage de mettre à jour la connexion WAN du campus. Quelles sont les deux options WAN qui sont des exemples d'architecture WAN privée ? (Choisissez deux réponses.)

- **ligne louée**
- câble
- ligne d'abonné numérique
- **réseau étendu Ethernet**
- Wi-Fi municipal

_27. Reportez-vous à l'illustration. L'administrateur réseau dont l'adresse IP est 10.0.70.23/25 doit avoir accès au serveur FTP de l'entreprise (10.0.54.5/28). Le serveur FTP est également un serveur Web accessible à tous les employés internes sur les réseaux au sein de l'adresse 10.x.x.x. Aucun autre trafic ne doit être autorisé vers ce serveur. Quelle liste de contrôle d'accès étendue serait utilisée pour filtrer ce trafic et comment cette liste de contrôle d'accès serait-elle appliquée ? (Choisissez deux réponses.)



```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 105 out
```

```
R2(config)# interface gi0/0
R2(config-if)# ip access-group 105 in
```

```
access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20
liste d'accès 105 permis hôte tcp 10.0.70.23 hôte 10.0.54.5 eq 21
liste d'accès 105 permis tcp 10.0.0.0 0.255.255.255 hôte 10.0.54.5 eq www
liste d'accès 105 refuser ip n'importe quel hôte 10.0.54.5
access-list 105 permit ip any any
```

```
liste d'accès 105 permis ip hôte 10.0.70.23 hôte 10.0.54.5
access-list 105 permit tcp any host 10.0.54.5 eq www
liste d'accès 105 permis ip tout tout
```

```
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out
```

```
access-list 105 permit tcp host 10.0.54.5 any eq www
liste d'accès 105 permis hôte tcp 10.0.70.23 hôte 10.0.54.5 eq 20
liste d'accès 105 permis hôte tcp 10.0.70.23 hôte 10.0.54.5 eq 21
```

Explication : Les deux premières lignes de l'ACL autorisent l'accès FTP de l'hôte 10.0.70.23 au serveur dont l'adresse IP est 10.0.54.5. La ligne suivante de l'ACL autorise l'accès HTTP au serveur à partir de n'importe quel hôte dont l'adresse IP commence par le chiffre 10. La quatrième ligne de l'ACL refuse tout autre type de trafic vers le serveur à partir de n'importe quelle adresse IP source. La dernière ligne de l'ACL autorise toute autre chose au cas où d'autres serveurs ou périphériques seraient ajoutés au réseau 10.0.54.0/28. Étant donné que le trafic est filtré à partir de tous les autres emplacements et pour le périphérique hôte 10.0.70.23, le meilleur endroit pour placer cette ACL est le plus proche du serveur.

_32. Reportez-vous à l'illustration. Un administrateur réseau est en train de configurer une ACL pour limiter la connexion aux lignes vty R1 aux seuls postes de travail du groupe informatique du réseau 192.168.22.0/28. L'administrateur vérifie les connexions Telnet réussies d'un poste de travail avec IP 192.168.22.5 à R1 avant que l'ACL ne soit appliquée. Cependant, une fois l'ACL appliquée à l'interface Fa0/0, les connexions Telnet sont refusées. Quelle est la cause de

l'échec de la connexion ?

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# access-list 120 deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255
R1(config)# access-list 120 permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq 23
R1(config)# access-list 120 permit ip any any
R1(config)# line vty 0 4
R1(config-line)# password admin-in
R1(config-line)# access-class 120 in
R1(config-line)# exit
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 10.0.10.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# ip access-group 120 in
R1(config-if)# end
R1#

R1# show access-lists
Extended IP access list 120
  deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255 (16 match(es))
  permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq telnet
  permit ip any any
R1#
```

- L'activation du mot de passe secret n'est pas configurée sur R1.
- **Le réseau du groupe informatique est inclus dans l'instruction de refus.**
- Le permis ACE spécifie un numéro de port erroné.
- L'ACE d'autorisation doit spécifier l'adresse IP du protocole au lieu de tcp.
- La commande de connexion n'a pas été saisie pour les lignes vty.

_Explication : La plage d'adresses IP source dans l'ACE de refus est 192.168.20.0 0.0.3.255, qui couvre les adresses IP de 192.168.20.0 à 192.168.23.255. Le réseau du groupe informatique 192.168.22.0/28 est inclus dans le réseau 192.168.20/22. Par conséquent, la connexion est refusée. Pour résoudre ce problème, l'ordre des ACE de refus et d'autorisation doit être inversé.

_33. Quelle fonctionnalité mGRE fournit-il à la technologie DMVPN ?

- **Il permet la création de tunnels alloués dynamiquement via une source de tunnel permanente au niveau du concentrateur et des destinations de tunnel alloués dynamiquement au niveau des rayons.**
- Il assure le transport sécurisé d'informations privées sur des réseaux publics, tels qu'Internet.
- Il s'agit d'une solution logicielle Cisco permettant de créer plusieurs VPN de manière simple, dynamique et évolutive.
- Il crée une base de données de cartographie distribuée des adresses IP publiques pour tous les rayons du tunnel VPN.

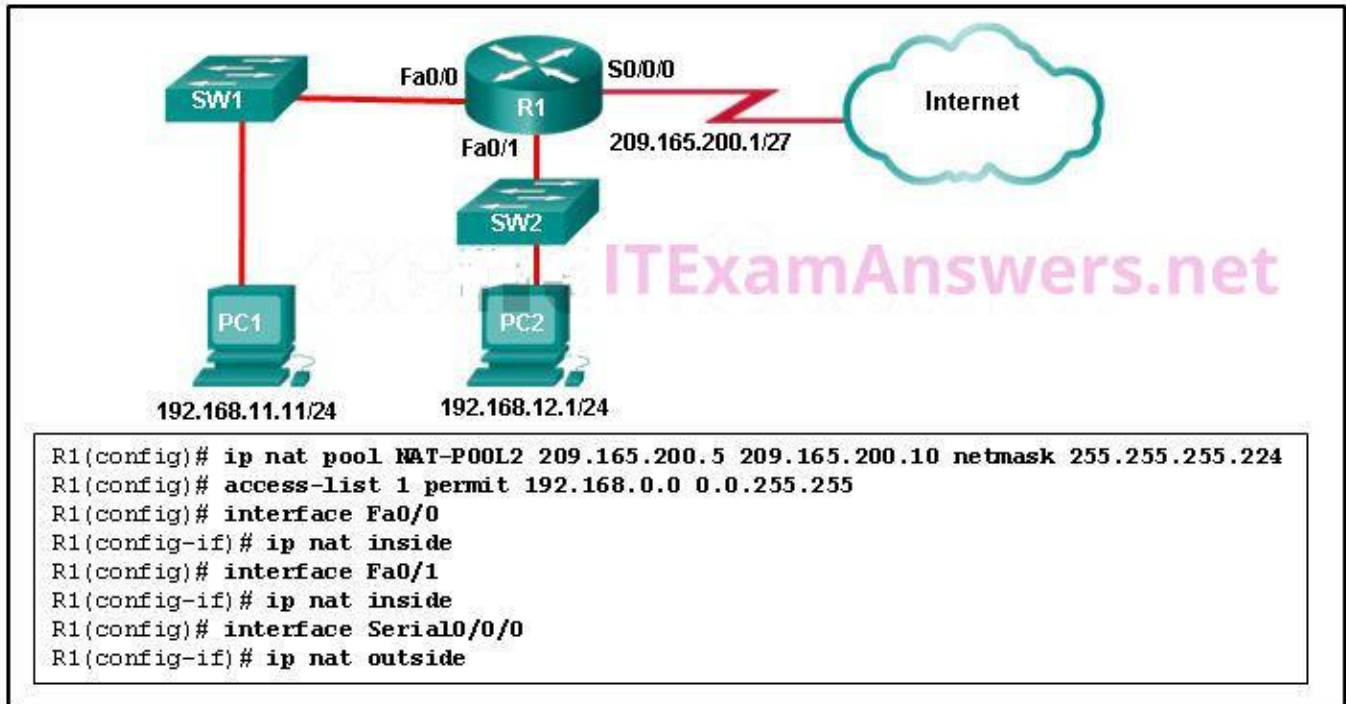
_Explication : DMVPN est construit sur trois protocoles, NHRP, IPsec et mGRE. NHRP est le protocole de mappage d'adresse distribué pour les tunnels VPN. IPsec crypte les communications sur les tunnels VPN. Le protocole mGRE permet la création dynamique de plusieurs tunnels en étoile à partir d'un hub VPN permanent.

_34. Qu'est-ce qui est utilisé pour préremplir la table de contiguïté sur les périphériques Cisco qui utilisent CEF pour traiter les paquets ?

- le FIB
- la table de routage
- **le tableau ARP**

- le DSP

_39. Reportez-vous à l'illustration. R1 est configuré pour NAT comme affiché. Quel est le problème avec la configuration ?



- **NAT-POOL2 n'est pas lié à ACL 1.**
- L'interface Fa0/0 doit être identifiée comme une interface NAT externe.
- Le pool NAT est incorrect.
- La liste d'accès 1 est mal configurée.

Explication : R1 doit avoir NAT-POOL2 lié à ACL 1. Ceci est accompli avec la commande R1(config)#ip nat inside source list 1 pool NAT-POOL2. Cela permettrait au routeur de vérifier tout le trafic intéressant et s'il correspond à ACL 1, il serait traduit en utilisant les adresses dans NAT-POOL2.

_41. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des applications telles que John the Ripper, THC Hydra, RainbowCrack et Medusa ?

- pour capturer et analyser les paquets dans les LAN Ethernet traditionnels ou les WLAN
- pour sonder et tester la robustesse d'un pare-feu en utilisant des paquets falsifiés spécialement créés
- **pour faire des suppositions répétées afin de déchiffrer un mot de passe**

_44. Un attaquant redirige le trafic vers une fausse passerelle par défaut pour tenter d'intercepter le trafic de données d'un réseau commuté. Quel type d'attaque pourrait y parvenir ?

- Inondation TCP SYN
- Tunnelisation DNS
- **Usurpation DHCP**
- Empoisonnement du cache ARP

Explication : dans les attaques d'usurpation DHCP, un attaquant configure un faux serveur DHCP sur le réseau pour émettre des adresses DHCP aux clients dans le

but de forcer les clients à utiliser une fausse passerelle par défaut, et autres faux services. La surveillance DHCP est une fonctionnalité du commutateur Cisco qui peut atténuer les attaques DHCP. La privation d'adresses MAC et l'espionnage d'adresses MAC ne sont pas des attaques de sécurité reconnues. L'usurpation d'adresse MAC est une menace pour la sécurité du réseau.

_46. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise.

Pourquoi l'équipe utiliserait-elle des renifleurs de paquets ?

- pour détecter les outils installés dans les fichiers et les répertoires qui permettent aux pirates d'accéder et de contrôler à distance un ordinateur ou un réseau
- pour détecter toute preuve de piratage ou de logiciel malveillant dans un ordinateur ou un réseau
- pour sonder et tester la robustesse d'un pare-feu en utilisant des paquets falsifiés spécialement créés
- **pour capturer et analyser les paquets dans les LAN Ethernet traditionnels ou les WLAN**

_48. Mettez en correspondance la méthode HTTP avec l'opération RESTful.

POST ->> Créer

OBTENIR ->> Lis

METTRE/PATCH ->> Mettre à jour/Remplacer ? Modifier

Delet ->> Supprimer

_50. Quelle est l'une des raisons d'utiliser la commande ip ospf priority lorsque le protocole de routage OSPF est utilisé ?

- pour activer le processus de voisinage OSPF
- **pour influencer le processus d'élection DR/BDR**
- fournir une porte dérobée pour la connectivité pendant le processus de convergence
- pour rationaliser et accélérer le processus de convergence

_52. Quelle est la caractéristique de la topologie spine-leaf à deux niveaux de l'architecture de fabric Cisco ACI ?

- Les commutateurs spine et leaf sont toujours liés via des commutateurs principaux.
- Les commutateurs de colonne se fixent aux commutateurs de feuille et s'attachent les uns aux autres pour la redondance.
- Les commutateurs à lames s'attachent toujours aux épines et ils sont reliés entre eux par une ligne principale.
- **Les commutateurs à lames s'attachent toujours aux épines, mais ils ne s'attachent jamais les uns aux autres.**

_53. Quels sont les deux scénarios qui entraîneraient une incompatibilité duplex ? (Choisissez deux réponses.)

- **connecter un appareil avec négociation automatique à un autre qui est manuellement réglé sur full-duplex**
- démarrage et arrêt d'une interface de routeur pendant une opération normale
- connecter un appareil avec une interface fonctionnant à 100 Mbps à un autre avec une interface fonctionnant à 1 000 Mbps
- configuration incorrecte du routage dynamique

- **régler manuellement les deux appareils connectés sur différents modes duplex**

_55. Quels sont les deux types d'attaques utilisées sur les résolveurs DNS ouverts ? (Choisissez deux réponses.)

- **amplification et réflexion**
- **utilisation des ressources**
- flux rapide
- Empoisonnement ARP
- amorti

_Explication : Trois types d'attaques utilisées sur les résolveurs ouverts DNS sont les suivants : Empoisonnement du cache DNS – l'attaquant envoie des informations falsifiées usurpées pour rediriger les utilisateurs de sites légitimes vers des sites malveillants

Attaques par amplification et réflexion DNS – l'attaquant envoie un volume accru d'attaques pour masquer la véritable source de l'attaque

Attaques d'utilisation des ressources DNS – une attaque par déni de service (DoS) qui consomme les ressources du serveur

_57. Quels types de ressources sont nécessaires pour un hyperviseur de type 1 ?

- un VLAN dédié
- **une console de gestion**
- un système d'exploitation hôte

_59. Quels sont les trois composants utilisés dans la partie requête d'une requête d'API RESTful typique ? (Choisissez trois réponses.)

- ressources
- protocole
- Serveur d'API
- **format**
- **clé**
- **paramètres**

_60. Un utilisateur signale que lorsque l'URL de la page Web de l'entreprise est entrée dans un navigateur Web, un message d'erreur indique que la page ne peut pas être affichée. Le technicien du service d'assistance demande à l'utilisateur d'entrer l'adresse IP du serveur Web pour voir si la page peut être affichée. Quelle méthode de dépannage est utilisée par le technicien ?

- descendant
- ascendant
- **diviser pour régner**
- remplacement

_61. Quel protocole fournit des services d'authentification, d'intégrité et de confidentialité et est un type de VPN ?

- MD5
- AES
- **IPsec**
- ESP

_62. Quelle affirmation décrit une caractéristique des commutateurs Cisco Catalyst 2960 ?

- Ils sont mieux utilisés comme commutateurs de couche de distribution.
- **Les nouveaux commutateurs Cisco Catalyst 2960-C prennent en charge l'intercommunication PoE.**

- Ce sont des commutateurs modulaires.
- Ils ne prennent pas en charge une interface virtuelle commutée (SVI) active avec les versions d'IOS antérieures à 15.x.

_63. Quel composant de l'architecture ACI traduit les règles d'application en programmation réseau ?

- l'hyperviseur
- **le contrôleur d'infrastructure de politique d'application**
- le commutateur Nexus 9000
- les points de terminaison du profil de réseau d'application

_64. Quelles sont les deux informations à inclure dans un diagramme de topologie logique d'un réseau ? (Choisissez deux réponses.)

- type d'appareil
- spécification du câble
- **identifiant d'interface**
- Version OS/IOS
- **type de connexion**
- type de câble et identifiant

_Explique : L'identifiant de l'interface et le type de connexion doivent être inclus dans un diagramme de topologie logique car ils indiquent quelle interface est connectée à d'autres appareils du réseau avec un type spécifique tel que LAN, WAN, point à point, etc. La version du système d'exploitation/IOS, le type d'appareil, le type et l'identifiant du câble et les spécifications du câble sont généralement inclus dans un diagramme de topologie physique.

_68. Dans un grand réseau d'entreprise, quelles sont les deux fonctions exécutées par les routeurs au niveau de la couche de distribution ? (Choisissez deux réponses.)

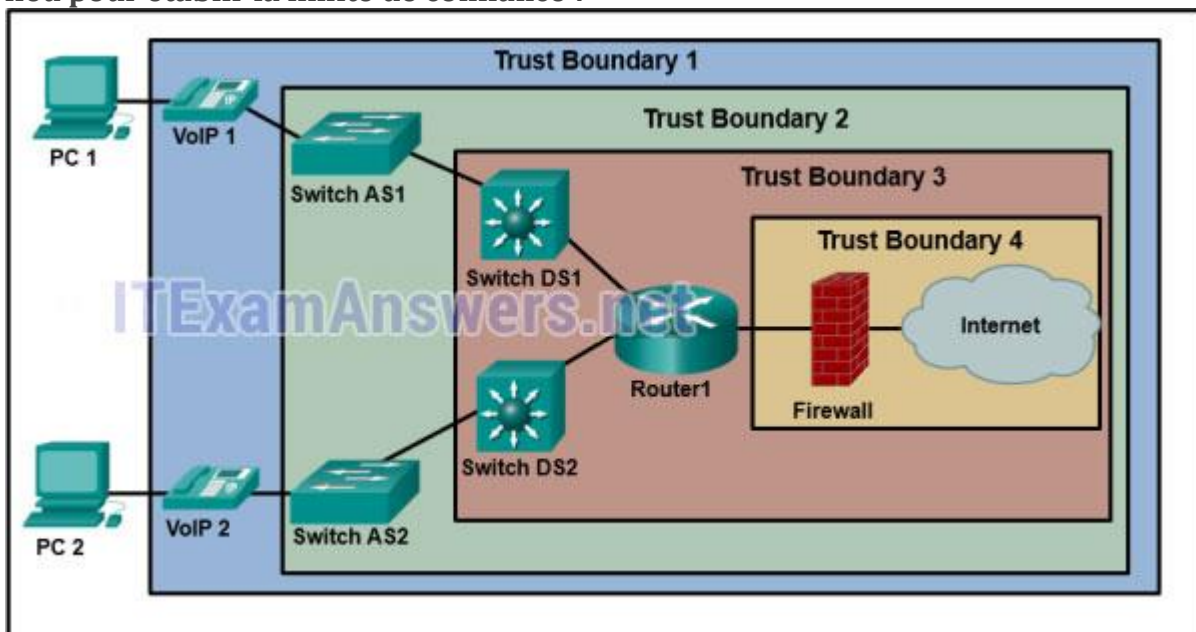
- connecter les utilisateurs au réseau
- fournir une dorsale de réseau haut débit
- **connecter des réseaux distants**
- fournir une alimentation par Ethernet aux appareils
- **assurer la sécurité du trafic de données**

_69. Quels sont les deux énoncés décrivant l'utilisation d'algorithmes asymétriques ? (Choisissez deux réponses.)

- Les clés publiques et privées peuvent être utilisées de manière interchangeable.
- Si une clé publique est utilisée pour chiffrer les données, une clé publique doit être utilisée pour déchiffrer les données.
- **Si une clé privée est utilisée pour chiffrer les données, une clé publique doit être utilisée pour déchiffrer les données.**
- **Si une clé publique est utilisée pour chiffrer les données, une clé privée doit être utilisée pour déchiffrer les données.**
- Si une clé privée est utilisée pour chiffrer les données, une clé privée doit être utilisée pour déchiffrer les données.

_Explique : Les algorithmes asymétriques utilisent deux clés : une clé publique et une clé privée. Les deux clés sont capables du processus de chiffrement, mais la clé correspondante complémentaire est requise pour le déchiffrement. Si une clé publique chiffre les données, la clé privée correspondante déchiffre les données. L'inverse est également vrai. Si une clé privée chiffre les données, la clé publique correspondante déchiffre les données.

_70. Reportez-vous à l'illustration. Un administrateur réseau a déployé QoS et a configuré le réseau pour marquer le trafic sur les téléphones VoIP ainsi que sur les commutateurs de couche 2 et de couche 3. Où le marquage initial doit-il avoir lieu pour établir la limite de confiance ?



- Frontière de confiance 4
- Frontière de confiance 3
- **Frontière de confiance 1**
- Frontière de confiance 2

Explique : Le trafic doit être classé et marqué aussi près que possible de sa source. La limite de confiance identifie à quel périphérique le trafic marqué doit être approuvé. Le trafic marqué sur les téléphones VoIP serait considéré comme fiable lorsqu'il se déplace vers le réseau de l'entreprise.

_71. Quels sont les deux avantages de l'extension de la connectivité de la couche d'accès aux utilisateurs via un support sans fil ? (Choisissez deux réponses.)

- **coûts réduits**
- diminution du nombre de points de défaillance critiques
- **flexibilité accrue**
- augmentation de la disponibilité de la bande passante
- plus d'options de gestion du réseau

_72. Quels sont les deux objectifs du lancement d'une attaque de reconnaissance sur un réseau ? (Choisissez deux réponses.)

- **pour rechercher l'accessibilité**
- pour récupérer et modifier des données
- **pour recueillir des informations sur le réseau et les appareils**
- pour empêcher d'autres utilisateurs d'accéder au système
- pour augmenter les privilèges d'accès

_74. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :

```
access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 192.31.7.45 eq dns .
```


_Si un paquet avec une adresse source de 10.1.1.201, une adresse de destination de 192.31.7.45 et un protocole de 23 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- autorisé
- **refusé**

_75. Reportez-vous à l'illustration. À partir de quel emplacement ce routeur a-t-il chargé l'IOS ?

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

<output omitted>

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router#
```

- **mémoire flash**
- NVRAM ?
- RAM
- ROM
- un serveur TFTP ?

_76. Reportez-vous à l'illustration. Quel format de données est utilisé pour représenter les données pour les applications d'automatisation de réseau ?

```
{
  "message": "success",
  "username": "jsmith01",
  "user_info": {
    "First_name": "John",
    "Last_name": "Smith"
  }
}
```

- XML
- YAML
- HTML
- **JSON**

_Explique : Les formats de données courants utilisés dans de nombreuses applications, y compris l'automatisation du réseau et la programmabilité, sont les suivants :

- **_JavaScript Object Notation (JSON)** : dans JSON, les données connues sous le nom d'objet sont une ou plusieurs paires clé/valeur entre accolades { }. Les clés doivent être des chaînes entre guillemets doubles " ". Les clés et les valeurs sont séparées par deux-points.
- **_Langage de balisage extensible (XML)** : en XML, les données sont incluses dans un ensemble de balises associées <tag>data</tag>.
- **_YAML n'est pas un langage de balisage (YAML)** : dans YAML, les données connues sous le nom d'objet sont constituées d'une ou de plusieurs paires clé/valeur. Les paires clé-valeur sont séparées par deux-points sans utiliser de guillemets. YAML utilise l'indentation pour définir sa structure, sans utiliser de crochets ni de virgules.

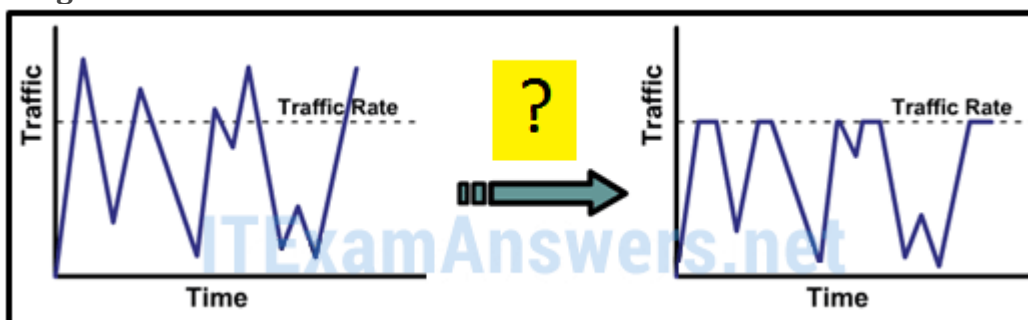
_77. Quelle étape QoS doit avoir lieu avant que les paquets puissent être marqués ?

- **classification**
- mise en forme
- faire la queue
- police

_79. Une entreprise doit interconnecter plusieurs succursales dans une zone métropolitaine. L'ingénieur réseau recherche une solution qui fournit un trafic convergé à haut débit, y compris la voix, la vidéo et les données sur la même infrastructure réseau. La société souhaite également une intégration facile à son infrastructure LAN existante dans ses bureaux. Quelle technologie recommander ?

- Frame Relay
- **réseau étendu Ethernet**
- VSAT
- RNIS

_80. Reportez-vous à l'illustration. Lorsque le trafic est transféré vers une interface de sortie avec traitement QoS, quelle technique d'évitement de congestion est utilisée ?



- mise en forme du trafic
- détection précoce aléatoire pondérée
- classification et marquage
- **contrôle de la circulation**

_Explique : La mise en forme du trafic met en mémoire tampon les paquets excédentaires dans une file d'attente, puis transfère le trafic sur des incréments de temps, ce qui crée un débit de sortie de paquets lissé. La régulation du trafic supprime le trafic lorsque la quantité de trafic atteint un débit maximal configuré, ce

qui crée un débit de sortie qui apparaît comme une dent de scie avec des crêtes et des creux.

_81. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :

```
access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 10.1.3.8 eq dns .
```

_Si un paquet avec une adresse source de 10.1.3.8, une adresse de destination de 10.10.3.8 et un protocole de 53 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- **refusé**
- autorisé

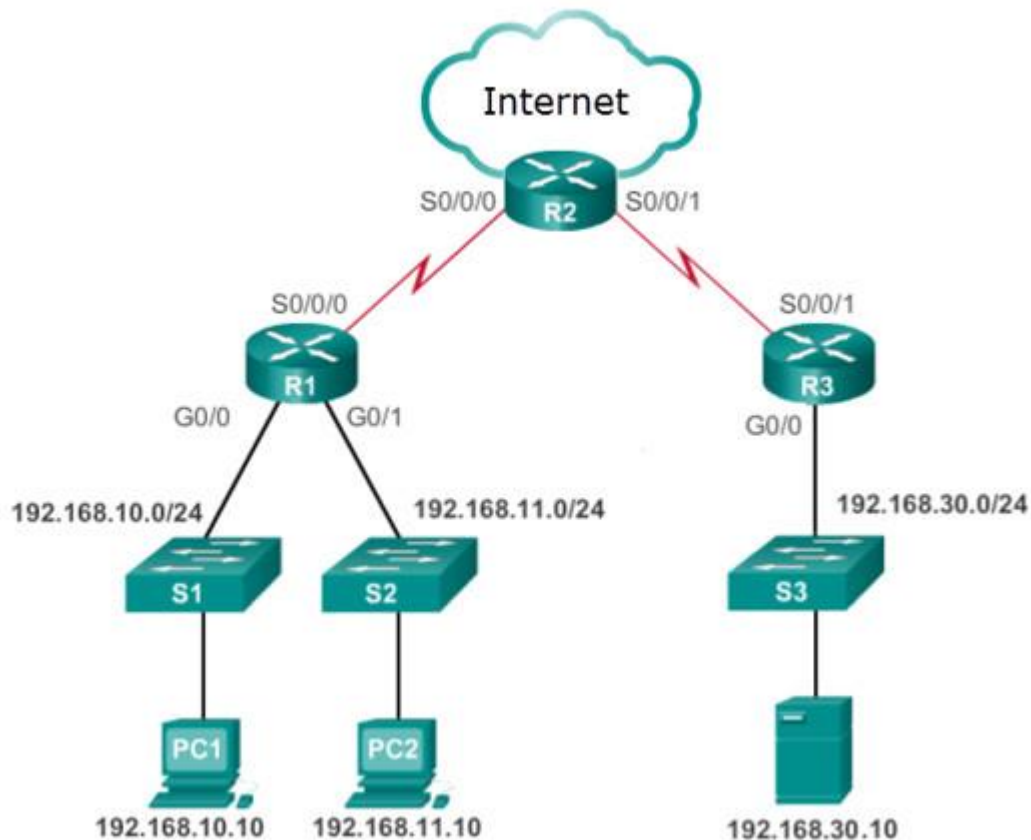
_82. Reportez-vous à l'illustration. À quoi sert la commande marquée d'une flèche affichée dans la sortie de configuration partielle d'un routeur haut débit Cisco ?

```
interface FastEthernet 0/0
ip address 10.10.10.1 255.255.255.0
ip nat inside
no cdp enable
hold-queue 32 in
hold-queue 100 out
!
interface FastEthernet 0/1
ip address dhcp
ip nat outside
no cdp enable
!
ip classless
ip http server
!
ip nat inside source list 102 interface fastethernet 0/1 overload
access-list 102 permit ip 10.10.10.0 0.0.0.255 any ←
no cdp run
!
```

- définit les adresses autorisées dans le routeur
- **définit les adresses pouvant être traduites**
- définit les adresses attribuées à un pool NAT
- définit les adresses autorisées à sortir du routeur

_86. Reportez-vous à l'illustration. De nombreux employés perdent le temps de l'entreprise à accéder aux médias sociaux sur leurs ordinateurs de travail. L'entreprise veut arrêter cet accès. Quel est le meilleur type et emplacement ACL à

utiliser dans cette situation ?



- LCA étendue sortante sur l'interface WAN R2 vers Internet
- ACL standard sortant sur l'interface WAN R2 vers Internet
- ACL standard sortant sur R2 S0/0/0
- **LCA étendues entrantes sur R1 G0/0 et G0/1**

_87. Reportez-vous à l'illustration. Un administrateur essaie de configurer PAT sur R1, mais PC-A ne parvient pas à accéder à Internet. L'administrateur tente d'envoyer une requête ping à un serveur sur Internet à partir de PC-A et collecte les débogages présentés dans l'exposition. D'après ce résultat, quelle est probablement la cause du problème ?

The screenshot shows a network diagram with PC-A connected to a switch, which is connected to router R1 (Fa0/1) and then to the Internet (Fa0/0). The IP address of the switch is 192.168.219.1/24 and the IP address of the Internet is 209.165.200.226/27. Below the diagram is a terminal window showing the output of the command 'R1# debug ip nat'.

```
R1# debug ip nat
*Jan 10 06:30:37.142: NAT*: s=192.168.219.22->209.165.201.10,
d=64.100.0.122 [24]
*Jan 10 06:30:37.150: NAT*: s=192.168.219.22->209.165.201.10,
d=64.100.0.122 [25]
*Jan 10 06:30:37.154: NAT*: s=192.168.219.22->209.165.201.10,
d=64.100.0.122 [26]
*Jan 10 06:30:37.158: NAT*: s=192.168.219.22->209.165.201.10,
d=64.100.0.122 [27]
*Jan 10 06:30:37.162: NAT*: s=192.168.219.22->209.165.201.10,
d=64.100.0.122 [28]
```

- Les entrelacs NAT intérieur et extérieur ont été configurés à l'envers
- **L'adresse globale interne n'est pas sur le même sous-réseau que le FAI**

- L'adresse sur Fa0/0 doit être 64.100.0.1.
- La liste d'accès source NAT correspond à la mauvaise plage d'adresses.

_Explique : La sortie de debug ip nat montre chaque paquet qui est traduit par le routeur. Le "s" est l'adresse IP source du paquet et le "d" est la destination. L'adresse après la flèche ("->") indique l'adresse traduite. Dans ce cas, l'adresse traduite se trouve sur le sous-réseau 209.165.201.0 mais l'interface faisant face au FAI se trouve dans le sous-réseau 209.165.200.224/27. Le FAI peut abandonner les paquets entrants ou ne pas être en mesure de réacheminer les paquets de retour vers l'hôte car l'adresse se trouve dans un sous-réseau inconnu.

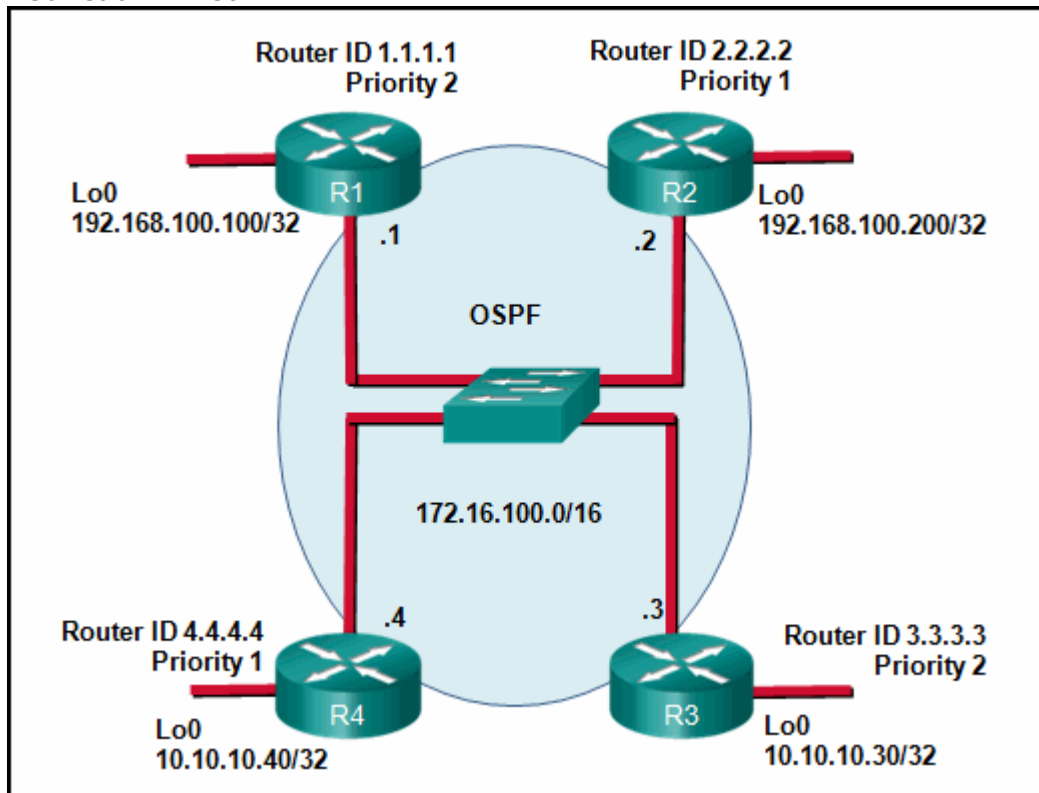
_90. Dans quel état OSPF l'élection DR/BDR est-elle effectuée ?

- ExStart
- Init
- **Bidirectionnel**
- Échange

_92. Quel est l'état opérationnel final qui se formera entre un DR OSPF et un DROTHER une fois que les routeurs auront atteint la convergence ?

- chargement
- établi
- **complet**
- bidirectionnel

_93. Reportez-vous à l'illustration. Si le commutateur redémarre et que tous les routeurs doivent rétablir les contiguïtés OSPF, quels routeurs deviendront les nouveaux DR et BDR ?



- **Le routeur R3 deviendra le DR et le routeur R1 deviendra le BDR.**
- Le routeur R4 deviendra le DR et le routeur R3 deviendra le BDR.
- Le routeur R1 deviendra le DR et le routeur R2 deviendra le BDR.
- Le routeur R3 deviendra le DR et le routeur R2 deviendra le BDR.

_Explique : les élections OSPF d'un DR sont basées sur les éléments suivants par ordre de priorité :

- priorité la plus élevée de 1 à 255 (0 = jamais un DR)
- ID de routeur le plus élevé
- l'adresse IP la plus élevée d'un bouclage ou d'une interface active en l'absence d'ID de routeur configuré manuellement. Les adresses IP de bouclage ont une priorité plus élevée que les autres interfaces.

Dans ce cas, les routeurs R3 et R1 ont la priorité de routeur la plus élevée. Entre les deux, R3 a l'ID de routeur le plus élevé. Par conséquent, R3 deviendra le DR et R1 deviendra le BDR.

_94. Quel type de serveur serait utilisé pour conserver un enregistrement historique des messages provenant des périphériques réseau surveillés ?

- DNS
- imprimer
- DHCP
- **syslog**
- authentification

_95. Lorsque QoS est implémenté dans un réseau convergé, quels sont les deux facteurs qui peuvent être contrôlés pour améliorer les performances du réseau pour le trafic en temps réel ? (Choisissez deux réponses.)

- adressage des paquets
- **délai**
- **jitter**
- routage de paquets
- vitesse de liaison

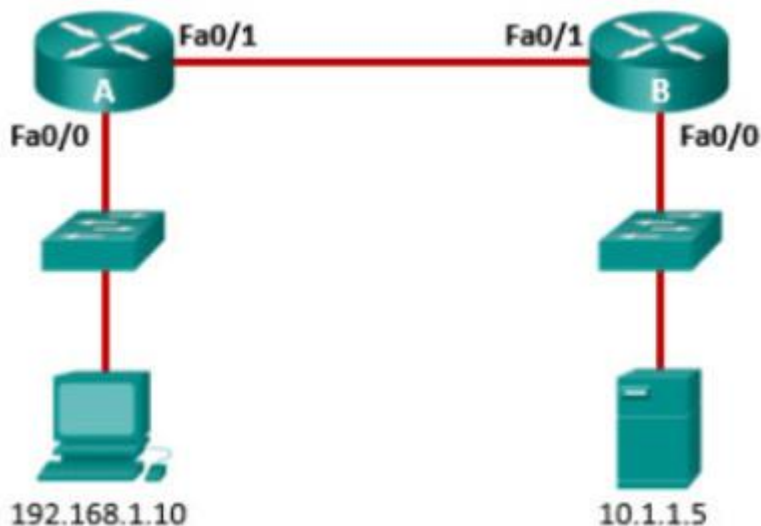
_Explique : Le délai est la latence entre un appareil émetteur et récepteur. La gigue est la variation du retard des paquets reçus. Le délai et la gigue doivent être contrôlés afin de prendre en charge le trafic voix et vidéo en temps réel.

_97. Quel protocole envoie des annonces périodiques entre les appareils Cisco connectés afin de connaître le nom de l'appareil, la version de l'IOS, ainsi que le nombre et le type d'interfaces ?

- **CDP**
- SNMP
- NTP
- LLDP

_99. Reportez-vous à l'illustration. Un administrateur configure l'ACL suivante afin d'empêcher les appareils du sous-réseau 192.168.1.0 d'accéder au serveur sur 10.1.1.5 :

```
access-list 100 deny ip 192.168.1.0 0.0.0.255 host 10.1.1.5  
  
access-list 100 permit ip any any
```



_Où l'administrateur doit-il placer cette ACL pour optimiser l'utilisation des ressources réseau ?

- **entrant sur le routeur A Fa0/0**
- sortant sur le routeur B Fa0/0
- sortant sur le routeur A Fa0/1
- entrant sur le routeur B Fa0/1

_100. Quel type de paquet OSPFv2 est utilisé pour transférer les informations de changement de lien OSPF ?

- reconnaissance de l'état du lien
- **mise à jour de l'état des liens**
- bonjour
- description de la base de données

_102. Quel type de VPN permet la multidiffusion et la diffusion trafic rapide via un VPN de site à site sécurisé ?

- VPN multipoint dynamique
- VPN SSL
- Interface de tunnel virtuel IPsec
- **GRE sur IPsec**

_105. Un administrateur configure l'OSPF à zone unique sur un routeur. L'un des réseaux qui doit être annoncé est 192.168.0.0 255.255.254.0. Quel masque générique l'administrateur utiliserait-il dans la déclaration de réseau OSPF ?

- 0.0.7.255
- **0.0.1.255**
- 0.0.3.255
- 0.0.15.255

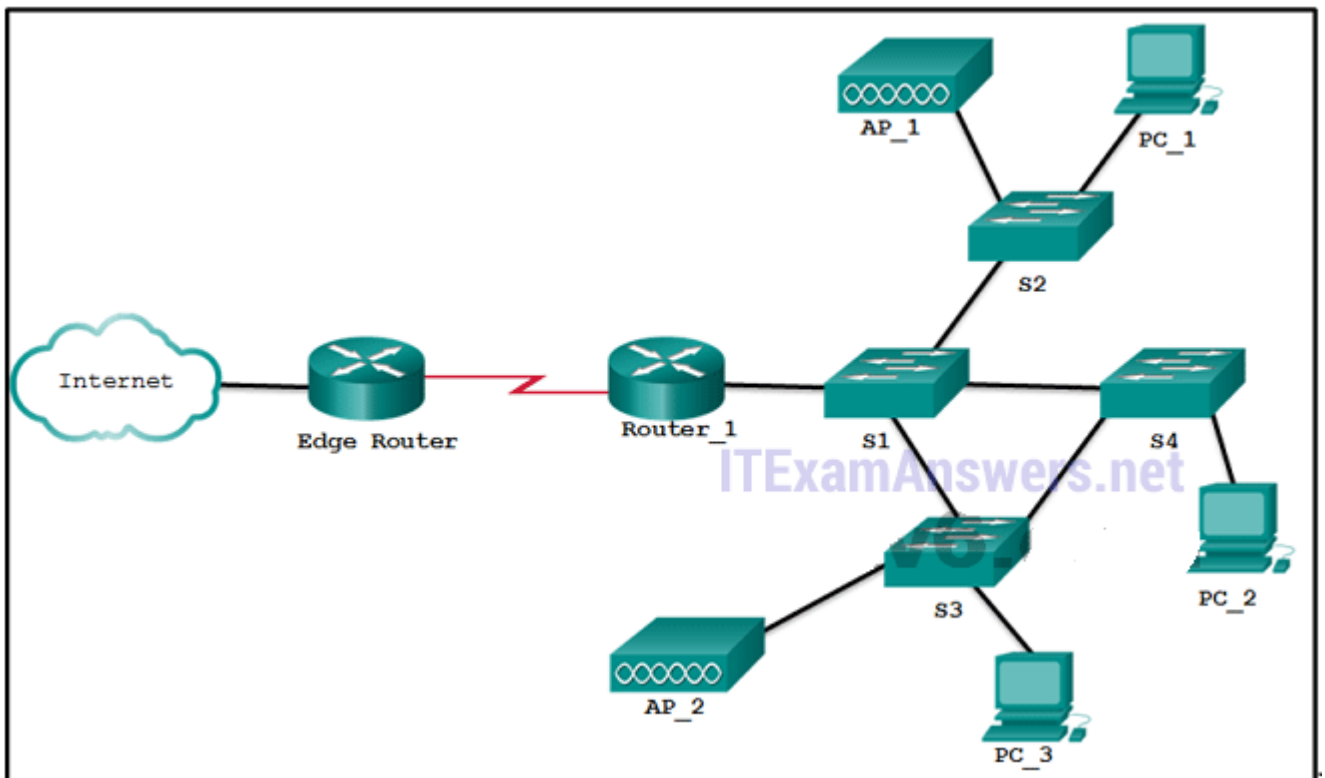
_107. Comment la virtualisation facilite-t-elle la reprise après sinistre dans un centre de données ?

- **Le matériel n'a pas besoin d'être identique.**
- **(Autre cas) Le matériel sur le site de récupération ne doit pas nécessairement être identique à l'équipement de production.**
- L'alimentation est toujours fournie.
- Moins d'énergie est consommée.
- Le provisionnement du serveur est plus rapide.

_Explique : La reprise après sinistre est la manière dont une entreprise s'y prend pour accéder aux applications, aux données et au matériel susceptibles d'être affectés lors d'un sinistre. La virtualisation offre une indépendance matérielle, ce qui

signifie que le site de reprise après sinistre n'a pas besoin d'avoir exactement l'équipement que l'équipement en production. Le provisionnement de serveur est pertinent lorsqu'un serveur est créé pour la première fois. Bien que les centres de données disposent de générateurs de secours, l'ensemble du centre de données est conçu pour la reprise après sinistre. Un centre de données particulier ne pourrait jamais garantir que le centre de données lui-même ne serait jamais sans électricité.

_108. Reportez-vous à l'illustration. Quels appareils existent dans le domaine de panne lorsque le commutateur S3 perd de l'alimentation ?



- S4 et PC_2
- **PC_3 et AP_2**
- AP_2 et AP_1
- PC_3 et PC_2
- S1 et S4

Un domaine de défaillance est la zone d'un réseau qui est touchée lorsqu'un périphérique critique tel que le commutateur S3 connaît une défaillance ou rencontre des problèmes.

_111. Quelle étape du processus de routage de l'état des liens est décrite par un routeur créant une base de données d'état des liens basée sur les LSA reçus ?

- exécuter l'algorithme SPF
- **construire la table de topologie**
- sélectionner l'ID du routeur
- déclarer un voisin inaccessible

_112. Quel protocole utilise des agents résidant sur des appareils gérés pour collecter et stocker des informations sur l'appareil et son fonctionnement ?

- SYSLOG
- TFTP
- CBWFQ

- **SNMP**

_113. Un administrateur configure l'OSPF à zone unique sur un routeur. L'un des réseaux qui doit être annoncé est 10.27.27.0 255.255.255.0. Quel masque générique l'administrateur utiliserait-il dans la déclaration de réseau OSPF ?

- 0.0.0.63
- **0.0.0.255**
- 0.0.0.31
- 0.0.0.15

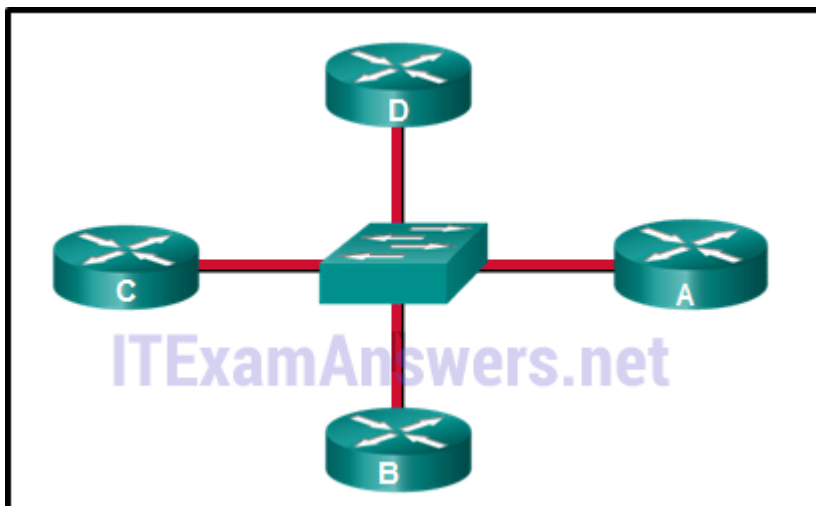
_114. Quand un routeur compatible OSPF passera-t-il de l'état Down à l'état Init ?

- lorsqu'une interface compatible OSPF devient active
- dès que le routeur démarre
- **lorsque le routeur reçoit un paquet Hello d'un routeur voisin**
- dès que le processus d'élection DR/BDR est terminé

_115. Quel type de trafic est décrit comme ayant un volume élevé de données par paquet ?

- données
- **vidéo**
- voix

_118. Reportez-vous à l'illustration. Quelle conclusion peut-on tirer de ce réseau multiaccès OSPF ?



- Si le DR arrête de produire des paquets Hello, un BDR sera élu, puis il se promouvra pour assumer le rôle de DR.
- **Avec une élection du DR, le nombre de contiguïtés passe de 6 à 3.**
- Lorsqu'un DR est élu, tous les autres routeurs non DR deviennent DROTHER.
- Tous les routeurs DROTHER enverront des LSA au DR et au BDR pour la multidiffusion 224.0.0.5.

Sur les réseaux multi-accès OSPF, un DR est élu pour être le point de collecte et de distribution des LSA envoyés et reçus. Un BDR est également élu en cas d'échec du DR. Tous les autres routeurs non DR ou BDR deviennent DROTHER. Au lieu d'inonder les LSA vers tous les routeurs du réseau, les DROTHER n'envoient leurs LSA qu'au DR et au BDR à l'aide de l'adresse de multidiffusion 224.0.0.6. S'il n'y a pas d'élection DR/BDR, le nombre d'adjacences requises est $n(n-1)/2 = > 4(4-1)/2 = 6$. Avec l'élection, ce nombre est réduit à 3.

_120. Quel type de VPN se connecte à l'aide de la fonctionnalité Transport Layer Security (TLS) ?

- **VPN SSL**
- Interface de tunnel virtuel IPsec
- GRE sur IPsec
- VPN multipoint dynamique

_122. Une entreprise a consolidé plusieurs serveurs et recherche un programme ou un firmware pour créer et contrôler des machines virtuelles qui ont accès à tout le matériel des serveurs consolidés. Quel service ou technologie répondrait à cette exigence ?

- ACI Cisco
- réseau défini par logiciel
- **Hyperviseur de type 1**
- APIC-EM

_123. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour identifier les adresses locales internes à traduire ?

- ip nat inside source list 24 interface serial 0/1/0 surcharge
- ip nat inside source list 14 pool POOL-STAT surcharge
- **liste d'accès 10 permis 172.19.89.0 0.0.0.255**
- ip nat dans la liste des sources ACCTNG pool POOL-STAT

_125. Reportez-vous à l'illustration. Un administrateur essaie de sauvegarder la configuration en cours d'exécution du routeur sur une clé USB et entre la commande `copy usbflash0:/R1-config running-config` sur la ligne de commande du routeur. Après avoir retiré la clé USB et l'avoir connectée à un PC, l'administrateur découvre que la configuration en cours n'a pas été correctement sauvegardée dans le fichier de configuration R1. Quel est le problème ?

```
R1# show file systems
File Systems:

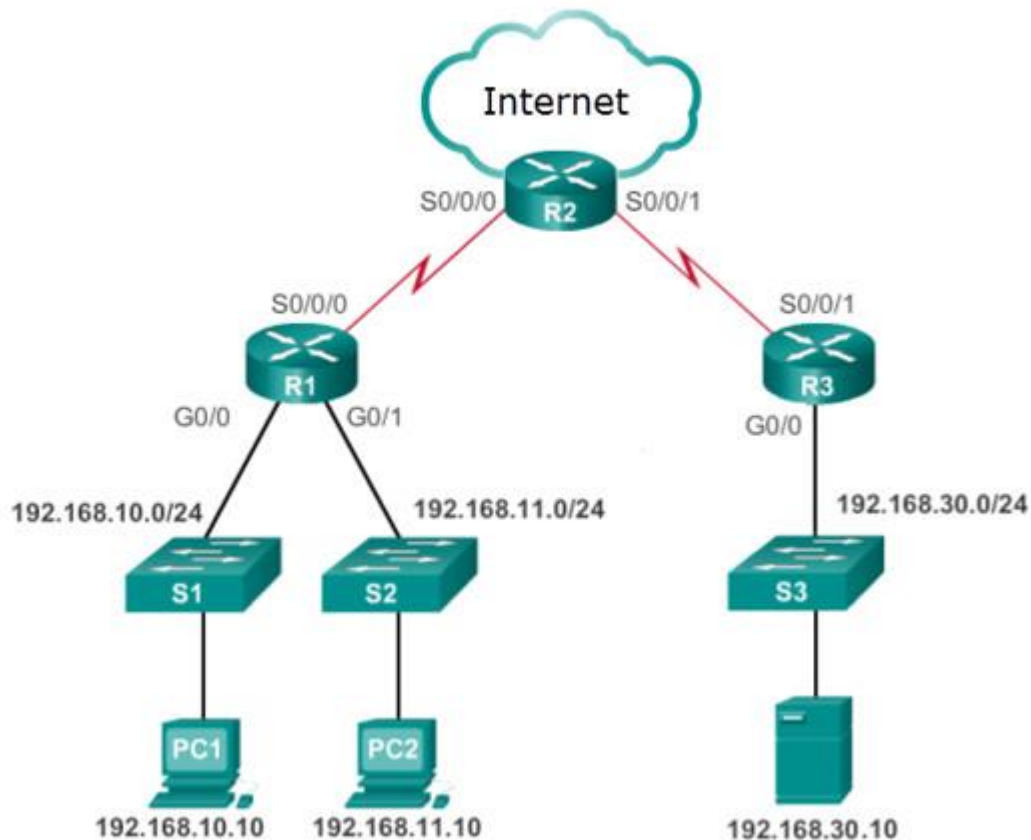
      Size (b)      Free (b)      Type  Flags  Prefixes
      -          -          opaque  rw    archive:
      -          -          opaque  rw    system:
      -          -          opaque  rw    tmpsys:
      -          -          opaque  rw    null:
      -          -          network rw    tftp:
* 256487424      184819712      disk    rw    flash0: flash:#
      -          -          disk    rw    flash1:
      262136      249270        nvram   rw    nvram:
      -          -          opaque  wo    syslog:
      -          -          opaque  rw    xmodem:
      -          -          opaque  rw    ymodem:
      -          -          network rw    rcp:
      -          -          network rw    http:
      -          -          network rw    ftp:
      -          -          network rw    scp:
      -          -          opaque  ro    tar:
      -          -          network rw    https:
      -          -          opaque  ro    cns:
4050042880      3774152704    usbflash  rw    usbflash0:
```

- Le fichier existe déjà sur la clé USB et ne peut pas être écrasé.
- Le disque n'a pas été correctement formaté avec le système de fichiers FAT16.
- Il n'y a plus d'espace sur la clé USB.
- La clé USB n'est pas reconnue par le routeur.
- **La commande utilisée par l'administrateur était incorrecte.**

_126. Quels sont les trois types de VPN qui sont des exemples de VPN site à site gérés par l'entreprise ? (Choisissez trois réponses.)

- VPN MPLS de couche 3
- **VPN IPsec**
- **VPN multipoint dynamique Cisco**
- **GRE sur VPN IPsec**
- VPN SSL sans client
- VPN IPsec basé sur le client

_127. Reportez-vous à l'illustration. Les employés du 192.168.11.0/24 travaillent sur des informations extrêmement sensibles et ne sont pas autorisés à accéder en dehors de leur réseau. Quel est le meilleur type et emplacement ACL à utiliser dans cette situation ?



- ACL standard entrant sur les lignes vty R1
- LCA étendue entrante sur R1 G0/0
- **ACL standard entrant sur R1 G0/1**
- LCA étendue entrante sur R3 S0/0/1

_128. Dans un réseau OSPF, quelles sont les deux déclarations décrivant la base de données d'état des liens (LSDB) ? (Choisissez deux réponses.)

- **Il peut être visualisé à l'aide de la commande show ip ospf database.**
- Une table de voisinage est créée sur la base de la LSDB.
- Il contient une liste des meilleurs itinéraires vers un réseau particulier.
- Il contient une liste de tous les routeurs voisins avec lesquels un routeur a établi une communication bidirectionnelle.
- **Tous les routeurs d'une zone ont une base de données d'état de liens identique.**

_129. Dans un réseau OSPF, quelle structure OSPF est utilisée pour créer la table des voisins sur un routeur ?

- **base de données de contiguïté**
- base de données d'état des liens
- table de routage
- base de données de transfert

_130. Quel protocole est utilisé dans un système composé de trois éléments : un gestionnaire, des agents et une base de données d'informations ?

- MPLS
- SYSLOG
- **SNMP**
- TFTP

_131. Quel type de trafic est décrit comme n'étant pas résilient aux pertes ?

- données
- **vidéo**
- voix

Explication : le trafic vidéo a tendance à être imprévisible, incohérent et en rafale par rapport au trafic vocal. Par rapport à la voix, la vidéo est moins résistante aux pertes et contient un plus grand volume de données par paquet.

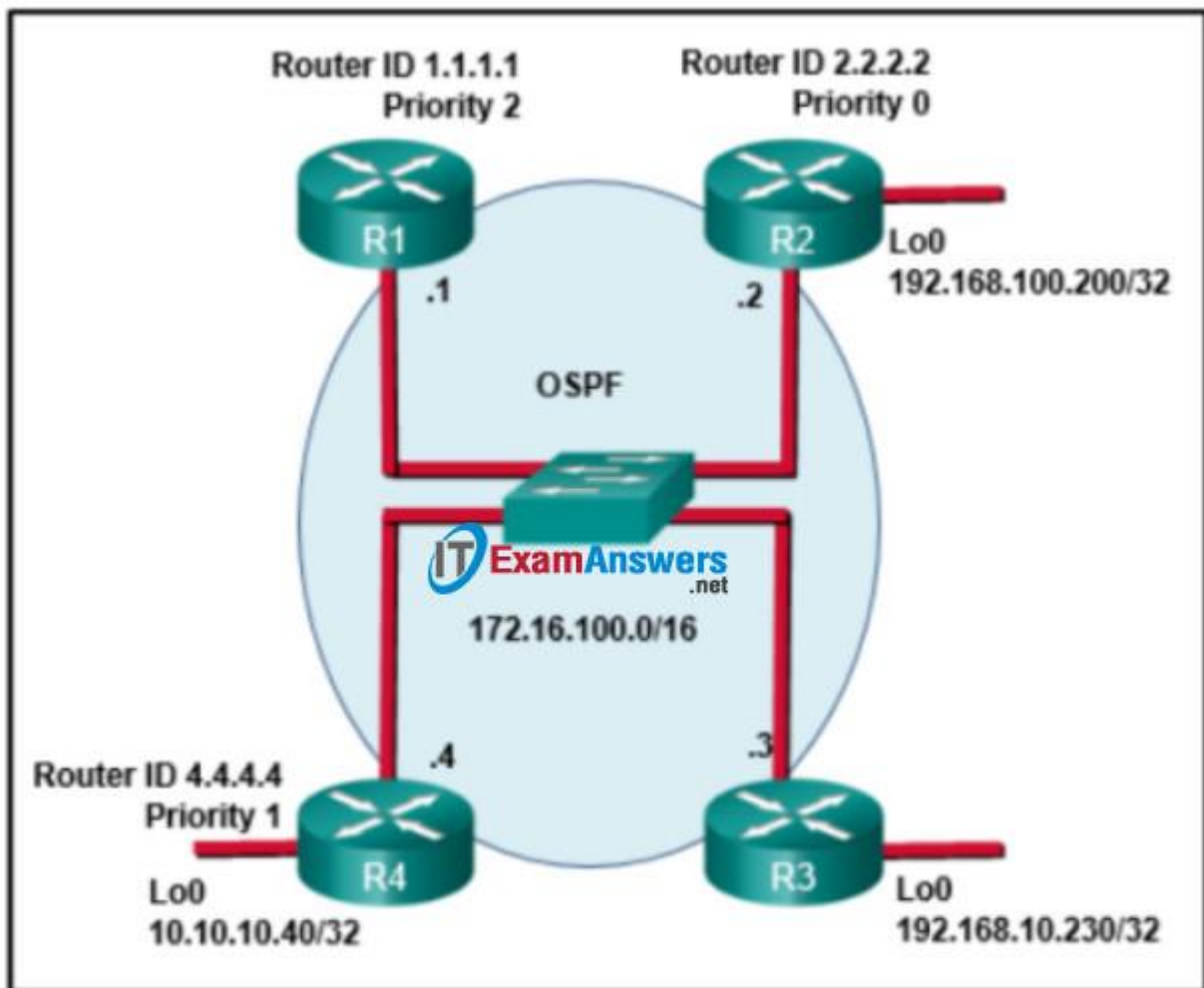
_135. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :

```
access-list 101 permit udp 192.168.100.32 0.0.0.7 host 198.133.219.76 eq telnet .
```

_Si un paquet avec une adresse source de 198.133.219.100, une adresse de destination de 198.133.219.170 et un protocole de 23 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- **refusé**
- autorisé

_140. Reportez-vous à l'illustration. Si le commutateur redémarre et que tous les routeurs doivent rétablir les contiguïtés OSPF, quels routeurs deviendront les nouveaux DR et BDR ?



Enterprise Networking, Security, and Automation (Version 7.00) – Examen final ENSA

- Le routeur R2 deviendra le DR et le routeur R4 deviendra le BDR.
- **Le routeur R1 deviendra le DR et le routeur R3 deviendra le BDR.**
- Le routeur R4 deviendra le DR et le routeur R3 deviendra le BDR.
- Le routeur R3 deviendra le DR et le routeur R2 deviendra le BDR.

_141. Un étudiant, effectuant un semestre d'études à l'étranger, a pris des centaines de photos sur un smartphone et souhaite les sauvegarder en cas de perte. Quel service ou technologie répondrait à cette exigence ?

- ACI Cisco
- **services cloud**
- réseau défini par logiciel
- serveurs dédiés

_143. Quels sont les trois énoncés généralement considérés comme les meilleures pratiques pour le placement des ACL ? (Choisissez trois réponses.)

- **Filtrez le trafic indésirable avant qu'il ne transite par une liaison à faible bande passante.**
- **Placez les ACL standard à proximité de l'adresse IP de destination du trafic.**
- Placez les ACL standard à proximité de l'adresse IP source du trafic.
- Placez les ACL étendues à proximité de l'adresse IP de destination du trafic.
- **Placez les ACL étendues à proximité de l'adresse IP source du trafic.**
- Pour chaque ACL entrante placée sur une interface, il doit y avoir une ACL sortante correspondante.

Explique : Les ACL étendues doivent être placées aussi près que possible de l'adresse IP source, afin que le trafic qui doit être filtré ne traverse pas le réseau et n'utilise pas les ressources du réseau. Étant donné que les ACL standard ne spécifient pas d'adresse de destination, elles doivent être placées aussi près que possible de la destination. Placer une ACL standard près de la source peut avoir pour effet de filtrer tout le trafic et de limiter les services aux autres hôtes. Le filtrage du trafic indésirable avant qu'il n'entre dans les liaisons à faible bande passante préserve la bande passante et prend en charge les fonctionnalités du réseau. Les décisions concernant le placement d'ACL entrantes ou sortantes dépendent des exigences à respecter.

_145. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour afficher toutes les traductions statiques qui ont été configurées ?

- **afficher les traductions ip nat**
- afficher les traductions ip pat
- afficher le cache IP
- afficher la configuration en cours

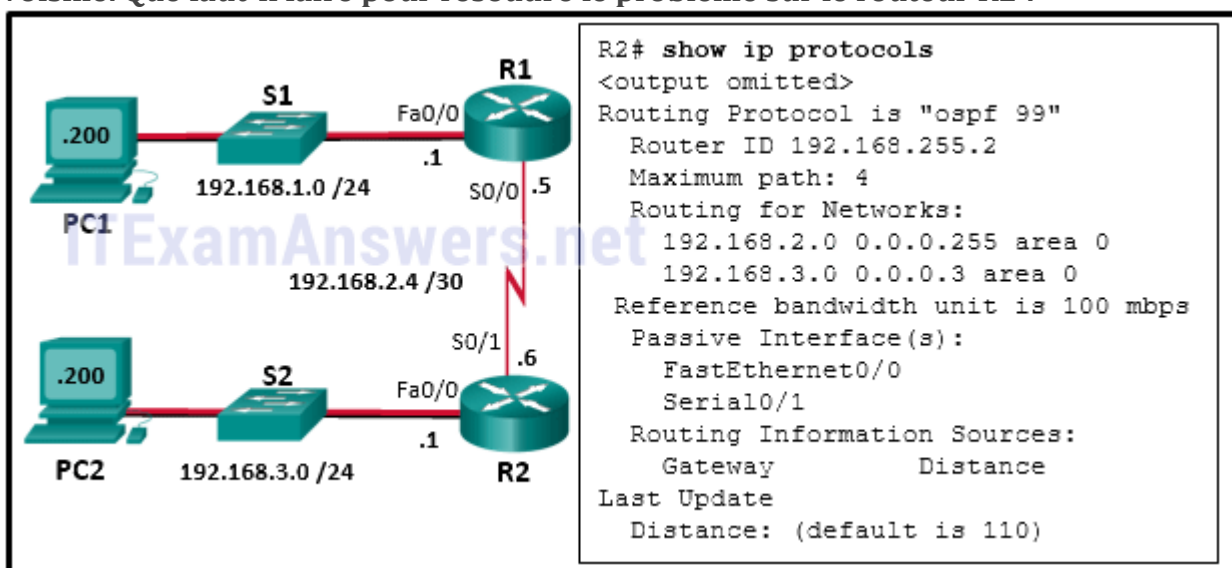
_147. Quel type de VPN est le choix préféré pour la prise en charge et la facilité de déploiement pour l'accès à distance ?

- **VPN SSL**
- GRE sur IPsec
- VPN multipoint dynamique
- Interface de tunnel virtuel IPsec

_149. Quel mécanisme de mise en file d'attente ne permet pas de hiérarchiser ou de mettre en mémoire tampon, mais transfère simplement les paquets dans l'ordre dans lequel ils arrivent ?

- **FIFO**
- LLQ
- CBWFQ
- WFQ

_150. Reportez-vous à l'illustration. Un administrateur réseau a configuré OSPFv2 sur les deux routeurs Cisco. Les routeurs sont incapables de former une contiguïté voisine. Que faut-il faire pour résoudre le problème sur le routeur R2 ?



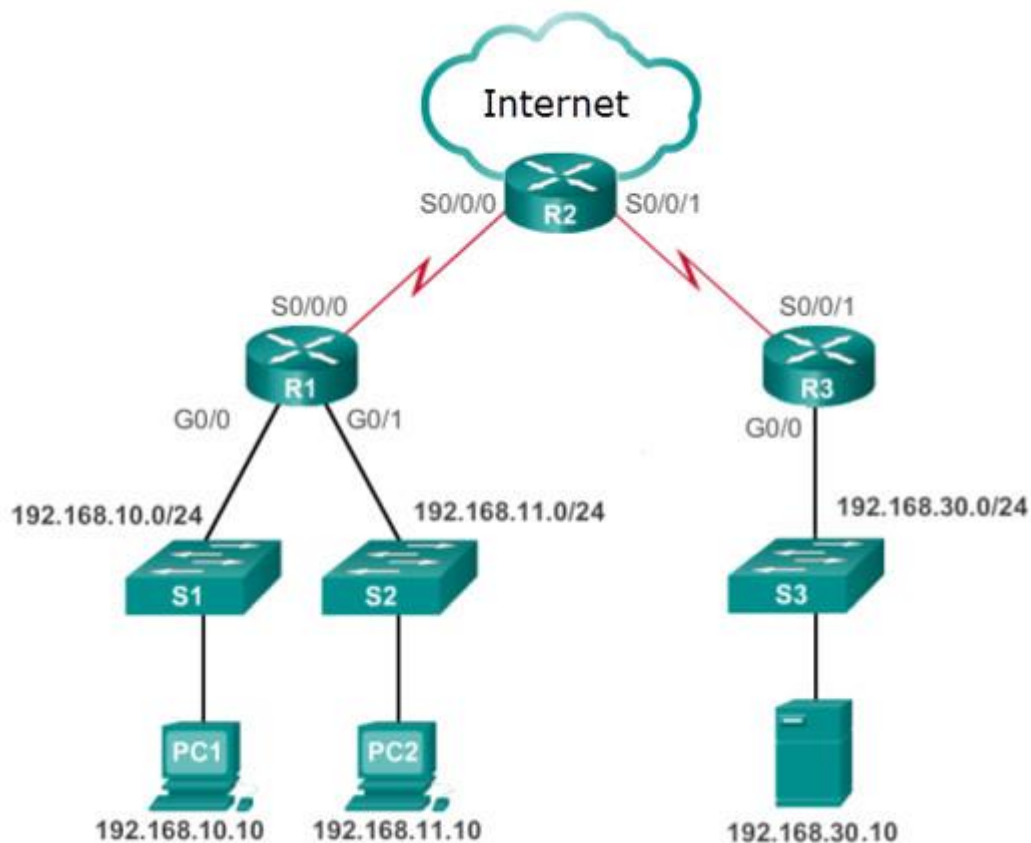
- **Implémentez la commande no passive-interface Serial0/1.**

- Mettre en œuvre la commande `network 192.168.2.6 0.0.0.0 area 0` sur le routeur R2.
- Changez l'ID du routeur du routeur R2 en 2.2.2.2.
- Mettre en œuvre la commande `network 192.168.3.1 0.0.0.0 area 0` sur le routeur R2.

_151. Un administrateur réseau résout un problème OSPF qui implique la contiguïté des voisins. Que doit faire l'administrateur ?

- Assurez-vous que la priorité du routeur est unique sur chaque routeur.
- Assurez-vous que la sélection DR/BDR est terminée.
- Assurez-vous que l'ID du routeur est inclus dans le paquet Hello.
- **Assurez-vous que les minuteurs d'intervalle hello et dead sont les mêmes sur tous les routeurs.**

_152. Reportez-vous à l'illustration. Les privilèges Internet d'un employé ont été révoqués en raison d'un abus, mais l'employé a toujours besoin d'accéder aux ressources de l'entreprise. Quel est le meilleur type et emplacement ACL à utiliser dans cette situation ?



CCNA 3 v7 Modules 3 à 5 : Réponses à l'examen de sécurité réseau 49/[légende]

- ACL standard entrant sur l'interface WAN R2 se connectant à Internet
- **ACL standard sortant sur l'interface WAN R2 vers Internet**
- ACL standard entrant sur R1 G0/0
- ACL standard sortant sur R1 G0/0

Explication : – Les ACL standard autorisent ou refusent les paquets en fonction uniquement de l'adresse IPv4 source. Étant donné que tous les types de trafic sont autorisés ou refusés, les ACL standard doivent être situées aussi près que possible de la destination.

– Les ACL étendues autorisent ou refusent les paquets en fonction de l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination, etc. Étant donné que le filtrage des ACL étendues est si spécifique, les ACL étendues doivent être situées aussi près que possible de la source du trafic à filtrer. Le trafic indésirable est refusé à proximité du réseau source sans traverser l'infrastructure réseau.

_153. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :

```
access-list 100 permit tcp 192.168.10.0 0.0.0.255 172.17.200.0 0.0.0.255 eq  
www .
```

_Si un paquet avec une adresse source de 192.168.10.244, une adresse de destination de 172.17.200.56 et un protocole de 80 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- refusé
- **autorisé**

_154. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des applications telles que Nmap, SuperScan et Angry IP Scanner ?

- pour détecter les outils installés dans les fichiers et les répertoires qui permettent aux pirates d'accéder et de contrôler à distance un ordinateur ou un réseau
- pour détecter toute preuve de piratage ou de logiciel malveillant dans un ordinateur ou un réseau
- pour désosser les fichiers binaires lors de l'écriture d'exploits et de l'analyse de logiciels malveillants
- **pour sonder les périphériques réseau, les serveurs et les hôtes à la recherche de ports TCP ou UDP ouverts**

_155. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour afficher les traductions PAT dynamiques créées par le trafic ?

- afficher les traductions ip pat
- afficher le cache IP
- afficher la configuration en cours
- **afficher les traductions ip nat**

_156. Un administrateur configure l'OSPF à zone unique sur un routeur. L'un des réseaux qui doit être annoncé est 172.16.91.0 255.255.255.192. Quel masque générique l'administrateur utiliserait-il dans la déclaration de réseau OSPF ?

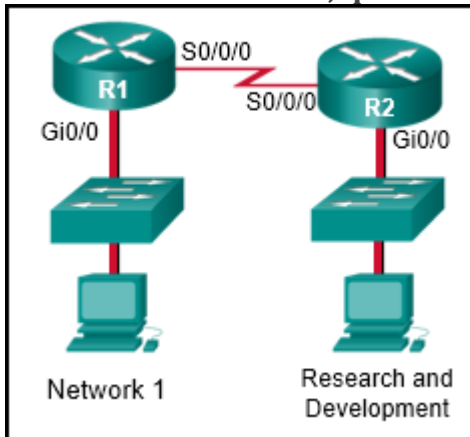
- 0.0.31.255
- **0.0.0.63**
- 0.0.15.255
- 0.0.7.255

_157. Quel type de trafic est décrit comme nécessitant une latence inférieure à 400 ms ?

- **vidéo**
- données

- voix

_160. Reportez-vous à l'illustration. La société a décidé qu'aucun trafic provenant de tout autre réseau existant ou futur ne peut être transmis au réseau de Recherche et Développement. De plus, aucun trafic provenant du réseau de Recherche et Développement ne peut être transmis à d'autres réseaux existants ou futurs de l'entreprise. L'administrateur réseau a décidé que les listes de contrôle d'accès étendues sont mieux adaptées à ces exigences. Sur la base des informations fournies, que va faire l'administrateur réseau ?

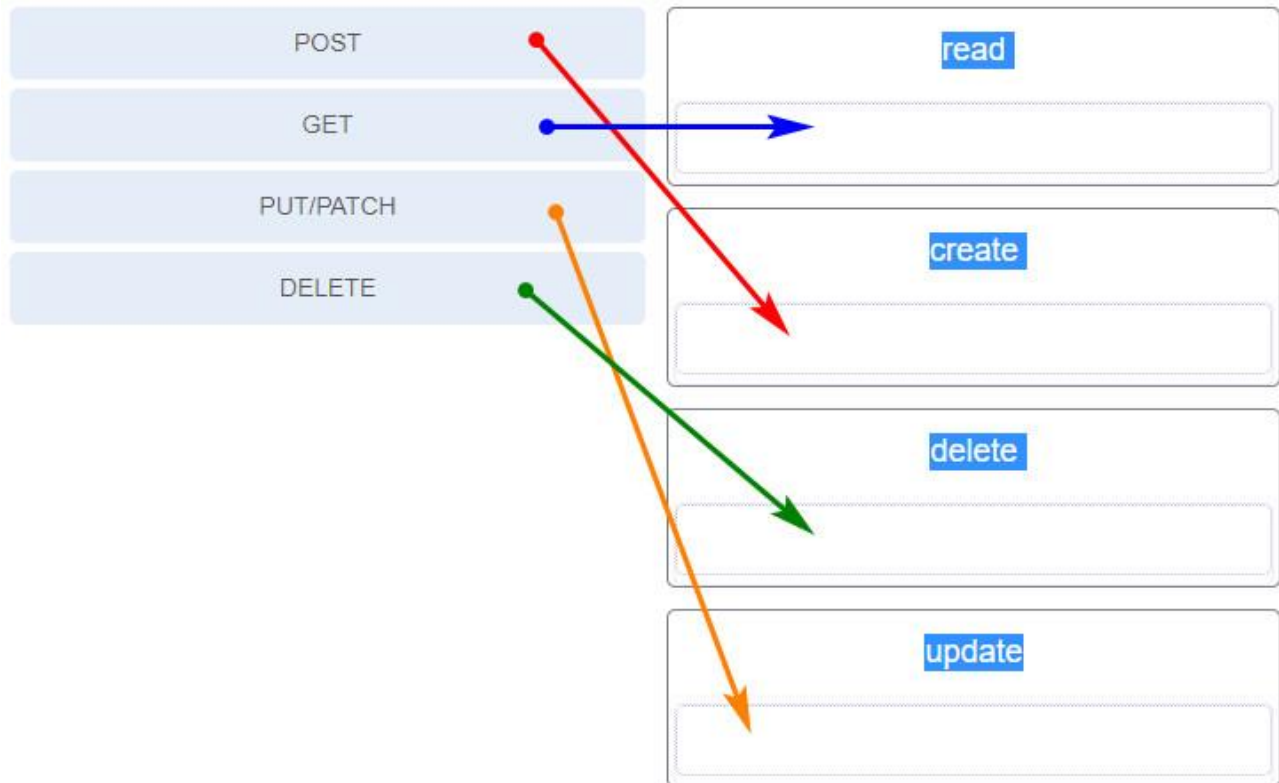


- Une ACL sera placée sur l'interface R1 Gi0/0 et une ACL sera placée sur l'interface R2 Gi0/0.
- Seule une ACL numérotée fonctionnera dans cette situation.
- Une ACL sera placée sur l'interface R2 Gi0/0 et une ACL sera placée sur l'interface R2 S0/0/0.
- **Deux ACL (une dans chaque direction) seront placées sur l'interface R2 Gi0/0.**

_161. Quel protocole utilise des nombres de strates plus petits pour indiquer que le serveur est plus proche de la source horaire autorisée que des nombres de strates plus grands ?

- TFTP
- SYSLOG
- **NTP**
- MPLS

_163. Mettez en correspondance la méthode HTTP avec l'opération RESTful.



_165. Quel type de trafic est décrit comme ayant tendance à être imprévisible, incohérent et saccadé ?

- **vidéo**
- voix
- données

_167. Quel type de trafic est décrit comme composé de trafic nécessitant une priorité plus élevée s'il est interactif ?

- voix
- **données**
- vidéo

_168. Quel type de VPN offre une option flexible pour connecter un site central à des sites de succursale ?

- Interface de tunnel virtuel IPsec
- VPN MPLS
- **VPN multipoint dynamique**
- GRE sur IPsec

_172. Quelle étape du processus de routage à état des liens est décrite par un routeur envoyant des paquets Hello à toutes les interfaces compatibles OSPF ?

- échange de publicités d'état de lien
- choix du routeur désigné
- Injecter la route par défaut
- **établir des contiguïtés de voisinage**

_173. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des outils médico-légaux ?

- pour obtenir des systèmes d'exploitation spécialement conçus et préchargés avec des outils optimisés pour le piratage
- **pour détecter toute preuve de piratage ou de logiciel malveillant dans un ordinateur ou un réseau**
- pour détecter les outils installés dans les fichiers et les répertoires qui permettent aux pirates d'accéder et de contrôler à distance un ordinateur ou un réseau
- pour désosser les fichiers binaires lors de l'écriture d'exploits et de l'analyse de logiciels malveillants

_176. Un ingénieur réseau a remarqué que certaines entrées de route réseau attendues ne s'affichent pas dans la table de routage. Quelles sont les deux commandes qui fourniront des informations supplémentaires sur l'état des adjacences de routeur, les intervalles de minuterie et l'ID de zone ? (Choisissez deux réponses.)

- afficher les protocoles IP
- **afficher ip ospf voisin**
- afficher la configuration en cours
- **afficher l'interface ip ospf**
- afficher ip route ospf

_Explication : La commande show ip ospf interface affichera les informations de la table de routage qui sont déjà connues. Les commandes show running-configuration et show ip protocols afficheront les aspects de la configuration OSPF sur le routeur mais n'afficheront pas les détails de l'état de contiguïté ni les détails de l'intervalle de temporisation.

_177. Quel type de VPN implique le transfert du trafic sur le backbone via l'utilisation d'étiquettes réparties entre les routeurs principaux ?

- **VPN MPLS**
- GRE sur IPsec
- Interface de tunnel virtuel IPsec
- VPN multipoint dynamique

_179. Une entreprise a passé un contrat avec une société de sécurité réseau pour l'aider à identifier les vulnérabilités du réseau de l'entreprise. L'entreprise envoie une équipe pour effectuer des tests d'intrusion sur le réseau de l'entreprise. Pourquoi l'équipe utiliserait-elle des systèmes d'exploitation de piratage ?

- pour détecter toute preuve de piratage ou de logiciel malveillant dans un ordinateur ou un réseau
- **pour obtenir des systèmes d'exploitation spécialement conçus et préchargés avec des outils optimisés pour le piratage**
- pour encoder les données, à l'aide de schémas algorithmiques, afin d'empêcher tout accès non autorisé aux données chiffrées
- pour désosser les fichiers binaires lors de l'écriture d'exploits et de l'analyse de logiciels malveillants

_180. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour identifier une interface comme faisant partie du réseau mondial externe ?

- ip tcp à l'intérieur
- liste d'accès 10 permis 172.19.89.0 0.0.0.255
- ip nat à l'intérieur

- **ip nat extérieur**

_181. Pour éviter d'acheter du nouveau matériel, une entreprise souhaite tirer parti des ressources système inactives et consolider le nombre de serveurs tout en autorisant plusieurs systèmes d'exploitation sur une seule plate-forme matérielle. Quel service ou technologie répondrait à cette exigence ?

- centre de données
- services cloud
- **virtualisation**
- serveurs dédiés

_Expliquez : La virtualisation des serveurs tire parti des ressources inactives et consolide le nombre de serveurs requis. Cela permet également à plusieurs systèmes d'exploitation d'exister sur une seule plate-forme matérielle.

_182. Quel type de VPN achemine les paquets via des interfaces de tunnel virtuel pour le chiffrement et le transfert ?

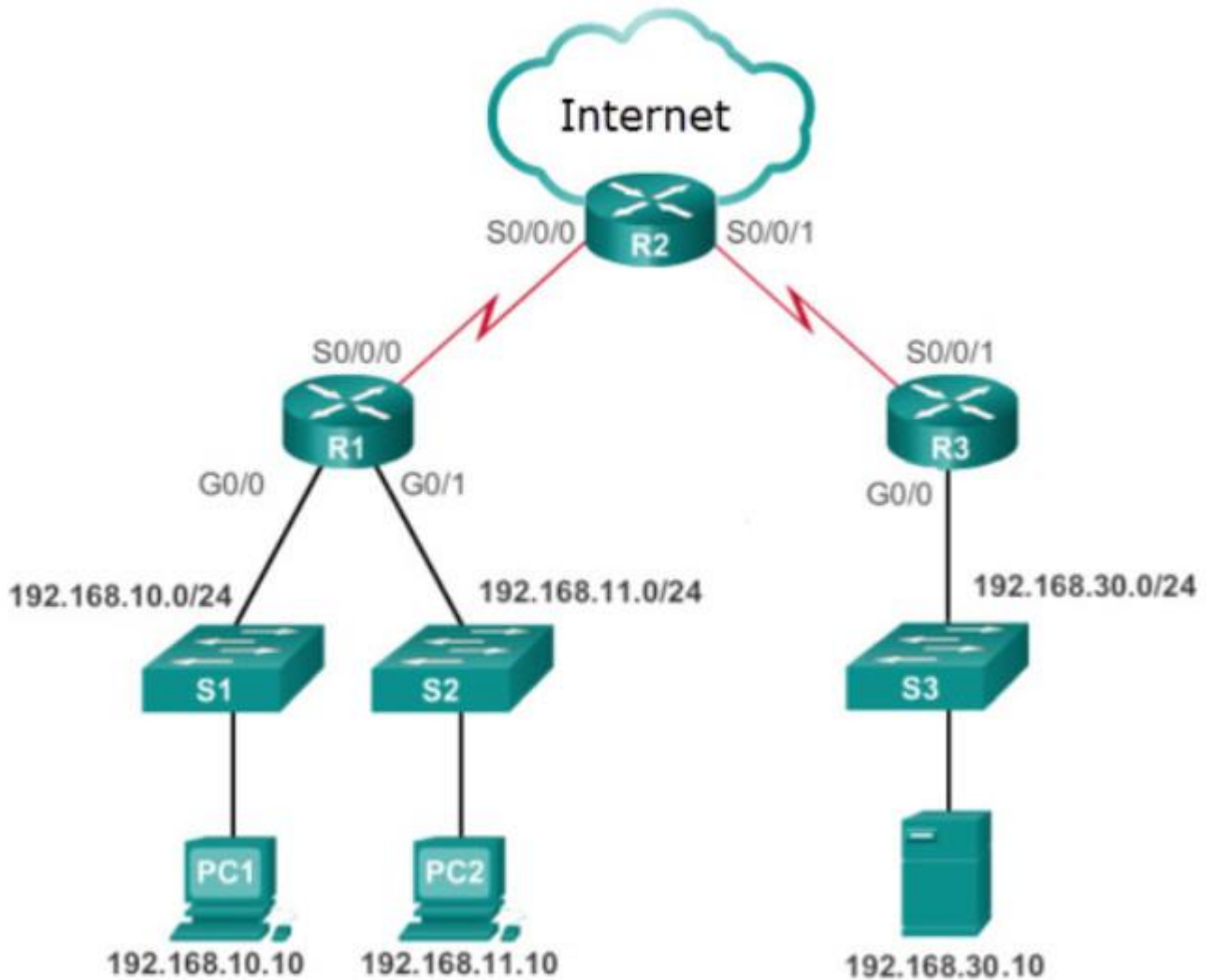
- VPN MPLS
- **Interface de tunnel virtuel IPsec**
- VPN multipoint dynamique
- GRE sur IPsec

_184. Quel type de trafic est décrit comme utilisant TCP ou UDP en fonction du besoin de récupération d'erreur ?

- vidéo
- voix
- **données**

_185. Reportez-vous à l'illustration. Le PDG de la société demande qu'une ACL soit créée pour autoriser le trafic de courrier électronique vers Internet et refuser l'accès FTP. Quel est le meilleur type et emplacement ACL à utiliser dans cette

situation ?



- **LCA étendue sortante sur l'interface WAN R2 vers Internet**
- ACL standard sortant sur R2 S0/0/0
- LCA étendue entrante sur R2 S0/0/0
- ACL standard entrant sur l'interface WAN R2 se connectant à Internet

_186. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour définir un pool d'adresses à traduire ?

- ip nat à l'intérieur de la source statique 172.19.89.13 198.133.219.65
- ip nat inside source list 24 interface serial 0/1/0 surcharge
- **piscine ip nat POOL-STAT 64.100.14.17 64.100.14.30 masque de réseau 255.255.255.240**
- ip nat extérieur

_187. Quel est le nom de la couche dans la conception du réseau commuté sans frontières de Cisco qui est considérée comme l'épine dorsale utilisée pour la connectivité haut débit et l'isolation des pannes ?

- lien de données
- accès
- **essentiel**
- réseau
- accès au réseau

_Explique : Les trois couches de la conception du réseau de commutation sans frontières Cisco sont l'accès, la distribution et le cœur. Les commutateurs de la couche d'accès sont ceux utilisés pour connecter les périphériques finaux au réseau. Les commutateurs de la couche de distribution acceptent les connexions des commutateurs de la couche d'accès et fournissent des fonctions de commutation, de routage et de politique d'accès. La couche centrale est appelée backbone et les commutateurs principaux ont généralement des connexions redondantes à haut débit.

_188. Une ACL est appliquée en entrée sur l'interface du routeur. L'ACL se compose d'une seule entrée :

```
access-list 210 permit tcp 172.18.20.0 0.0.0.47 any eq ftp
```

_Si un paquet avec une adresse source de 172.18.20.40, une adresse de destination de 10.33.19.2 et un protocole de 21 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- **autorisé**
- refusé

_189. Quel type de trafic est décrit comme consistant en un trafic dont la priorité est inférieure s'il n'est pas stratégique ?

- vidéo
- **données**
- voix

_191. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :

```
access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www .
```

Si un paquet avec une adresse source de 192.168.10.45, une adresse de destination de 10.10.3.27 et un protocole de 80 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- **autorisé**
- refusé

_192. Quel protocole permet au gestionnaire d'interroger les agents pour accéder aux informations de la MIB de l'agent ?

- CBWFQ
- SYSLOG
- TFTP
- **SNMP**

_195. Quel terme décrit l'ajout d'une valeur à l'en-tête du paquet, aussi proche que possible de la source, afin que le paquet corresponde à une politique définie ?

- police
- **marquage routier**
- détection précoce aléatoire pondérée (WRED)
- mise en forme du trafic
- chute de la queue

_196. Quels sont les trois facteurs liés au trafic qui influenceraient la sélection d'un type de lien WAN particulier ? (Choisissez trois réponses.)

- coût du lien

- **quantité de trafic**
- distance entre les sites
- fiabilité
- **besoins de sécurité**
- **type de trafic**

_Explique : Les facteurs liés au trafic qui influencent la sélection d'un type de lien WAN particulier incluent le type de trafic, la quantité de trafic, les exigences de qualité et les exigences de sécurité. Les exigences de qualité incluent la garantie que le trafic qui ne peut pas tolérer les retards bénéficie d'un traitement prioritaire, ainsi que le trafic transactionnel commercial important.

_197. Quelle commande serait utilisée dans le cadre de la configuration de NAT ou PAT pour lier les adresses locales internes au pool d'adresses disponibles pour la traduction PAT ?

- ip nat inside source list ACCTNG pool POOL-STAT
- délai de traduction ip nat 36000
- **ip nat à l'intérieur de la liste source 14 pool POOL-STAT surcharge**
- ip nat à l'intérieur de la source statique 172.19.89.13 198.133.219.65

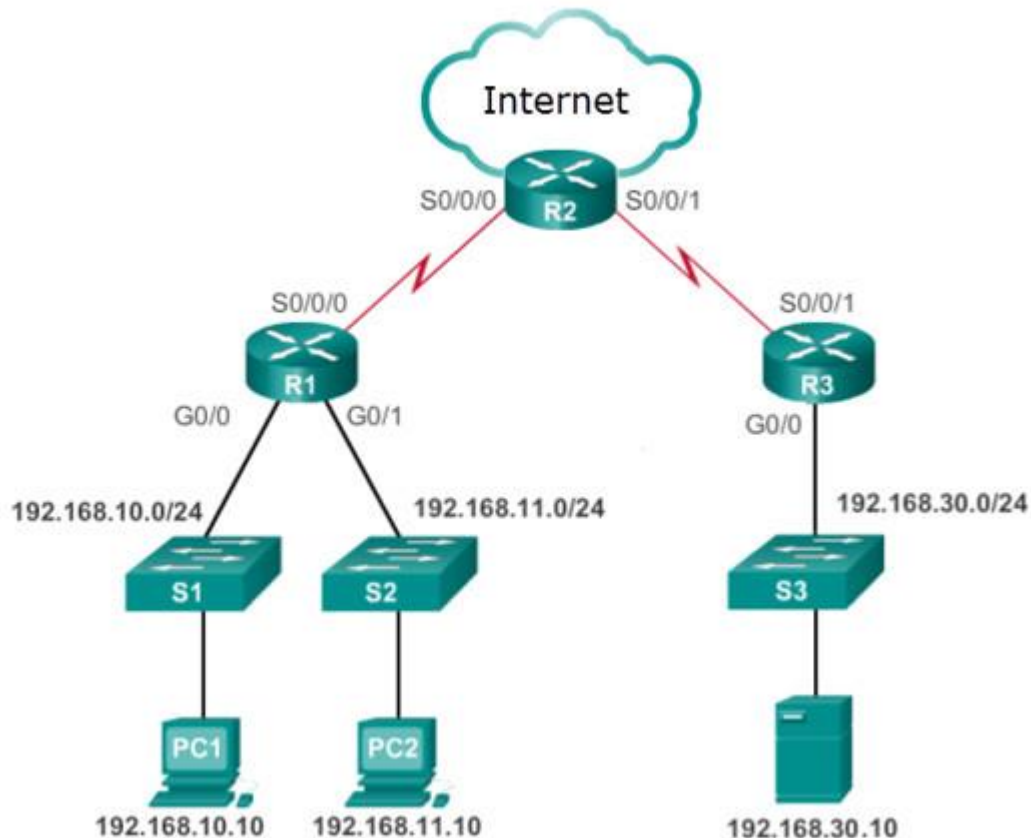
_198. Quel protocole est un protocole de découverte de couche 2 indépendant du fournisseur qui doit être configuré séparément pour transmettre et recevoir des paquets d'informations ?

- SNMP
- MPLS
- **LLDP**
- NTP

_199. Une ACL est appliquée en entrée sur une interface de routeur. L'ACL se compose d'une seule entrée :access-list 210 permit tcp 172.18.20.0 0.0.0.31 172.18.20.32 0.0.0.31 eq ftp . Si un paquet avec une adresse source de 172.18.20.55, une adresse de destination de 172.18.20.3 et un protocole de 21 est reçu sur l'interface, le paquet est-il autorisé ou refusé ?

- autorisé
- **refusé**

_200. Reportez-vous à l'illustration. La politique de l'entreprise exige que l'accès au réseau de serveurs soit limité aux seuls employés internes. Quel est le meilleur type et emplacement ACL à utiliser dans cette situation ?



La

politique de l'entreprise exige que l'accès au réseau de serveurs soit limité aux employés internes uniquement. Quel est le meilleur type et emplacement ACL à utiliser dans cette situation

- **LCA étendue sortante sur R2 S0/0/1**
- ACL standard sortant sur R2 S0/0/0
- ACL standard entrant sur l'interface WAN R2 se connectant à Internet
- LCA étendue entrante sur R2 S0/0/0

_201. Un technicien travaille sur un commutateur de couche 2 et remarque qu'un message %CDP-4-DUPLEX_MISMATCH continue d'apparaître pour le port G0/5. Quelle commande le technicien doit-il émettre sur le commutateur pour lancer le processus de dépannage ?

- afficher les voisins cdp
- show ip interface brief
- **afficher l'interface g0/5**
- afficher le cdp

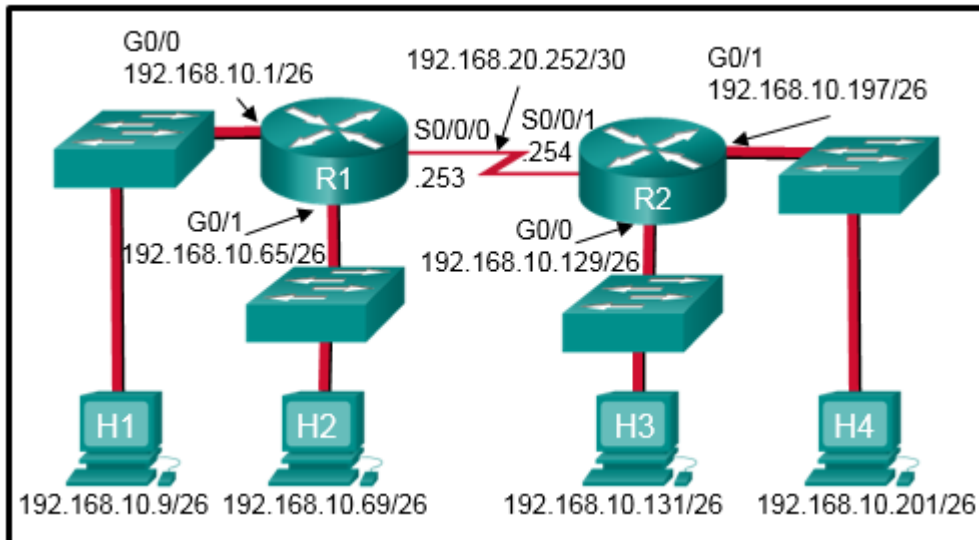
_202. Quelle ressource virtuelle serait installée sur un serveur réseau pour fournir un accès direct aux ressources matérielles ?

- VMware Fusion
- une console de gestion
- un VLAN dédié
- **un hyperviseur de type 1**

_Explique : Hyperviseurs de type 1, l'hyperviseur est installé directement sur le serveur ou le matériel réseau. Ensuite, des instances d'un système d'exploitation sont installées sur l'hyperviseur, comme illustré dans la figure. Les hyperviseurs de type 1 ont un accès direct aux ressources matérielles. Par conséquent, elles sont

plus efficaces que les architectures hébergées. Les hyperviseurs de type 1 améliorent l'évolutivité, les performances et la robustesse.

_203. Reportez-vous à l'illustration. Un administrateur réseau a configuré une ACL standard pour autoriser uniquement les deux réseaux LAN connectés à R1 à accéder au réseau qui se connecte à l'interface R2 G0/1. Lorsque vous suivez les bonnes pratiques, à quel endroit l'ACL standard doit-elle être appliquée ?



Réseaux d'entreprise, sécurité et automatisation (version 7.00) – Examen final ENSA[*caption*]

- R2 G0/1 entrant
- R2 S0/0/1 sortant
- R1 S0/0/0 sortant
- **R2 G0/1 sortant**
- R2 G0/0 sortant

_204. Quelle base de données OSPF est identique sur tous les routeurs convergés au sein de la même zone OSPF ?

- voisin
- transfert
- **état du lien**
- adjacence

Explique : Quelle que soit la zone OSPF dans laquelle un routeur réside, la base de données de contiguïté, la table de routage et la base de données de transfert sont uniques pour chaque routeur. La base de données d'état des liens répertorie les informations sur tous les autres routeurs d'une zone et est identique sur tous les routeurs OSPF participant à cette zone.

_205. Quelles sont les deux fonctionnalités à prendre en compte lors de la création d'une ACL nommée ? (Choisissez deux réponses.)

- **Utilisez des caractères alphanumériques si nécessaire.**
- Utilisez des caractères spéciaux, tels que ! ou * pour montrer l'importance de l'ACL.
- Modifier l'ACL à l'aide d'un éditeur de texte.
- **Soyez descriptif lors de la création du nom ACL.**
- Utilisez un espace pour faciliter la lecture afin de séparer le nom de la description

Explication : Ce qui suit résume les règles à suivre pour les ACL nommées :

- Attribuez un nom pour identifier l'objectif de l'ACL.
- Les noms peuvent contenir des caractères alphanumériques.
- Les noms ne peuvent pas contenir d'espaces ni de ponctuation.
- C'est suggéré que le nom soit écrit en MAJUSCULES.
- Les entrées peuvent être ajoutées ou supprimées dans l'ACL.

_206. Mettez en correspondance la méthode API RESTful à la fonction CRUD.

POST	READ
GET	GET
PUT/PATCH	CREATE
DELETE	POST
	DELETE
	DELETE
	UPDATE
	PUT/PATCH

Mettez en correspondance la méthode API RESTful à la fonction CRUD.

_207. Quel type de trafic est décrit comme nécessitant au moins 384 Kbit/s de bande passante ?

- voix
- données
- **vidéo**

_208. Quelle étape du processus de routage à état des liens est décrite par un routeur insérant les meilleurs chemins dans la table de routage ?

- déclarer un voisin inaccessible
- exécuter l'algorithme SPF
- chemins d'équilibrage de charge à coût égal
- **choisir le meilleur itinéraire**

_209. Toute entreprise a décidé de réduire son empreinte environnementale en réduisant les coûts énergétiques, en déménageant dans une installation plus petite et en favorisant le télétravail. Quel service ou technologie répondrait à cette exigence ?

- centre de données
- virtualisation

- **services cloud**
- serveurs dédiés

_210. Quelle technique QoS lisse le débit de sortie des paquets ?

- police
- **mise en forme**
- détection précoce aléatoire pondérée
- Services intégrés (IntServ)
- marquage

_212. Un technicien réseau configure SNMPv3 et a défini un niveau de sécurité SNMPv3 authPriv. Quelle est la fonctionnalité d'utilisation de ce niveau ?

- authentifie un paquet en utilisant uniquement l'algorithme SHA
- authentifie un paquet par une correspondance de chaîne du nom d'utilisateur ou de la chaîne de communauté
- **authentifie un paquet en utilisant soit la méthode HMAC avec MD5, soit la méthode SHA**
- authentifie un paquet en utilisant les algorithmes HMAC MD5 ou HMAC SHA et un nom d'utilisateur