Quelles sont les deux conditions qui poussent à préférer la norme 802.11g à la norme 802.11a ? (Choisissez deux réponses.)

La portée de la norme 802.11a est plus courte que celle de la norme 802.11g.

La bande de fréquence de 2,4 GHz n'est pas aussi fréquentée que la bande de fréquence de 5 GHz.

La norme 802.11a est plus vulnérable aux interférences RF émanant des appareils courants.

La norme 802.11a utilise une technique de modulation plus onéreuse que celle de la norme 802.11g.

La norme 802.11g est compatible en amont avec la norme 802.11b. La norme 802.11a ne l'est pas.

2 Quels périphériques centralisent l'administration des réseaux locaux sans fil importants qui se composent de centaines de points d'accès ? (Choisissez deux réponses.)

☐ Cartes réseau sans fil gérées

☒ **Contrôleur de réseau local sans fil**

☒ **Points d'accès ultra-légers**

☐ Système d'exploitation de réseau sans fil

☐ Antenne sans fil

3 Quelles conditions ou restrictions s'appliquent aux points d'accès sans fil Cisco ? (Choisissez deux réponses.)

☐ Les points d'accès utilisent WLC pour réduire le problème de nœud caché.

☒ **L'atténuation du signal RF restreint directement la portée du point d'accès.**

☒ **L'accès au média est contrôlé à l'aide d'un mécanisme « distribué ».**

☐ Un point d'accès est un périphérique de couche 2 qui fonctionne comme un commutateur Ethernet 802.3.

☐ L'accès multiple avec écoute de porteuse/évitement de collision (CSMA/CA) utilise une fonction de coordination sans restriction nommée PCF.

4 Quelles méthodes d'authentification sont spécifiées dans la norme 802.11 pour prendre en charge le processus d'association du client ? (Choisissez deux réponses.)

☐ Protocole LEAP

☒ **Clé partagée**

☐ AES

☐TKIP

☒**Ouverture de l'authentification**

5 Quelles affirmations relatives à la sécurité du réseau sont vraies ? (Choisissez trois réponses.)

☒**L'ouverture de l'authentification n'utilise pas de client ou de vérification AP.**

☐Le fonctionnement du protocole 802.11i est identique à celui du protocole WPA.

☐Un client sans fil s'associe d'abord à un point d'accès, puis s'authentifie pour accéder au réseau.

☒**Le protocole 802.11i intègre un serveur RADIUS pour l'authentification au niveau de l'entreprise.**

☐Le protocole 802.11i utilise l'algorithme de chiffrement 3DES.

☒**Le protocole TKIP permet de modifier les clés par paquet.**

6 Quelles restrictions ou additions relatives aux protocoles de sécurité sans fil sont valides ? (Choisissez deux réponses.)

☒**Lorsque vous utilisez le protocole 802.1x dans le cadre de la sécurité sans fil, les clients sont autorisés à s'associer à l'authentification ouverte pour le trafic RADIUS.**

☐Le mode personnel WPA2 permet d'utiliser RADIUS dans les environnements SOHO.

☒**Un serveur AAA est nécessaire pour la partie RADIUS du protocole 802.1x.**

☐Les clés pré-partagées ne sont pas autorisées dans le cadre de l'authentification avec WPA2.

☐WPA a introduit des mesures de sécurité : masquage du SSID et filtrage d'adresse MAC.

☐Contrairement à WPA, WPA2 propose l'authentification de port 802.1x.

7 Quelles affirmations relatives à la configuration des points d'accès sont vraies ? (Choisissez deux réponses.)

☐ Les points d'accès doivent être configurés avec WPA uniquement s'ils n'autorisent pas le chiffrement WEP.

☐ Définissez la bande radio standard ou 20 MHz si vous utilisez des périphériques Wireless-N, Wireless-B et Wireless-G.

☒ **Si vous avez sélectionné l'option Wide, le canal 40 MHz est sélectionné pour le paramètre de bande radio et le canal standard devient un canal secondaire pour Wireless-N.**

☐ La désactivation de la diffusion du SSID empêche toute connexion non autorisée au point d'accès.

☒ **AES fournit davantage de sécurité que TKIP.**

8 Quelle méthode d'installation fournit la connectivité à un nouveau réseau sans fil ?

○ Configurer le protocole WEP sur le point d'accès uniquement

⊙ **Configurer l'accès ouvert sur le point d'accès et sur chaque périphérique qui s'y connecte**

○ Configurer le chiffrement complet sur le point d'accès, tout en maintenant ouvert chaque périphérique connecté au réseau

○ Configurer le chiffrement complet sur chaque périphérique du réseau local sans fil, tout en maintenant ouverts les paramètres de point d'accès

9

Lisez l'exposé. Lors de la configuration du point d'accès sans fil, quel paramètre l'administrateur utilise-t-il pour configurer l'identifiant unique que les périphériques client utilisent pour différencier ce réseau sans fil des autres ?

○ Network Mode

⊙ **Network Name (SSID)**

○ Radio Band

○ Wide Channel

○ Standard Channel

10 Quelles affirmations relatives à la configuration du client sans fil sont vraies ? (Choisissez deux réponses.)

☐ La conservation d'un SSID nul sur un client Windows XP entraîne la diffusion d'une requête de SSID nul et le déclenchement d'une diffusion du SSID à partir du point d'accès.

☐ Le filtrage d'adresse MAC empêche un réseau sans fil de s'afficher dans les connexions réseau, à moins que l'adresse MAC spécifique ne soit autorisée sur le point d'accès.

☒ **L'ajout manuel d'un réseau et la configuration du SSID connu rend le réseau visible lorsque vous cliquez sur l'icône Connexions réseau de Windows XP, même si le SSID n'est pas en cours de diffusion.**

☐ Un réseau sans fil nécessite que le SSID et la clé réseau soient visibles comme un réseau disponible.

☒ **Les SSID par défaut de points d'accès de fabricants spécifiques sont généralement connus et permettent de créer des connexions sans fil sauvages.**

11 Les utilisateurs sans fil d'un réseau se plaignent de faibles performances dans un petit périmètre d'une pièce. En

s'éloignant de cette zone, les performances augmentent considérablement. Quelle est la première étape pour trouver une solution à ce problème ?

- ⦿ **Il peut s'agir d'un chevauchement de canal RF. Le technicien doit vérifier les canaux en cours d'utilisation sur chaque point d'accès sans fil et les définir comme canaux sans chevauchement.**
- ○ Les paramètres d'alimentation RF peuvent être trop bas sur les points d'accès sans fil couvrant la pièce. Augmentez la puissance de sortie RF sur tous les points d'accès sans fil.
- ○ Installez un nouveau point d'accès sans fil au centre de cette zone pour garantir sa couverture.
- ○ Vérifiez que les points d'accès sans fil disposent d'une alimentation électrique suffisante et d'une connectivité au réseau filaire.

12 Quelle est la méthode préférentielle d'identification des interférences RF lorsque les points d'accès sans fil sont déployés dans un environnement fréquenté ?

- ○ Effectuer une évaluation manuelle du site, retirer tous les périphériques qui génèrent des interférences, puis installer les points d'accès.
- ○ Installer les points d'accès, puis modifier les canaux RF jusqu'à obtention du meilleur signal.
- ○ Effectuer une étude du site assistée par logiciel, puis installer les points d'accès en fonction des résultats obtenus.
- ○ Configurer tous les points d'accès sur des trépieds, puis, à l'aide d'un ordinateur portable, tester la connectivité en tous points de la zone.
- ⦿ **Effectuer une étude manuelle du site, suivie d'une étude assistée par logiciel.**

13 Quelles propriétés peuvent être modifiées pour améliorer le temps d'attente des clients du réseau local sans fil lors du roaming entre les points d'accès et de la tentative d'authentification à un nouveau point d'accès ? (Choisissez deux réponses.)

- ☒ **Augmenter la fréquence d'envoi des trames beacon par le point d'accès**
- ☒ **Augmenter l'intervalle d'analyse du client**
- ☐ Augmenter le nombre d'adresses IP disponibles dans le pool de serveurs du protocole DHCP
- ☐ Modifier les canaux ad hoc sur le client en définissant les mêmes canaux que ceux utilisés par les points d'accès
- ☐ Définir le type d'authentification OPEN sur le client