

- 7.1.2 Normes des réseaux locaux sans fil

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.
-

- 7.2.2 Protocoles de sécurité sans fil

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

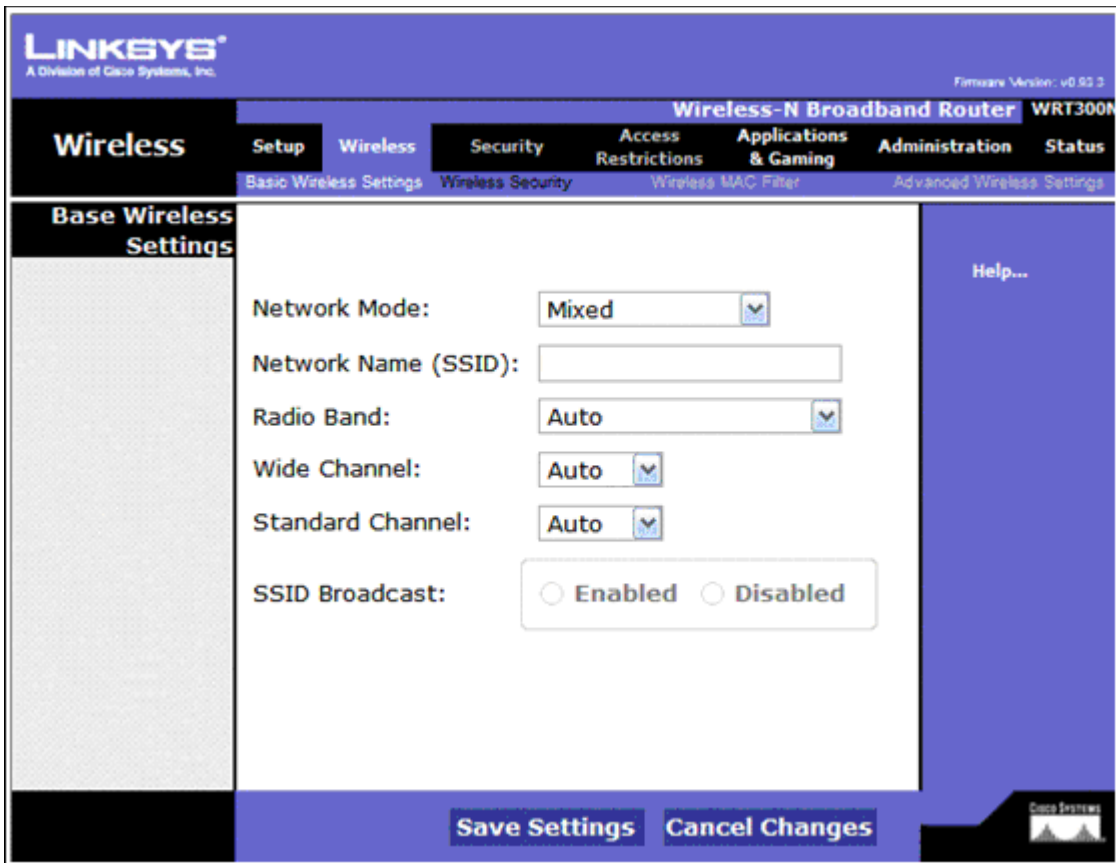
- Le protocole 802.11i utilise l'algorithme de chiffrement 3DES.
 - Une** authentification ouverte n'utilise aucune vérification du client ou de l'AP.
 - Le fonctionnement du protocole 802.11i est identique à celui du protocole WPA.
 - Le** protocole 802.11i intègre un serveur RADIUS pour l'authentification au niveau de l'entreprise.
 - Un client sans fil s'associe d'abord à un point d'accès, puis s'authentifie pour accéder au réseau.
-

- 7.3.1 Configuration du point d'accès sans fil

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
-

- 7.3.1 Configuration du point d'accès sans fil



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

- 7.2.3 Sécurisation d'un réseau local sans fil

Quelles affirmations relatives à la sécurité du réseau sans fil sont vraies ? (Choisissez deux réponses.)

- Le filtrage d'adresses MAC empêche la consultation du contenu des trames sans fil.
- La fourniture d'un client sans fil avec la clé de réseau permet de rendre visible un réseau disponible.
- La désactivation d'un point d'accès pour la diffusion du SSID empêche la découverte du point d'accès.
- Les SSID par défaut de points d'accès de fabricants spécifiques sont généralement connus et permettent de créer des connexions sans fil sauvages.
- L'ajout manuel d'un réseau et la définition du SSID connu sur un client sans fil rendent le réseau visible même si le SSID n'est pas diffusé.

- 7.4.2 Paramètres de canaux incorrects

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.
-

- 7.1.3 Composants d'une infrastructure sans fil

Quels sont les périphériques intégrés à de nombreux routeurs sans fil ? (Choisissez trois réponses.)

- Passerelle** de connexion à d'autres infrastructures réseau
 - Commutateur** Ethernet intégré
 - Station de gestion du réseau
 - Serveur VTP
 - Point** d'accès sans fil
 - Concentrateur de réseau privé virtuel
-

- 7.1.3 Composants d'une infrastructure sans fil

Quelle méthode d'accès le point d'accès sans fil utilise-t-il pour offrir une connectivité et un accès distribué à des utilisateurs multiples ?

- CSMA/CD
 - Passage de jeton
 - CSMA/CA**
 - interrogation
-

- 7.2.1 Menaces de sécurité sur les réseaux locaux sans fil

Pourquoi la sécurité est-elle si importante sur les réseaux sans fil ?

- Normalement, les réseaux sans fil sont plus lents que les réseaux câblés.
 - Les télévisions et autres appareils peuvent avoir des interférences avec les signaux sans fil.
 - Les réseaux** sans fil diffusent des données sur un support facile d'accès.
 - Les facteurs environnementaux comme les orages peuvent toucher les réseaux sans fil.
-

- 7.1.2 Normes des réseaux locaux sans fil

Quelle norme technologique sans fil propose la meilleure compatibilité avec les anciennes normes sans fil, mais a les meilleures performances ?

- 802.11a
 - 802.11b
 - 802.11g
 - 802.11n**
-

- 7.2.1 Menaces de sécurité sur les réseaux locaux sans fil

Quels sont les énoncés caractéristiques de la sécurité des réseaux sans fil ? (Choisissez deux réponses.)

- Un point d'accès** non autorisé représente un risque de sécurité pour le réseau local.
 - Les réseaux sans fil offrent les mêmes fonctions de sécurité que les réseaux câblés.
 - L'utilisation du chiffrement permet d'empêcher l'association des clients non autorisés avec un point d'accès.
 - Un pirate a besoin de l'adresse physique d'au moins un périphérique du réseau pour lancer une attaque.
 - Si la diffusion SSID** est désactivée, le pirate doit connaître le SSID auquel se connecter.
-

- 7.4.3 Résolution des problèmes radio et de logiciel au niveau des points d'accès

Quel processus de conception de réseau permet de déterminer où placer des points d'accès ?

- Évaluation de site**
 - Évaluation des risques
 - Conception d'évolutivité
 - Analyse des protocoles du réseau
-

- 7.2.2 Protocoles de sécurité sans fil

Quelle fonction de sécurité sans fil permet à l'administrateur réseau de configurer un point d'accès avec des identificateurs uniques de carte réseau sans fil, de sorte que seules ces cartes réseau puissent se connecter au réseau sans fil ?

- Authentification
 - Diffusion SSID
 - Filtrage d'adresse MAC
 - Protocole EAP (Extensible Authentication Protocol)
 - Radius (Remote Authentication Dial-In User Service)
-

- 7.1.4 Fonctionnement sans fil

Que transmet un client sans fil pour découvrir les réseaux WLAN disponibles ?

- Beacon
 - Mot de passe
 - Requête d'analyse
 - Demande d'association
-

- 7.4.2 Paramètres de canaux incorrects

Dans un réseau local sans fil (WLAN), lors de la mise en oeuvre des points d'accès sans fil, pourquoi chaque point d'accès doit-il utiliser un canal de communication différent ?

- Pour garder les utilisateurs sur des sous-réseaux différents
 - Pour contrôler la largeur de bande passante utilisée
 - Pour empêcher les interférences entre signaux
 - Pour sécuriser le trafic
-

- 7.2.2 Protocoles de sécurité sans fil

Quelle est l'objectif de l'authentification dans un WLAN ?

- Convertir les données en texte clair avant la transmission
- Indiquer les canaux de communication sur lesquels les données doivent circuler

- Déterminer** qu'il s'agit de l'hôte correct qui utilise le réseau
 - Permettre à l'hôte de choisir quel canal utiliser
-

- 7.2.1 Menaces de sécurité sur les réseaux locaux sans fil

Que se passe-t-il lorsqu'un point d'accès non autorisé est ajouté à un WLAN ?

- Les points d'accès autorisés peuvent transmettre l'excès de trafic aux points d'accès non autorisés pour réduire les encombrements.
 - Des utilisateurs** non autorisés peuvent accéder aux serveurs internes et créer une faille au niveau de la sécurité.
 - Tout le trafic qui utilise le même canal que le point d'accès non autorisé sera chiffré.
 - Tout le trafic qui utilise le même canal que le point d'accès non autorisé devra s'authentifier.
-

- 7.2.1 Menaces de sécurité sur les réseaux locaux sans fil

Quelle procédure permet d'empêcher une attaque de type « l'homme du milieu » ?

- Forcer tous** les périphériques d'un WLAN à s'authentifier et contrôler ceux qui sont inconnus.
 - Autoriser les points d'accès à envoyer un SSID à chaque périphérique qui souhaite utiliser le réseau.
 - Configurer le filtrage MAC sur tous les points d'accès autorisés.
 - Désactiver la diffusion SSID
-

- 7.1.3 Composants d'une infrastructure sans fil

Quelle fonction le point d'accès sans fil fournit-il ?

- Il assigne dynamiquement une adresse IP à l'hôte.
 - Il fournit les services DHCP locaux.
 - Il convertit les** données de l'encapsulation de trame 802.11 à 802.3.
 - Il fournit une passerelle pour la connexion à d'autres réseaux.
-

- 7.1.3 Composants d'une infrastructure sans fil

Quel problème majeur l'accès multiple avec écoute de porteuse et évitement de collision (CSMA/CA) permet-il de résoudre dans les réseaux sans fils ?

- Saturation de bande passante
 - Problèmes de confidentialité
 - Conflit d'accès** aux supports
 - Interfonctionnement des périphériques
-

- 7.1.4 Fonctionnement sans fil

Qu'utilise un point d'accès sans fil pour permettre aux clients WLAN de trouver les réseaux disponibles dans une zone donnée ?

- Réponse d'association
 - Beacon**
 - Clé
 - Requête d'analyse
-