



Activation de l'accès réseau sans fil invité

L'extension du réseau de l'entreprise avec Cisco Small Business Wireless Access Point est une solution simple qui permet de connecter les employés aux opérations commerciales, quel que soit leur emplacement (sur site ou à distance). Un point d'accès sans fil (AP) Cisco Small Business tel que le WAP4410N peut être facilement intégré au réseau filaire existant afin de fournir un réseau sans fil N, offrant une vitesse et une sécurité équivalentes à celles d'une connexion filaire standard. La fonctionnalité Cisco d'accès invité sans fil vous permet d'offrir la même mobilité et la même commodité aux clients et aux autres visiteurs.

Elle représente une méthode pratique et rentable pour proposer l'accès sans fil aux visiteurs, tout en préservant la sécurité de votre réseau interne. Un réseau invité peut servir de nombreux objectifs commerciaux importants, y compris la rationalisation des opérations commerciales avec les partenaires, et l'hospitalité envers les clients. Un réseau invité sans fil peut offrir les fonctionnalités de base suivantes :

- Accès Internet pour les invités par l'intermédiaire d'une connexion sans fil ouverte.
- Le trafic sur le réseau invité doit être complètement séparé du réseau de l'entreprise, afin d'empêcher qu'un invité accède aux ressources réseau internes.
- L'accès sans fil peut être isolé au niveau de chaque invité, afin d'empêcher que les invités communiquent entre eux sur le réseau.

Ce conseil avancé fournit un guide pas-à-pas de la configuration requise pour activer l'accès invité sans fil dans un réseau Cisco Small Business, y compris le routage entre réseaux locaux virtuels (VLAN), l'agrégation, SSID, les paramètres de sécurité sans fil sur le routeur, le commutateur et les points d'accès.

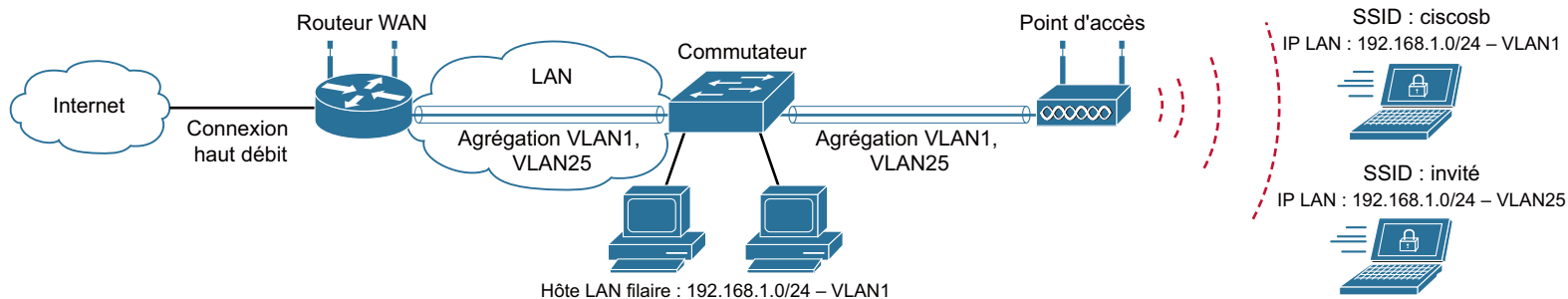
Principales caractéristiques

La combinaison de la fonction de routage entre réseaux locaux virtuels (VLAN) assurée par le routeur Cisco RV avec la fonctionnalité d'isolation SSID sans fil fournie par un point d'accès de type PME constitue une solution d'accès invité sans fil simple et sécurisée sur tout type de réseau d'entreprise Cisco existant, sans coût supplémentaire. Toutefois, un point d'accès (AP) sans fil pour PME n'offre pas exactement les mêmes fonctionnalités d'accès invité que celles d'une solution Cisco Unified Wireless.

Routage entre réseaux locaux virtuels (VLAN) - Les périphériques réseau situés dans des réseaux locaux virtuels (VLAN) différents ne peuvent pas communiquer entre eux sans un routeur qui achemine le trafic entre ces derniers. Dans un réseau d'entreprise, le routeur assure le routage entre les réseaux locaux virtuels pour les réseaux filaires et sans fil. Lorsque le routage entre réseaux locaux virtuels est désactivé au niveau d'un réseau local virtuel spécifique, les hôtes situés sur ce dernier ne peuvent pas communiquer avec les hôtes ou les périphériques installés sur un autre réseau local virtuel.

Isolation SSID sans fil - Il existe deux types d'isolation SSID sans fil. Lorsque l'isolation sans fil (au sein de SSID) est activée, les hôtes situés sur le même SSID ne

Figure 1 Activation de l'accès invité WLAN



213266

peuvent pas se voir. Lorsque l'isolation sans fil (entre SSID) est activée, le trafic sur un SSID n'est pas acheminé vers un autre SSID.

Produits proposés

- Point d'accès sans fil N Cisco WAP4410N avec PoE (Power over Ethernet)
- Routeur du pare-feu VPN sans fil N Cisco RV120W
- Commutateur intelligent Cisco SLM224P ou SLM224G

Conseils de conception

Réseau local virtuel (VLAN) invité - Un réseau local virtuel distinct doit être créé sur l'ensemble du réseau pour l'accès invité. VLAN ID 25 est utilisé pour le réseau local virtuel invité dans l'exemple fourni dans ce document. Le VLAN par défaut (VLAN 1) est utilisé pour toutes les communications de données filaires et sans fil. Le VLAN voix (VLAN 100) peut être utilisé pour toutes les communications de données.

ROUTAGE ENTRE RÉSEAUX LOCAUX VIRTUELS - Le routeur d'entreprise Cisco assure le routage entre réseaux locaux virtuels pour les différents réseaux locaux virtuels qu'il regroupe à partir de commutateurs ou des ports de commutation intégrés sur le routeur. Le routage entre réseaux locaux virtuels (VLAN) doit être activé pour les réseaux locaux virtuels standard, et désactivé pour le réseau local virtuel invité.

SSID sans fil - Les points d'accès (AP) Cisco pour PME prennent en charge plusieurs SSID, dont un pour le réseau interne et un autre pour le réseau invité. Dans l'exemple fourni dans ce document, le SSID pour le réseau sans fil interne est le SSID par défaut (ciscosb) qui est préconfiguré sur le WAP4410N. Il est recommandé de changer le SSID par défaut afin de renforcer la sécurité. Le SSID de l'accès invité sans fil est *guest*.

Sécurité sans fil - Il est important d'appliquer la sécurité sans fil sur le réseau local WLAN interne. WPA2 Personal et WPA2 Entreprise fournissent l'un comme l'autre une protection sans fil appropriée. WPA2 Personal utilise une clé partagée, tandis que WPA2 Entreprise utilise un nom d'utilisateur/mot de passe pour chaque employé, ce qui nécessite un serveur d'authentification externe. Pour le WLAN invité, l'authentification ouverte illustrée dans notre exemple est pratique. Toutefois, l'authentification personnelle WPA/WPA2 peut être appliquée, selon les exigences de sécurité.

Isolation sans fil - L'isolation sans fil entre les SSID doit être activée au niveau de chaque SSID. L'isolation sans fil au sein du SSID doit être activée pour le SSID invité, et désactivée pour le SSID utilisé pour le WLAN interne. Cette configuration permet aux hôtes du WLAN d'entreprise de communiquer entre eux, contrairement aux invités.

Agrégation - Différents SSID sont mappés sur différents VLAN sur points d'accès. Dans cet exemple, le SSID *ciscosb* est mappé sur VLAN 1 et le SSID *guest* est mappé sur le VLAN 25 invité. Ceci connecte le point d'accès au commutateur à l'aide d'une

agrégation. L'activation de la configuration VLAN sur WAP4410N modifie la connexion Ethernet en mode d'agrégation. VLAN 1 est considéré comme le VLAN natif sans étiquetage, tandis que VLAN 25 est étiqueté sur l'agrégation. La connexion Ethernet entre le routeur et le commutateur est également une agrégation qui transporte les paquets étiquetés de différents VLAN, tel que VLAN 1 pour les données, VLAN 100 pour la voix et VLAN 25 pour l'accès invité.

Schéma du réseau

Figure 1 illustre un exemple de mise en œuvre de l'accès invité sans fil à l'aide d'un point d'accès (AP) sans fil, d'un routeur et d'un commutateur Cisco professionnels. Le point d'accès sans fil est connecté au commutateur et utilise l'interface d'agrégation pour transporter plusieurs paquets VLAN. Le commutateur est connecté au routeur WAN par l'intermédiaire de l'interface d'agrégation, et le routeur WAN assure le routage entre les réseaux locaux virtuels (VLAN). Le routeur WAN est connecté à l'Internet par l'intermédiaire d'une connexion Internet haut débit. Tous les hôtes filaires sont connectés au commutateur, et les périphériques sans fil sont connectés au point d'accès.

Le SSID (ciscosb) par défaut est mappé sur VLAN 1 sur le réseau 192.168.1.0/24. Le SSID d'accès invité (guest) est mappé sur VLAN 25 sur le réseau 192.168.2.0/24. En conséquence, un ordinateur portable assigné à une adresse IP sur le réseau invité peut accéder à Internet, mais pas au réseau interne.

Configuration de l'accès réseau sans fil invité

Cette section décrit la configuration de l'accès réseau sans fil invité sur un routeur Cisco Small Business, un commutateur et un point d'accès Cisco.

Liste de contrôle de préconfiguration

Sur le réseau filaire - Le réseau filaire d'entreprise existant doit être construit avec un routeur Cisco Small Business, tel qu'un RV120W et un commutateur de la gamme Cisco SLM. Le réseau étendu WAN et le paramètre LAN doivent être configurés sur le routeur RV120W. Le commutateur SLM est connecté au routeur WAN à l'aide d'une agrégation, et chaque hôte interne est relié par câble au commutateur. Le réseau local virtuel par défaut (VLAN 1) ou tout autre réseau local virtuel dédié est utilisé pour toutes les communications de données.

En option, le VLAN voix est utilisé pour les communications vocales. Tous les hôtes internes peuvent accéder à Internet et communiquer entre eux.

Sur le réseau sans fil - Le point d'accès (AP) Cisco WAP4410N est connecté au commutateur SLM et est configuré en mode PA. Le SSID par défaut ou un nouveau SSID est utilisé pour les communications sans fil internes avec la sécurité sans fil WPA ou WPA2 activée pour ce SSID. Les ordinateurs portables internes connectés à ce réseau sans fil peuvent accéder aux ressources Internet et aux ressources réseau internes.

Reportez-vous aux autres conseils avancés Cisco Small Business concernant la connexion d'un routeur et d'un commutateur avec plusieurs réseaux locaux virtuels

(VLAN), la configuration de l'accès WAN, la création d'un réseau sans fil de base et l'activation de la sécurité sans fil.

Ajout et configuration d'un VLAN d'accès invité sur un routeur RV

Cette section décrit l'ajout de VLAN 25 pour l'accès invité, la configuration du routage entre réseaux locaux virtuels (VLAN) et la vérification des paramètres de sous-réseau IP sur le routeur RV120W.

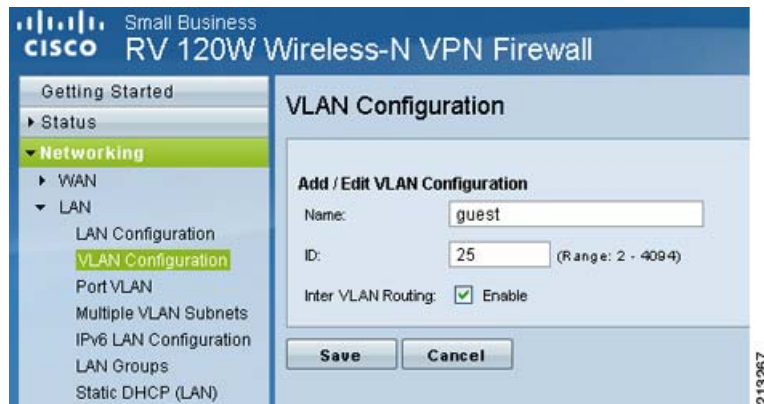
Étape 1 Accédez à **Networking > LAN > VLAN Configurations** et cliquez sur **Add** pour ajouter un réseau local virtuel.

Étape 2 Entrez *guest* comme nom, et 25 pour l'ID, et cliquez sur **Save**.



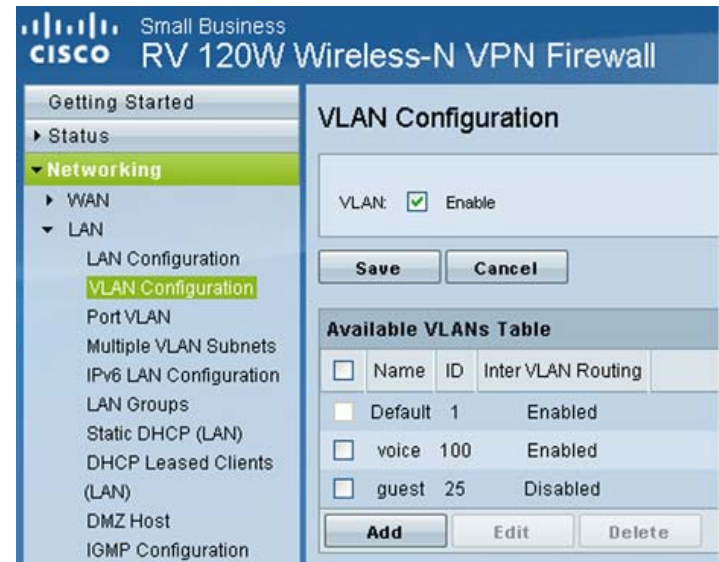
Remarque Ne cochez pas la case *Enable* en regard de l'option *Inter VLAN Routing*.

Figure 2 Ajout/modification de la configuration du réseau local virtuel (VLAN)



La page récapitulative (Figure 3) affiche tous les réseaux locaux virtuels (VLAN), y compris le réseau local virtuel invité qui vient d'être ajouté. Le routage entre réseaux locaux virtuels est activé pour les autres réseaux locaux virtuels, à l'exception du réseau local virtuel invité.

Figure 3 Activation et enregistrement de la configuration du réseau local virtuel



Étape 3 Si un commutateur est connecté au routeur, accédez à **Networking > LAN > Port VLAN**, sélectionnez le port d'agrégation qui est connecté au commutateur et cliquez sur **Edit**.

Figure 4 Réseau local virtuel (VLAN) des ports



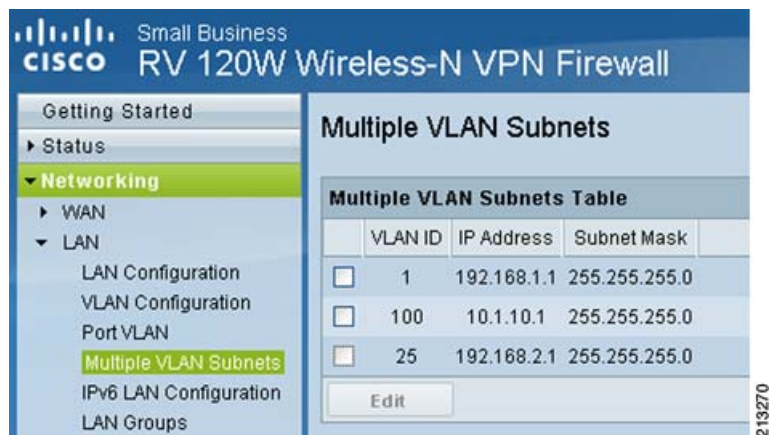
Étape 4 Cochez la case correspondant à VLAN 25 dans la section VLAN Membership Configuration et cliquez sur **Save**.



Remarque Si vous souhaitez activer l'accès réseau invité filaire sur le routeur, vous pouvez le faire à ce stade. Définissez le port de commutation intégré en mode d'accès et entrez 25 dans la zone PVID.

Étape 5 Accédez à **Networking > LAN > Multiple VLAN Subnets** pour vérifier l'adresse réseau IP du VLAN invité.

Figure 5 Sous-réseaux locaux virtuels (VLAN) multiples



Le VLAN 25 apparaît déjà ici. Il est affecté au réseau 192.168.2.0/24, et le protocole DHCP est également activé sur ce sous-réseau par défaut. Sélectionnez **VLAN 25** et cliquez sur le bouton **Edit** si vous souhaitez modifier l'adresse IP du sous-réseau local virtuel (VLAN) invité.

Ajout d'un réseau local virtuel (VLAN) d'accès invité au commutateur du réseau local (LAN)

Cette section explique comment ajouter un VLAN 25 d'accès invité sur le commutateur de réseau local SLM224G et inclure ce réseau local virtuel VLAN sur son agrégation vers le routeur. Si le point d'accès (AP) est connecté au routeur directement, veuillez ignorer cette section. Reportez-vous aux autres conseils avancés concernant la configuration du réseau local virtuel (VLAN) et de l'agrégation sur les commutateurs d'entreprise Cisco.

Étape 1 Accédez à **VLAN Management > Create VLAN**, entrez 25 dans le champ VLAN ID, et tapez *guest* pour le nom du réseau local virtuel (VLAN).

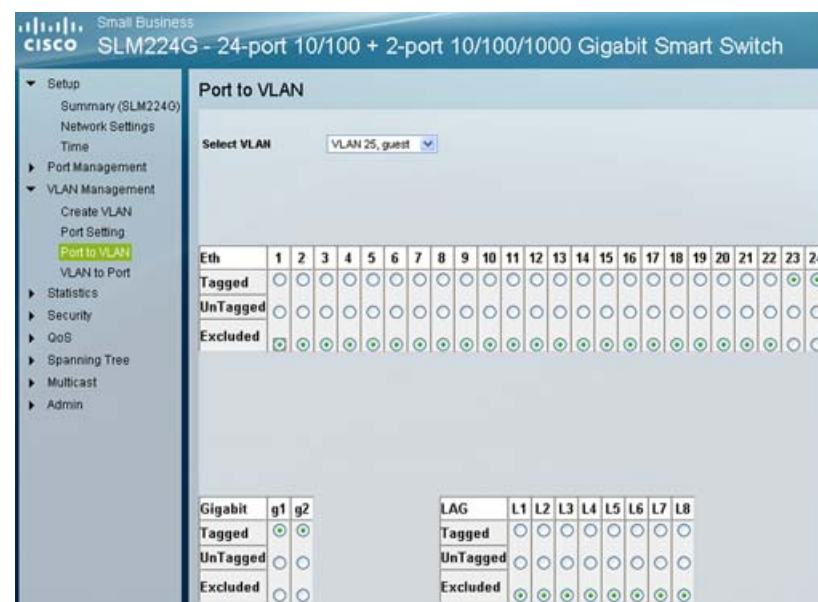
Étape 2 Accédez à **VLAN Management > Port to VLAN**, et sélectionnez « VLAN 25, guest » dans la liste déroulante.

Étape 3 Activez la case d'option **Tagged** pour l'interface d'agrégation.

La valeur par défaut est Excluded. Les interfaces d'agrégation font référence à l'interface connectée au routeur, ainsi qu'à l'interface connectée au point d'accès (AP).

Dans ce cas, Gigabit Interface g1 est connecté au routeur, et Ethernet 23, 24 sont connectés sur le point d'accès (AP) WAP4410N.

Figure 6 Port vers réseau local virtuel (VLAN)



Remarque Si vous souhaitez configurer l'accès réseau invité filaire pour le commutateur, vous pouvez également le faire à ce stade, en définissant le port de commutation correspondant en mode d'accès, avec VLAN 25 non étiqueté.

Configuration des paramètres WLAN invité sur un point d'accès WAP4410N

Dans cette section, vous allez ajouter un SSID pour l'accès invité et configurer ses paramètres sans fil sur le WAP4410N.

Étape 1 Accédez à **Wireless > Basic Settings** pour ajouter un nouveau SSID.

Étape 2 Entrez *guest* pour le SSID 2, activez la diffusion SSID et cliquez sur **Save**.

Figure 7 Paramètres sans fil de base



Étape 3 Accédez à **Wireless > Security** pour valider la configuration SSID actuelle.

La page initiale montre les paramètres de sécurité du premier SSID. Le paramètre de sécurité actuel concerne ciscosb qui utilise le SSID par défaut. Le mode de sécurité est défini sur la valeur WPA2-Personal. Vérifiez que l'option *Wireless Isolation (between SSID)* est activée (**Enabled**), et que l'option *Wireless Isolation (within SSID)* est désactivée (**Disabled**).

Figure 8 Sécurité sans fil



Étape 4 Dans la même page ci-dessus, sélectionnez le SSID invité dans la liste déroulante.

Étape 5 Définissez les options **Wireless Isolation (between SSID)** et **Wireless Isolation (within SSID)** sur la valeur **Enabled**, et désactivez **Security Mode** en sélectionnant la case d'option **Disabled**.

Figure 9 Activation de l'accès invité



Étape 6 Accédez à **Wireless > VLAN and QoS** pour mapper le SSID sur des réseaux locaux virtuels différents, et activez la case **Enabled** pour **VLAN**.

L'écran est mis à jour. Conservez VLAN 1 comme *Default VLAN ID* et *AP management VLAN*.

Étape 7 Conservez **VLAN Tag** avec la valeur **Untagged** et, dans la section QoS (QS), entrez **25** dans la zone VLAN ID pour le nom du SSID invité, puis cliquez sur le bouton **Save**.

Figure 10 VLAN et la qualité de service (QoS)



Validation de la configuration

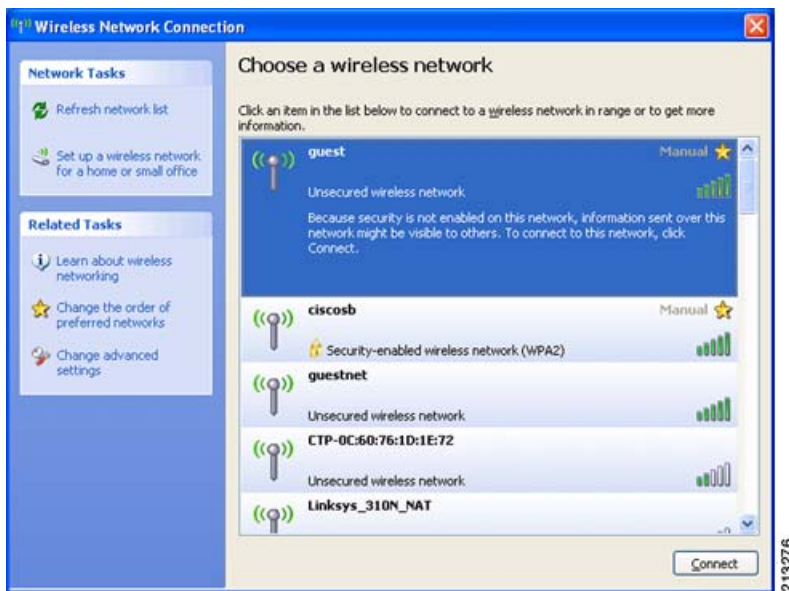
Étape 1 À partir d'un ordinateur portable sans fil, cliquez avec le bouton droit sur l'icône de connexion sans fil dans la barre d'état Windows dans la zone de notification, et sélectionnez **Afficher les réseaux sans fil disponibles**.

Étape 2 Sélectionnez SSID d'accès invité dans la liste et cliquez sur **Connexion**.

Le client sans fil doit être connecté au point d'accès et obtenir une adresse IP DHCP.

Étape 3 Vérifiez que l'ordinateur portable invité peut accéder à Internet et aux hôtes internes.

Figure 11 Validation de la configuration



CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, le logo Cisco, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband et Welcome to the Human Network sont des marques commerciales ; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card et One Million Acts of Green sont des marques de services et Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLXN, IOS, iPhone, IronPort, le logo IronPort, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx et le logo WebEx sont des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web sont la propriété de leurs détenteurs respectifs. L'utilisation du mot « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1002R) Les adresses de protocole Internet (IP) utilisées dans ce document ne sont pas supposées correspondre à des adresses réelles. Tous les exemples, résultats d'affichage de commandes et chiffres auxquels il est fait référence dans ce document sont donnés à titre indicatif uniquement. L'utilisation de toute adresse IP réelle à titre d'exemple est non intentionnelle et fortuite.

©2010 Cisco Systems, Inc. Tous droits réservés.



Par exemple, l'ordinateur portable connecté au WLAN invité doit pouvoir envoyer une requête ping www.cisco.com mais non pas 192.168.1.1 ou tout hôte avec une adresse IP interne (privée) (192.168.1.0/24).

Autres considérations

Gestion de l'accès invité sans fil

La fonction d'accès invité sans fil avancé peut rediriger les navigateurs invités vers une page de portail captive, qui peut afficher des informations, exiger un nom d'utilisateur et un mot de passe, ou exiger des invités qu'ils acceptent les termes et les conditions avant de les autoriser à continuer. Le point d'accès (AP) de la gamme Cisco Small Business Pro et la solution Cisco Unified Wireless fournissent ces fonctionnalités avancées, si nécessaire.

Utilisation du Wireless-N AP intégré sur un routeur WAN

Certains routeurs RV Cisco Small Business, notamment le RV120W, fournissent un Wireless-N AP intégré. L'accès invité sans fil peut être mis en œuvre sur un routeur WAN en suivant des étapes similaires à celles affichées pour le WAP4410N dans la section "Configuration de l'accès réseau sans fil invité" section à la page 2. Comme pour la configuration du WAP4410N, vous devez créer un SSID d'accès invité et le mapper sur un réseau local virtuel (VLAN) invité (le VLAN 25 est utilisé dans notre exemple).