



Für kleine  
und mittlere  
Unternehmen



## Aktivieren eines WLAN-Gastzugangs

Mit Cisco Small Business Access Point können Firmennetzwerke in kleinen und mittleren Unternehmen einfach erweitert werden. Mitarbeiter im Büro und unterwegs erhalten so jederzeit Zugriff auf Geschäftsvorgänge. Ein Wireless Access Point (AP) der Cisco Small Business-Serie, wie z. B. der WAP4410N, kann leicht in ein bestehendes Kabelnetzwerk integriert werden. Damit wird ein Wireless-N-Netzwerk bereitgestellt, dessen Geschwindigkeit und Sicherheit einer herkömmlichen Kabelverbindung in nichts nachstehen. Der Cisco Wireless-Gastzugang ermöglicht Ihnen die Bereitstellung der gleichen Mobilität und des gleichen Komforts für Kunden und andere Besucher.

Der Cisco Wireless-Gastzugang ist eine bequeme und kostengünstige Möglichkeit, einen drahtlosen Zugang für Besucher zu schaffen und gleichzeitig die Sicherheit des internen Netzwerks aufrechtzuerhalten. Ein Netzwerkzugang für Gäste hat viele wichtige Geschäftsaspekte. So können beispielsweise Geschäftsprozesse mit Partnern beschleunigt werden, und für Ihre Kunden ist er ein Zeichen Ihrer Gastfreundschaft. Ein WLAN für Gäste kann die folgenden Grundfunktionen zur Verfügung stellen:

- Internetzugang für Gäste über eine offene drahtlose Verbindung
- Vollständige Trennung des Gast-Netzwerks vom Firmennetzwerk, sodass kein Gast auf interne Netzwerkressourcen zugreifen kann
- Isolierter drahtloser Netzwerkzugang für jeden einzelnen Gast, um zu verhindern, dass Gäste miteinander über das Netzwerk kommunizieren

Dieser Smart Tip ist eine schrittweise Anleitung zur Konfiguration eines drahtlosen Gästezugangs für ein Cisco Small Business-Netzwerk. Darin enthalten sind Hinweise zu VLAN-übergreifendem Routing, Trunks, SSID und den Wireless-Sicherheitseinstellungen für Router, Switch und Access Points.

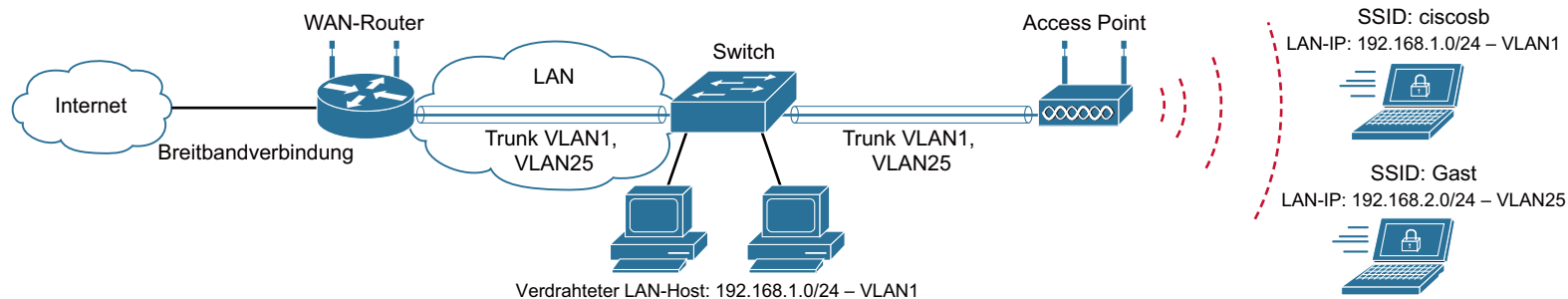
### Hauptmerkmale

Die Kombination von VLAN-übergreifendem Routing des Cisco RV-Routers mit der Wireless SSID-Isolierung der Small Business Wireless Access Points ermöglicht einen einfachen und sicheren Wireless-Gastzugang zu jedem vorhandenen Cisco Small Business-Netzwerk ohne zusätzliche Kosten. Natürlich bietet ein Small Business Wireless Access Point nicht genau dieselben Gastzugangsfunktionen wie eine Cisco Unified Wireless-Lösung.

**VLAN-übergreifendes Routing** – Netzwerkgeräte in verschiedenen VLANs können ohne einen Router, der den Verkehr zwischen den VLANs routet, nicht miteinander kommunizieren. In Netzwerken kleinerer und mittlerer Unternehmen führt der Router das VLAN-übergreifende Routing häufig sowohl für das LAN als auch das WLAN aus. Wenn das VLAN-übergreifende Routing für ein bestimmtes VLAN deaktiviert ist, können Hosts in diesem VLAN nicht mit Hosts oder Geräten anderer VLANs kommunizieren.

**Wireless SSID-Isolierung** – Es gibt zwei Arten der Wireless SSID-Isolierung. Bei aktivierter Wireless-Isolierung (innerhalb SSID) können Hosts mit der gleichen SSID einander nicht erkennen. Bei aktivierter Wireless-Isolierung (zwischen SSIDs) wird der Datenverkehr einer SSID an keinen andere SSID weitergeleitet.

Abbildung 1 Aktivieren des WLAN-Gastzugangs



213266

## Beschriebene Produkte

- Cisco WAP4410N Wireless-N Access Point mit Power over Ethernet (PoE)
- Cisco RV120W Wireless-N VPN Firewall-Router
- Cisco SLM224P oder SLM224G Smart Switch

## Tipps zur Ausführung

**Gast-VLAN** – Für einen Gastzugang muss ein separates neues VLAN über das gesamte Netzwerk erstellt werden. Im Beispiel in diesem Dokument wird die VLAN-ID 25 für das Gast-VLAN verwendet. Das Standard-VLAN (VLAN 1) wird für den gesamten LAN- und WLAN-Datenverkehr genutzt. Das Sprach-VLAN (VLAN 100) kann für alle Sprachverbindungen verwendet werden.

**VLAN-übergreifendes Routing** – Der Cisco Small Business-Router führt VLAN-übergreifendes Routing für verschiedene VLANs durch, die er von Switches oder integrierten Switch-Ports auf dem Router aggregiert. Das VLAN-übergreifende Routing sollte für alle regulären VLANs aktiviert und für das Gast-VLAN deaktiviert werden.

**Wireless SSID** – Cisco Small Business APs unterstützen mehrere SSIDs. Somit wird die Verwendung einer SSID für das interne Netzwerk und einer anderen SSID für das Gast-Netzwerk ermöglicht. In diesem Beispiel wird die auf dem WAP4410N vorkonfigurierte Standard-SSID (ciscosb) für das interne WLAN verwendet. Für eine höhere Sicherheit wird die Änderung der Standard-SSID empfohlen. Die SSID für den WLAN-Gastzugang lautet *guest*.

**Wireless-Sicherheit** – Die Anwendung von Wireless-Sicherheit auf das interne Netzwerk ist von großer Bedeutung. WPA2-Personal und WPA2-Enterprise bieten beide gute Wireless-Sicherheit. WPA2-Personal verwendet einen gemeinsamen Schlüssel, während WPA2-Enterprise von jedem Mitarbeiter die Eingabe von Benutzername/Kennwort verlangt. Dafür wird ein externer Authentifizierungsserver benötigt. Die offene Authentifizierung für das Gast-WLAN in unserem Beispiel ist eine komfortable Lösung. Abhängig von den Sicherheitsanforderungen kann jedoch auch die persönliche WPA/WPA2-Authentifizierung angewendet werden.

**Wireless-Isolierung** – Die Wireless-Isolierung zwischen SSIDs sollte für jede SSID aktiviert werden. Die Wireless-Isolierung innerhalb der SSID sollte für die Gast-SSID aktiviert und für die SSID des internen WLAN deaktiviert sein. Diese Konfiguration ermöglicht den Hosts im Firmen-WLAN, miteinander zu kommunizieren. Gästen hingegen ist die Kommunikation untereinander verwehrt.

**Trunk** – Verschiedene SSIDs sind verschiedenen VLANs der Access Points zugeordnet. In diesem Beispiel ist die SSID *ciscosb* VLAN 1 zugewiesen und die SSID *guest* dem Gast-VLAN 25. Dadurch wird der Access Point über einen Trunk mit dem Switch verbunden. Das Aktivieren der VLAN-Konfiguration des WAP4410N bewirkt einen Wechsel der Ethernet-Verbindung zum Trunk-Modus. VLAN 1 wird als natives VLAN ohne Kennzeichnung (Tagging) behandelt, während VLAN 25 über den Trunk markiert wird. Die Ethernet-Verbindung zwischen Router und Switch fungiert ebenfalls als Trunk, der markierte Pakete von verschiedenen VLANs verarbeitet, z. B. Daten von VLAN 1, Sprachpakete von VLAN 100 und den Gastzugang von VLAN 25.

## Netzwerkdiagramm

Abbildung 1 zeigt die Beispielimplementierung eines drahtlosen Gastzugangs mithilfe von Cisco Small Business Wireless AP, Router und Switch. Der Wireless AP verbindet sich mit dem Switch und nutzt die Trunk-Schnittstelle zum Transport mehrerer VLAN-Pakete. Der Switch ist über die Trunk-Schnittstelle mit dem WAN-Router verbunden, der das VLAN-übergreifende Routing durchführt. Die Verbindung zum Internet wird über eine Breitband-Internetverbindung hergestellt. Alle verdrahteten Hosts stellen eine Verbindung mit dem Switch her, alle drahtlose Geräte stellen eine Verbindung mit dem Access Point her.

Die Standard-SSID (ciscosb) ist VLAN 1 des Netzwerks 192.168.1.0/24 zugeordnet. Die Gastzugangs-SSID (guest) ist VLAN 25 des Netzwerks 192.168.2.0/24 zugeordnet. Das führt dazu, dass ein Laptop, dem eine IP-Adresse im Gastnetzwerk zugewiesen wurde, zwar auf das Internet zugreifen kann, nicht aber auf das interne Netzwerk.

## Konfigurieren des WLAN-Gastzugangs

In diesem Abschnitt wird die Konfiguration eines drahtlosen Netzwerkzugangs für Gäste für einen Cisco Small Business-Router, Switch und Access Point beschrieben.

### Checkliste für die Vorkonfiguration

**Kabelnetzwerk** – Das vorhandene Kabelnetzwerk sollte aus den folgenden Komponenten bestehen: einem Cisco Small Business-Router, z. B. RV120W, und einem Switch der Cisco SLM-Serie. Die WAN- und LAN-Einstellung sollte auf dem RV120W-Router konfiguriert werden. Der SLM-Switch wird über einen Trunk mit dem WAN-Router verbunden, und jeder interne Host wird mit dem Switch verbunden. Das Standard-VLAN (VLAN 1) oder ein beliebiges dediziertes VLAN wird zur Datenkommunikation verwendet.

Optional wird das Sprach-VLAN für Sprachverbindungen genutzt. Alle internen Hosts können auf das Internet zugreifen und miteinander kommunizieren.

**Wireless-Netzwerk** – Der Cisco WAP4410N AP ist mit dem SLM-Switch verbunden und im AP-Modus konfiguriert. Für die interne Wireless-Kommunikation mit für diese SSID aktivierter WPA- oder WPA2-Wireless-Sicherheit wird die Standard-SSID oder eine neue SSID verwendet. Interne mit dem Wireless-Netzwerk verbundene Laptops haben sowohl Zugriff auf das Internet als auch auf interne Netzwerkressourcen.

In anderen Smart Tips-Dokumenten zur Cisco Small Business-Serie finden Sie Informationen dazu, wie Router und Switch mit mehreren VLANs verbunden werden, wie der WAN-Zugang konfiguriert wird, wie ein drahtloses Basisnetzwerk erstellt wird und wie Wireless-Sicherheit aktiviert wird.

### Hinzufügen und Konfigurieren des Gastzugang-VLAN auf einem RV-Router

In diesem Abschnitt wird das VLAN 25 für den Gastzugang hinzugefügt, das VLAN-übergreifende Routing konfiguriert und die IP-Subnetzeinstellungen auf dem Router RV120W überprüft.

**Schritt 1** Wechseln Sie zu **Networking > LAN > VLAN-Konfigurationen**, und klicken Sie dann auf **Hinzufügen**, um ein VLAN hinzuzufügen.

**Schritt 2** Geben Sie als Namen *guest* und als ID 25 ein, und klicken Sie auf **Speichern**.



**Hinweis** Achten Sie darauf, das Kontrollkästchen *Aktivieren* für *VLAN-übergreifendes Routing* nicht zu aktivieren.

**Abbildung 2** Hinzufügen/Bearbeiten der VLAN-Konfiguration



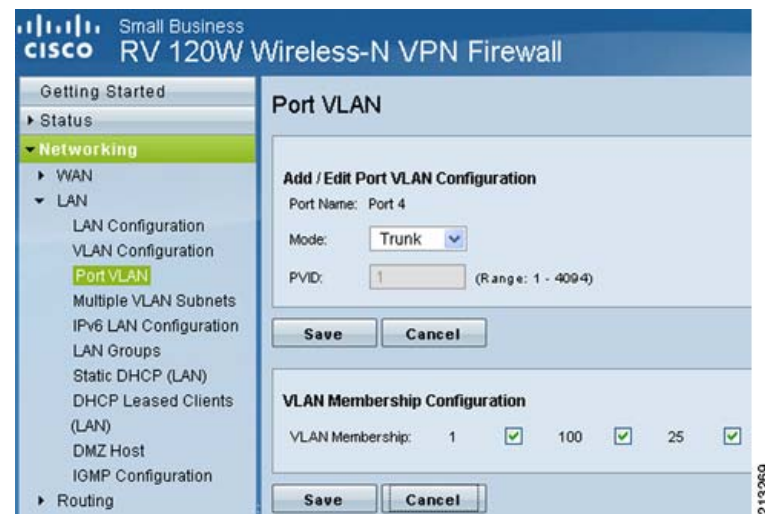
Die Übersichtsseite (Abbildung 3) zeigt alle VLANs, inklusive des Gast-VLAN, das gerade erst hinzugefügt wurde. Beachten Sie, dass VLAN-übergreifendes Routing für alle VLANs außer dem Gast-VLAN aktiviert wurde.

**Abbildung 3** Aktivieren und Speichern der VLAN-Konfiguration



**Schritt 3** Falls ein Switch mit dem Router verbunden ist, wechseln Sie zu **Networking > LAN > Port-VLAN**, wählen Sie den Trunk-Port aus, der mit dem Switch verbunden ist, und klicken Sie dann auf **Bearbeiten**.

**Abbildung 4** Port-VLAN

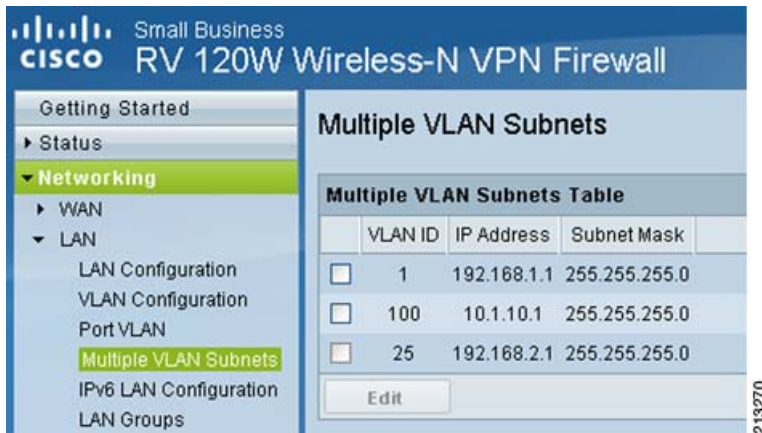


Schritt 4 Aktivieren Sie das Kontrollkästchen für VLAN 25 im Abschnitt für die Konfiguration der VLAN-Mitgliedschaft, und klicken Sie dann auf **Speichern**.

**Hinweis** Wenn Sie auf dem Router einen kabelgebundenen LAN-Gastzugang aktivieren möchten, können Sie diesen ebenfalls hier einrichten. Legen Sie den integrierten Switchport auf Zugriffsmodus mit 25 als PVID fest.

Schritt 5 Wechseln Sie zu **Networking > LAN > Mehrere VLAN-Subnetze**, um die IP-Netzwerkadresse für das Gast-VLAN zu überprüfen.

Abbildung 5 Mehrere VLAN-Subnetze



VLAN 25 wird hier bereits angezeigt. Es ist dem Netzwerk 192.168.2.0/24 zugeordnet, und DHCP ist auf diesem Subnetz standardmäßig aktiviert. Wählen Sie **VLAN 25** aus, und klicken Sie auf die Schaltfläche **Bearbeiten**, wenn Sie diese IP-Adresse des Gast-VLAN-Subnetzes ändern möchten.

### Hinzufügen des Gastzugang-VLAN zum LAN-Switch

In diesem Abschnitt wird das Gastzugang-VLAN 25 dem LAN-Switch SLM224G hinzugefügt und dieses VLAN in seinen Trunk zum Router eingefügt. Wenn der AP direkt mit dem Router verbunden ist, kann dieser Abschnitt übersprungen werden. Informationen zum Konfigurieren von VLAN und Trunk auf Cisco Small Business-Switches finden Sie in weiteren Smart Tips-Dokumenten.

Schritt 1 Wechseln Sie zu **VLAN-Management > VLAN erstellen**, geben Sie als VLAN-ID 25 und als VLAN-Namen *guest* ein.

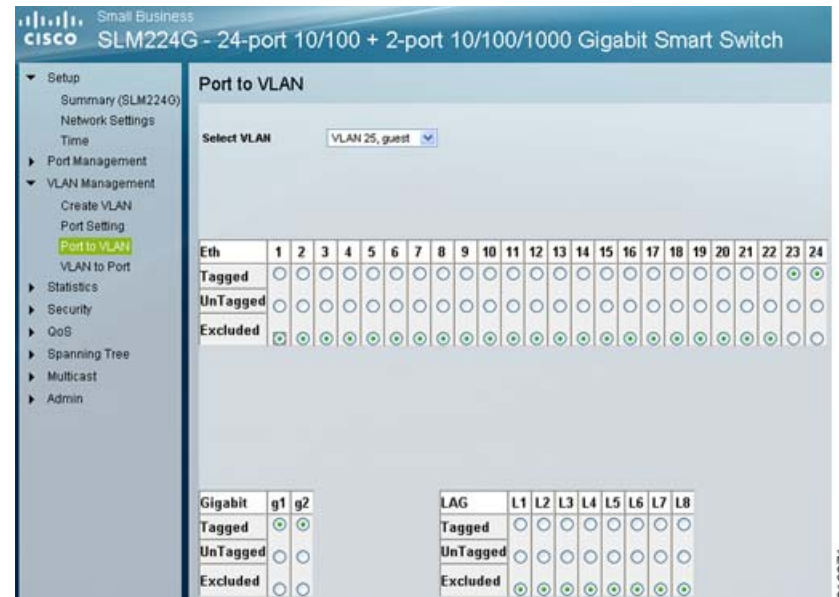
Schritt 2 Wechseln Sie zu **VLAN-Management > Port zu VLAN**, und wählen Sie in der Dropdownliste "VLAN 25, guest" aus.

Schritt 3 Aktivieren Sie die Option **Tagged** für die Trunk-Schnittstelle.

Der Standardwert ist ausgenommen. Die Trunk-Schnittstellen beziehen sich sowohl auf die Schnittstelle, die mit dem Router verbunden ist, als auch auf die Schnittstelle, die mit dem AP verbunden ist.

In diesem Fall ist die Gigabit-Schnittstelle g1 mit dem Router verbunden, und Ethernet 23, 24 sind mit AP WAP4410N verbunden.

Abbildung 6 Port zu VLAN



**Hinweis** Wenn Sie einen kabelgebundenen Gastzugang für einen Switch konfigurieren möchten, können Sie das hier tun, indem Sie den entsprechenden Switch-Port auf Zugriffsmodus mit VLAN 25 als unmarkiert festlegen.

### Konfigurieren der Gast-WLAN-Einstellungen für den Access Point WAP4410N

In diesem Abschnitt werden die SSID für den Gastzugang hinzugefügt und die Wireless-Einstellungen von WAP4410N festgelegt.

Schritt 1 Wechseln Sie zu **Wireless > Grundeinstellungen**, um eine neue SSID hinzuzufügen.

Schritt 2 Geben Sie als SSID2 *guest* ein, aktivieren Sie die SSID-Übertragung, und klicken Sie auf **Speichern**.

Abbildung 7 Grundlegende Wireless-Einstellungen



Schritt 3 Wechseln Sie zu **Wireless > Sicherheit**, um die aktuelle SSID-Konfiguration zu überprüfen.

Die erste Seite zeigt die Sicherheitseinstellungen für die erste SSID. Die aktuelle Sicherheitseinstellung gilt für die Standard-SSID ciscosb. Der Sicherheitsmodus ist auf "WPA2-Personal" festgelegt. Stellen Sie sicher, dass die *Wireless-Isolierung (zwischen SSIDs) aktiviert* und die *Wireless-Isolierung (innerhalb SSID) deaktiviert* ist.

Abbildung 8 Wireless-Sicherheit



Schritt 4 Wählen Sie auf derselben Seite die Gast-SSID aus der Dropdown-Liste aus.

Schritt 5 Legen Sie sowohl **Wireless-Isolierung (zwischen SSIDs)** als auch **Wireless Isolierung (innerhalb SSID)** auf **Aktiviert** und **Sicherheitsmodus** auf **Deaktiviert** fest.

Abbildung 9 Aktivieren des Gastzugangs



Schritt 6 Wechseln Sie zu **Wireless > VLAN und QoS**, um die SSID verschiedenen VLANs zuzuordnen, und aktivieren Sie **Aktiviert** für **VLAN**.

Die Anzeige wird aktualisiert. Behalten Sie VLAN 1 als *Standard-VLAN-ID* und *AP-Management-VLAN* bei.

Schritt 7 Behalten Sie das *VLAN-Tag* als **Untagged** bei, und geben Sie im QoS-Abschnitt **25** als VLAN-ID für den Gast-SSID-Namen ein. Klicken Sie anschließend auf **Speichern**.

Abbildung 10 VLAN und QoS



## Validieren der Konfiguration

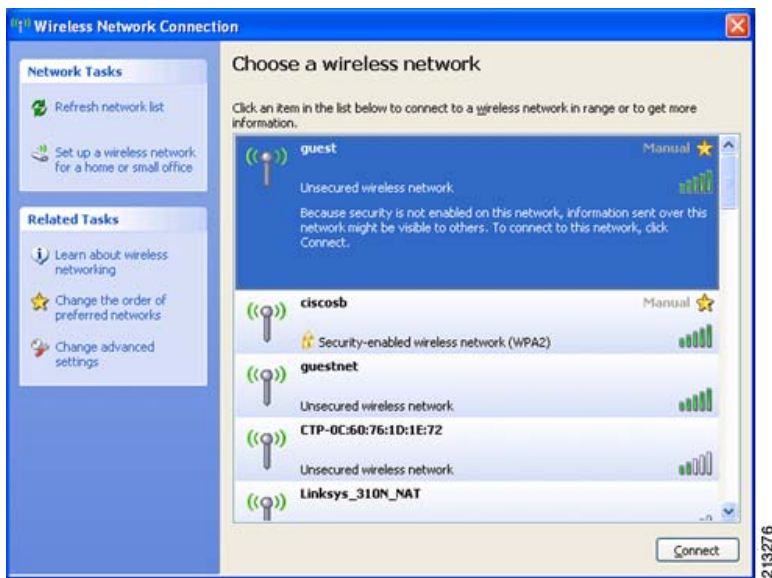
Schritt 1 Klicken Sie auf einem Wireless-Laptop im Benachrichtigungsbereich mit der rechten Maustaste auf das Windows Wireless-Taskleistensymbol , und wählen Sie **Verfügbares Wireless-Netzwerk anzeigen**.

Schritt 2 Wählen Sie die SSID „guest“ aus der Liste aus, und klicken Sie auf **Verbinden**.

Der Wireless-Client sollte mit dem Access Point verbunden sein und eine DHCP-IP-Adresse beziehen.

Schritt 3 Überprüfen Sie, ob das Gäste-Laptop auf das Internet und auf interne Hosts zugreifen kann.

### Abbildung 11 Validieren der Konfiguration



CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, das Cisco Logo, 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 und Welcome to the Human Network sind Marken, Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (stilisiert), Cisco Store, Flip Gift Card und One Million Acts of Green sind Dienstleistungsmarken, und Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, das Cisco Certified Internetwork Expert-Logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, das Cisco Systems Logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLXN, IOS, iPhone, IronPort, das IronPort Logo, 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 und das WebEx Logo sind eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und bestimmten anderen Ländern.

Alle anderen in diesem Dokument bzw. auf dieser Website erwähnten Handelsmarken sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1002R) Bei den in diesem Dokument verwendeten IP-Adressen soll es sich nicht um tatsächlich existierende Adressen handeln. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben und Abbildungen dienen lediglich der Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

© 2010 Cisco Systems, Inc. Alle Rechte vorbehalten.



Das Laptop sollte beispielsweise in der Lage sein, im Gäste-WLAN [www.cisco.com](http://www.cisco.com) zu pingen, nicht aber 192.168.1.1 oder andere Hosts mit internen (privaten) IP-Adressen (192.168.1.0/24).

## Sonstige Angaben

### Verwalten des WLAN-Gastzugangs

Mit einem erweiterten WLAN-Gastzugang können Gastbrowser zu einem Startportal umgeleitet werden, wo zusätzliche Informationen angezeigt werden oder Benutzername und Kennwort abgefragt werden. Es ist auch möglich, dass Benutzer zuerst speziellen Nutzungsbestimmungen zustimmen müssen, bevor sie fortfahren können. Ein erweiterter WLAN-Gastzugang wie oben beschrieben kann im Bedarfsfall mit dem AP der Cisco Small Business Pro-Serie und der Cisco Unified Wireless-Lösung bereitgestellt werden.

### Verwenden des integrierten Wireless AP auf einem WAN-Router

Einige Cisco Small Business RV-Router, wie der RV120W, bieten einen integrierten Wireless-N AP. Wireless-Gastzugang für einen WAN-Router kann mit ähnlichen Schritten wie den für den WAP4410N in „Konfigurieren des WLAN-Gastzugangs“ auf Seite 2 gezeigten implementiert werden. Wie bei der Konfiguration des WAP4410N müssen Sie eine Gast-SSID erstellen und einem Gast-VLAN zuordnen. In unserem Beispiel war dies VLAN 25.