

Enabling Wireless Guest Network Access

Expanding the small business network with Cisco Small Business Wireless Access Point is an easy way to connect employees to business operations, whether they're on-site or remote. A Cisco Small Business wireless access point (AP), such as the WAP4410N, can be easily integrated into the existing wired network to provide a Wireless-N network with speed and security rivaling a typical wired connection. The Cisco wireless Guest Access feature lets you offer the same mobility and convenience to clients and other visitors.

The Cisco Wireless Guest Access feature provides a convenient, cost-effective way to offer wireless access for visitors while maintaining the security of your internal network. A guest network can serve many important business purposes, including streamlining business with partners and providing hospitality for clients. A wireless guest network can provide the following basic functionality:

- Provide Internet access to guests through an open wireless connection
- Traffic on the guest network must be kept completely separate from the business network to prevent a guest from accessing internal network resources
- Wireless access for each guest can be isolated to prevent guests from communicating with each other over the network

This smart tip provides step-by-step guidance for the configuration required to enable wireless guest access in a Cisco small business network, including inter-VLAN routing, trunk, SSID, and wireless security settings on the router, switch, and access points.

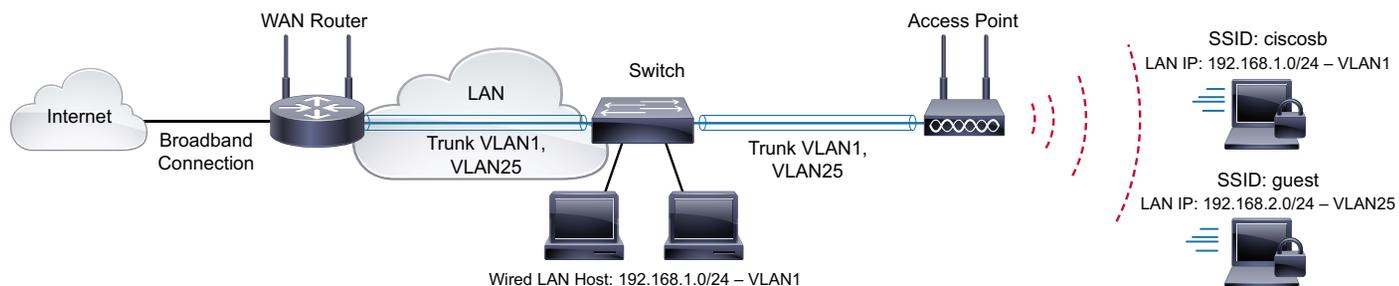
Key Features

Combining the Inter-VLAN routing feature provided by the Cisco RV router with the wireless SSID isolation feature provided by a small business access point provides a simple and secure solution for wireless guest access on any existing Cisco small business network at no additional cost. However, a small business wireless AP does not offer quite the same Guest Access functionality that is provided by a Cisco Unified Wireless solution.

Inter-VLAN routing—Network devices in different VLANs cannot communicate with each other without a router to route traffic between the VLANs. In a small business network, the router performs the Inter-VLAN routing for both the wired and wireless networks. When Inter-VLAN routing is disabled for a specific VLAN, hosts on that VLAN will not be able to communicate with hosts or devices on another VLAN.

Wireless SSID Isolation — there are two types of wireless SSID isolation. When Wireless Isolation (within SSID) is enabled, hosts on the same SSID will not be able to see each other. When Wireless Isolation (between SSID) is enabled, traffic on one SSID is not forwarded to any other SSID.

Figure 1 Enabling WLAN Guest Access



213266

Featured Products

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

Design Tips

Guest VLAN—A separate new VLAN must be created across the whole network for guest access. VLAN ID 25 is used for guest VLAN in the example provided in this document. The Default VLAN (VLAN 1) is used for all the wired and wireless data communication. The Voice VLAN (VLAN 100) can be used for all voice communications.

Inter-VLAN Routing—The Cisco small business router performs Inter-VLAN routing for different VLANs that it aggregates from switches or the integrated switchports on the router. Inter-VLAN routing should be enabled for regular VLANs and disabled for the guest VLAN.

Wireless SSID—Cisco small business APs support multiple SSIDs, which allows one SSID for the internal network and another SSID for the guest network. In the example used in this document, the SSID for the internal wireless network is the default SSID (ciscosb), which is preconfigured on the WAP4410N. It is recommended to change the default SSID to provide some additional security. The SSID for guest wireless access is *guest*.

Wireless Security—It is important to apply wireless security on the internal WLAN. WPA2 Personal or WPA2 Enterprise both provide good wireless protection. WPA2 Personal uses a shared key, while WPA2 Enterprise uses username/password for each employee, which requires an external authentication server. For the guest WLAN, the open authentication shown in our example is convenient. However, WPA/WPA2 personal authentication can be applied, depending on security requirements.

Wireless Isolation—Wireless Isolation between SSIDs should be enabled for each SSID. Wireless Isolation within the SSID should be enabled for the guest SSID and disabled for the SSID used for the internal WLAN. This configuration lets hosts in the small office WLAN communicate with each other, while guests cannot.

Trunk—Different SSIDs are mapped to different VLANs on access points. In this example, SSID *ciscosb* is mapped to VLAN 1 and the SSID *guest* is mapped to guest VLAN 25. This connects the access point to the switch using a trunk. Enabling VLAN configuration on WAP4410N changes the Ethernet connection into trunk mode. VLAN 1 is treated as the native VLAN without tagging, while VLAN 25 is tagged over the trunk. The Ethernet connection between the router and the switch is also a trunk, which carries packets tagged from different VLANs, such as VLAN 1 for data, VLAN 100 for voice, and VLAN 25 for guest access.

Network Diagram

Figure 1 illustrates the sample implementation for wireless guest access using a Cisco small business wireless AP, router and switch. The wireless AP connects to the switch and uses the trunk interface to transport multiple VLAN packets. The switch connects to the WAN router through the trunk interface and the WAN router performs Inter-VLAN routing. The WAN router connects to the Internet through a broadband Internet connection. All wired hosts connect to the switch and wireless devices connect to the access point.

The default SSID (ciscosb) is mapped to VLAN 1 on the 192.168.1.0/24 network. The guest access SSID (guest) is mapped to VLAN 25 on the 192.168.2.0/24 network. As a result, a laptop assigned an IP address on the guest network can access the Internet but not the internal network.

Configuring Guest Wireless Network Access

This section describes how to configure Guest wireless network access on a Cisco Small Business Router, Switch and Access Point.

Preconfiguration Checklist

On the Wired Network—The existing small office wired network should be built using a Cisco Small Business router, such as an RV120W, and a Cisco SLM series switch. The WAN and LAN setting should be configured on the RV120W router. The SLM switch is connected to the WAN router using a trunk and each internal host is wired to the switch. The default VLAN (VLAN 1), or any dedicated VLAN is used for data communication.

Optionally, the voice VLAN is used for voice communication. All the internal hosts are able to access Internet and communicate with each other.

On the Wireless Network—The Cisco WAP4410N AP is connected to the SLM switch and is configured in AP mode. The default SSID or a new SSID is used for internal wireless communication with WPA or WPA2 wireless security enabled for this SSID. Internal laptops connected to this wireless network can access both Internet and internal network resources.

Please refer to other Cisco Small Business Smart Tips on how to connect router and switch with multiple VLANs, how to configure WAN access, and how to create basic wireless network and enable wireless security.

Adding and Configuring Guest Access VLAN on an RV Router

The task of this section is to add VLAN 25 for guest access, configure Inter-VLAN routing, and verify IP subnet settings on the RV120W router.

Step 1 Go to **Networking > LAN > VLAN Configurations** and click **Add** to add a VLAN.

Step 2 Enter *guest* for the name and 25 for the ID and click **Save**.



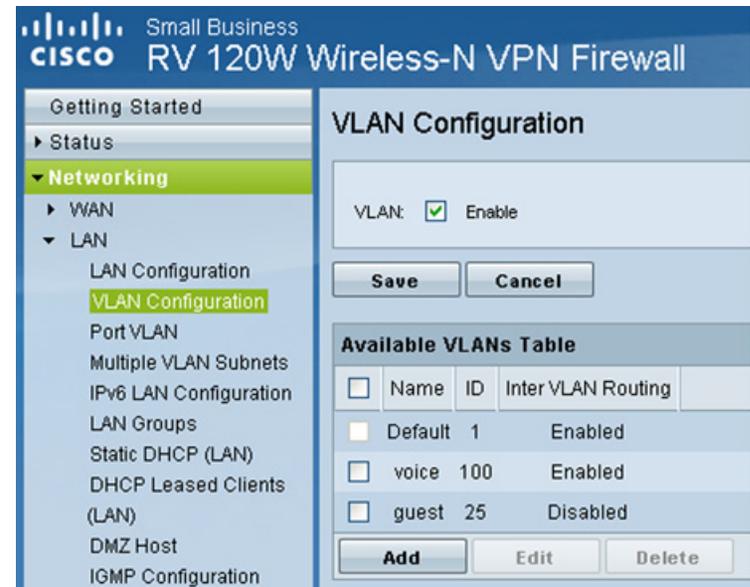
Note Do not check the *Enable* box for *Inter VLAN Routing*.

Figure 2 Add/Edit VLAN Configuration



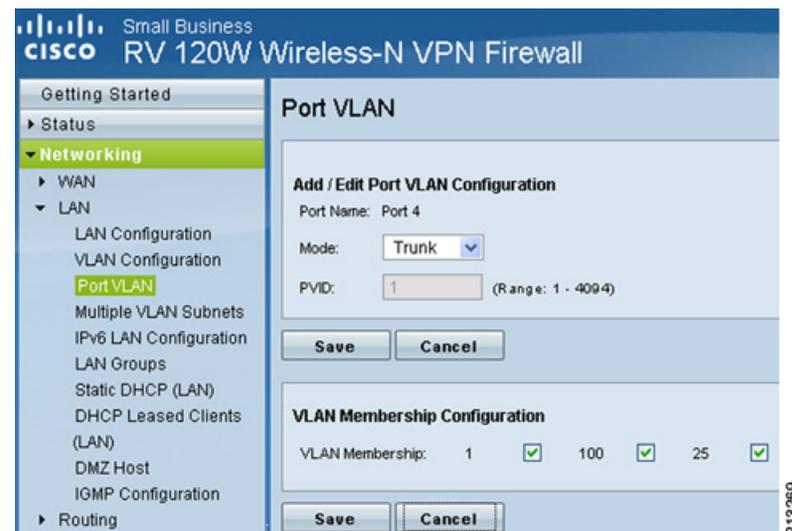
The summary page (Figure 3) shows all the VLANs, including the guest VLAN that was just added. Note that Inter VLAN routing is enabled for the other VLANs, except the guest VLAN.

Figure 3 Enable and Save VLAN Configuration



Step 3 If a switch is connected to the router, go to **Networking > LAN > Port VLAN**, select the trunk port that is connected to the switch, and click **Edit**.

Figure 4 Port VLAN



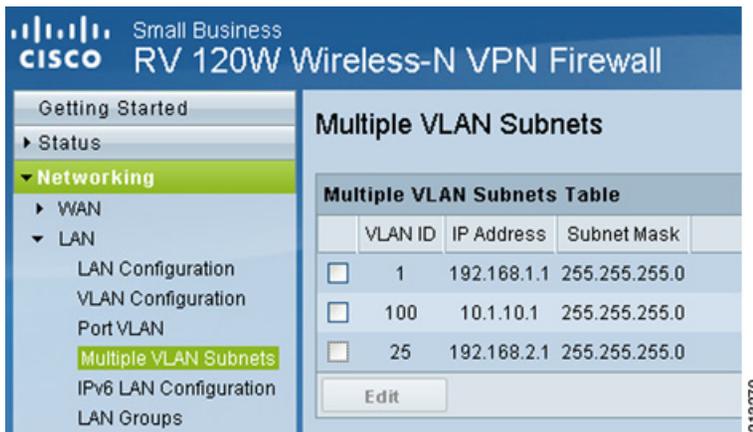
Step 4 Check the box for VLAN 25 in the VLAN Membership Configuration section and click **Save**.



Note If you want to enable wired guest network access on the router, this is also the place to do so. Set the integrated switch port to Access mode with 25 as the PVID.

Step 5 Go to **Networking > LAN > Multiple VLAN Subnets** to verify the IP network address for the guest VLAN.

Figure 5 Multiple VLAN Subnets



The VLAN 25 already appears here. It is assigned with 192.168.2.0/24 network and DHCP is also enabled on that subnet by default. Select *VLAN 25* and click **Edit** button if you want to change this IP address of the guest VLAN subnet.

Adding Guest Access VLAN to the LAN Switch

The task of this section is to add guest access VLAN 25 on the LAN switch SLM224G and include this VLAN on its trunk to the router. If the AP is connected to the router directly, please skip this section. Please refer to other smart tips on how to configure VLAN and trunk on Cisco small business switches.

Step 1 Go to **VLAN Management > Create VLAN**, input 25 for VLAN ID and *guest* for VLAN name.

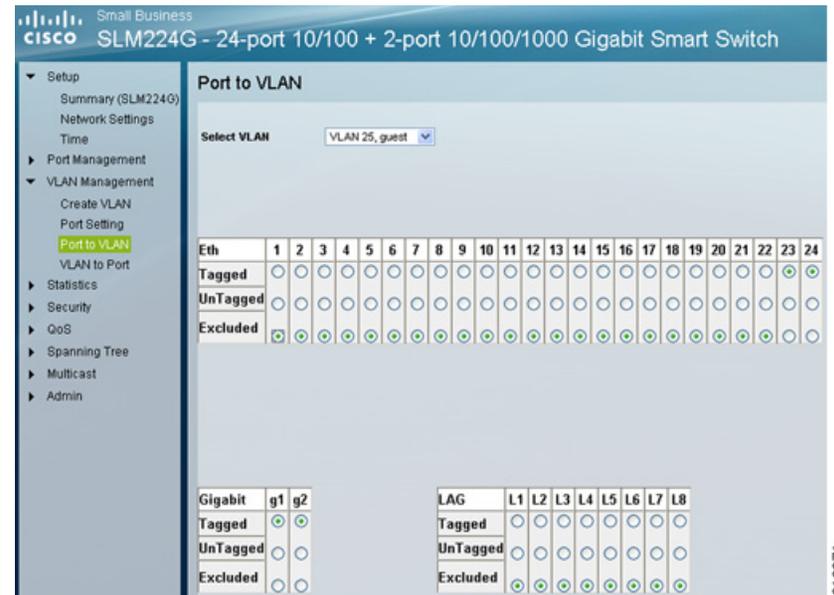
Step 2 Go to **VLAN Management > Port to VLAN**, select “VLAN 25, guest” in the drop-down list.

Step 3 Enabled the **Tagged** radio button for the trunk interface.

The default value is excluded. The trunk interfaces refer to both the interface connected to the router and the interface connected to the AP.

In this case, Gigabit Interface g1 is connected to the router and Ethernet 23, 24 are connected to the AP WAP4410N.

Figure 6 Port to VLAN



Note If you want to configure wired guest network access for switch, this is also the place to do so by setting the corresponding switch port to Access mode with VLAN 25 as untagged.

Configuring Guest WLAN Settings on a WAP4410N Access Point

In this section, you add SSID for guest access and configure its wireless settings on the WAP4410N.

Step 1 Go to **Wireless > Basic Settings** to add a new SSID.

Step 2 Enter *guest* for the SSID 2, enable the SSID broadcast, and click **Save**.

Figure 7 Basic Wireless Settings



Step 3 Go to **Wireless > Security** to validate the current SSID configuration.

The initial page shows the security settings for the first SSID. The current security setting is for ciscomb, which is the default SSID. The security mode is set to WPA2-Personal. Make sure that *Wireless Isolation (between SSID)* is **Enabled** while *Wireless Isolation (within SSID)* is **Disabled**.

Figure 8 Wireless Security



Step 4 In the same above page, select guest SSID from the drop-down list.

Step 5 Set both **Wireless Isolation (between SSID)** and **Wireless Isolation (within SSID)** to **Enabled** and set **Security Mode** to **Disabled**.

Figure 9 Enabling Guest Access



Step 6 Go to **Wireless > VLAN and QoS** to map the SSID to different VLANs and check **Enabled** for **VLAN**.

The screen will be updated. Keep the VLAN 1 as the *Default VLAN ID* and *AP management VLAN*.

Step 7 Keep the **VLAN Tag** as **Untagged** and in the QoS section, enter **25** as the VLAN ID for guest SSID name, and click the **Save** button.

Figure 10 VLAN and QoS



Validating the Configuration

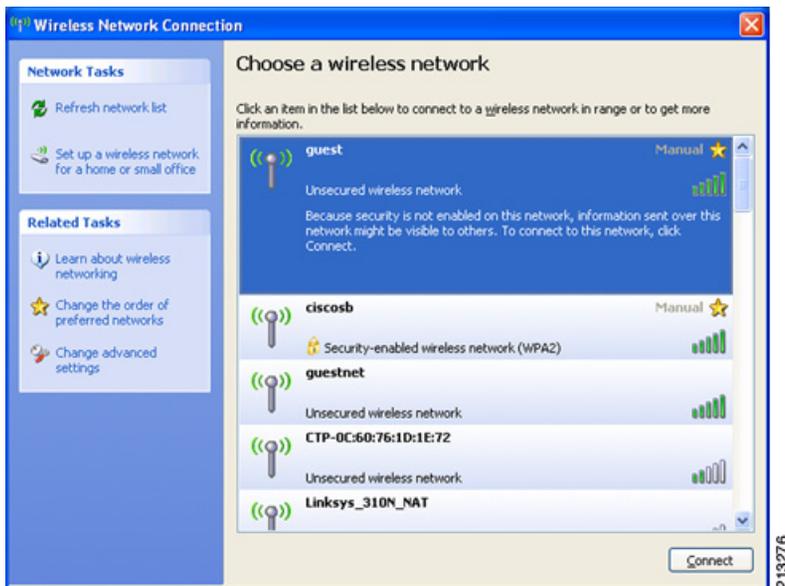
Step 1 From a wireless laptop, right-click the windows wireless tray icon in the notification area and select **View Available Wireless Network**.

Step 2 Select the SSID guest from the list and click **Connect**.

The wireless client should connect to the access point and get a DHCP IP address.

Step 3 Verify if the guest laptop can access the Internet and if the laptop can access internal hosts.

Figure 11 Validating the Configuration



219276

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2012 Cisco Systems, Inc. All rights reserved.

For example, the laptop connected to the Guest WLAN should be able to ping www.cisco.com but not 192.168.1.1 or any host with an internal (private) IP address (192.168.1.0/24).

Other Considerations

Managing Wireless Guest Access

The Advanced Wireless Guest Access feature can redirect guest browsers to a captive portal page, which can display information, require a user name and password, or require guests to consent to terms and conditions before allowing them to continue. The Cisco Small Business Pro series AP and the Cisco Unified Wireless Solution provide these advanced features, if required.

Using the Integrated Wireless AP on a WAN Router

Some Cisco small business RV routers, such as the RV120W, provide an integrated Wireless-N AP. Wireless Guest Access can be implemented on a WAN router by following similar steps to those shown for the WAP4410N in the "Configuring Guest Wireless Network Access" section on page 2. As with the WAP4410N configuration, you must create a guest SSID and map it to a guest VLAN, which in our example was VLAN 25.

