



print



email

Article ID: 4941

Enabling Multiple Wireless Networks on RV320 VPN Router, WAP321 Wireless-N Access Point, and Sx300 Series Switches

Objective

In an ever-changing business environment, your small business network has to be powerful, flexible, accessible, and highly reliable, especially when growth is a high priority. Since wireless devices became affordable, convenience, and are easy to use, their usage has been exponentially grew in recent years. Authentication permits the network devices to verify and guarantee legitimacy of a user and protect the network from unauthorized users. Wireless connectivity can offer to the user's mobility capability and option when wired networks are difficult to deploy. Some of the benefits of wireless networks are: Cost efficient and easy-to-deploy, Scalability, and Availability of networks resources. Nowadays is important to deploy a secure and manageable wireless network infrastructure.

The Cisco RV320 Dual Gigabit WAN VPN Router with an intuitive user interface enables you to be up and running in minutes. Providing reliable, highly secure access connectivity for you and your employees that is so transparent you will not know it is there. The Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup is a sleek, affordable, and easy-to-deploy device that delivers fast, highly secure wireless connectivity. It supports high-speed connections with Gigabit Ethernet LAN interface for demanding applications. Bridges wired LANs together wirelessly, making it easier for small businesses to expand their networks.

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

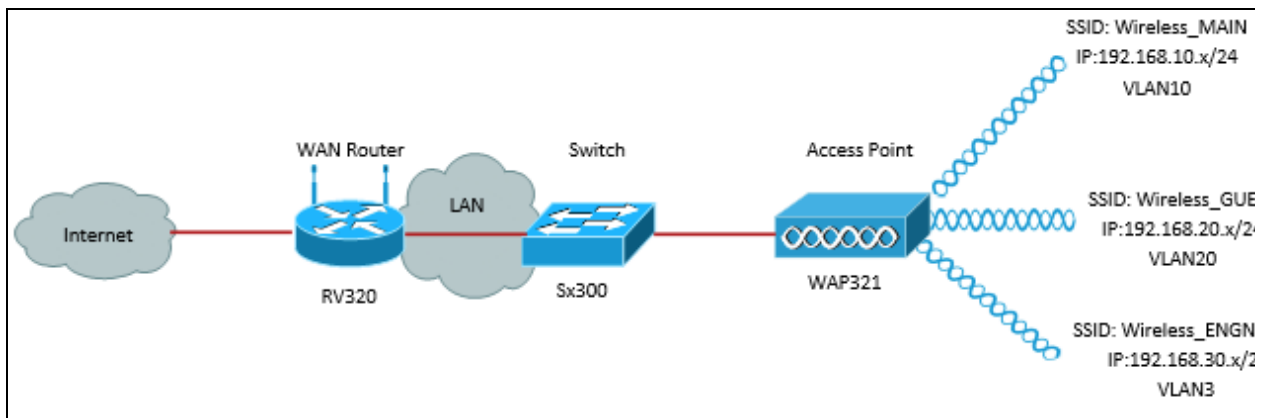
Applicable Device

- RV320 VPN Router
- WAP321 Wireless-N Access Point
- Sx300 Series Switch

Software Version

- 1.1.0.09 (RV320)
- 1.0.4.2 (WAP321)
- 1.3.5.58 (Sx300)

Network Topology



The image above illustrates a sample implementation for Wireless access using multiple SSIDs with a Cisco small business WAP, switch and router. The WAP 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. All wireless devices connect to the WAP.

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 access on any existing Cisco small business network.

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.

IEEE 802.1x

The IEEE 802.1x standard specifies methods used to implement port-based networks access control that is used to provide authenticated network access to Ethernet networks. Port-based authentication is a process that allows only credential exchanges to traverse the network until the user connected to the port is authenticated. The port is called an uncontrolled port during the time the credentials exchanges. The port is called a controlled port after the authentication is completed. This is based on two virtual ports existing within a single physical port.

This uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. This standard was originally designed for wired Ethernet networks, however it has been adapted for use on 802.11 wireless LANs.

RV320 Configuration

In this scenario we want the RV320 to act as the DHCP server for the network, so we will need to set that up as well as configure separate VLANs on the device. To start, log into the router by connecting to one of the Ethernet ports and going to 192.168.1.1 (assuming you have not already changed the IP address of the router).

Step 1. Log in to the web configuration utility and choose **Port Management > VLAN Membership**. A new page opens:

VLAN: ☒ Enable

Create VLANs and assign the Outgoing Frame Type.

Up to four new VLANs can be created. VLAN IDs must be in the range (4...4094)

VLAN Table									Items 1-3 of 3	5	per page
<input type="checkbox"/>	VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4			
<input type="checkbox"/>	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged			
<input type="checkbox"/>	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged			
<input type="checkbox"/>	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged			
<input type="text"/>	10	Wireless_MAIN	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged			
<input type="text"/>	20	Wireless_GUEST	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged			
<input type="text"/>	30	Wireless_ENGNRING	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged			

Page 1 of 1

Step 2. We are creating 3 separate VLANs to represent different target audiences. Click **Add** to add a new line and edit the VLAN ID and Description. You will also need to make sure that the VLAN is set to Tagged on any interfaces that they will need to travel on.

Step 3. Log in to the web configuration utility and choose **DHCP Menu > DHCP Setup**. The *DHCP Setup* page opens:

DHCP Setup

☒ IPv4 ☐ IPv6

☒ VLAN ☐ Option 82

VLAN ID:

Device IP Address:

Subnet Mask:

DHCP Mode: ☐ Disable ☒ DHCP Server ☐ DHCP Relay

Remote DHCP Server:

Client Lease Time: min (Range: 5 - 43200, Default: 1440)

Range Start:

Range End:

DNS Server:

Static DNS 1:

Static DNS 2:

WINS Server:

TFTP Server and Configuration Filename (Option 66/150 & 67):

TFTP Server Host Name:

TFTP Server IP:

Configuration Filename:

Step 4. In the VLAN ID drop box, select the VLAN you are setting up the address pool for (in this example VLANs 10, 20, and 30).

Step 5. Configure the device IP address for this VLAN, and set the IP address Range. You can also enable or disable DNS proxy here if you wish, and this will be dependent on the network. In this example, DNS Proxy will work to forward DNS requests.

Step 6. Click Save and repeat this step for each VLAN.

Step 7. Log in to the web configuration utility and choose **Port Management > 802.1x Configuration**. The *802.1X Configuration* page opens:

802.1X Configuration		
Configuration		
<input checked="" type="checkbox"/> Port-Based Authentication		
RADIUS IP:	<input type="text" value="192.168.1.32"/>	
RADIUS UDP Port:	<input type="text" value="1812"/>	
RADIUS Secret:	<input type="text" value="ciscorad"/>	
Port Table		
Port	Administrative State	Port State
1	<input type="text" value="Force Authorized"/>	Link Down
2	<input type="text" value="Force Authorized"/>	Link Down
3	<input type="text" value="Force Authorized"/>	Link Down
4	<input type="text" value="Force Authorized"/>	Authorized
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Step 8. Enable Port-Based Authentication and configure the IP address of the server.

RADIUS Secret is the authentication key used to communicate with the server.

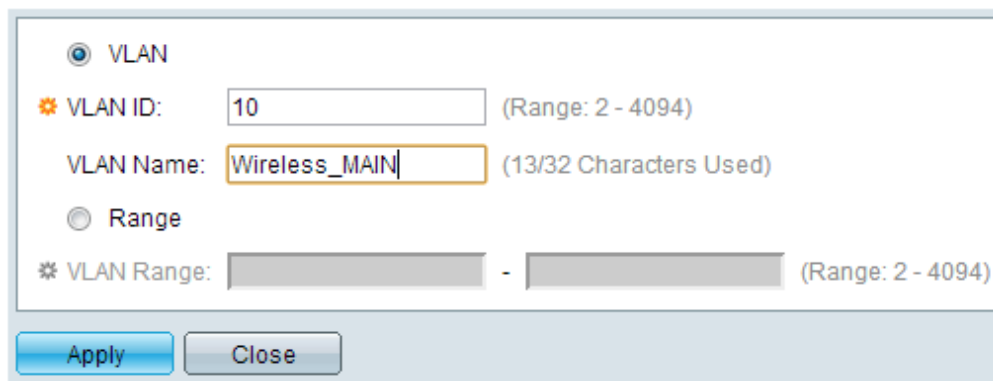
Step 9. Choose which ports will use this authentication and click **Save**.

Sx300 Configuration

The SG300-10MP switch works as an intermediary between the router and the WAP321 in order to simulate a realistic network environment. The configuration on the switch is as follows.

Step 1. Log in to the web configuration utility and choose **VLAN Management > Create VLAN**. A new page opens:

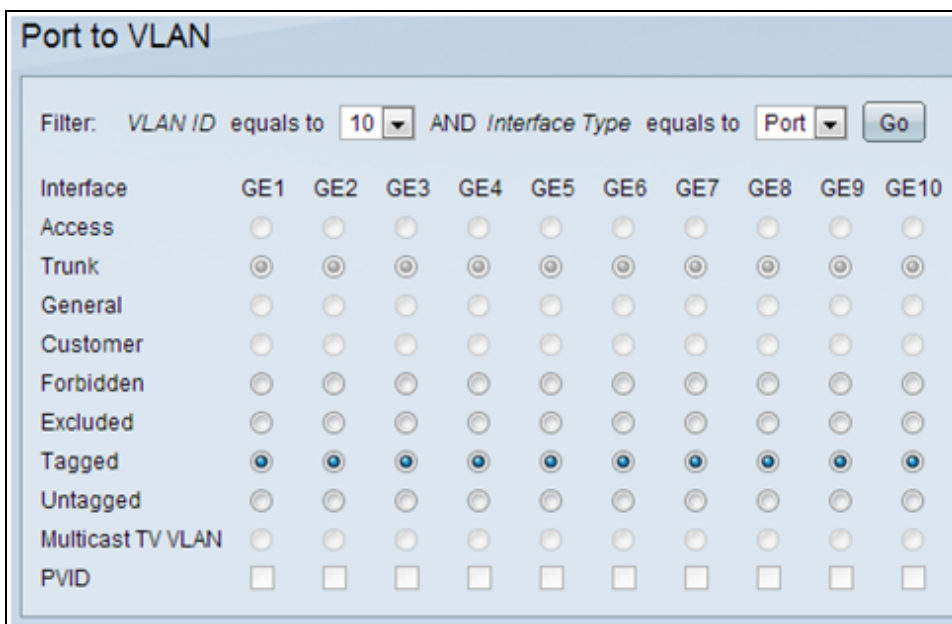
Step 2. Click **Add**. A new window appears.



A dialog box for configuring a VLAN. It has two radio buttons: 'VLAN' (selected) and 'Range'. Under 'VLAN', there is a 'VLAN ID' field with the value '10' and a '(Range: 2 - 4094)' label. Below it is a 'VLAN Name' field with the value 'Wireless_MAIN' and a '(13/32 Characters Used)' label. Under 'Range', there is a 'VLAN Range' field with two empty boxes and a '(Range: 2 - 4094)' label. At the bottom are 'Apply' and 'Close' buttons.

Step 3. Enter the VLAN ID and the VLAN Name (use the same as the description from Section I). Click Apply, and then repeat this step for VLANs 20 and 30.

Step 4. Log in to the web configuration utility and choose **VLAN Management > Port to VLAN**. A new page opens:



The 'Port to VLAN' configuration page. At the top, there is a filter section: 'Filter: VLAN ID equals to' with a dropdown menu showing '10', followed by 'AND Interface Type equals to' with a dropdown menu showing 'Port', and a 'Go' button. Below this is a table with 11 columns representing interfaces: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8, GE9, GE10. The rows represent different port configurations: Access, Trunk, General, Customer, Forbidden, Excluded, Tagged, Untagged, Multicast TV VLAN, and PVID. Each cell in the table contains a radio button. The 'Tagged' row has all radio buttons selected.

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
General	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Excluded	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Untagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multicast TV VLAN	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PVID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 5. At the top of the page set the "VLAN ID equals to" to the VLAN you are adding (in this case, VLAN 10) and then click **Go** on the right. This will update the page with the settings for that VLAN.

Step 6. Change the setting on each port so that VLAN 10 is now "Tagged" instead of "Excluded." Repeat this step for VLANs 20 and 30.

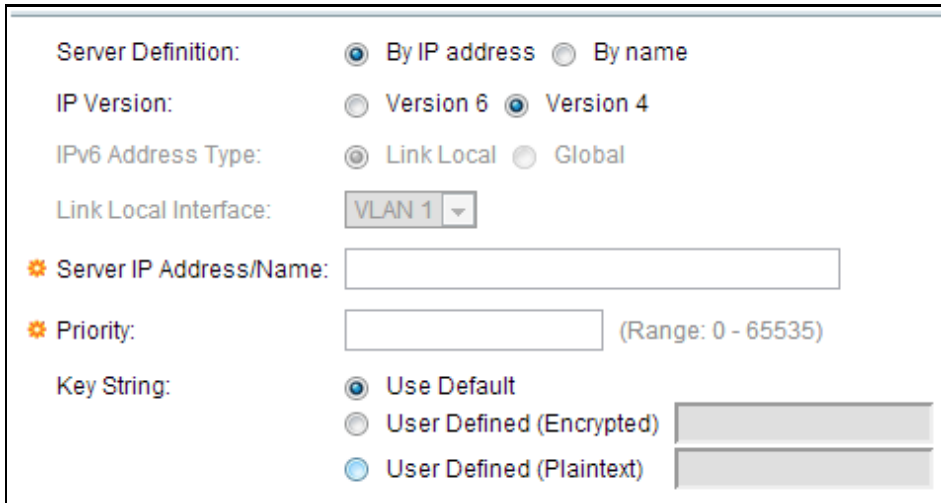
Step 7. Log in to the web configuration utility and choose **Security > Radius**. The *RADIUS* page opens:



The 'RADIUS' configuration page. At the top, it says 'RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounti'. Below this is a section for 'RADIUS Accounting' with four radio buttons: 'Port Based Access Control (802.1X, MAC Based)' (selected), 'Management Access', 'Both Port Based Access Control and Management Access', and 'None'.

Step 8. Choose the method of access control to be used by the RADIUS server, either management access control or port-based authentication. Choose Port Based Access Control and click **Apply**.

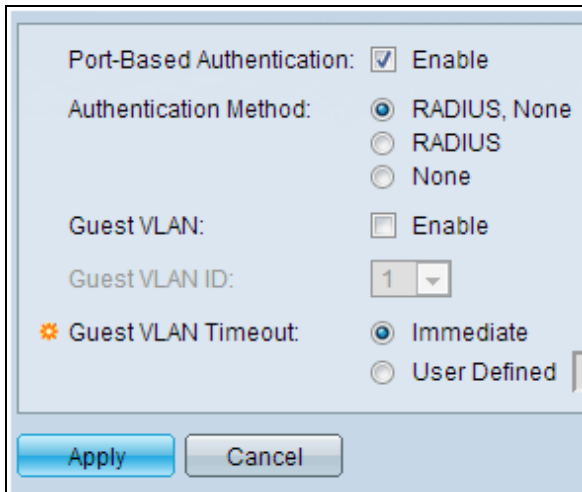
Step 9. Click **Add** at the bottom of the page to add a new server to authenticate to.



The screenshot shows a configuration window for a RADIUS server. The 'Server Definition' section has 'By IP address' selected. 'IP Version' is set to 'Version 4'. 'IPv6 Address Type' is set to 'Link Local'. 'Link Local Interface' is set to 'VLAN 1'. The 'Server IP Address/Name' field is empty. The 'Priority' field is empty, with a range of 0 to 65535. The 'Key String' section has 'Use Default' selected, with 'User Defined (Encrypted)' and 'User Defined (Plaintext' options also visible but not selected.

Step 10. In the window that appears you will configure the IP address of the server, in this case 192.168.1.32. You will need to set a priority for the server, but since in this example we only have one server to authenticate to the priority does not matter. This is important if you have multiple RADIUS servers to choose from. Configure the authentication key and the rest of the settings can be left as default.

Step 11. Log in to the web configuration utility and choose **Security > 802.1X > Properties**. A new page opens:

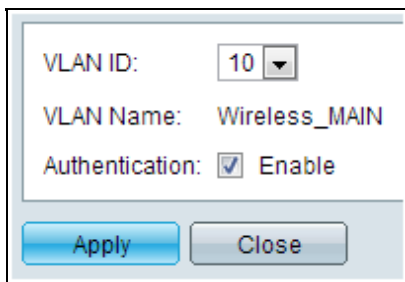


The screenshot shows the '802.1X Properties' configuration window. 'Port-Based Authentication' is checked and set to 'Enable'. 'Authentication Method' has 'RADIUS, None' selected. 'Guest VLAN' is unchecked. 'Guest VLAN ID' is set to '1'. 'Guest VLAN Timeout' has 'Immediate' selected. At the bottom, there are 'Apply' and 'Cancel' buttons.

Step 12. Check **Enable** to turn on 802.1x authentication and choose the authentication method. In this case we are using a RADIUS server so choose the first or second option.

Step 13. Click **Apply**.

Step 14. Choose one of the VLANs and click **Edit**. A new window appears.

A small dialog box with a light blue border. It contains three fields: 'VLAN ID:' with a dropdown menu showing '10', 'VLAN Name:' with the text 'Wireless_MAIN', and 'Authentication:' with a checked checkbox and the text 'Enable'. At the bottom are two buttons: 'Apply' and 'Close'.

Step 15. check **Enable** to allow authentication on that VLAN and click Apply. Repeat for each VLAN.

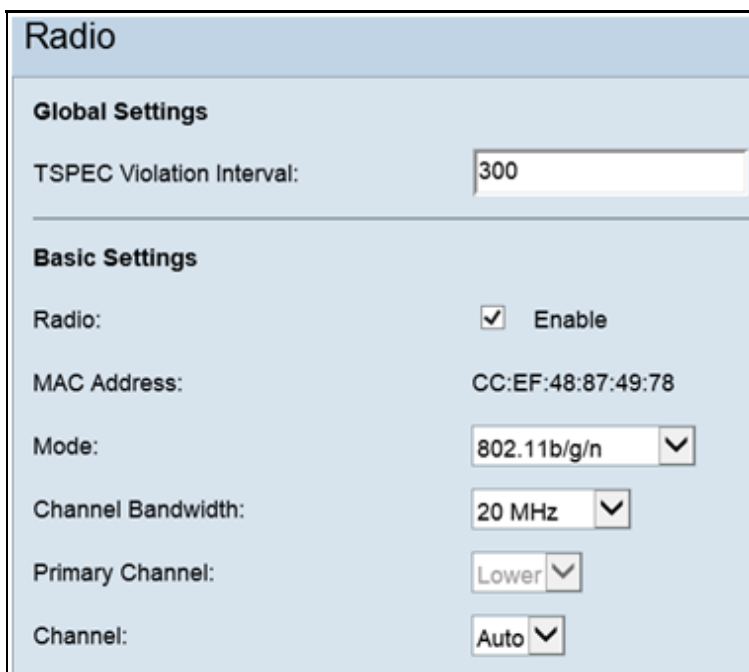
WAP321 Configuration

Virtual Access Points (VAPs) segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple access points in one physical WAP device. Up to four VAPs are supported on the WAP121 and up to eight VAPs are supported on the WAP321.

Each VAP can be independently enabled or disabled, with the exception of VAP0. VAP0 is the physical radio interface and remains enabled as long as the radio is enabled. To disable operation of VAP0, the radio itself must be disabled.

Each VAP is identified by a user-configured Service Set Identifier (SSID). Multiple VAPs cannot have the same SSID name. SSID broadcasts can be enabled or disabled independently on each VAP. SSID broadcast is enabled by default.

Step 1. Log in to the web configuration utility and choose **Wireless > Radio**. The *Radio* page opens:

A web configuration page titled 'Radio'. It has two sections: 'Global Settings' and 'Basic Settings'. Under 'Global Settings', there is a 'TSPEC Violation Interval' field with the value '300'. Under 'Basic Settings', there are several fields: 'Radio:' with a checked checkbox and the text 'Enable'; 'MAC Address:' with the value 'CC:EF:48:87:49:78'; 'Mode:' with a dropdown menu showing '802.11b/g/n'; 'Channel Bandwidth:' with a dropdown menu showing '20 MHz'; 'Primary Channel:' with a dropdown menu showing 'Lower'; and 'Channel:' with a dropdown menu showing 'Auto'.

Step 2. Click the **Enable** check box to enable the Wireless Radio.

Step 3. Click **Save**. The Radio will then be turned on.

Step 4. Log in to the web configuration utility and choose **Wireless > Networks**. The *Network* page opens:

Virtual Access Points (SSIDs)							
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	Cisco1	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	2	Cisco2	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	3	Cisco3	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>

Buttons: Add, Edit, Delete, Save

Note: The default SSID for VAP0 is ciscosb. Every additional VAP created has a blank SSID name. The SSIDs for all VAPs can be configured to other values.

Step 5. Click the check mark buttons on the left side to edit the SSIDs:

Virtual Access Points (SSIDs)							
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	10	Wireless_MAIN	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	20	Wireless_GUEST	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	30	Wireless_ENGNRING	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>

Buttons: Add, Edit, Delete, Save

Note: All the SSID's may be edited at once by checking the field to the left.

Step 6. Click the **Save** button once the SSIDs have been entered.

Each VAP is associated with a VLAN, which is identified by a VLAN ID (VID). A VID can be any value from 1 to 4094, inclusive. The WAP121 supports five active VLANs (four for WLAN plus one management VLAN). The WAP321 supports nine active VLANs (eight for WLAN plus one management VLAN).

By default, the VID assigned to the configuration utility for the WAP device is 1, which is also the default untagged VID. If the management VID is the same as the VID assigned to a VAP, then the WLAN clients associated with this specific VAP can administer the WAP device. If needed, an access control list (ACL) can be created to disable administration from WLAN clients.

Step 7. Enter the value needed to the VLAN ID in VLAN ID box, and click the **Save** button once the VLAN IDs have been entered.

Step 8. Log in to the web configuration utility and choose **System Security > 802.1X Supplicant**. The *802.1X Supplicant* page opens:

802.1X Supplicant

Supplicant Configuration

Administrative Mode: ☒ Enable

EAP Method: MD5

Username: example-username (Range: 1 - 64 Characters)

Password: ***** (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 18:43:36 2019 GMT

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: ☒ HTTP ☐ TFTP

Filename: Choose File No file chosen

Upload

Save

Step 9. Check **Enable** in the Administrative Mode field to enable the device to act as a supplicant in 802.1X authentication.

Step 10. Choose the appropriate type of Extensible Authentication Protocol (EAP) method from the drop-down list in the EAP Method field.

Step 11. Enter the username and password that the access point uses to get authentication from the 802.1X authenticator in the Username and Password fields. The length of the username and password must be from 1 to 64 alphanumeric and symbol characters. This should already be configured on the authentication server.

Step 12. Click **Save** to save the settings.

Note: The Certificate File Status area shows whether the certificate file is present or not. The SSL certificate is a digitally signed certificate by a certificate authority that allows the web browser to have a secure communication with the web server. To manage and configure the SSL certificate refer to the article *Secure Socket Layer (SSL) Certificate Management on the Cisco WAP121 and WAP321 Access Points*.

Step 13. Log in to the web configuration utility and choose **Security > RADIUS Server**. The *RADIUS Server* page opens:

RADIUS Server

Server IP Address Type: ☒ IPv4 ☐ IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)

Key-2: (Range: 1 - 64 Characters)

Key-3: (Range: 1 - 64 Characters)

Key-4: (Range: 1 - 64 Characters)

RADIUS Accounting: ☒ Enable

Step 14. Enter the parameters, and click the **Save** button once the Radius Server parameters have been entered.

© 2013 Cisco Systems, Inc. All rights reserved.