Configuring Virtual Access Points (VAPs) on the WAP121 and WAP321

Objective

Virtual Access Points (VAPs) simulate multiple access avenues in one physical WAP device; VAPs are similar to Ethernet VLANs. Each VAP can be enabled or disabled independently and is identified by a user-configured Service Set Identifier (SSID). Up to four VAPs are supported on the WAP121 and up to eight VAPs are supported on the WAP321.

The objective of this document is to show you how to configure Virtual Access Points on the WAP121 and WAP321.

Applicable Devices

- WAP121
- WAP321

Software Version

- 1.0.3.4
- 1.0.4.4 or higher

Procedure

Step 1. Log in to the Access Point Configuration Utility and choose Wireless > Networks. The Networks page opens:
Step 2. (optional) VAP No. 0 is the physical radio interface and remains enabled as long as the radio is enabled. If VAP No. 0 is the only VAP configured on the system, and you need to add additional VAPs, click **add**.

Step 3. To edit the VAP, click the checkmark box to the left of the VAP no., and click **Edit** to modify the information within the boxes.

- **VLAN ID** — The Virtual Identification of the VLAN is the parameter used to associate with the VAP. A VLAN ID can be any value from 1 to 4094.
Note: Verify that the VLAN ID is properly configured on the network. Network errors may arise if the VAP communicates with wireless clients on an improperly configured VLAN. The WAP121 supports five active VLANs (four WLAN plus one management VLAN), and the WAP321 supports nine active VLANs (eight WLAN plus one management VLAN).

- SSID Name — A name for the wireless network. The default SSID for VAP0 is "ciscosb" and each additional VAP created will have a blank SSID name. The SSID can contain any case-sensitive, alphanumeric entry between 2 to 32 characters.

Note: The same SSID name cannot be used for multiple VAPs.

- Broadcast SSID — Configuring this parameter enables or disables the broadcast of the SSID in its beacon frames. SSID broadcast is enabled by default.

Note: Suppressing SSID broadcast prevents clients from accidentally connecting to the network, however, it only offers minimal level of protection and does not prevent security threats to connect or monitor unencrypted traffic. SSID broadcasts can be independently enabled or disabled on each VAP.

Security — The type of authentication protocol required to access to the Virtual Access Point.

- None - Open or no security. This is the default option.
- WPA Personal - More advanced security in comparison to WEP, and can support keys of length 8-63 characters. For more information, refer to Step 4.
- WPA Enterprise - The most advanced method of security. It uses Protected Extensible Authentication Protocol (PEAP) in which every wireless user under WAP is authorized with individual usernames and passwords. These passwords can even support AES encryption standards. It also uses Transport Layer Security (TLS) in addition to PEAP, in which every user also needs to provide an additional certificate to gain access. For more information, refer to Step 5.
  Note: It is recommended to use WPA Personal or WPA Enterprise as the authentication type as it provides stronger security protection.

- MAC Filtering — Specifies whether the clients that can access the VAP are restricted to a configured global list of MAC addresses.
  - Disabled — All clients can access the upstream network.
  - Local — The set of clients that can access the upstream network is restricted to the clients specified in a locally defined MAC address list.
  - Radius — The set of clients that can access the upstream network is restricted to the clients specified in a MAC address list on a RADIUS server.

- Channel Isolation — When disabled, wireless clients can communicate with each other by sending traffic through the WAP device. When enabled, the WAP device
blocks communication between wireless clients on the same VAP. The WAP device still allows data traffic on the network between itself and the wireless clients.

Step 4. (Optional) If you want your network to use a pre-shared key (PSK), which is only used for an initial check of credentials, select **WPA Personal** in the **Security** dropdown menu.

<table>
<thead>
<tr>
<th>VAP No</th>
<th>VLAN ID</th>
<th>SSID Name</th>
<th>SSID Broadcast</th>
<th>Security</th>
<th>MAC Filter</th>
<th>Channel Isolation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Default</td>
<td></td>
<td>None</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td></td>
<td>0</td>
<td>WPA Personal</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

- **WPA Versions** — Select the check box of the type of client stations the network can support. If the network has a mix of clients that supports WPA2 or WPA, select both checkboxes.

- **Cipher Suites** — You can select TKIP, CCMP (AES), or both. Both TKIP and AES clients can associate with the WAP device. Temporary Key Integrity Protocol is an out of data security standard used to replace Wireless Equivalence Privacy (WEP) encryption. CCMP is the standard encryption process used for WAP2. WPA clients must have either a valid TKIP key or a valid AES-CCMP key to associate with the WAP device.

- **Key** — The secure key for WPA Personal security. The field should contain a string of at least 8 characters to a maximum of 63 characters.

- **Broadcast Key Refresh Rate** — The interval at which the broadcast key is refreshed for clients associated with this VAP. The default is 300 seconds and the valid range is from 0 to 86400 seconds.

Step 5. (Optional) If you want your network to use a RADIUS server to authenticate users, select **WPA Enterprise** in the **Security** dropdown menu.
**WPA Versions** — Select the check box of the type of client stations the network can support. If the network has a mix of clients that supports WPA2 or WPA, select both checkboxes.

— Enable pre-authentication — Enabling this option allows WPA2 wireless clients to send pre-authentication packets. The pre-authentication information is relayed from the WAP device that the client is currently using to the target WAP device. Enabling this option is beneficial for roaming clients who connect to multiple access points.

**Cipher Suites** — You can select TKIP, CCMP(AES), or both. Both TKIP and AES clients can associate with the WAP device. Temporary Key Integrity Protocol is an out of data security standard used to replace Wireless Equivalence Privacy (WEP) encryption. CCMP is the standard encryption process used for WAP2. WPA clients configured to use WPA with RADIUS must have either a valid TKIP key or a valid AES-CCMP key and a RADIUS Key to associate with the WAP device.

**Use Global RADIUS server settings** — Enabled by default, each VAP uses the global RADIUS settings previously defined for the WAP device. Unchecking this box allows the administrator to configure each VAP to use a different set of RADIUS servers.

— Server IP Address Type — The IP version that the RADIUS server uses. The WAP device will contact only the RADIUS server for the address type selected in this field.
— Server IP Address 1 — The address for the primary RADIUS server for this VAP. If IPv4 is selected as the Server IP Address Type, enter the IP address of the RADIUS server that all VAPs use by default, for example, 192.168.10.23. If IPv6 is selected, enter the IPv6 address of the primary global RADIUS server, for example, 2001:DB8:1234::abcd.

— Server IP Address 2 to 4 — Up to three additional IPv4 and/or IPv6 addresses can be entered in to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.

— Key 1 — The securekey for the global RADIUS server. You must configure the same key on the WAP device and on your RADIUS server.

— Key 2 to 4 — The RADIUS key associated with the configured backup RADIUS servers. The IP Address number corresponds to the key number.

— Enable RADIUS Accounting — Tracks and measures the resources a particular user has consumed such as system time and amount of data transmitted.

• Enable RADIUS Accounting — Tracks and measures the resources a particular user has consumed such as system time and amount of data transmitted and received.

• Active Server — Enables the administrative selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is up.

• Broadcast Key Refresh Rate — The interval at which the broadcast key is refreshed for clients associated with this VAP. The default is 300 seconds and the valid range is from 0 to 86400 seconds.

• Session Key Refresh Rate — The interval at which the WAP device refreshes session keys for each client associated with the VAP.

Step 6. Click Save. The changes are saved to the Startup Configuration.