

Konfigurieren von Virtual Access Points (VAPs) auf dem WAP121 und WAP321

Ziel

Virtuelle Access Points (VAPs) simulieren mehrere Zugriffswege in einem physischen WAP-Gerät. VAPs ähneln Ethernet Virtual Local Area Networks (VLANs). Jeder VAP kann unabhängig aktiviert oder deaktiviert werden und wird durch einen benutzerdefinierten Service Set Identifier (SSID) oder auch als Netzwerknamen bezeichnet. Sie können auf dem Cisco WAP121 bis zu vier VAPs und auf dem Cisco WAP321 bis zu acht VAPs konfigurieren.

In diesem Dokument wird erläutert, wie Sie virtuelle Access Points auf den Cisco WAP121- und WAP321-Access Points konfigurieren.

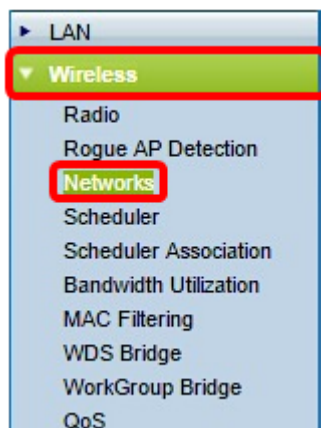
Anwendbare Geräte

- WAP121
- WAP321

Softwareversion

- 1,0/6,5

Schritt 1: Melden Sie sich beim webbasierten Access Point-Dienstprogramm an, und wählen Sie **Wireless > Networks** aus.



Schritt 2: Klicken Sie in der Tabelle Virtual Access Points (SSIDs) auf die Schaltfläche **Hinzufügen**.

Hinweis: VAP No. 0 ist die physische Standard-Funkschnittstelle und kann je nach Ihren Vorstellungen geändert werden. Dieser VAP kann nicht gelöscht werden und bleibt aktiviert, solange die Funkübertragung aktiviert ist.

Networks

Virtual Access Points (SSIDs)

	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Add Edit Delete

Schritt 3: Aktivieren Sie das Kontrollkästchen neben der VAP-Nummer, und klicken Sie dann auf **Bearbeiten**.

Virtual Access Points (SSIDs)

	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Add Edit Delete

Schritt 4: Geben Sie im Feld "VLAN ID" (VLAN-ID) die VLAN-ID ein, mit der Sie den von Ihnen erstellten VAP verknüpfen möchten. Eine VLAN-ID kann ein beliebiger Wert zwischen 1 und 4094 sein.

Hinweis: Überprüfen Sie, ob die VLAN-ID im Netzwerk richtig konfiguriert ist. Wenn der VAP mit Wireless-Clients in einem falsch konfigurierten VLAN kommuniziert, können Netzwerkfehler auftreten. Der WAP121 unterstützt fünf aktive VLANs (vier WLANs plus ein Management-VLAN), und der WAP321 unterstützt neun aktive VLANs (acht WLANs plus ein Management-VLAN).

Virtual Access Points (SSIDs)

	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Add Edit Delete

Hinweis: In diesem Beispiel wird die VLAN-ID 2 verwendet. Dies ist die Standardeinstellung.

Schritt 5: Erstellen Sie im Feld *SSID Name* einen Namen für den VAP. Die SSID kann einen beliebigen alphanumerischen Eintrag zwischen 2 und 32 Zeichen enthalten, bei dem zwischen Groß- und Kleinschreibung unterschieden wird.

Virtual Access Points (SSIDs)

	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	1st VAP	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Add Edit Delete

Schritt 6: Aktivieren Sie das Kontrollkästchen SSID-Broadcast. Dadurch kann der VAP für jedes Wireless-Gerät in seinem Bereich sichtbar sein.

Hinweis: Der SSID-Broadcast ist standardmäßig aktiviert. Durch die Deaktivierung des SSID-Broadcast wird verhindert, dass Wireless-Clients eine Verbindung zum Netzwerk herstellen, da der VAP nicht sichtbar ist. Der VAP bietet jedoch nur einen minimalen Schutz und verhindert keine Sicherheitsbedrohungen für die Verbindung oder Überwachung von nicht verschlüsseltem Datenverkehr. SSID-Broadcasts können auf jedem VAP unabhängig aktiviert oder deaktiviert werden.

Virtual Access Points (SSIDs)								
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	1st VAP	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Add Edit Delete

Schritt 7: Wählen Sie eine Option aus der Dropdown-Liste "Security" (Sicherheit) aus, je nachdem, welche Sicherheitsmethode Sie für den VAP verwenden möchten. Folgende Optionen stehen zur Verfügung:

- Keine - offen oder keine Sicherheit. Dies ist die Standardoption. Wenn diese Option ausgewählt ist, fahren Sie mit [Schritt 10 fort](#).
- WPA Personal: Erweiterte Sicherheit im Vergleich zu WEP und Unterstützung von Schlüsseln mit 8 bis 63 Zeichen Länge.
- WPA Enterprise - Die fortschrittlichste Sicherheitsmethode. Es verwendet Protected Extensible Authentication Protocol (PEAP), in dem jeder Wireless-Benutzer unter WAP mit individuellen Benutzernamen und Kennwörtern autorisiert ist. Diese Kennwörter können Advanced Encryption Standard (AES) unterstützen. Zusätzlich zu PEAP wird auch Transport Layer Security (TLS) verwendet, bei dem jeder Benutzer ein zusätzliches Zertifikat bereitstellen muss, um Zugriff zu erhalten.

Virtual Access Points (SSIDs)								
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	1st VAP	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>

Add Edit Delete


Hinweis: In diesem Beispiel wird WPA Personal ausgewählt.

Schritt 8: Erstellen Sie im Feld *Schlüssel* ein Kennwort für den VAP. Dies ist das Kennwort, das jeder Wireless-Client für die Verbindung mit dem Wireless-Netzwerk eingeben muss.

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Key Strength Meter:  Strong

Broadcast Key Refresh Rate: (Range: 0-86400)

Hinweis: Das Schlüsselstärkemessgerät gibt die Stärke des von Ihnen erstellten Kennworts an.


Schritt 9: Geben Sie einen Wert in der Aktualisierungsrate für den Sendeschlüssel ein. Dabei

handelt es sich um das Intervall, in dem der Broadcast-(Gruppen-)Schlüssel für Clients aktualisiert wird, die diesem VAP zugeordnet sind. Der gültige Bereich liegt zwischen 0 und 86.400 Sekunden.

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Key Strength Meter:  Strong

Broadcast Key Refresh Rate: (Range: 0-86400)

Hinweis: In diesem Beispiel wird der Standardwert 300 verwendet.

Schritt 10: Wählen Sie eine Option aus der Dropdown-Liste "MAC Filter" (MAC-Filter) aus, um festzulegen, ob die Clients, die auf den VAP zugreifen können, auf eine konfigurierte globale Liste mit MAC-Adressen beschränkt sind. Folgende Optionen stehen zur Verfügung:

- Disabled (Deaktiviert): Alle Clients können auf das Upstream-Netzwerk zugreifen.
- Locale (Gebietsschema) - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die Clients beschränkt, die in einer lokal definierten MAC-Adressliste angegeben sind.
- Radius - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die in einer MAC-Adressliste auf einem RADIUS-Server angegebenen Clients beschränkt.

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	1st VAP	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	
							<input checked="" type="button" value="Disabled"/> <input type="button" value="Local"/> <input type="button" value="RADIUS"/>	

Show Details

Add Edit Delete

Hinweis: In diesem Beispiel wird die Standardeinstellung Disabled (Deaktiviert) ausgewählt.


Schritt 11: (Optional) Aktivieren Sie das Kontrollkästchen **Kanalisolierung**, wenn das WAP-Gerät die Kommunikation zwischen den Wireless-Clients auf demselben VAP blockieren soll. Das WAP-Gerät lässt weiterhin Datenverkehr zwischen seinen Wireless-Clients und den kabelgebundenen Geräten im Netzwerk über eine WDS-Verbindung und mit anderen Wireless-Clients zu, die einem anderen VAP zugeordnet sind, jedoch nicht zwischen den Wireless-Clients.

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	1st VAP	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input checked="" type="checkbox"/>	

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

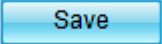
Key: (Range: 8-63 Characters)

Key Strength Meter:  Strong

Broadcast Key Refresh Rate: (Range: 0-86400)

Schritt 12: Wiederholen Sie die Schritte 2 bis 11 für jeden VAP, den Sie hinzufügen

möchten. Sie können auf dem Cisco WAP121 bis zu vier VAPs und auf dem Cisco WAP321 bis zu acht VAPs konfigurieren.

Schritt 13: Klicken Sie auf die  Schaltfläche.

Sie sollten jetzt virtuelle Access Points für Ihre WAP121- und WAP321-Access Points erfolgreich konfiguriert haben.