

Aktivieren mehrerer Wireless-Netzwerke auf RV320 VPN-Routern, WAP321 Wireless-N Access Points und Switches der Serie Sx300

Ziel

In einer sich ständig ändernden Geschäftsumgebung muss Ihr Netzwerk für kleine und mittlere Unternehmen leistungsfähig, flexibel, zugänglich und äußerst zuverlässig sein, insbesondere wenn Wachstum eine Priorität darstellt. Die Beliebtheit von Wireless-Geräten ist exponentiell angestiegen, was keine Überraschung ist. Wireless-Netzwerke sind kosteneffizient, einfach bereitzustellen, flexibel, skalierbar und mobil und stellen scheinbar Netzwerkressourcen bereit. Mit der Authentifizierung können Netzwerkgeräte die Legitimität eines Benutzers überprüfen und gewährleisten und gleichzeitig das Netzwerk vor nicht autorisierten Benutzern schützen. Es ist wichtig, eine sichere und verwaltbare Wireless-Netzwerkinfrastruktur bereitzustellen.

Der Cisco RV320 Dual-Gigabit-WAN VPN-Router bietet Ihnen und Ihren Mitarbeitern zuverlässige und hochsichere Zugriffsverbindungen. Der Cisco WAP321 Wireless-N Selectable-Band Access Point mit Single-Point-Einrichtung unterstützt Hochgeschwindigkeitsverbindungen mit Gigabit Ethernet. Bridges verbinden LANs drahtlos miteinander, was kleinen Unternehmen die Erweiterung ihrer Netzwerke erleichtert.

Dieser Artikel enthält eine schrittweise Anleitung für die Konfiguration, die für die Aktivierung des Wireless-Zugriffs in einem Cisco Small Business-Netzwerk erforderlich ist, einschließlich VLAN-übergreifendem Routing (Virtual Local Area Network), mehreren Service Set Identifiers (SSIDs) und Wireless-Sicherheitseinstellungen am Router, Switch und Access Points.

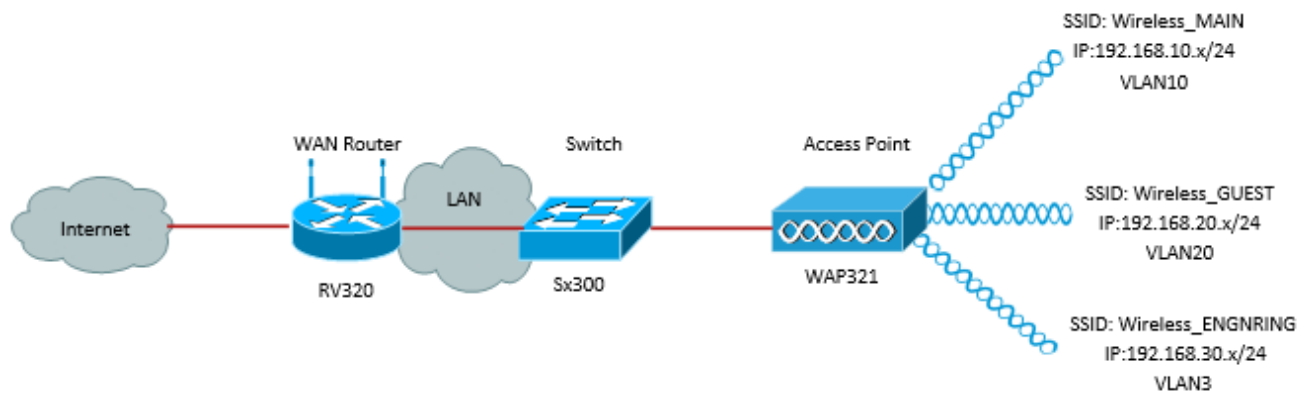
Anwendbare Geräte

- RV320 VPN-Router
- WAP321 Wireless-N Access Point
- Switch der Serie Sx300

Softwareversion

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

Netzwerktopologie



Das Bild oben zeigt eine Beispielimplementierung für den Wireless-Zugriff mithilfe mehrerer SSIDs mit einem Cisco Small Business WAP, Switch und Router. Der WAP stellt eine Verbindung zum Switch her und verwendet die Trunk-Schnittstelle, um mehrere VLAN-Pakete zu transportieren. Der Switch stellt über die Trunk-Schnittstelle eine Verbindung zum WAN-Router her, und der WAN-Router führt Inter-VLAN-Routing durch. Der WAN-Router stellt eine Verbindung zum Internet her. Alle Wireless-Geräte sind mit dem WAP verbunden.

Hauptmerkmale

Die Kombination der vom Cisco RV-Router bereitgestellten VLAN-übergreifenden Routing-Funktion mit der Wireless-SSID-Isolierungsfunktion eines Small Business Access Points bietet eine einfache und sichere Lösung für den Wireless-Zugriff auf bestehende Cisco Small Business-Netzwerke.

Inter-VLAN-Routing

Netzwerkgeräte in verschiedenen VLANs können ohne einen Router zur Weiterleitung des Datenverkehrs zwischen den VLANs nicht miteinander kommunizieren. In einem Small Business-Netzwerk führt der Router das VLAN-übergreifende Routing für die kabelgebundenen und Wireless-Netzwerke durch. Wenn Inter-VLAN-Routing für ein bestimmtes VLAN deaktiviert ist, können Hosts in diesem VLAN nicht mit Hosts oder Geräten in einem anderen VLAN kommunizieren.

Wireless SSID-Isolierung

Es gibt zwei Arten von Wireless-SSID-Isolierung. Wenn die Wireless-Isolierung (innerhalb der SSID) aktiviert ist, können Hosts derselben SSID einander nicht sehen. Wenn die Wireless-Isolierung (zwischen SSIDs) aktiviert ist, wird der Datenverkehr einer SSID nicht an eine andere SSID weitergeleitet.

IEEE 802.1x

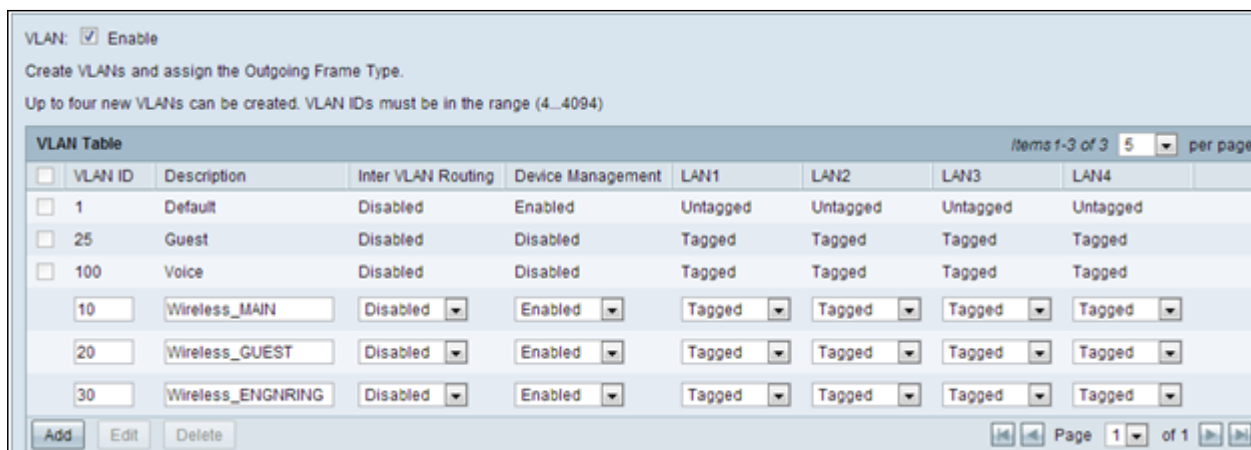
Der IEEE 802.1x-Standard legt Methoden für die Implementierung einer portbasierten Netzwerkzugriffskontrolle fest, die für den authentifizierten Netzwerkzugriff auf Ethernet-Netzwerke verwendet wird. Die Port-basierte Authentifizierung ist ein Prozess, der nur den Austausch von Anmeldeinformationen über das Netzwerk ermöglicht, bis der mit dem Port verbundene Benutzer authentifiziert wird. Der Port wird während des Austauschs der Anmeldeinformationen als unkontrollierter Port bezeichnet. Der Port wird nach Abschluss der Authentifizierung als kontrollierter Port bezeichnet. Dies basiert auf zwei virtuellen Ports, die sich in einem einzelnen physischen Port befinden.

Dabei werden die physischen Merkmale der Switched LAN-Infrastruktur zur Authentifizierung von Geräten verwendet, die an einen LAN-Port angeschlossen sind. Der Zugriff auf den Port kann verweigert werden, wenn der Authentifizierungsprozess fehlschlägt. Dieser Standard wurde ursprünglich für kabelgebundene Ethernet-Netzwerke entwickelt, wurde jedoch für die Verwendung in 802.11-WLANs angepasst.

RV320-Konfiguration

In diesem Szenario soll der RV320 als DHCP-Server für das Netzwerk fungieren. Dies muss eingerichtet und separate VLANs auf dem Gerät konfiguriert werden. Melden Sie sich zunächst beim Router an, indem Sie eine Verbindung zu einem der Ethernet-Ports herstellen und zu 192.168.1.1 wechseln (vorausgesetzt, Sie haben die IP-Adresse des Routers noch nicht geändert).

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Port Management > VLAN Membership aus**. Eine neue Seite wird geöffnet. Wir erstellen drei separate VLANs, um verschiedene Zielgruppen zu repräsentieren. Klicken Sie auf **Hinzufügen**, um eine neue Zeile hinzuzufügen und die VLAN-ID und -Beschreibung zu bearbeiten. Sie müssen außerdem sicherstellen, dass das VLANs auf allen Schnittstellen, die für die Anreise benötigt werden, auf *Tagged* festgelegt ist.



The screenshot shows the 'VLAN Table' configuration page. At the top, there is a checkbox for 'VLAN: Enable' which is checked. Below it, instructions state: '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)'. The table has columns for 'VLAN ID', 'Description', 'Inter VLAN Routing', 'Device Management', and four LAN ports (LAN1, LAN2, LAN3, LAN4). The existing entries are: VLAN 1 (Default, Disabled, Enabled, Untagged), VLAN 25 (Guest, Disabled, Disabled, Tagged), and VLAN 100 (Voice, Disabled, Disabled, Tagged). Three new entries are being added: VLAN 10 (Wireless_MAIN, Disabled, Enabled, Tagged), VLAN 20 (Wireless_GUEST, Disabled, Enabled, Tagged), and VLAN 30 (Wireless_ENGNRING, Disabled, Enabled, Tagged). Each entry has dropdown menus for the routing and management settings and checkboxes for each LAN port. At the bottom, there are 'Add', 'Edit', and 'Delete' buttons, and a pagination indicator showing 'Page 1 of 1'.

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="checkbox"/>	10	Wireless_MAIN	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="checkbox"/>	20	Wireless_GUEST	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="checkbox"/>	30	Wireless_ENGNRING	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged

Schritt 2: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **DHCP Menu > DHCP Setup aus**. Die Seite *DHCP-Setup* wird geöffnet:

- Wählen Sie im Dropdown-Feld VLAN ID (VLAN-ID) das VLAN aus, für das Sie den Adresspool einrichten (in diesem Beispiel VLANs 10, 20 und 30).
- Konfigurieren Sie die Geräte-IP-Adresse für dieses VLAN, und legen Sie den IP-Adressbereich fest. Sie können den DNS-Proxy hier auch aktivieren oder deaktivieren, wenn Sie möchten. Dies hängt vom Netzwerk ab. In diesem Beispiel leitet der DNS-Proxy DNS-Anfragen weiter.
- Klicken Sie auf **Speichern**, und wiederholen Sie diesen Schritt für jedes VLAN.

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:

Save
Cancel

Schritt 3: Wählen Sie im Navigationsbereich **Port Management > 802.1x Configuration** aus. Die Seite *802.1X-Konfiguration* wird geöffnet:

- Aktivieren Sie die Port-basierte Authentifizierung, und konfigurieren Sie die IP-Adresse des Servers.
- RADIUS Secret ist der Authentifizierungsschlüssel, der für die Kommunikation mit dem Server verwendet wird.
- Wählen Sie aus, welche Ports diese Authentifizierung verwenden, und klicken Sie auf **Speichern**.

802.1X Configuration

Configuration

Port-Based Authentication

RADIUS IP:

RADIUS UDP Port:

RADIUS Secret:

Port Table

Port	Administrative State	Port State
1	Force Authorized	Link Down
2	Force Authorized	Link Down
3	Force Authorized	Link Down
4	Force Authorized	Authorized

Save Cancel

Sx300-Konfiguration

Der Switch SG300-10MP fungiert als Vermittler zwischen dem Router und dem WAP321, um eine realistische Netzwerkumgebung zu simulieren. Die Konfiguration für den Switch ist wie folgt:

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VLAN Management > Create VLAN aus**. Eine neue Seite wird geöffnet:

Schritt 2: Klicken Sie auf **Hinzufügen**. Ein neues Fenster wird angezeigt. Geben Sie die VLAN-ID und den VLAN-Namen ein (verwenden Sie die gleiche Beschreibung wie in Abschnitt I). Klicken Sie auf Apply, und wiederholen Sie diesen Schritt für die VLANs 20 und 30.

VLAN

VLAN ID: (Range: 2 - 4094)

VLAN Name: (13/32 Characters Used)

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Schritt 3: Wählen Sie im Navigationsbereich **VLAN Management > Port to VLAN aus**. Eine neue Seite wird geöffnet:

- Legen Sie oben auf der Seite dem VLAN, das Sie hinzufügen (in diesem Fall VLAN 10), die "VLAN-ID gleich" fest, und klicken Sie dann rechts **auf Go**. Dadurch wird die Seite mit den Einstellungen für dieses VLAN aktualisiert.
- Ändern Sie die Einstellung für jeden Port, sodass VLAN 10 jetzt "Tagged" anstatt "Excluded"

(Ausgeschlossen) lautet. Wiederholen Sie diesen Schritt für die VLANs 20 und 30.

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"/>

Schritt 4: Wählen Sie im Navigationsbereich **Security > Radius (Sicherheit > Radius)** aus. Die Seite *RADIUS* wird geöffnet:

- Wählen Sie die Methode der Zugriffskontrolle für den RADIUS-Server aus, entweder die Zugriffskontrolle für die Verwaltung oder die Port-basierte Authentifizierung. Wählen Sie Port Based Access Control aus, und klicken Sie auf **Apply**.
- Klicken Sie unten auf der Seite auf **Hinzufügen**, um einen neuen Server für die Authentifizierung hinzuzufügen.

RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounti

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based)
 Management Access
 Both Port Based Access Control and Management Access
 None

Schritt 5: Im angezeigten Fenster konfigurieren Sie die IP-Adresse des Servers, in diesem Fall 192.168.1.32. Sie müssen eine Priorität für den Server festlegen. Da in diesem Beispiel jedoch nur ein Server für die Authentifizierung in der Priorität vorhanden ist, spielt dies keine Rolle. Dies ist wichtig, wenn Sie mehrere RADIUS-Server zur Auswahl haben. Konfigurieren Sie den Authentifizierungsschlüssel, und die übrigen Einstellungen können als Standard beibehalten werden.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

✱ Server IP Address/Name:

✱ Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext)

Schritt 6: Wählen Sie im Navigationsbereich **Security > 802.1X > Properties aus**. Eine neue Seite wird geöffnet:

- Aktivieren Sie **Aktivieren**, um die 802.1x-Authentifizierung zu aktivieren, und wählen Sie die Authentifizierungsmethode aus. In diesem Fall verwenden wir einen RADIUS-Server, wählen Sie daher die erste oder zweite Option.
- Klicken Sie auf **Übernehmen**.

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID:

✱ Guest VLAN Timeout: Immediate
 User Defined

Schritt 7: Wählen Sie eines der VLANs aus, und klicken Sie auf **Bearbeiten**. Ein neues Fenster wird angezeigt. Aktivieren Sie **Aktivieren**, um die Authentifizierung für dieses VLAN zuzulassen, und klicken Sie auf **Übernehmen**. Wiederholen Sie die Schritte für jedes VLAN.

VLAN ID:

VLAN Name:

Authentication: Enable

WAP321-Konfiguration

Virtual Access Points (VAPs) segmentieren das WLAN in mehrere Broadcast-Domänen, die das WLAN-Äquivalent zu Ethernet-VLANs darstellen. VAPs simulieren mehrere Access

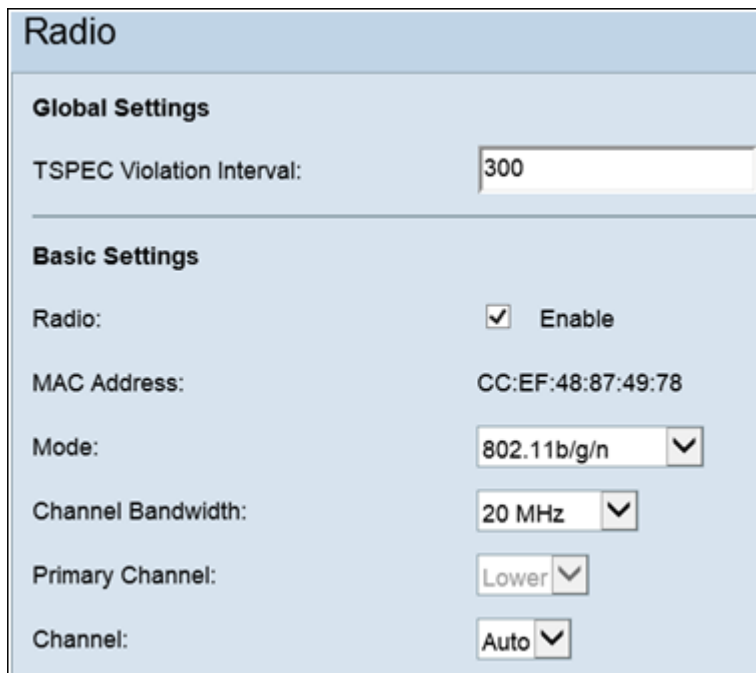
Points in einem physischen WAP-Gerät. Der WAP121 unterstützt bis zu vier VAPs und der WAP321 bis zu acht VAPs.

Mit Ausnahme von VAP0 kann jeder VAP unabhängig aktiviert oder deaktiviert werden. VAP0 ist die physische Funkschnittstelle und bleibt aktiviert, solange die Funkverbindung aktiviert ist. Um den Betrieb von VAP0 zu deaktivieren, muss die Funkübertragung selbst deaktiviert werden.

Jeder VAP wird durch einen benutzerdefinierten Service Set Identifier (SSID) identifiziert. Mehrere VAPs können nicht denselben SSID-Namen haben. SSID-Broadcasts können auf jedem VAP unabhängig aktiviert oder deaktiviert werden. SSID-Broadcast ist standardmäßig aktiviert.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Wireless > Radio aus**. Die Seite *Radio* wird geöffnet:

- Klicken Sie auf das Kontrollkästchen **Aktivieren**, um die Wireless-Funkübertragung zu aktivieren.
- Klicken Sie auf **Speichern**. Das Radio wird dann eingeschaltet.



Radio

Global Settings

TSPEC Violation Interval: 300

Basic Settings

Radio: Enable

MAC Address: CC:EF:48:87:49:78

Mode: 802.11b/g/n

Channel Bandwidth: 20 MHz

Primary Channel: Lower

Channel: Auto

Schritt 2. Wählen Sie im Navigationsbereich **Wireless > Networks aus**. Die Seite *Netzwerk* wird geöffnet:



Networks

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"/>
Show Details							
1	<input checked="" type="checkbox"/>	2	Cisco2	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							
2	<input checked="" type="checkbox"/>	3	Cisco3	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							

Add Edit Delete

Save

Hinweis: Die Standard-SSID für VAP0 ist ciscosb. Jeder zusätzliche VAP hat einen leeren

SSID-Namen. Die SSIDs für alle VAPs können für andere Werte konfiguriert werden.

Schritt 3: Jeder VAP ist einem VLAN zugeordnet, das durch eine VLAN-ID (VID) identifiziert wird. Eine VID kann einen beliebigen Wert zwischen 1 und 4094 (einschließlich) aufweisen. Der WAP121 unterstützt fünf aktive VLANs (vier für WLAN und ein Management-VLAN). Der WAP321 unterstützt neun aktive VLANs (acht für WLAN und ein Management-VLAN).

Die VID, die dem Konfigurationsprogramm für das WAP-Gerät zugewiesen ist, ist standardmäßig die 1, d. h. die standardmäßige nicht gekennzeichnete VID. Wenn die Management-VID mit der VID übereinstimmt, die einem VAP zugewiesen ist, können die diesem VAP zugeordneten WLAN-Clients das WAP-Gerät verwalten. Bei Bedarf kann eine Zugriffskontrollliste (ACL) erstellt werden, um die Administration von WLAN-Clients zu deaktivieren.

In diesem Bildschirm sollten folgende Schritte ausgeführt werden:

- Klicken Sie auf die Häkchentasten auf der linken Seite, um die SSIDs zu bearbeiten:
- Geben Sie den für die VLAN-ID erforderlichen Wert im VLAN-ID-Feld ein.
- Klicken Sie nach Eingabe der SSIDs auf die **Schaltfläche Speichern**.

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

Schritt 4: Wählen Sie im Navigationsbereich **Systemicherheit > 802.1X Supplicant** aus. Die Seite *802.1X Supplicant* wird geöffnet:

- Aktivieren Sie im Feld Verwaltungsmodus die **Option Aktivieren**, um das Gerät als Komponente bei der 802.1X-Authentifizierung zu aktivieren.
- Wählen Sie in der Dropdown-Liste im Feld "EAP-Methode" den entsprechenden Typ der Extensible Authentication Protocol (EAP)-Methode aus.
- Geben Sie den Benutzernamen und das Kennwort ein, mit dem der Access Point die Authentifizierung vom 802.1X-Authentifizierer in den Feldern Benutzername und Kennwort abrufen. Benutzername und Kennwort müssen zwischen 1 und 64 alphanumerische Zeichen und Symbolzeichen lang sein. Dies sollte bereits auf dem Authentifizierungsserver konfiguriert werden.
- Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

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

Hinweis: Im Bereich Status der Zertifikatsdatei wird angezeigt, ob die Zertifikatsdatei vorhanden ist oder nicht. Das SSL-Zertifikat ist ein digital signiertes Zertifikat von einer Zertifizierungsstelle, das dem Webbrowser eine sichere Kommunikation mit dem Webserver ermöglicht. Informationen zum Verwalten und Konfigurieren des SSL-Zertifikats finden Sie im Artikel [Secure Socket Layer \(SSL\) Certificate Management auf WAP121 und WAP321 Access Points](#).

Schritt 5: Wählen Sie im Navigationsbereich **Security > RADIUS Server (Sicherheit > RADIUS-Server)** aus. Die Seite *RADIUS Server* wird geöffnet. Geben Sie die Parameter ein, und klicken Sie auf die Schaltfläche **Speichern**, sobald die Radius-Server-Parameter eingegeben wurden.

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

Save