

Activation de plusieurs réseaux sans fil sur le routeur VPN RV320, le point d'accès sans fil N WAP321 et les commutateurs de la gamme Sx300

Objectif

Dans un environnement professionnel en constante évolution, le réseau de votre petite entreprise doit être puissant, flexible, accessible et hautement fiable, en particulier lorsque la croissance est une priorité. La popularité des périphériques sans fil a augmenté de façon exponentielle, ce qui n'est pas surprenant. Les réseaux sans fil sont rentables, faciles à déployer, flexibles, évolutifs et mobiles, et fournissent des ressources réseau en toute transparence. L'authentification permet aux périphériques réseau de vérifier et de garantir la légitimité d'un utilisateur tout en protégeant le réseau contre les utilisateurs non autorisés. Il est important de déployer une infrastructure réseau sans fil sécurisée et gérable.

Le routeur VPN double WAN Gigabit Cisco RV320 offre une connectivité d'accès fiable et hautement sécurisée pour vous et vos employés. Le point d'accès à bande réglable Cisco WAP321 Wireless-N avec configuration par point unique prend en charge les connexions haut débit avec Gigabit Ethernet. Les ponts connectent les réseaux locaux sans fil, ce qui permet aux petites entreprises d'étendre leurs réseaux plus facilement.

Cet article fournit des instructions détaillées sur la configuration requise pour activer l'accès sans fil dans un réseau Cisco Small Business, notamment le routage entre réseaux locaux virtuels (VLAN), plusieurs SSID (Service Set Identifier) et les paramètres de sécurité sans fil sur le routeur, le commutateur et les points d'accès.

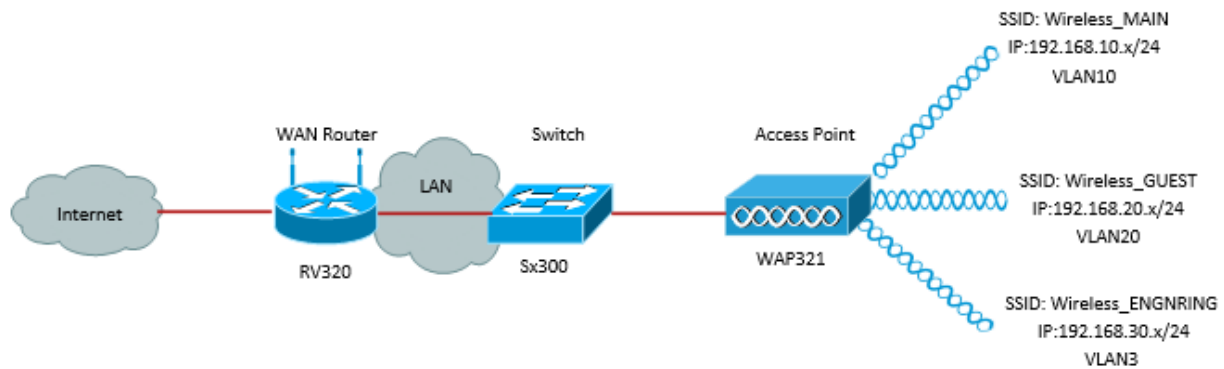
Périphériques pertinents

- Routeur VPN RV320
- Point d'accès sans fil N WAP321
- Commutateur Sx300

Version du logiciel

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

Topologie du réseau



L'image ci-dessus illustre un exemple de mise en oeuvre d'un accès sans fil utilisant plusieurs SSID avec un WAP, un commutateur et un routeur Cisco Small Business. Le WAP se connecte au commutateur et utilise l'interface trunk pour transporter plusieurs paquets VLAN. Le commutateur se connecte au routeur WAN via l'interface d'agrégation et le routeur WAN effectue le routage entre VLAN. Le routeur WAN se connecte à Internet. Tous les périphériques sans fil se connectent au WAP.

Fonctionnalités principales

L'association de la fonctionnalité de routage inter-VLAN fournie par le routeur Cisco RV et de la fonctionnalité d'isolation SSID sans fil fournie par un point d'accès de petite entreprise constitue une solution simple et sécurisée pour l'accès sans fil sur tout réseau Cisco de petite entreprise existant.

Routage inter-VLAN

Les périphériques réseau de différents VLAN ne peuvent pas communiquer entre eux sans un routeur pour acheminer le trafic entre les VLAN. Dans un réseau de petite entreprise, le routeur effectue le routage inter-VLAN pour les réseaux filaires et sans fil. Lorsque le routage inter-VLAN est désactivé pour un VLAN spécifique, les hôtes de ce VLAN ne peuvent pas communiquer avec les hôtes ou les périphériques d'un autre VLAN.

Isolation SSID sans fil

Il existe deux types d'isolation SSID sans fil. Lorsque l'isolation sans fil (au sein du SSID) est activée, les hôtes du même SSID ne peuvent pas se voir. Lorsque l'isolation sans fil (entre SSID) est activée, le trafic sur un SSID n'est transféré à aucun autre SSID.

IEEE 802.1x

La norme IEEE 802.1x spécifie les méthodes utilisées pour mettre en oeuvre un contrôle d'accès basé sur les ports qui est utilisé pour fournir un accès réseau authentifié aux réseaux Ethernet. L'authentification basée sur les ports est un processus qui permet uniquement aux échanges d'informations d'identification de traverser le réseau jusqu'à ce que l'utilisateur connecté au port soit authentifié. Le port est appelé port non contrôlé pendant l'échange des informations d'identification. Le port est appelé port contrôlé une fois

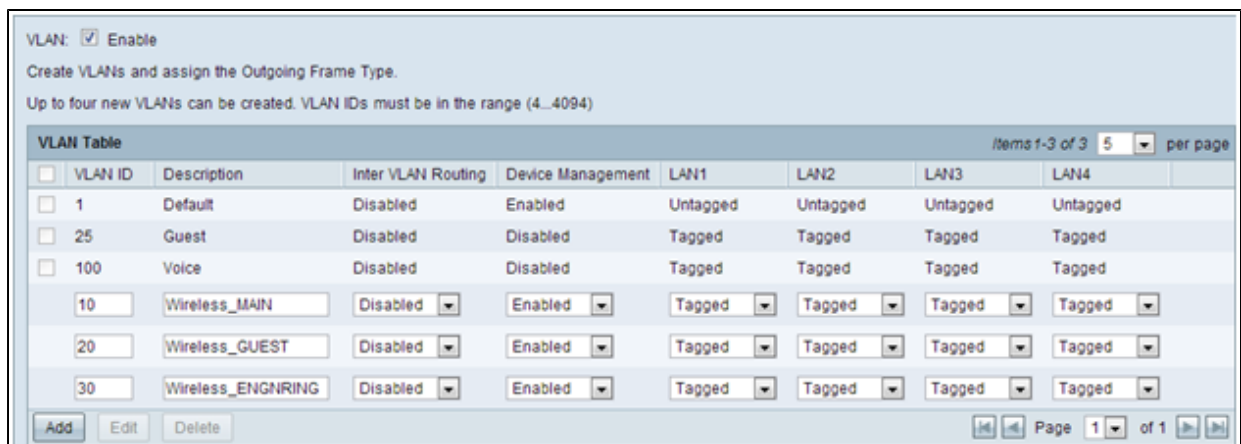
l'authentification terminée. Il est basé sur deux ports virtuels existant au sein d'un seul port physique.

Cette méthode utilise les caractéristiques physiques de l'infrastructure LAN commutée pour authentifier les périphériques connectés à un port LAN. L'accès au port peut être refusé si le processus d'authentification échoue. Cette norme a été conçue à l'origine pour les réseaux Ethernet câblés, mais elle a été adaptée pour être utilisée sur les réseaux locaux sans fil 802.11.

Configuration du RV320

Dans ce scénario, nous voulons que le routeur RV320 agisse en tant que serveur DHCP pour le réseau. Nous devons donc le configurer et configurer des réseaux locaux virtuels distincts sur le périphérique. Pour commencer, connectez-vous au routeur en vous connectant à l'un des ports Ethernet et en accédant à 192.168.1.1 (en supposant que vous n'avez pas déjà modifié l'adresse IP du routeur).

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Port Management > VLAN Membership. Une nouvelle page s'ouvre. Nous créons 3 VLAN distincts pour représenter différents publics cibles. Cliquez sur Add pour ajouter une nouvelle ligne et modifier l'ID et la description du VLAN. Vous devrez également vous assurer que le VLAN est défini sur Tagged sur toutes les interfaces sur lesquelles ils devront voyager.



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

Page 1 of 1

Étape 2. Connectez-vous à l'utilitaire de configuration Web et sélectionnez DHCP Menu > DHCP Setup. La page DHCP Setup s'ouvre :

- Dans la liste déroulante VLAN ID, sélectionnez le VLAN pour lequel vous configurez le pool d'adresses (dans cet exemple, les VLAN 10, 20 et 30).
- Configurez l'adresse IP du périphérique pour ce VLAN et définissez la plage d'adresses IP. Vous pouvez également activer ou désactiver le proxy DNS ici si vous le souhaitez, et cela dépendra du réseau. Dans cet exemple, le proxy DNS fonctionnera pour transférer les requêtes DNS.
- Cliquez sur Save et répétez cette étape pour chaque VLAN.

DHCP Setup

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:

Étape 3. Dans le volet de navigation, sélectionnez Port Management > 802.1x Configuration. La page 802.1X Configuration s'ouvre :

- Activez l'authentification basée sur les ports et configurez l'adresse IP du serveur.
- Le secret RADIUS est la clé d'authentification utilisée pour communiquer avec le serveur.
- Choisissez les ports qui utiliseront cette authentification et cliquez sur Save.

802.1X Configuration

Configuration

Port-Based Authentication

RADIUS IP:

RADIUS UDP Port:

RADIUS Secret:

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

Configuration Sx300

Le commutateur SG300-10MP sert d'intermédiaire entre le routeur et le WAP321 afin de simuler un environnement réseau réaliste. La configuration du commutateur est la suivante.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et sélectionnez VLAN Management > Create VLAN. Une nouvelle page s'ouvre :

Étape 2. Cliquez sur Add. Une nouvelle fenêtre s'affiche. Saisissez l'ID et le nom du VLAN (utilisez la même description que celle de la section I). Cliquez sur Apply, puis répétez cette étape pour les VLAN 20 et 30.

VLAN

Range

* VLAN ID: (Range: 2 - 4094)

VLAN Name: (13/32 Characters Used)

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

Étape 3. Dans le volet de navigation, sélectionnez VLAN Management > Port to VLAN. Une nouvelle page s'ouvre :

- En haut de la page, définissez l'« ID de VLAN égal à » pour le VLAN que vous ajoutez (dans ce cas, VLAN 10), puis cliquez sur Go à droite. La page est alors mise à jour avec les paramètres de ce VLAN.
- Modifiez le paramètre sur chaque port de sorte que le VLAN 10 soit désormais « Balisé » au lieu de « Exclu ». Répétez cette étape pour les VLAN 20 et 30.

Port to VLAN

Filter: VLAN ID equals to AND Interface Type equals to

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"/>

Étape 4. Dans le volet de navigation, sélectionnez Security > Radius . La page RADIUS s'ouvre :

- Choisissez la méthode de contrôle d'accès à utiliser par le serveur RADIUS, soit le contrôle d'accès de gestion, soit l'authentification basée sur les ports. Choisissez Port Based Access Control et cliquez sur Apply.
- Cliquez sur Add au bas de la page pour ajouter un nouveau serveur auquel s'authentifier.

RADIUS

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

Étape 5. Dans la fenêtre qui s'affiche, vous allez configurer l'adresse IP du serveur, en l'occurrence 192.168.1.32. Vous devrez définir une priorité pour le serveur, mais puisque dans cet exemple, nous n'avons qu'un seul serveur à authentifier à la priorité n'a pas d'importance. Ceci est important si vous avez le choix entre plusieurs serveurs RADIUS. Configurez la clé d'authentification et les autres paramètres peuvent être conservés par défaut.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

✱ Server IP Address/Name:

✱ Priority: (Range: 0 - 65535)

Key String: Use Default

User Defined (Encrypted)

User Defined (Plaintext)

Étape 6. Dans le volet de navigation, sélectionnez Security > 802.1X > Properties. Une nouvelle page s'ouvre :

- Cochez Enable pour activer l'authentification 802.1x et choisissez la méthode d'authentification. Dans ce cas, nous utilisons un serveur RADIUS. Choisissez donc la première ou la deuxième option.


- Cliquez sur Apply.

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

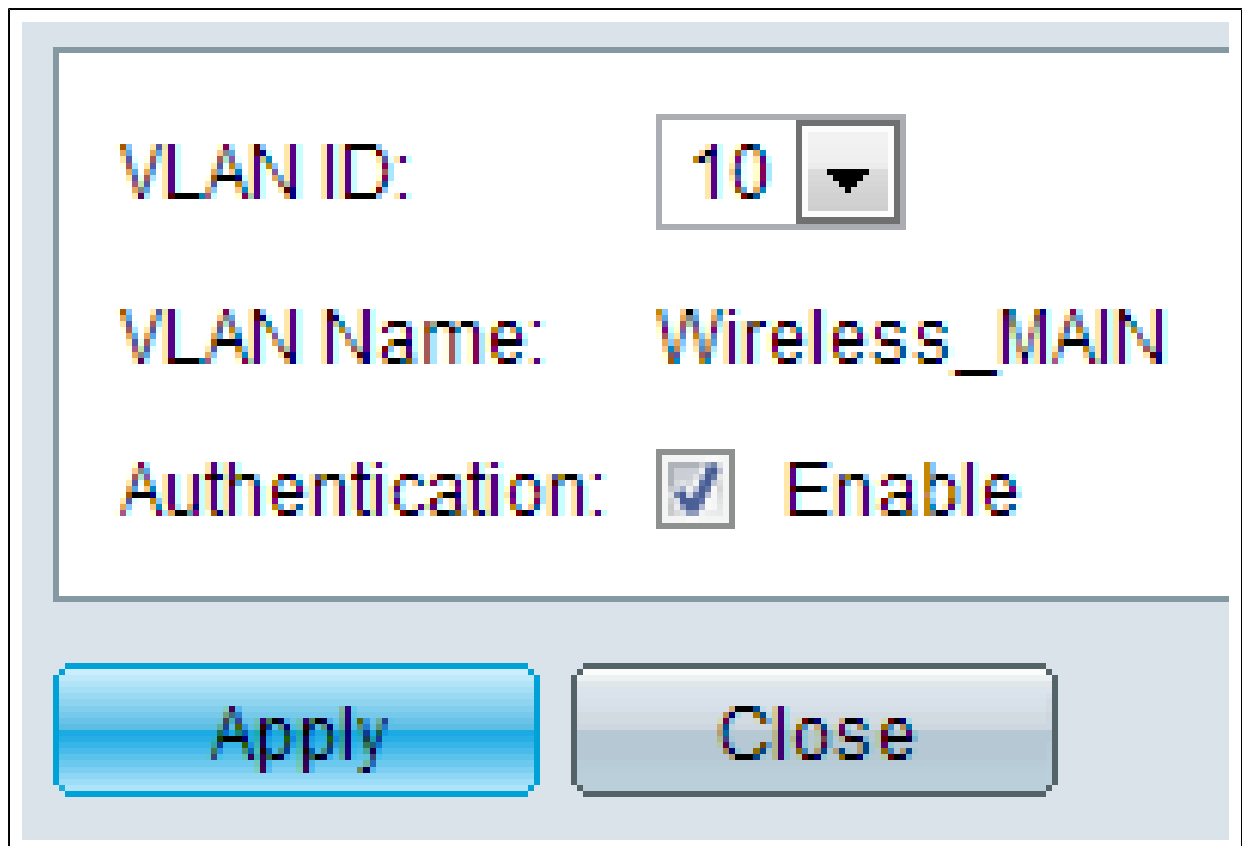
Guest VLAN: Enable

Guest VLAN ID: 1 ▼

 Guest VLAN Timeout: Immediate
 User Defined

Apply Cancel

Étape 7. Choisissez l'un des VLAN et cliquez sur Edit. Une nouvelle fenêtre s'affiche. Cochez Enable pour autoriser l'authentification sur ce VLAN et cliquez sur Apply. Répétez l'opération pour chaque VLAN.



VLAN ID: 10

VLAN Name: Wireless_MAIN

Authentication: Enable

Apply Close

Configuration WAP321

Les points d'accès virtuels (VAP) segmentent le réseau local sans fil en plusieurs domaines de diffusion qui sont l'équivalent sans fil des réseaux locaux virtuels Ethernet. Les VAP simulent plusieurs points d'accès dans un périphérique WAP physique. Le WAP121 prend en charge jusqu'à quatre VAP et le WAP321 jusqu'à huit VAP.

Chaque VAP peut être activé ou désactivé indépendamment, à l'exception de VAP0. VAP0 est l'interface radio physique et reste activée tant que la radio est activée. Pour désactiver le fonctionnement de VAP0, la radio elle-même doit être désactivée.

Chaque VAP est identifié par un SSID (Service Set Identifier) configuré par l'utilisateur. Plusieurs VAP ne peuvent pas avoir le même nom SSID. Les diffusions SSID peuvent être activées ou désactivées indépendamment sur chaque VAP. La diffusion SSID est activée par défaut.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et sélectionnez Wireless > Radio. La page Radio s'ouvre :

- Cochez la case Enable pour activer la radio sans fil.
- Cliquez sur Save. La radio est alors activée.

Radio

Global Settings

TSPEC Violation Interval:

Basic Settings

Radio: Enable

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

Mode: ▾

Channel Bandwidth: ▾

Primary Channel: ▾

Channel: ▾

Étape 2. Dans le volet de navigation, sélectionnez Wireless > Networks. La page Réseau s'ouvre :

Networks

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"/>	<input type="text" value="1"/>	<input type="text" value="Cisco1"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/> ▾	<input type="text" value="Disabled"/> ▾	<input type="checkbox"/>	Show Details
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	<input type="text" value="Cisco2"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/> ▾	<input type="text" value="Disabled"/> ▾	<input type="checkbox"/>	Show Details
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	<input type="text" value="Cisco3"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/> ▾	<input type="text" value="Disabled"/> ▾	<input type="checkbox"/>	Show Details

Remarque : le SSID par défaut pour VAP0 est ciscosb. Chaque VAP supplémentaire créé a

un nom SSID vide. Les SSID de tous les VAP peuvent être configurés sur d'autres valeurs.

Étape 3. Chaque VAP est associé à un VLAN, qui est identifié par un ID de VLAN (VID). Un VID peut être n'importe quelle valeur comprise entre 1 et 4094 inclus. Le WAP121 prend en charge cinq VLAN actifs (quatre pour le WLAN plus un VLAN de gestion). Le WAP321 prend en charge neuf VLAN actifs (huit pour le WLAN plus un VLAN de gestion).

Par défaut, le VID attribué à l'utilitaire de configuration pour le périphérique WAP est 1, qui est également le VID non balisé par défaut. Si le VID de gestion est le même que le VID attribué à un VAP, alors les clients WLAN associés à ce VAP spécifique peuvent administrer le périphérique WAP. Si nécessaire, une liste de contrôle d'accès (ACL) peut être créée pour désactiver l'administration des clients WLAN.

Sur cet écran, vous devez effectuer les étapes suivantes :

- Cliquez sur les boutons de coche à gauche pour modifier les SSID :
- Entrez la valeur nécessaire à l'ID de VLAN dans la zone ID de VLAN
- Cliquez sur le bouton Save une fois que les SSID ont été entrés.

The screenshot shows a web interface titled "Networks" with a section for "Virtual Access Points (SSIDs)". It contains a table with columns: VAP No., Enable, VLAN ID, SSID Name, SSID Broadcast, Security, MAC Filter, and Channel Isolation. There are three rows of configuration, each with a "Show Details" link below it. At the bottom, there are buttons for "Add", "Edit", "Delete", and "Save".

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"/>
Show Details							
1	<input checked="" type="checkbox"/>	20	Wireless_GUEST	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							
2	<input checked="" type="checkbox"/>	30	Wireless_ENGRING	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>
Show Details							

Buttons: Add, Edit, Delete, Save

Étape 4. Dans le volet de navigation, sélectionnez System Security > 802.1X Supplicant. La page 802.1X Supplicant s'ouvre :

- Cochez Enable dans le champ Administrative Mode pour permettre au périphérique d'agir en tant que demandeur dans l'authentification 802.1X.
- Choisissez le type approprié de méthode EAP (Extensible Authentication Protocol) dans la liste déroulante du champ EAP Method.
- Entrez le nom d'utilisateur et le mot de passe que le point d'accès utilise pour obtenir l'authentification auprès de l'authentificateur 802.1X dans les champs Username et Password. La longueur du nom d'utilisateur et du mot de passe doit être comprise entre 1 et 64 caractères alphanumériques et symboles. Ce paramètre doit déjà être configuré sur le serveur d'authentification.
- Cliquez sur Save pour enregistrer les paramètres.

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
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: No file chosen

Remarque : la zone Certificate File Status indique si le fichier de certificat est présent ou non. Le certificat SSL est un certificat signé numériquement par une autorité de certification qui permet au navigateur Web d'avoir une communication sécurisée avec le serveur Web. Pour gérer et configurer le certificat SSL, consultez l'article [Gestion des certificats SSL \(Secure Socket Layer\) sur les points d'accès WAP121 et WAP321](#)

Étape 5. Dans le volet de navigation, sélectionnez Security > RADIUS Server. La page RADIUS Server s'ouvre. Entrez les paramètres, et cliquez sur le bouton Save une fois que les paramètres du serveur Radius ont été entrés.

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.