Meervoudige draadloze netwerken mogelijk maken op RV320 VPN-router, WAP321 Wireless-N access point en SX300 Series-switches

Doel

In een voortdurend veranderend bedrijfsklimaat moet uw netwerk van kleine bedrijven krachtig, flexibel, toegankelijk en zeer betrouwbaar zijn, vooral wanneer groei een prioriteit is. De populariteit van draadloze apparaten is exponentieel toegenomen, wat geen verrassing is. Draadloze netwerken zijn kostenefficiënt, makkelijk in te zetten, flexibel, schaalbaar en mobiel en voorzien naadloos van netwerkbronnen. Verificatie maakt netwerkapparaten mogelijk om de legitimiteit van een gebruiker te controleren en te garanderen en tegelijkertijd het netwerk te beschermen tegen onbevoegde gebruikers. Het is belangrijk om een veilige en beheersbare draadloze netwerkinfrastructuur in te voeren.

De Cisco RV320 VPN-router met dubbel Gigabit WAN biedt een betrouwbare, zeer beveiligde toegangsconnectiviteit voor u en uw werknemers. Cisco WAP321 Wireless-N access point met bandselectie en Single Point Setup ondersteunt snelle verbindingen met Gigabit Ethernet. Bruggen verbinden LAN's draadloos, waardoor het voor kleine bedrijven gemakkelijker wordt om hun netwerken uit te breiden.

Dit artikel biedt stap voor stap richtlijnen voor de configuratie die nodig is om draadloze toegang in een Cisco-netwerk voor kleine bedrijven mogelijk te maken, inclusief routing tussen Virtual Area Network (VLAN), meerdere Service Set Identifier (SSID's) en draadloze beveiligingsinstellingen op de router, switch en access points.

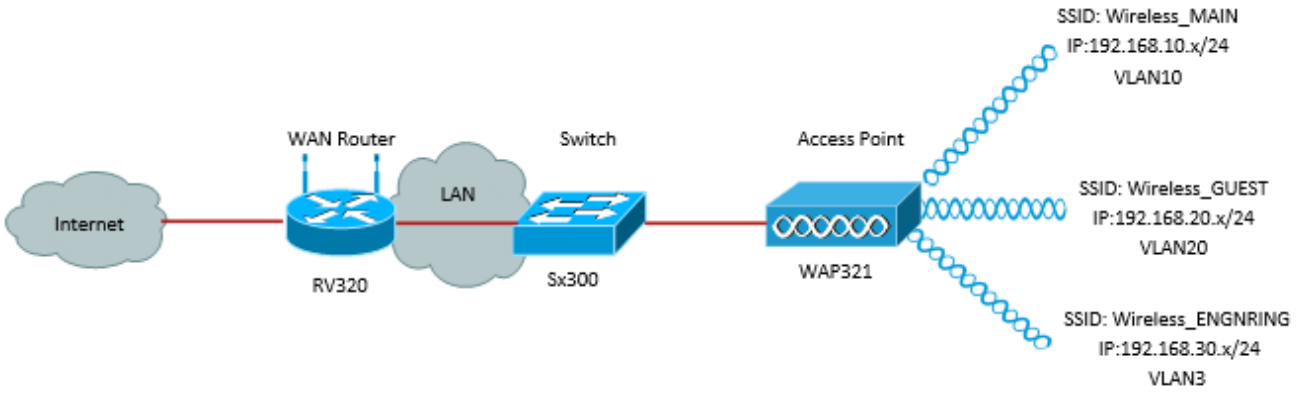
Toepasselijke apparaten

- RV320 VPN-router
- WAP321 Wireless-N access point
- SX300 Series-switch

Softwareversie

- 1.1.0.09 (RV320)
- 1.0.4.2 (WAP321)
- 1.3.5.58 (SX300)

Netwerktopologie



Het bovenstaande beeld illustreert een voorbeeldimplementatie voor draadloze toegang met behulp van meerdere SSID's met een kleine WAP, schakelaar en router van Cisco. WAP verbindt zich met de switch en gebruikt de interface van de romp om meerdere VLAN-pakketten te transporteren. De switch sluit aan op de WAN-router door de interface van de romp en de WAN-router voert routing tussen VLAN's uit. De WAN-router sluit aan op het internet. Alle draadloze apparaten aansluiten op de WAP.

Belangrijkste kenmerken

Een combinatie van de routing tussen VLAN's die door de Cisco RV-router wordt geleverd met de draadloze SSID-scheidingsfunctie die door een access point voor kleine bedrijven wordt geboden, biedt een eenvoudige en beveiligde oplossing voor draadloze toegang op een bestaand Cisco-netwerk voor kleine bedrijven.

Inter-VLAN-routing

Netwerkapparaten in verschillende VLAN's kunnen niet met elk afzonderlijk VLAN's communiceren zonder router om verkeer tussen de VLAN's te routeren. In een klein bedrijfsnetwerk, voert de router de routing tussen VLAN's uit voor zowel de bekabelde als draadloze netwerken. Wanneer de routing tussen VLAN's voor een specifiek VLAN is uitgeschakeld, zullen hosts op dat VLAN niet met hosts of apparaten op een ander VLAN kunnen communiceren.

Draadloze SSID's (Isolation)

Er zijn twee soorten draadloze SSID isolatie. Wanneer draadloze isolatie (binnen SSID) wordt geactiveerd, zullen de hosts op dezelfde SSID niet in staat zijn elkaar te zien. Wanneer Wireless Isolation (tussen SSID) is ingeschakeld, wordt het verkeer op één SSID niet naar een andere SSID doorgestuurd.

IEEE 802.1x

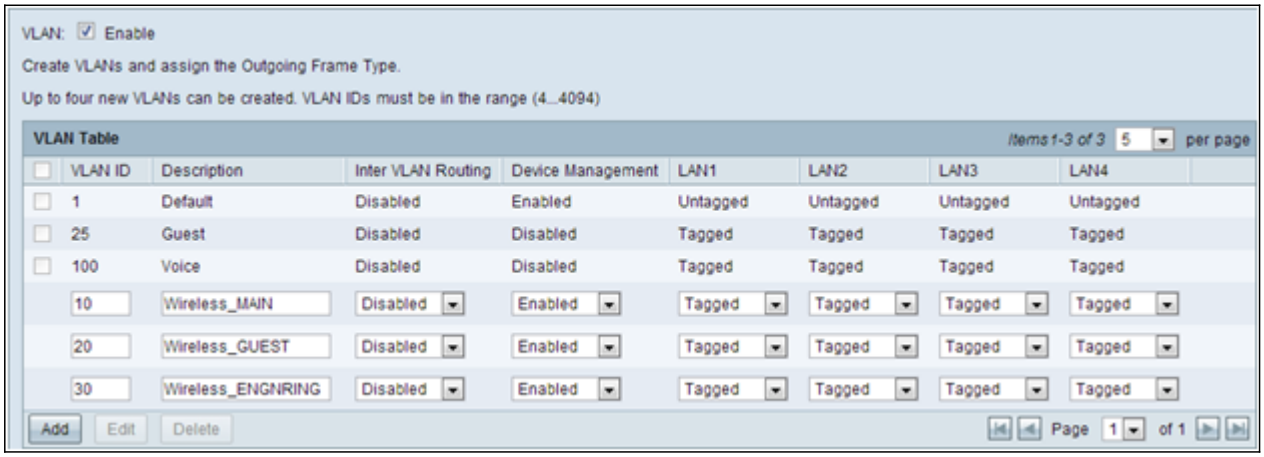
De standaard IEEE 802.1x specificeert methoden die worden gebruikt om poortgebaseerde toegangscontrole voor netwerken uit te voeren die wordt gebruikt om geauthenticeerde netwerktoegang tot Ethernet-netwerken te bieden. Havengebaseerde authenticatie is een proces waarbij alleen creditcard uitwisselingen het netwerk kunnen doorkruisen tot de gebruiker die aangesloten is op de poort echt is geworden. De haven wordt genoemd een ongecontroleerde haven tijdens de tijd van de geloofsbrieven uitwisseling. De haven wordt een gecontroleerde haven genoemd nadat de authenticatie is voltooid. Dit is gebaseerd op twee virtuele poorten die binnen één fysieke poort bestaan.

Dit gebruikt de fysieke eigenschappen van de switched LAN-infrastructuur om apparaten die op een LAN-poort zijn aangesloten te authentiseren. Toegang tot de haven kan worden geweigerd indien de authenticatieprocedure mislukt. Deze standaard is oorspronkelijk ontworpen voor bekabelde Ethernet-netwerken, maar is aangepast voor gebruik op 802.11 draadloze LAN's.

RV320-configuratie

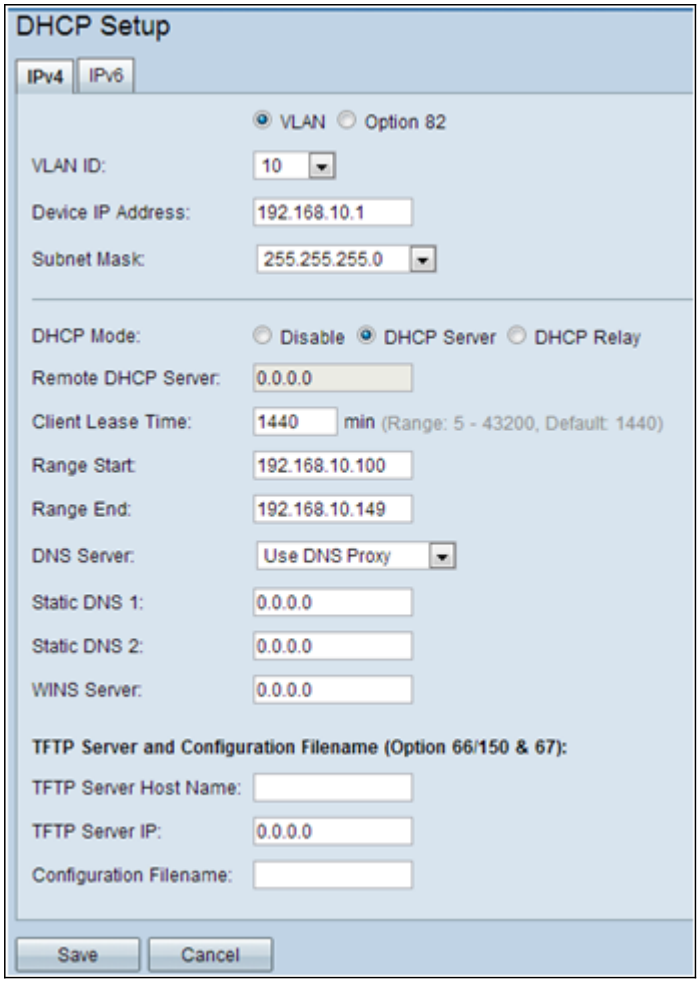
In dit scenario willen we dat RV320 als de DHCP-server voor het netwerk fungeert, dus moeten we dat instellen en afzonderlijke VLAN's op het apparaat configureren. Start, log in op de router door deze aan te sluiten op een van de Ethernet-poorten en naar 192.168.1.1 te gaan (ervan uitgaande dat u het IP-adres van de router niet al hebt gewijzigd).

Stap 1. Meld u aan bij het web-configuratieprogramma en kies **Port Management > VLAN-lidmaatschap**. Er wordt een nieuwe pagina geopend. We maken 3 afzonderlijke VLAN's om verschillende doelgroepen te vertegenwoordigen. Klik op **Add** om een nieuwe regel toe te voegen en de VLAN-id en -beschrijving te bewerken. U zal ook moeten verzekeren dat het VLAN op *Tagged* wordt ingesteld op om het even welke interfaces waarop zij zullen moeten reizen.



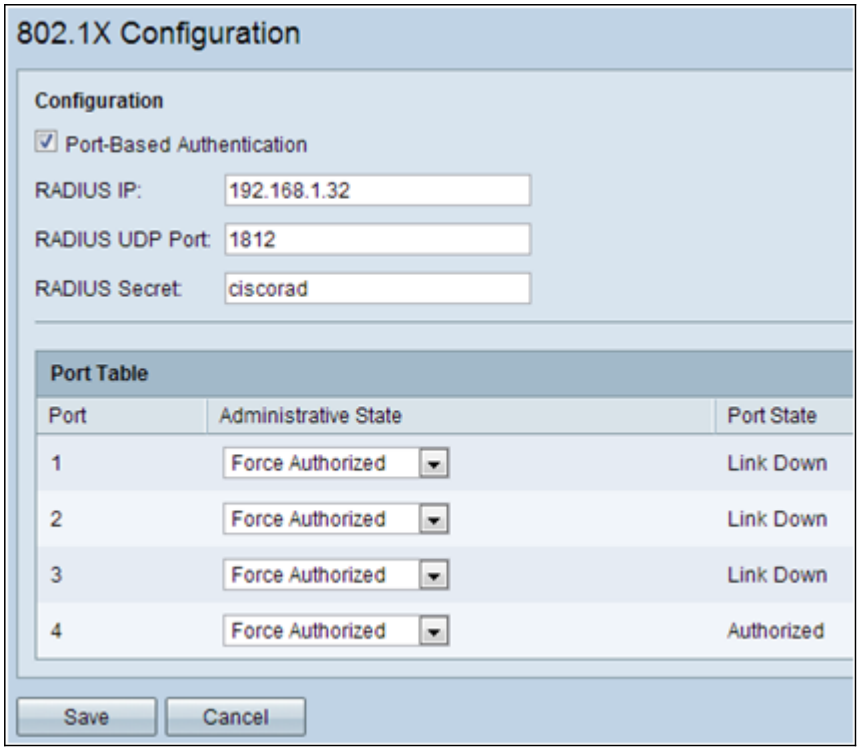
Stap 2. Meld u aan bij het programma voor webconfiguratie en selecteer **DHCP-menu > DHCP-instelling**. De pagina *DHCP Setup* wordt geopend:

- In het dialoogvenster VLAN-id selecteert u het VLAN dat u wilt instellen, de adrespool voor (in dit voorbeeld VLAN's 10, 20 en 30).
- Configureer het IP-adres van het apparaat voor dit VLAN en stel het IP-adresbereik in. U kunt DNS-proxy ook hier inschakelen of uitschakelen als u dit wilt. Dit is afhankelijk van het netwerk. In dit voorbeeld, zal DNS Proxy werken om DNS verzoeken door te sturen.
- Klik op **Opslaan** en herhaal deze stap voor elk VLAN.



Stap 3. Selecteer in het navigatiedeelvenster de optie **Port Management > 802.1x Configuration**. De pagina *802.1X configuratie* wordt geopend:

- Schakel Port-gebaseerde verificatie in en stel het IP-adres van de server in.
- RADIUS-geheim is de authenticatiesleutel die wordt gebruikt om met de server te communiceren.
- Kies welke poorten deze verificatie zullen gebruiken en klik op **Opslaan**.

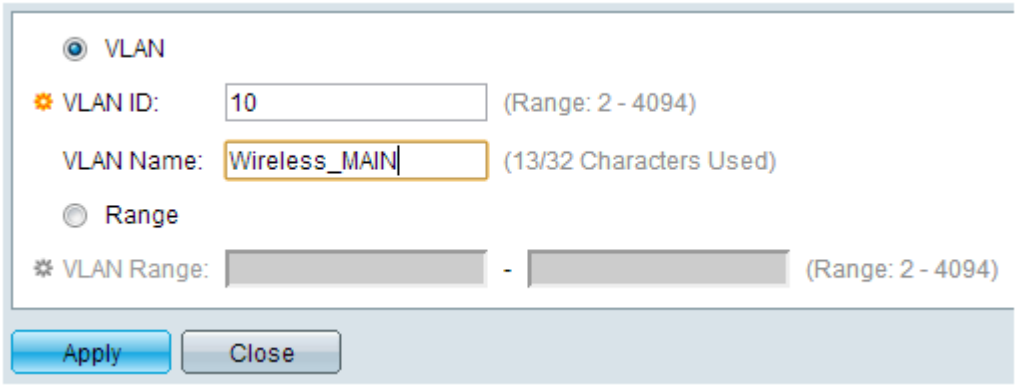


SX300-configuratie

De SG300-10MP-switch werkt als een intermediair tussen de router en WAP321 om een realistische netwerkomgeving te simuleren. De configuratie van de schakelaar is als volgt.

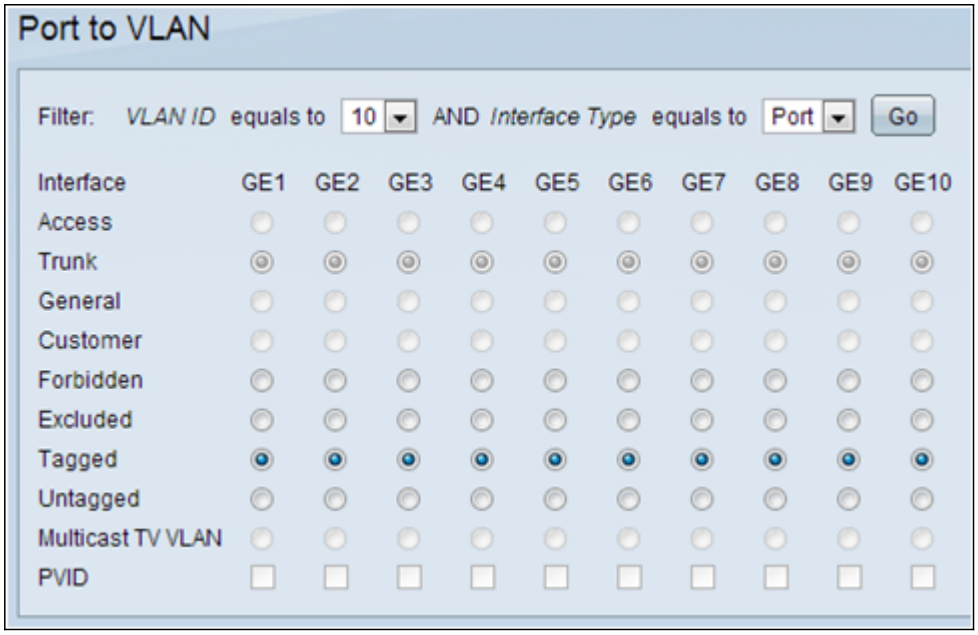
Stap 1. Meld u aan bij het web configuratie hulpprogramma en selecteer **VLAN-beheer > VLAN's maken**. Er wordt een nieuwe pagina geopend:

Stap 2. Klik op **Add**. Er verschijnt een nieuw venster. Voer de VLAN-id en de VLAN-naam in (gebruik dezelfde beschrijving als in sectie I). Klik op Toepassen en herhaal deze stap voor VLAN's 20 en 30.



Stap 3. Selecteer in het navigatiedeelvenster de optie **VLAN-beheer > Port-naar-VLAN**. Er wordt een nieuwe pagina geopend:

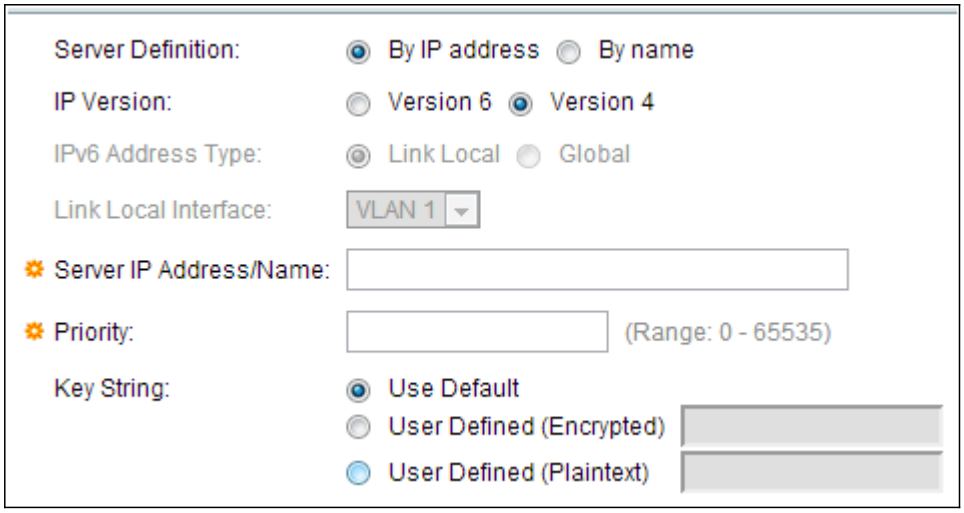
- Bovenaan de pagina stelt u de "VLAN-id is gelijk aan" aan het VLAN dat u toevoegt (in dit geval VLAN 10) en klikt u vervolgens op **Ga** rechts. Dit zal de pagina met de instellingen voor dat VLAN bijwerken.
- Wijzig de instelling op elke poort zodat VLAN 10 nu "Tagged" in plaats van "Uitgesloten is." Herhaal deze stap voor VLAN's 20 en 30.



Stap 4. Selecteer in het navigatiedeelvenster **Security > Straal**. De pagina *RADIUS* wordt geopend:

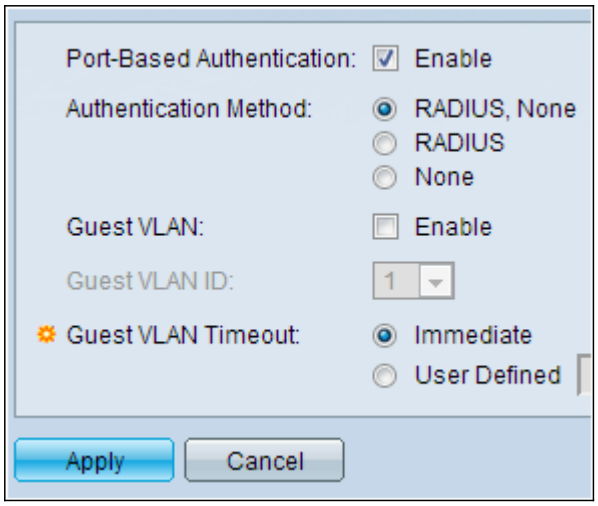
- Kies de methode van toegangscontrole die door de RADIUS-server moet worden gebruikt, ofwel beheer- en toegangscontrole of poortgebaseerde verificatie. Kies Port-Based Access Control en klik op **Toepassen**.
- Klik op **Add** onder in de pagina om een nieuwe server toe te voegen die voor authentiek moet zijn.

Stap 5. In het venster dat verschijnt, zult u het IP-adres van de server configureren, in dit geval 192.168.1.32. U moet een prioriteit voor de server instellen, maar aangezien we in dit voorbeeld slechts één server hebben om authenticatie aan de prioriteit te geven, maakt niet uit. Dit is belangrijk als u meerdere RADIUS-servers hebt om uit te kiezen. Configureer de verificatiesleutel en de rest van de instellingen kan standaard worden achtergelaten.

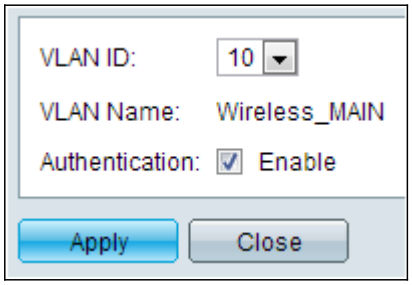


Stap 6. Selecteer in het navigatiedeelvenster **Security > 802.1x > Eigenschappen**. Er wordt een nieuwe pagina geopend:

- Controleer of 802.1x-verificatie kan worden ingeschakeld en kies de verificatiemethode. In dit geval gebruiken we een RADIUS-server en kies dus de eerste of tweede optie.
- Klik op **Toepassen**.



Stap 7. Kies een van de VLAN's en klik op **Bewerken**. Er verschijnt een nieuw venster. Controleer **Schakel** in om verificatie op dat VLAN toe te staan en klik op *Toepassen*. Doe dit voor elk VLAN.



WAP321-configuratie

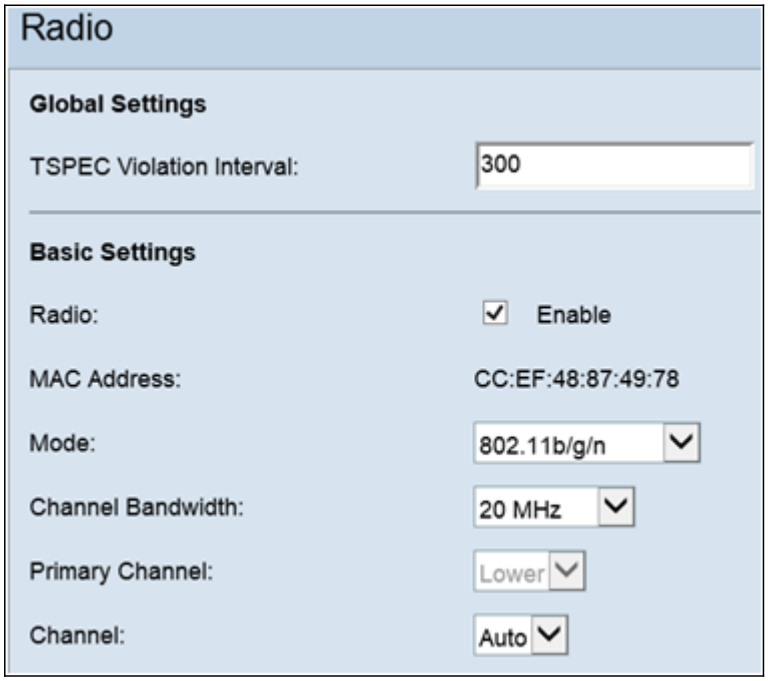
Virtual Access Point (VAP's) segmenteert het draadloze LAN-netwerk in meerdere broadcast-domeinen die het draadloze equivalent van Ethernet VLAN's zijn. VAP's simuleren meerdere toegangspunten in één fysiek WAP-apparaat. Er worden maximaal vier VAP's ondersteund op WAP121 en maximaal acht VAP's worden ondersteund op WAP321.

Elke VAP kan onafhankelijk worden ingeschakeld of uitgeschakeld, met uitzondering van VAP0. VAP0 is de fysieke radio-interface en blijft ingeschakeld zolang de radio is ingeschakeld. Om de werking van VAP0 uit te schakelen, moet de radio zelf worden uitgeschakeld.

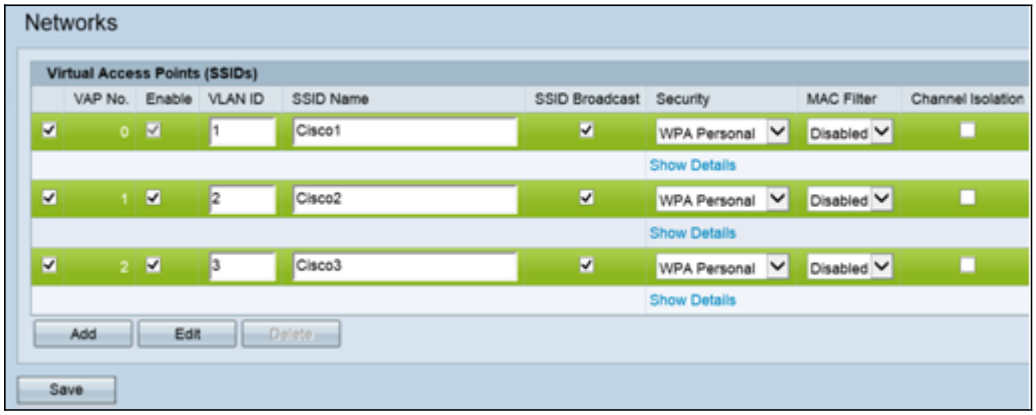
Elke VAP wordt geïdentificeerd door een door de gebruiker ingesteld Service Set Identifier (SSID). Meerdere VAP's kunnen niet dezelfde SSID-naam hebben. SSID's kunnen onafhankelijk op elke VAP worden ingeschakeld of uitgeschakeld. De uitzending van SSID wordt standaard ingeschakeld.

Stap 1. Meld u aan bij het web configuratieprogramma en selecteer **Draadloos > Radio**. De pagina *Radio* opent:

- Klik op het aanvinkvakje **Enable** om de draadloze radio in te schakelen.
- Klik op **Opslaan**. De radio wordt ingeschakeld.



Stap 2. Selecteer in het navigatiedeelvenster de optie **Draadloos > netwerken**. De pagina *Netwerk* opent:



Opmerking: De standaard SSID voor VAP0 is ciscosb. Elke extra VAP die is gemaakt, heeft een lege SSID naam. De SSID's voor alle VAP's kunnen worden ingesteld op andere waarden.

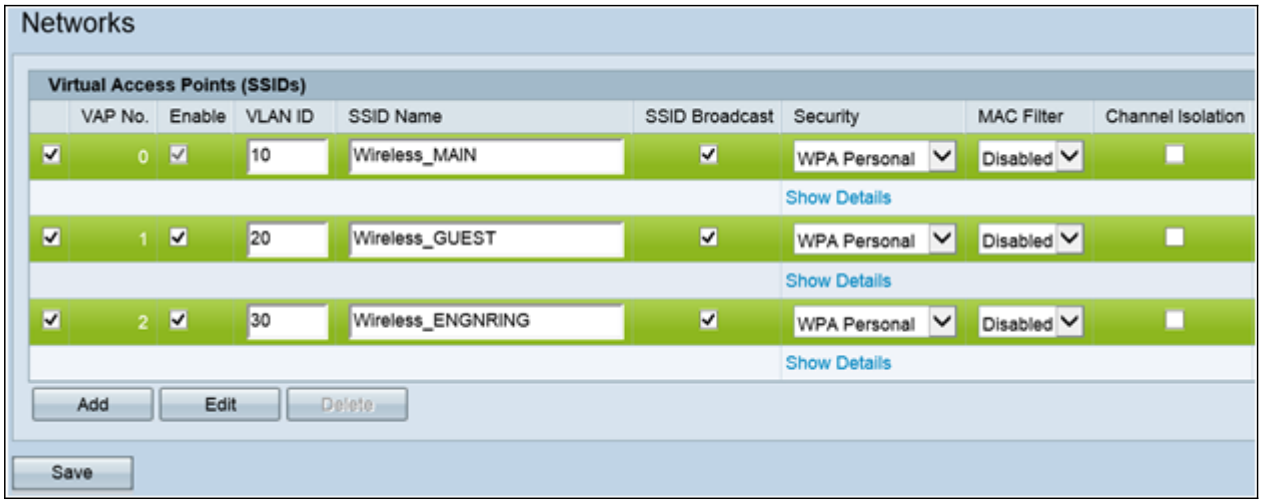
Stap 3. Elke VAP is gekoppeld aan een VLAN dat door een VLAN-id (VID) wordt

geïdentificeerd. Een VID kan elke waarde van 1 tot 4094 zijn, inclusief. WAP121 ondersteunt vijf actieve VLAN's (vier voor WLAN plus één beheerVLAN). WAP321 ondersteunt negen actieve VLAN's (acht voor WLAN plus één beheerVLAN).

Standaard is de VID die is toegewezen aan het configuratieprogramma voor het WAP-apparaat 1, wat ook de standaard niet-gelabelde VID is. Als de VID van het beheer gelijk is aan de VID die aan een VAP is toegewezen, kunnen de WLAN-clients die aan deze specifieke VAP zijn gekoppeld het WAP-apparaat beheren. Indien nodig kan een toegangscontrolelijst (ACL) worden gemaakt om beheer van WLAN-clients uit te schakelen.

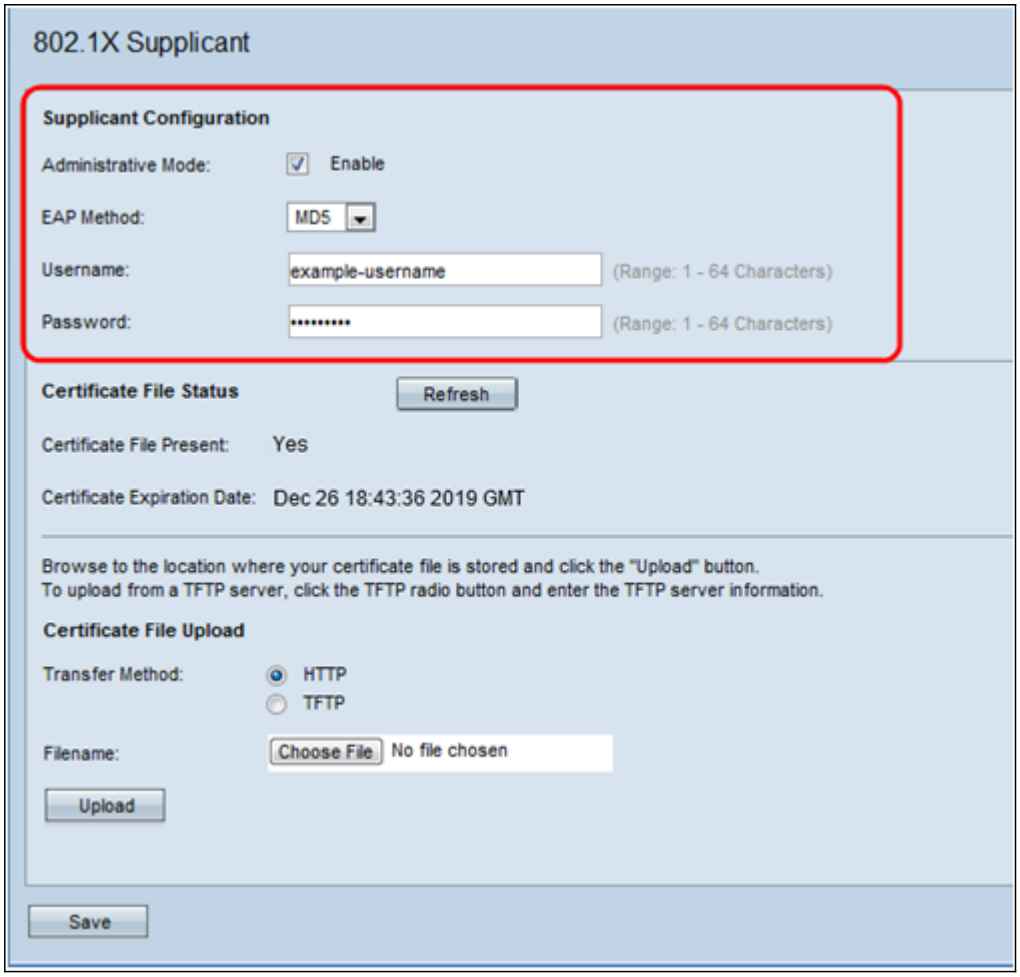
Op dit scherm dienen de volgende stappen te worden genomen:

- Klik op de knoppen aan de linkerkant om de SSID's te bewerken:
- Voer de waarde in die nodig is voor de VLAN-id in het veld VLAN-id
- Klik op de knop **Opslaan** nadat de SSID's zijn ingevoerd.



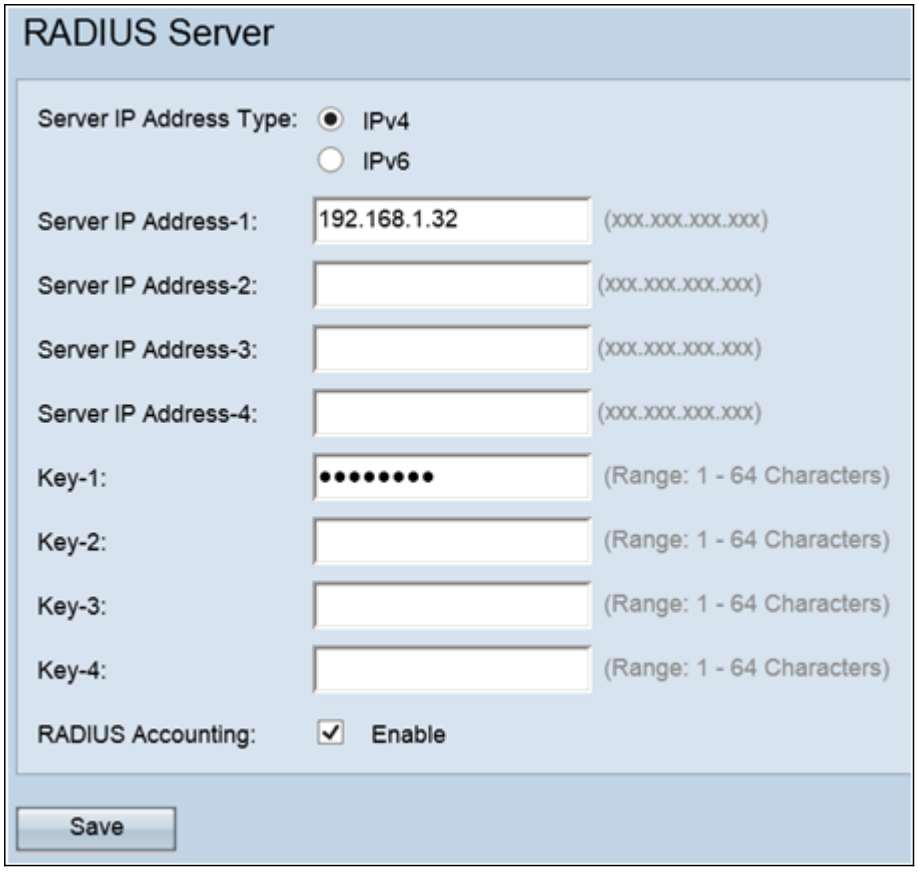
Stap 4. Selecteer in het navigatiedeelvenster **systeembeveiliging > 802.1X smeekbede**. De *verschoven 802.1X* pagina wordt geopend:

- Controleer in het veld **Administratieve** modus **inschakelen** om het apparaat in staat te stellen om als aanvrager op 802.1X-verificatie te reageren.
- Kies het juiste type van de MAP-methode (Extensible Authentication Protocol) in de vervolgkeuzelijst in het veld EAP-methode.
- Voer de gebruikersnaam en het wachtwoord in die het access point gebruikt om verificatie te krijgen van de 802.1X-authenticator in de velden Gebruikersnaam en Wachtwoord. De lengte van de gebruikersnaam en het wachtwoord moet van 1 tot 64 alfanumerieke tekens en symbolische tekens zijn. Dit zou al op de authenticatieserver moeten worden ingesteld.
- Klik op **Opslaan** om de instellingen op te slaan.



Opmerking: De status certificaatbestand toont aan of het certificaatbestand al dan niet aanwezig is. Het SSL-certificaat is een digitaal ondertekend certificaat door een certificeringsinstantie waarmee de webbrowser een veilige communicatie met de webserver kan hebben. Om het SSL-certificaat te beheren en te configureren verwijst u naar het artikel Secure Socket Layer (SSL) certificaatbeheer op WAP121 en WAP321 access points

Stap 5. Selecteer in het navigatiedeelvenster de optie **Security > RADIUS-server**. De pagina *RADIUS*-server wordt geopend. Voer de parameters in en klik op de knop **Opslaan** nadat de parameters voor Radius Server zijn ingevoerd.


RADIUS Server
Server IP Address Type:
IPv4
IPv6
Server IP Address-1:
192.168.1.32
(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