Abilitazione di più reti wireless su router VPN RV320, punto di accesso Wireless-N WAP321 e switch serie Sx300

Obiettivo

In un ambiente aziendale in continua evoluzione, la rete di piccole imprese deve essere potente, flessibile, accessibile e altamente affidabile, soprattutto quando la crescita è una priorità. La popolarità dei dispositivi wireless è cresciuta in modo esponenziale, il che non sorprende. Le reti wireless sono convenienti, facili da installare, flessibili, scalabili e mobili, fornendo senza problemi risorse di rete. L'autenticazione consente ai dispositivi di rete di verificare e garantire la legittimità di un utente proteggendo al contempo la rete da utenti non autorizzati. È importante installare un'infrastruttura di rete wireless sicura e gestibile.

Il router Cisco RV320 Dual Gigabit WAN VPN offre una connettività di accesso affidabile e altamente sicura per te e i tuoi dipendenti. L'access point Wireless-N Cisco WAP321 a banda selezionabile Wireless-N con Single Point Setup supporta connessioni ad alta velocità con Gigabit Ethernet. I bridge connettono le LAN in modalità wireless, semplificando l'espansione delle reti delle piccole aziende.

In questo documento viene fornita una guida dettagliata alla configurazione richiesta per abilitare l'accesso wireless in una rete Cisco per piccole imprese, inclusi il routing tra VLAN (Virtual Local Area Network), più SSID (Service Set Identifier) e le impostazioni di sicurezza wireless sul router, sullo switch e sui punti di accesso.

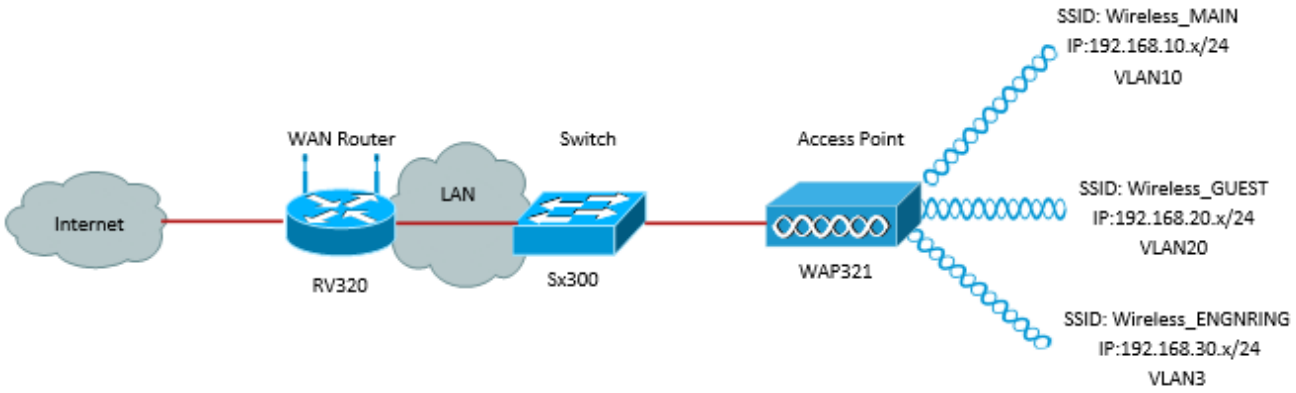
Dispositivi interessati

·RV320 VPN Router
· Access point Wireless-N WAP321
· Serie Sx300 Switch

Versione del software

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

Topologia della rete



Nell'immagine precedente viene mostrato un esempio di implementazione per l'accesso wireless che utilizza più SSID con un Cisco Small Business WAP, uno switch e un router. Il protocollo WAP si connette allo switch e utilizza l'interfaccia trunk per trasportare più pacchetti VLAN. Lo switch si connette al router WAN tramite l'interfaccia trunk e il router WAN esegue il routing tra VLAN. Il router WAN si connette a Internet. Tutte le periferiche wireless si connettono al WAP.

Caratteristiche principali

La combinazione della funzionalità di routing tra VLAN fornita dal router Cisco RV con la funzione di isolamento SSID wireless fornita da un access point per piccole imprese offre una soluzione semplice e sicura per l'accesso wireless su qualsiasi rete aziendale Cisco esistente.

Routing inter-VLAN

I dispositivi di rete di VLAN diverse non possono comunicare tra loro senza un router per indirizzare il traffico tra le VLAN. In una rete aziendale di piccole dimensioni, il router esegue il routing tra VLAN sia per le reti cablate che per le reti wireless. Quando il routing tra VLAN è disabilitato per una VLAN specifica, gli host su quella VLAN non saranno in grado di comunicare con gli host o i dispositivi su un'altra VLAN.

Isolamento SSID wireless

Esistono due tipi di isolamento SSID wireless. Quando l'isolamento wireless (all'interno di SSID) è abilitato, gli host sullo stesso SSID non saranno in grado di vedersi. Quando l'isolamento wireless (tra SSID) è abilitato, il traffico su un SSID non viene inoltrato a nessun altro SSID.

IEEE 802.1x

Lo standard IEEE 802.1x specifica i metodi utilizzati per implementare il controllo degli accessi alle reti basate sulle porte che viene utilizzato per fornire l'accesso autenticato alle reti Ethernet. L'autenticazione basata sulla porta è un processo che consente solo gli scambi di credenziali di attraversare la rete fino a quando l'utente connesso alla porta non viene autenticato. La porta viene chiamata porta non controllata durante lo scambio delle credenziali. Al termine dell'autenticazione, la porta viene definita porta controllata. Si basa su due porte virtuali esistenti all'interno di una singola porta fisica.

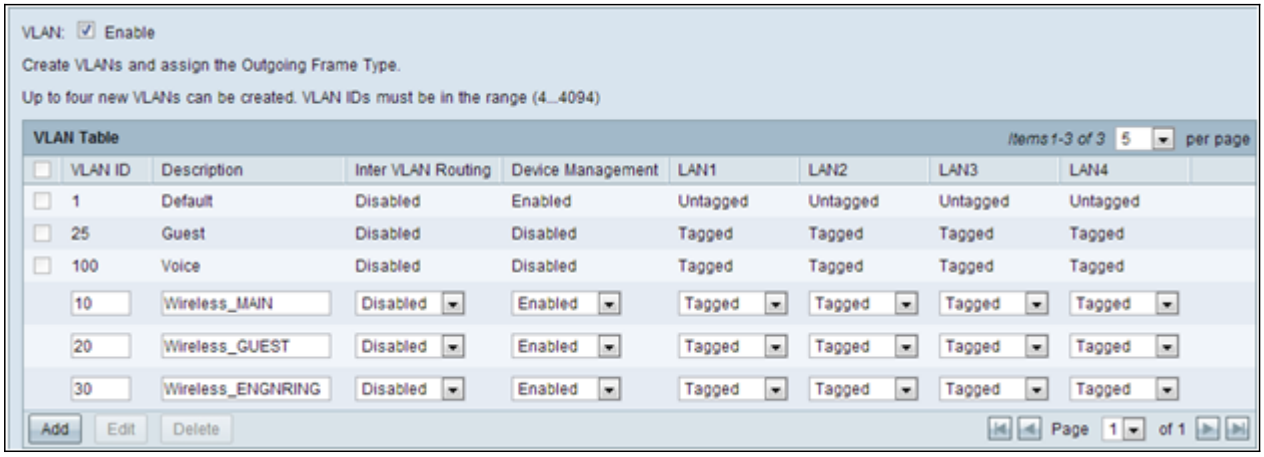
che utilizza le caratteristiche fisiche dell'infrastruttura LAN commutata per autenticare i dispositivi collegati a una porta LAN. L'accesso alla porta può essere negato se il processo

di autenticazione ha esito negativo. Questo standard è stato originariamente progettato per reti Ethernet cablate, ma è stato adattato per l'uso su LAN wireless 802.11.

Configurazione RV320

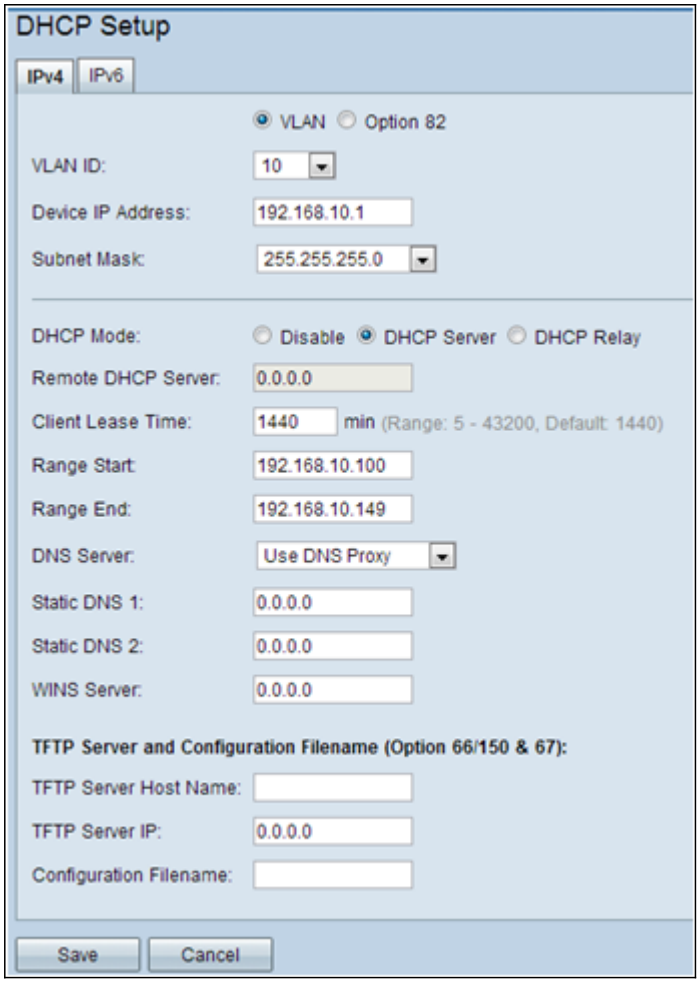
Poiché si desidera che l'RV320 funga da server DHCP per la rete, è necessario configurare anche la VLAN separata sul dispositivo. Per iniziare, accedere al router connettendosi a una delle porte Ethernet e andando alla versione 192.168.1.1 (supponendo di non aver già modificato l'indirizzo IP del router).

Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Port Management > VLAN Membership**. Viene visualizzata una nuova pagina. Stiamo creando 3 VLAN separate per rappresentare gruppi di destinatari diversi. Fare clic su **Add** per aggiungere una nuova linea e modificare l'ID VLAN e la descrizione. Inoltre, è necessario verificare che la VLAN sia impostata su *Tagged* sulle interfacce su cui devono viaggiare.



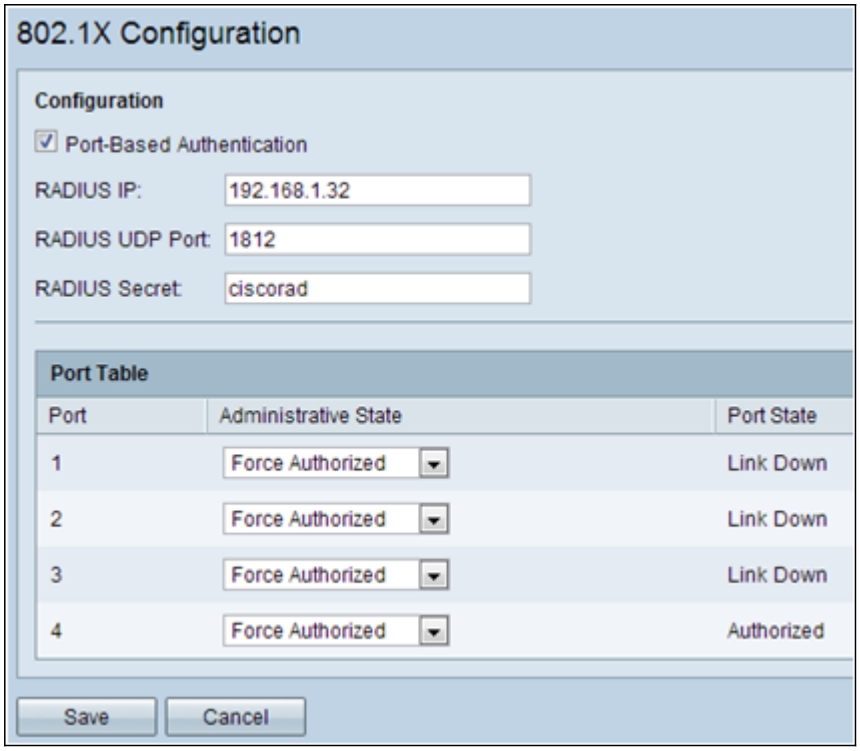
Passaggio 2. Accedere all'utility di configurazione Web e selezionare **DHCP Menu > DHCP Setup**. Viene visualizzata la pagina *DHCP Setup*:

- Nella casella di riepilogo ID VLAN, selezionare la VLAN per cui si sta configurando il pool di indirizzi (in questo esempio le VLAN 10, 20 e 30).
- Configurare l'indirizzo IP del dispositivo per la VLAN e impostare l'intervallo di indirizzi IP. Se lo si desidera, è inoltre possibile attivare o disattivare il proxy DNS, che dipenderà dalla rete. In questo esempio, il proxy DNS funzionerà per inoltrare le richieste DNS.
- Fare clic su **Save** (Salva), quindi ripetere l'operazione per ciascuna VLAN.



Passaggio 3. Nel riquadro di navigazione, selezionare **Port Management > 802.1x Configuration** (Gestione porte > Configurazione 802.1x). Viene visualizzata la pagina *Configurazione 802.1X*:

- Abilitare l'autenticazione basata sulla porta e configurare l'indirizzo IP del server.
- Segreto RADIUS è la chiave di autenticazione utilizzata per comunicare con il server.
- Scegliere le porte che utilizzeranno questa autenticazione e fare clic su **Salva**.

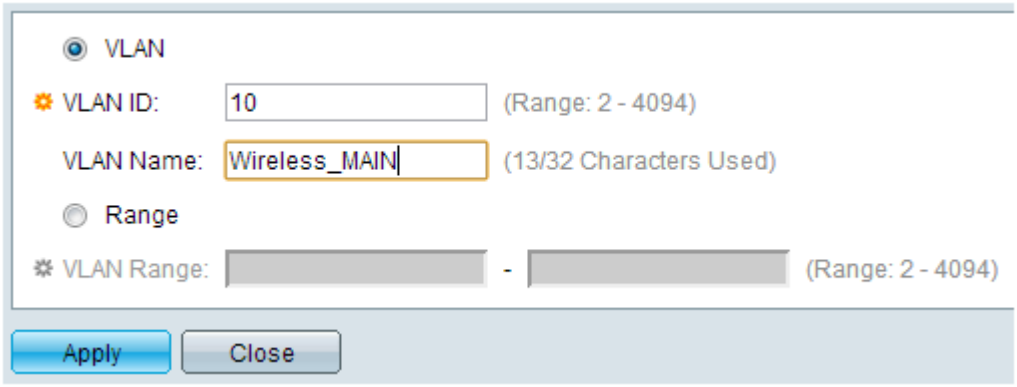


Configurazione Sx300

Lo switch SG300-10MP funziona da intermediario tra il router e il WAP321 per simulare un ambiente di rete realistico. La configurazione dello switch è la seguente.

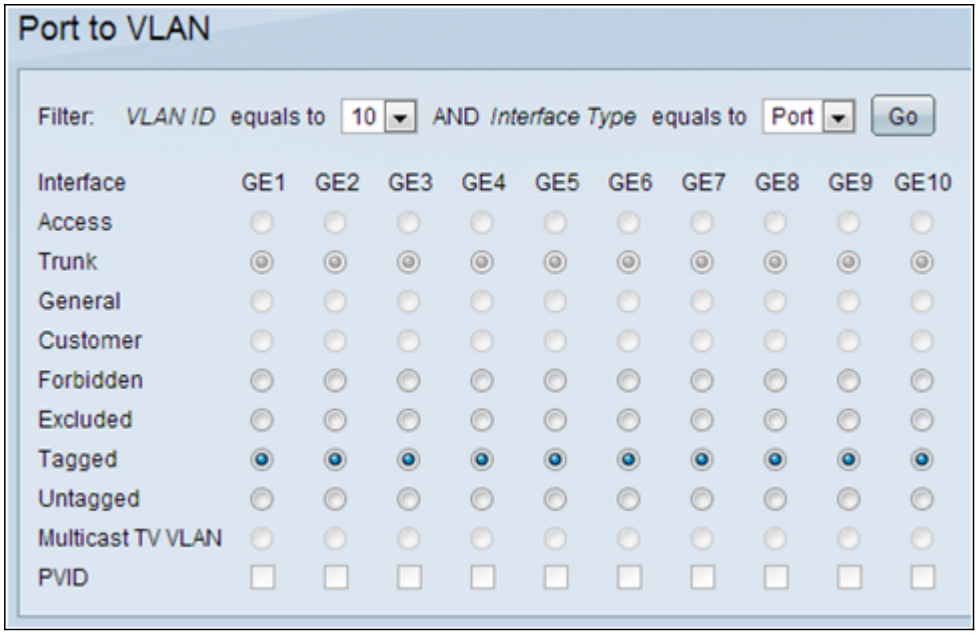
Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Gestione VLAN > Crea VLAN**. Viene visualizzata una nuova pagina:

Passaggio 2. Fare clic su **Add**. Viene visualizzata una nuova finestra. Immettere l'ID e il nome della VLAN (usare la stessa descrizione della sezione I). Fare clic su Apply (Applica), quindi ripetere l'operazione per le VLAN 20 e 30.



Passaggio 3. Nel riquadro di navigazione, selezionare **Gestione VLAN > Da porta a VLAN**. Viene visualizzata una nuova pagina:

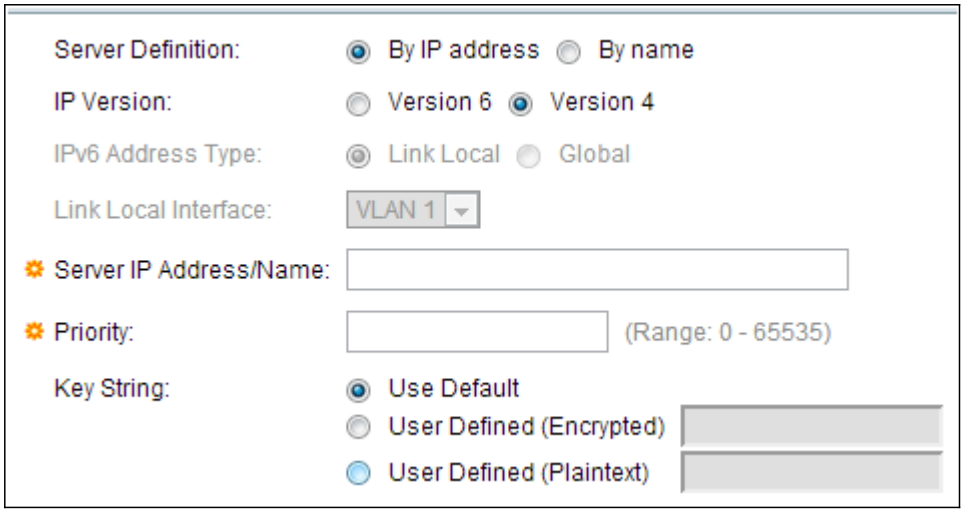
- Nella parte superiore della pagina, impostare "ID VLAN uguale a" sulla VLAN che si sta aggiungendo (in questo caso, VLAN 10), quindi fare clic su **Go** (Vai) a destra. La pagina verrà aggiornata con le impostazioni della VLAN.
- Modificare l'impostazione su ciascuna porta in modo che la VLAN 10 sia ora "Con tag" anziché "Esclusa". Ripetere questo passaggio per le VLAN 20 e 30.



Passaggio 4. Nel riquadro di navigazione, selezionare **Sicurezza > Raggio**. Viene visualizzata la pagina *RADIUS*:

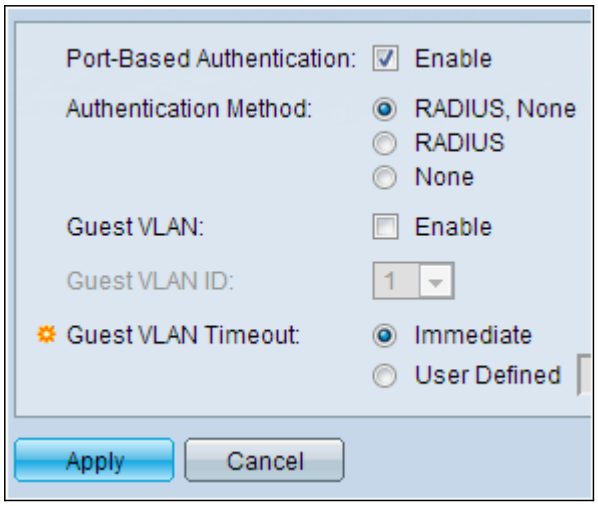
- Scegliere il metodo di controllo dell'accesso da utilizzare per il server RADIUS, ovvero il controllo dell'accesso di gestione o l'autenticazione basata sulla porta. Scegliere Controllo degli accessi basato sulla porta e fare clic su **Applica**.
- Fare clic su **Add** (Aggiungi) nella parte inferiore della pagina per aggiungere un nuovo server a cui eseguire l'autenticazione.

Passaggio 5. Nella finestra che viene visualizzata è necessario configurare l'indirizzo IP del server, in questo caso 192.168.1.32. Sarà necessario impostare una priorità per il server, ma poiché in questo esempio è disponibile un solo server per l'autenticazione in base alla priorità, ciò non ha alcuna importanza. Questa operazione è importante se si dispone di più server RADIUS tra cui scegliere. Configurare la chiave di autenticazione e le altre impostazioni possono essere lasciate come predefinite.

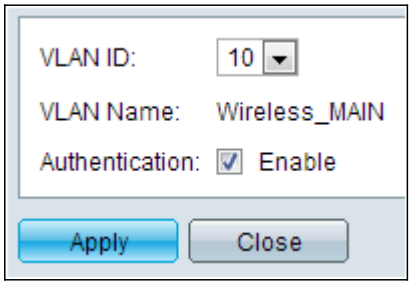


Passaggio 6. Nel riquadro di navigazione, selezionare **Sicurezza > 802.1X > Proprietà**. Viene visualizzata una nuova pagina:

- Selezionare **Abilita** per attivare l'autenticazione 802.1x e scegliere il metodo di autenticazione. In questo caso si utilizza un server RADIUS, quindi scegliere la prima o la seconda opzione.
- Fare clic su **Apply** (Applica).



Passaggio 7. Selezionare una delle VLAN e fare clic su **Edit** (Modifica). Viene visualizzata una nuova finestra. Selezionare **Enable** per consentire l'autenticazione sulla VLAN e fare clic su *Apply*. Ripetere l'operazione per ciascuna VLAN.



Configurazione WAP321

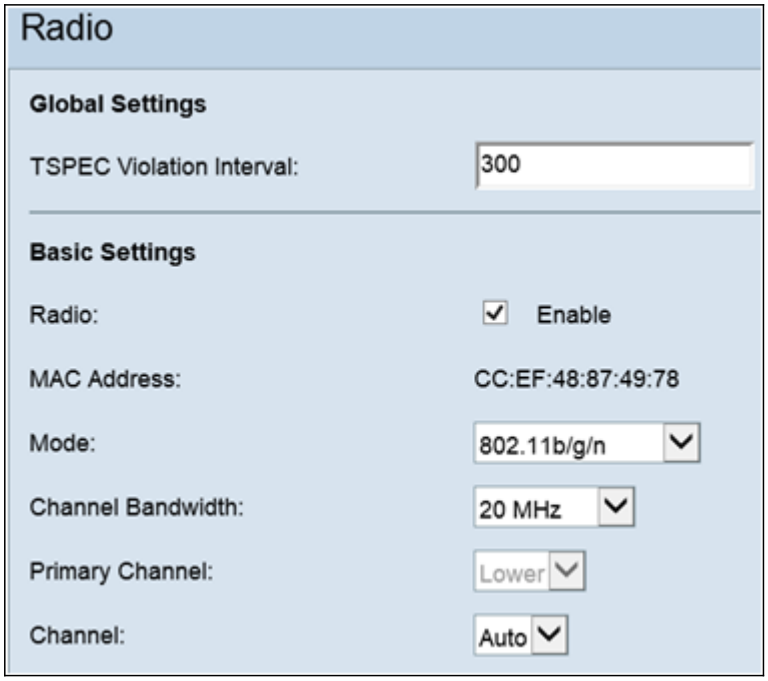
I punti di accesso virtuali (VAP) segmentano la LAN wireless in più domini di broadcast equivalenti wireless di VLAN Ethernet. I VAP simulano più punti di accesso in un unico dispositivo WAP fisico. Su WAP121 sono supportati fino a quattro VAP e su WAP321 ne sono supportati fino a otto.

Ogni VAP può essere abilitato o disabilitato in modo indipendente, ad eccezione di VAP0. VAP0 è l'interfaccia radio fisica e rimane abilitato finché la radio è abilitata. Per disattivare il funzionamento di VAP0, è necessario disattivare la radio stessa.

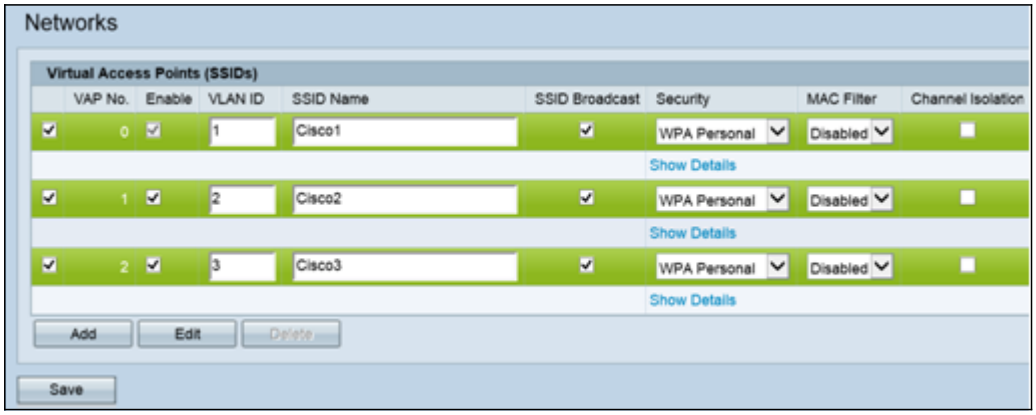
Ogni VAP è identificato da un SSID (Service Set Identifier) configurato dall'utente. Più VAP non possono avere lo stesso nome SSID. Le trasmissioni SSID possono essere abilitate o disabilitate in modo indipendente su ciascun VAP. La trasmissione SSID è attivata per impostazione predefinita.

Passaggio 1. Accedere all'utility di configurazione Web e selezionare **Wireless > Radio**. Viene visualizzata la pagina *Radio*:

- Selezionare la casella di controllo **Attiva** per attivare la radio wireless.
- Fare clic su **Salva**. La radio verrà accesa.



Passaggio 2. Nel pannello di navigazione, selezionare **Wireless > Reti**. Viene visualizzata la pagina *Rete*:



Nota: Il SSID predefinito per VAP0 è ciscosb. Ogni VAP aggiuntivo creato ha un nome SSID vuoto. Gli SSID di tutti i VAP possono essere configurati su altri valori.

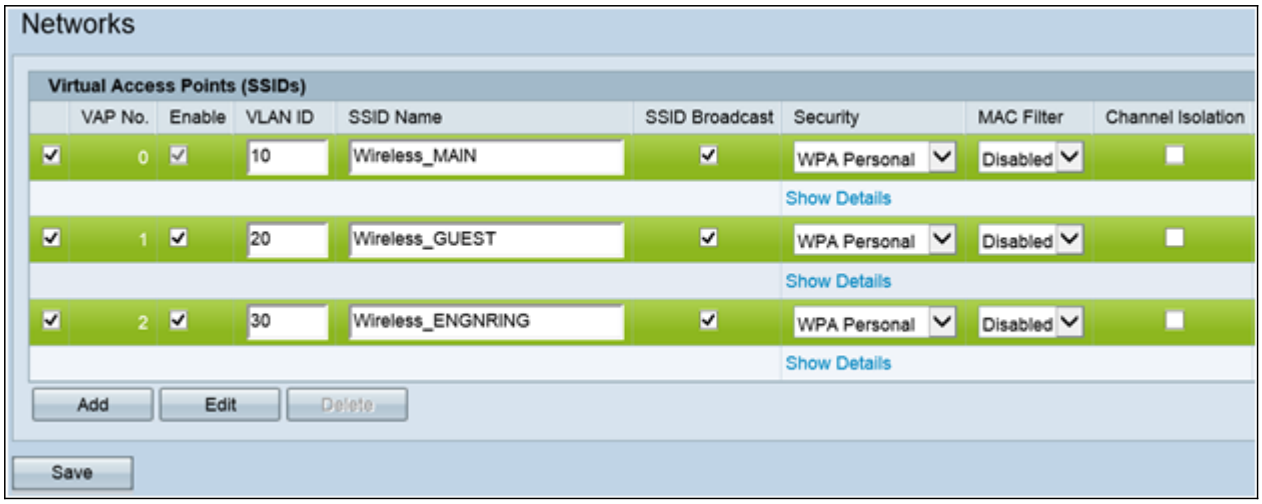
Passaggio 3. Ciascun VAP è associato a una VLAN, identificata da un ID VLAN (VID). Un VID può avere un valore compreso tra 1 e 4094 inclusi. Il protocollo WAP121 supporta cinque VLAN attive (quattro per la WLAN più una VLAN di gestione). La scheda WAP321

supporta nove VLAN attive (otto per WLAN più una VLAN di gestione).

Per impostazione predefinita, il VID assegnato all'utilità di configurazione per il dispositivo WAP è 1, che è anche il VID senza tag predefinito. Se il VID di gestione è lo stesso assegnato a un VAP, i client WLAN associati a questo VAP specifico possono amministrare il dispositivo WAP. Se necessario, è possibile creare un elenco di controllo di accesso (ACL) per disabilitare l'amministrazione dai client WLAN.

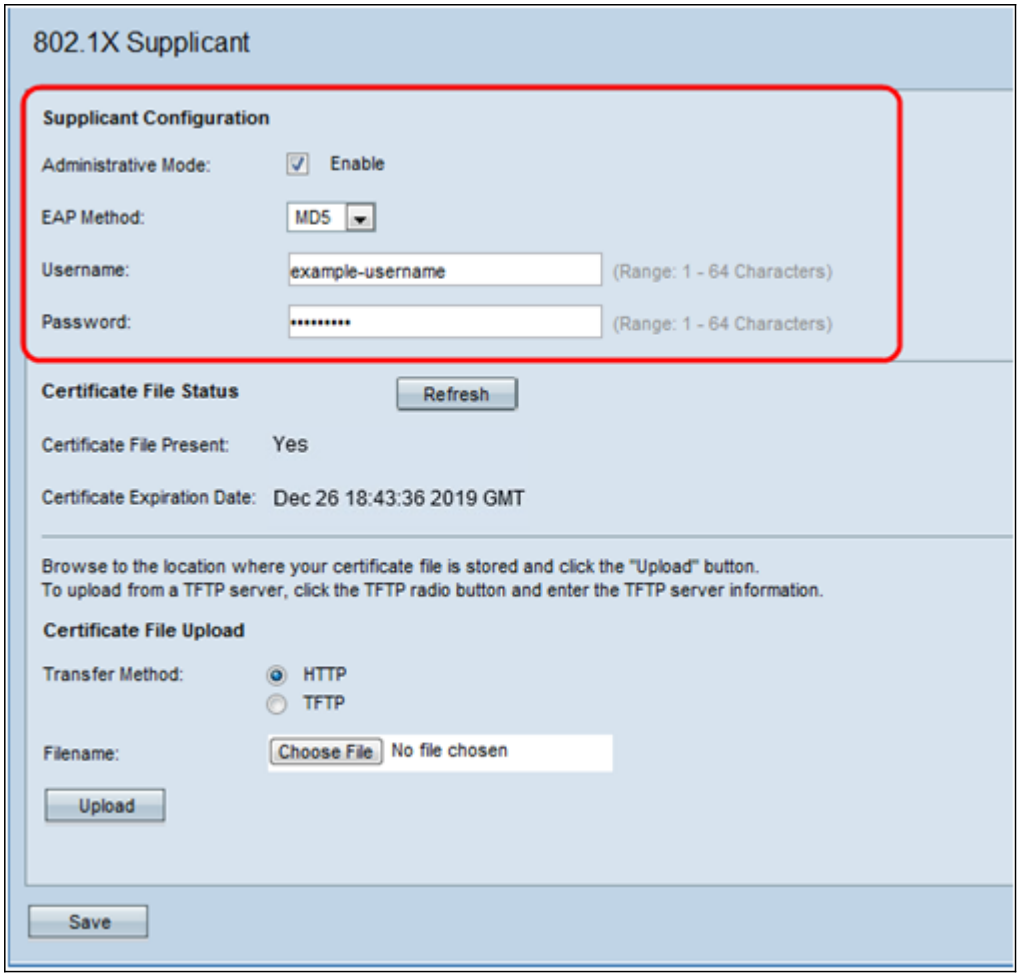
In questa schermata è necessario eseguire le seguenti operazioni:

- Fare clic sui pulsanti con il segno di spunta a sinistra per modificare gli SSID:
- Immettere il valore necessario per l'ID VLAN nella casella ID VLAN
- Fare clic sul pulsante **Save** (Salva) dopo aver immesso gli SSID.



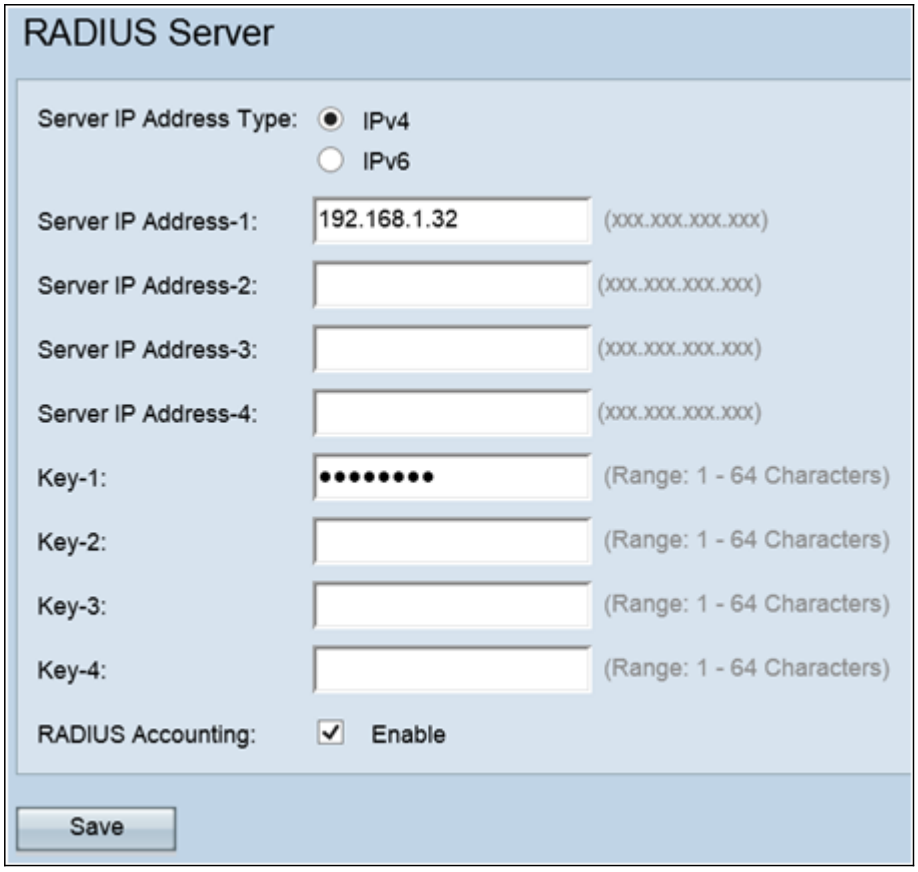
Passaggio 4. Nel pannello di navigazione, selezionare **System Security > 802.1X Supplicant** . Viene visualizzata la pagina *802.1X Supplicant*:

- Selezionare **Attiva** nel campo Modalità amministrativa per consentire al dispositivo di agire come supplicant nell'autenticazione 802.1X.
- Selezionare il tipo appropriato di metodo EAP (Extensible Authentication Protocol) dall'elenco a discesa nel campo Metodo EAP.
- Immettere il nome utente e la password utilizzati dal punto di accesso per ottenere l'autenticazione dall'autenticatore 802.1X nei campi Nome utente e Password. Il nome utente e la password devono avere una lunghezza compresa tra 1 e 64 caratteri alfanumerici e simboli. Questa impostazione deve essere già configurata nel server di autenticazione.
- Fare clic su **Salva** per salvare le impostazioni.



Nota: Nell'area Stato file certificato viene indicato se il file di certificato è presente o meno. Il certificato SSL è un certificato firmato digitalmente da un'autorità di certificazione che consente al browser di comunicare in modo sicuro con il server Web. Per gestire e configurare il certificato SSL, fare riferimento all'articolo Gestione certificati SSL (Secure Sockets Layer) sui punti di accesso WAP121 e WAP321

Passaggio 5. Nel riquadro di navigazione, selezionare **Sicurezza > Server RADIUS**. Viene visualizzata la pagina *Server RADIUS*. Immettere i parametri e fare clic sul pulsante **Salva** una volta immessi i parametri del server Radius.


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