GUIDA ALL'AMMINISTRAZIONE

Access point Wireless N WAP5511

e

Access point a banda selezionabile WAP561 con PoE

di Cisco Small Business

Sommario

1

Introduzione

In questo capitolo viene fornita un'introduzione all'utilità di configurazione basata sul Web per access point wireless (WAP, Wireless Access Point) e sono inclusi i seguenti argomenti:

Avvio dell'utilità di configurazione basata sul Web

In questa sezione vengono descritti i requisiti di sistema e come esplorare l'utilità di configurazione basata sul Web.

Browser supportati

- Internet Explorer 7.0 o versioni successive
- Chrome 5.0 o versioni successive
- Firefox 3.0 o versioni successive
- Safari 3.0 o versioni successive

Limitazioni del browser

- Se si utilizza Internet Explorer 6, non è possibile utilizzare direttamente un indirizzo IPv6 per accedere al dispositivo WAP. Tuttavia, è possibile utilizzare il server DNS (Domain Name System) per creare un nome di dominio che contenga l'indirizzo IPv6 e poi utilizzarlo nella barra degli indirizzi al posto dell'indirizzo IPv6.

- Se si utilizza Internet Explorer 8, è possibile configurare le impostazioni di sicurezza in Internet Explorer. Fare clic su **Strumenti > Opzioni Internet**, quindi selezionare la scheda **Sicurezza**. Selezionare **Intranet locale**, quindi **Siti**. Fare clic su **Avanzate**, quindi su **Aggiungi**. Aggiungere l'indirizzo intranet del dispositivo WAP (http://*<indirizzo IP>*) per la zona intranet locale. È possibile specificare l'indirizzo IP anche come indirizzo IP di sottorete, in modo da aggiungere tutti gli indirizzi della sottorete alla zona intranet locale.
- Se nella stazione di gestione sono presenti più interfacce IPv6, utilizzare l'indirizzo globale IPv6, invece di quello locale, per accedere al dispositivo WAP dal browser.

L'utilità di configurazione dell'access point basata sul Web si disconnette per impostazione predefinita dopo 10 minuti di inattività. Per istruzioni sulla modifica del periodo di timeout predefinito, vedere **Servizio HTTP/HTTPS**.

Per disconnettersi, fare clic su **Logout** nell'angolo superiore destro dell'utilità di configurazione dell'access point basata sul Web.

Utilizzo di Access Point Setup Wizard

Quando si accede al dispositivo WAP per la prima volta o dopo aver ripristinato le impostazioni predefinite, viene visualizzato l'Access Point Setup Wizard per agevolare le configurazioni iniziali. Attenersi ai seguenti passaggi per completare la procedura guidata:

NOTA Se si fa clic su **Annulla** per bypassare la procedura guidata, viene visualizzata la finestra di modifica della password. A questo punto, è possibile modificare la password predefinita per l'accesso. Per tutte le altre impostazioni, vengono applicate le configurazioni predefinite.

Dopo aver modificato la password, è necessario ripetere l'accesso.

PASSAGGIO 1 Nella finestra di benvenuto della procedura guidata, fare clic su **Avanti**. Viene visualizzata la finestra Configure Device - IP Address.

PASSAGGIO 2 Fare clic su **Dynamic IP Address (DHCP)** se si desidera che un server DHCP assegni un indirizzo IP al dispositivo WAP. In alternativa, selezionare **Static IP Address** per configurare l'indirizzo IP manualmente. Per la descrizione di questi campi, vedere **Impostazioni dell'indirizzo IPv4 e della VLAN**.

PASSAGGIO 3 Fare clic su **Avanti**. Viene visualizzata la finestra Single Point Setup - Set a Cluster. Per la descrizione del punto di installazione singolo, vedere **Punto di installazione singolo**.

PASSAGGIO 4 Per creare un nuovo punto di installazione singolo dei dispositivi WAP, selezionare **Create a New Cluster** e immettere un nome nel campo **New Cluster Name**. Se i dispositivi vengono configurati con lo stesso nome cluster e viene attivata la modalità Punto di installazione singolo su altri dispositivi WAP, i dispositivi entrano automaticamente a far parte del gruppo.

Per aggiungere il dispositivo a un cluster già presente nella rete, fare clic su **Join an Existing Cluster** e immettere il nome del cluster nel campo **Existing Cluster Name**.

Se non si desidera aggiungere il dispositivo al punto di installazione singolo in questo momento, fare clic su **Do not Enable Single Point Setup**.

(Facoltativo) È possibile immettere del testo nel campo AP Location per annotare la posizione fisica del dispositivo WAP.

PASSAGGIO 5 Fare clic su **Avanti**. Viene visualizzata la finestra Configure Device - Set System Date and Time.

PASSAGGIO 6 Selezionare il fuso orario appropriato, quindi impostare l'ora di sistema manualmente o configurare il dispositivo WAP in modo da ottenere l'ora da un server NTP. Per la descrizione di queste opzioni, vedere **Impostazioni relative all'ora**.

PASSAGGIO 7 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Security - Set Password.

PASSAGGIO 8 Immettere una password nella casella di testo **New Password**, quindi immetterla nuovamente nella casella di testo **Confirm Password**. Per ulteriori informazioni sulle password, vedere **Account utente**.

> **NOTA** Se si desidera disattivare le regole di protezione della password, è possibile deselezionare la casella Password Complexity. Tuttavia, si consiglia vivamente di mantenerle attive.

PASSAGGIO 9 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Security - Name Your Wireless Network per l'interfaccia Radio 1.

> **NOTA** In questa finestra e nella due successive (Wireless Security e VLAN ID) vengono configurate le impostazioni per l'interfaccia Radio 1. Successivamente, per i dispositivi WAP561, le finestre verranno visualizzate di nuovo per configurare le impostazioni per l'interfaccia Radio 2.

PASSAGGIO 10 Immettere un nome di rete nel campo **Network Name**. Questo nome verrà utilizzato come SSID per la rete wireless predefinita.

PASSAGGIO 11 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Security - Secure Your Wireless Network.

PASSAGGIO 12 Scegliere un tipo di crittografia di sicurezza e immettere una chiave di protezione. Per la descrizione di queste opzioni, vedere **Sicurezza del sistema**.

PASSAGGIO 13 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Security - Assign the VLAN ID For Your Wireless Network.

PASSAGGIO 14 Immettere un ID VLAN per il traffico ricevuto sulla rete wireless.

Si consiglia di assegnare al traffico wireless un ID VLAN diverso da quello predefinito (1), in modo da separarlo dal traffico di gestione sulla VLAN 1.

PASSAGGIO 15 Fare clic su **Avanti**.

PASSAGGIO 16 Per il dispositivo WAP561, nelle finestre Network Name, Wireless Security e VLAN ID è possibile configurare l'interfaccia Radio 2. Al termine della configurazione, fare clic su **Avanti**.

Viene visualizzata la finestra Enable Captive Portal - Create Your Guest Network.

PASSAGGIO 17 Scegliere se configurare un metodo di autenticazione per gli ospiti sulla rete, quindi fare clic su **Avanti**.

Se si fa clic su **No**, passare al **PASSAGGIO 25**.

Se si fa clic su **Sì**, viene visualizzata la finestra Enable Captive Portal - Name Your Guest Network.

PASSAGGIO 18 Immettere un nome nel campo **Guest Network Name** per l'interfaccia Radio 1. Per il dispositivo WAP561, selezionare se la rete ospite utilizza **Radio 1** o **Radio 2**.

PASSAGGIO 19 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Captive Portal - Secure Your Guest Network.

PASSAGGIO 20 Scegliere un tipo di crittografia di sicurezza per la rete ospite e immettere una chiave di protezione. Per la descrizione di queste opzioni, vedere **Sicurezza del sistema**.

PASSAGGIO 21 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Captive Portal - Assign the VLAN ID.

PASSAGGIO 22 Specificare un ID VLAN per la rete ospite. L'ID VLAN della rete ospite deve essere diverso dall'ID VLAN di gestione.

PASSAGGIO 23 Fare clic su **Avanti**. Viene visualizzata la finestra Enable Captive Portal - Enable Redirect URL.

PASSAGGIO 24 Selezionare **Enable Redirect URL** e specificare l'indirizzo IP o un nome di dominio completo nel campo Redirect URL (incluso http://). Se specificato, dopo l'autenticazione gli utenti della rete ospite vengono reindirizzati all'URL immesso.

PASSAGGIO 25 Fare clic su **Avanti**. Viene visualizzata la finestra Summary - Confirm Your Settings.

PASSAGGIO 26 Rivedere le impostazioni configurate. Fare clic su **Indietro** per riconfigurare una o più impostazioni. Se si fa clic su **Annulla**, vengono ripristinati tutti i valori precedenti o predefiniti delle impostazioni.

PASSAGGIO 27 Se le impostazioni sono corrette, fare clic su **Submit**. Le impostazioni di configurazione WAP vengono salvate e viene visualizzata una finestra di conferma.

PASSAGGIO 28 Fare clic su **Fine**. Viene visualizzata la finestra Getting Started.

Introduzione

Per semplificare la configurazione del dispositivo con una rapida navigazione, la finestra Getting Started fornisce i collegamenti per eseguire le attività comuni. Questa finestra viene visualizzata per impostazione predefinita ogni volta che si accede all'utilità di configurazione dell'access point basata sul Web.

Collegamenti della finestra Getting Started

Categoria	Nome collegamento (nella pagina)	Pagina collegata
Installazione iniziale	Run Setup Wizard	Utilizzo di Access Point Setup Wizard
	Configure Radio Settings	Radio
	Configure Wireless Network Settings	Reti
	Configure LAN Settings	LAN
	Run WPS	Configurazione WPS
	Configure Single Point Setup	Punto di installazione singolo
Stato dispositivo	System Summary	Riepilogo di sistema
	Wireless Status	Interfacce di rete

Collegamenti della finestra Getting Started (Continua)

Categoria	Nome collegamento (nella pagina)	Pagina collegata
Accesso rapido	Change Account Password	**Account utente**
	Upgrade Device Firmware	**Firmware di gestione**
	Backup/Restore Configuration	**Download/backup del file di configurazione**

Esplorazione delle finestre

In questa sezione vengono descritte le funzioni dell'utilità di configurazione dell'access point basata sul Web.

L'intestazione dell'utilità di configurazione contiene informazioni standard e viene visualizzata nella parte superiore di ogni finestra. Nell'intestazione sono presenti i seguenti pulsanti:

Pulsanti

Nome pulsante	Descrizione
(Utente)	Il nome account (Administrator o Guest) dell'utente che ha eseguito l'accesso al dispositivo WAP. Il nome utente predefinito è **cisco**.
Log Out	Fare clic per disconnettersi dall'utilità di configurazione dell'access point basata sul Web.
About	Fare clic per visualizzare il tipo di dispositivo WAP e il numero della versione.
Help	Fare clic per visualizzare la guida in linea. La guida in linea è stata concepita per essere visualizzata tramite i browser che utilizzano la codifica UTF-8. Se nella guida in linea vengono visualizzati caratteri errati, verificare che la codifica del browser sia impostata su UTF-8.

Sul lato sinistro di ogni pagina è presente un riquadro di spostamento o menu principale. Il riquadro di spostamento contiene un elenco delle principali funzioni dei dispositivi WAP. Se un elemento del menu principale è preceduto da una freccia, selezionarla per espandere l'elemento e visualizzare il relativo sottomenu. A questo punto, è possibile selezionare l'elemento desiderato nel sottomenu per visualizzare la relativa finestra.

Nella tabella di seguito vengono descritti i pulsanti più utilizzati visualizzati nelle diverse pagine del sistema.

Pulsanti di gestione

Nome pulsante	Descrizione
Aggiungi	Consente di aggiungere una nuova voce alla tabella o al database.
Annulla	Consente di annullare le modifiche apportate alla pagina.
Cancella tutto	Consente di cancellare tutte le voci della tabella dei log.
Elimina	Consente di eliminare una voce dalla tabella. Per poter utilizzare questo pulsante, è necessario selezionare prima una voce.
Modifica	Consente di modificare una voce esistente. Per poter utilizzare questo pulsante, è necessario selezionare prima una voce.
Refresh (Aggiorna)	Consente di visualizzare di nuovo la pagina corrente con i dati più recenti.
Salva	Consente di salvare le impostazioni o la configurazione.
Update (Aggiorna)	Consente di aggiornare le nuove informazioni nella configurazione di avvio.

2

Stato e statistiche

In questo capitolo viene descritto come visualizzare lo stato e le statistiche e vengono trattati i seguenti argomenti:

- **Riepilogo di sistema**
- **Interfacce di rete**
- **Statistiche relative al traffico**
- **Trasmissione/ricezione di WorkGroup Bridge**
- **Client associati**
- **Associazioni di client TSPEC**
- **Stato e statistiche TSPEC**
- **Statistiche AP TSPEC**
- **Statistiche radio**
- **Stato relativo agli avvisi tramite e-mail**
- **Log**

Riepilogo di sistema

Nella pagina System Summary vengono visualizzate le informazioni di base come la descrizione del modello hardware, la versione del software e il tempo trascorso dall'ultimo riavvio.

Per visualizzare le informazioni di sistema, selezionare **Status and Statistics** > **System Summary** nel riquadro di spostamento. In alternativa, selezionare **System Summary** sotto **Device Status** nella pagina Getting Started.

Nella pagina System Summary vengono visualizzate le informazioni seguenti:

- **PID VID**: il modello hardware e la versione del dispositivo WAP.
- **Serial Number**: il numero di serie del dispositivo WAP Cisco.
- **Base MAC Address**: l'indirizzo MAC del dispositivo WAP.
- **Firmware Version (Active Image)**: il numero di versione del firmware dell'immagine attiva.
- **Firmware MD5 Checksum (Active Image)**: il checksum dell'immagine attiva.
- **Firmware Version (Non-active)**: il numero di versione del firmware dell'immagine di backup.
- **Firmware MD5 Checksum (Non-active)**: il checksum dell'immagine di backup.
- **Host Name**: un nome assegnato al dispositivo.
- **System Uptime**: il tempo trascorso dall'ultimo riavvio.
- **System Time**: l'ora di sistema corrente.
-

Nella tabella TCP/UDP Service vengono mostrate le informazioni di base relative ai protocolli e ai servizi operativi sul dispositivo WAP.

- **Service**: il nome del servizio, se disponibile.
- **Protocol**: il protocollo di trasporto sottostante utilizzato dal servizio (TCP o UDP).
- **Local IP Address**: l'indirizzo IP, se presente, di un dispositivo remoto connesso al servizio sul dispositivo WAP. **All** indica che qualsiasi indirizzo IP sul dispositivo può utilizzare questo servizio.
- **Local Port**: il numero di porta del servizio.
- **Remote IP Address**: l'indirizzo IP di un host remoto, se presente, che sta utilizzando il servizio. **All** indica che il servizio è disponibile per tutti gli host remoti che accedono al sistema.
- **Remote Port**: il numero di porta di qualsiasi dispositivo remoto che comunica con il servizio.

- **Connection State**: lo stato del servizio. Per UDP, nella tabella vengono visualizzate solo le connessioni con stato Active o Established. Gli stati TCP sono i seguenti:
  - **Listening**: il servizio è in ascolto delle richieste di connessione.
  - **Attivo**: è attiva una sessione di connessione con trasmissione e ricezione di pacchetti.
  - **Established**: è attiva una sessione di connessione tra il dispositivo WAP e un server o un client, a seconda del ruolo di ciascun dispositivo in relazione al protocollo.
  - **Time Wait**: la sequenza di chiusura è stata avviata e il WAP attende che sia trascorso l'intervallo di timeout definito dal sistema, in genere 60 secondi, prima di terminare la connessione.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Interfacce di rete

Utilizzare la pagina Network Interfaces per visualizzare le informazioni di configurazione e stato relative alle interfacce cablate e wireless. Per visualizzare questa pagina, selezionare **Status and Statistics** > **Network Interface** nel riquadro di spostamento.

Nella pagina Network Interfaces vengono visualizzate le informazioni seguenti:

- **LAN Status**: queste impostazioni si applicano all'interfaccia interna.

  Per modificare un'impostazione, fare clic sul collegamento **Edit**. Viene visualizzata la pagina VLAN and IPv4 Address Settings. Per le descrizioni di questi campi, vedere **Impostazioni dell'indirizzo IPv4 e della VLAN**.

- **Radio Status**: queste impostazioni includono la modalità radio wireless (Enabled o Disabled), l'indirizzo MAC associato all'interfaccia radio (o entrambe le interfacce radio per i dispositivi WAP561), la modalità 802.11 (a/b/g/n) e il canale utilizzato dall'interfaccia.

  Per modificare le impostazioni wireless, fare clic sul collegamento **Edit**. Viene visualizzata la pagina Radio. Per le descrizioni di questi campi, vedere **Radio**.

- **Interface Status**: in questa tabella vengono elencate le informazioni di stato per ciascun VAP (Virtual Access Point) e ciascuna interfaccia WDS (Wireless Distribution System). Sui dispositivi WAP561, l'ID dell'interfaccia VAP è preceduto da WLAN0 o WLAN1 per indicare l'interfaccia radio associata. WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.

  Se il VAP è stato configurato, nella tabella vengono indicati il nome SSID, lo stato amministrativo (up o down), l'indirizzo MAC dell'interfaccia radio, l'ID VLAN, il nome di ogni profilo scheduler associato e lo stato attuale (attivo o inattivo). Lo stato indica se il VAP sta scambiando dati con un client.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Statistiche relative al traffico

Utilizzare la pagina Traffic Statistics per visualizzare le informazioni di base sul WAP. In questa pagina viene fornita anche una visualizzazione in tempo reale delle statistiche di trasmissione e ricezione per l'interfaccia Ethernet, i VAP (Virtual Access Points) ed eventuali interfacce WDS. Per tutte le statistiche di trasmissione e ricezione viene mostrato il totale dall'ultimo avvio del WAP. Se si riavvia il WAP, questi dati indicheranno i totali di trasmissione e ricezione dal riavvio.

Per visualizzare la pagina Traffic Statistics, selezionare **Status and Statistics** > **Traffic Statistics** nel riquadro di spostamento.

Nella pagina Traffic Statistics vengono mostrati i dati di riepilogo e le statistiche relative al traffico in ogni direzione.

- **Network Interface**: il nome dell'interfaccia Ethernet e di ciascuna interfaccia VAP e WDS.

  Nei dispositivi WAP561, il nome dell'interfaccia VAP è preceduto da WLAN0 e WLAN1 per indicare l'interfaccia radio. WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.

- **Total Packets**: i pacchetti totali inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP.

- **Total Bytes**: i byte totali inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP.

- **Total Dropped Packets**: il numero totale di pacchetti persi inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP.
- **Total Dropped Bytes**: il numero totale di byte persi inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP.
- **Errors**: il numero totale di errori relativi ai dati di trasmissione e ricezione sul dispositivo WAP.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Trasmissione/ricezione di WorkGroup Bridge

Nella pagina WorkGroup Bridge Transmit/Receive viene mostrata la quantità di pacchetti e byte per il traffico tra stazioni su un WorkGroup Bridge. Per ulteriori informazioni sulla configurazione di WorkGroup Bridge, vedere la sezione **WorkGroup Bridge**.

Per visualizzare la pagina WorkGroup Bridge Transmit/Receive, selezionare **Status and Statistics**> **WorkGroup Bridge** nel riquadro di spostamento.

Per ogni interfaccia di rete configurata come interfaccia WorkGroup Bridge vengono mostrati questi campi:

- **Network Interface**: nome dell'interfaccia Ethernet o VAP. Sui dispositivi WAP561, WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.
- **Status and Statistics**: mostra se l'interfaccia è disconnessa oppure se è configurata dall'amministratore come attiva o inattiva.
- **VLAN ID**: ID della VLAN (Virtual LAN). È possibile utilizzare le VLAN per creare più reti interne e ospiti sullo stesso dispositivo WAP. L'ID VLAN viene impostato nella scheda VAP.
- **Name (SSID)**: nome della rete wireless. Nota anche come SSID, questa chiave alfanumerica identifica in maniera univoca una rete locale wireless. Il nome SSID viene impostato nella scheda VAP.

Vengono visualizzate ulteriori informazioni per la direzione di trasmissione e ricezione per ciascuna interfaccia WorkGroup Bridge:

- **Total Packets**: il numero totale di pacchetti connessi mediante bridge tra i client cablati nell'interfaccia WorkGroup Bridge e la rete wireless.
- **Total Bytes**: il numero totale di byte connessi mediante bridge tra i client cablati nell'interfaccia WorkGroup Bridge e la rete wireless.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Client associati

È possibile utilizzare la pagina Associated Clients per visualizzare le stazioni client associate a un particolare access point.

Per visualizzare la pagina Associated Clients , selezionare **Status and Statistics** > **Associated Clients** nel riquadro di spostamento.

Le stazioni associate vengono visualizzate insieme alle informazioni relative al traffico di pacchetti trasmessi e ricevuti per ogni stazione.

- **Total Number of Associated Clients**: il numero totale di client associati al dispositivo WAP.
- **Network Interface**: il VAP associato al client. Nei dispositivi WAP561, il nome dell'interfaccia VAP è preceduto da WLAN0 e WLAN1 per indicare l'interfaccia radio. WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.
- **Station**: l'indirizzo MAC del client wireless associato.
- **Status**: lo stato Authenticated and Associated mostra lo stato di autenticazione e associazione IEEE 802.11 sottostante, che è presente indipendentemente dal tipo di sicurezza utilizzata dal client per collegarsi al dispositivo WAP. In questo campo non viene mostrato lo stato di autenticazione e associazione IEEE 802.1X.

  Di seguito vengono riportate alcune considerazioni relative a questo campo:

  - Se la modalità di protezione del dispositivo WAP è None oppure Static WEP, lo stato di autenticazione e associazione dei client viene visualizzato come previsto; ciò significa che se un client viene visualizzato come autenticato per un dispositivo WAP, è in grado di

trasmettere e ricevere dati. Questo dipende dal fatto che la modalità di protezione Static WEP utilizza soltanto l'autenticazione IEEE 802.11.

- Se il dispositivo WAP utilizza la protezione IEEE 802.1X o WPA, è possibile che un'associazione client venga visualizzata come autenticata (mediante la protezione IEEE 802.11), anche se non è effettivamente autenticata attraverso il secondo livello di sicurezza.

- **From Station/To Station**: i contatori del campo From Station indicano i pacchetti o i byte ricevuti dal client wireless. Quelli del campo To Station indicano il numero di pacchetti e byte trasmessi dal dispositivo WAP al client wireless.
  - **Packets**: numero di pacchetti ricevuti o trasmessi dal client wireless.
  - **Bytes**: numero di byte ricevuti o trasmessi dal client wireless.
  - **Drop Packets**: numero di pacchetti eliminati dopo essere stati ricevuti o trasmessi.
  - **Drop Bytes**: numero di byte persi dopo essere stati ricevuti o trasmessi.
  - **TS Violate Packets (From Station)**: numero di pacchetti inviati da un client STA al dispositivo WAP oltre il limite di larghezza di banda uplink attiva per il flusso di traffico (TS, Traffic Stream) oppure per una categoria di accesso che richiede un controllo di ammissione al quale il client STA non è stato ammesso.
  - **TS Violate Packets (To Station)**: numero di pacchetti inviati dal dispositivo WAP a un client STA oltre il limite di larghezza di banda downlink attiva per il flusso di traffico (TS, Traffic Stream) oppure per una categoria di accesso che richiede un controllo di ammissione al quale il client STA non è stato ammesso.
- **Up Time**: l'intervallo di tempo in cui il client è stato associato al dispositivo WAP.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Associazioni di client TSPEC

Nella pagina TSPEC Client Associations vengono fornite informazioni in tempo reale sui dati dei client TSPEC trasmessi e ricevuti dall'access point. Nelle tabelle di questa pagina vengono mostrati i pacchetti vocali e video trasmessi e ricevuti dall'inizio dell'associazione, insieme alle informazioni di stato.

Una TSPEC è una specifica del traffico inviata da un client wireless con funzionalità QoS a un dispositivo WAP che richiede una specifica quantità di risorse di rete per il flusso di traffico che rappresenta. Un flusso di traffico è una raccolta di pacchetti di dati identificati dal client wireless come elementi appartenenti a una particolare priorità utente. Un esempio di flusso di traffico vocale è un telefono Wi-Fi CERTIFIED che contrassegna i pacchetti di dati generati dal codec come traffico a priorità vocale. Un esempio di flusso di traffico video è un'applicazione che riproduce video su un computer portatile wireless dando priorità al feed di una videoconferenza ricevuta da un server aziendale.

Per visualizzare le statistiche sull'associazione di client TSPEC, selezionare **Status and Statistics > TSPEC Client Associations** nel riquadro di spostamento.

Nella pagina TSPEC Client Associations vengono visualizzate le informazioni seguenti:

Stato e statistiche:

- **Network Interface**: l'interfaccia radio utilizzata dal client. Sui dispositivi WAP561, WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.
- **SSID**: il nome SSID associato al client TS.
- **Station**: l'indirizzo MAC della stazione client.
- **TS Identifier**: l'identificatore della sessione di traffico TSPEC; i valori possibili sono compresi nell'intervallo da 0 a 7.
- **Access Category**: la categoria di accesso TS (voce o video).
- **Direction**: la direzione del traffico del TS. È possibile scegliere una delle direzioni seguenti:
  - uplink: dal client al dispositivo;
  - downlink: dal dispositivo al client;
  - bidirectional.

- **User Priority** (UP): priorità utente per il TS. Il valore UP viene inviato con ogni pacchetto nella rispettiva porzione dell'intestazione IP. I valori tipici sono i seguenti:
  - 6 o 7 per la voce;
  - 4 o 5 per il video.

  Il valore può essere diverso in base alle altre sessioni di traffico con priorità.
- **Medium Time**: tempo in cui il traffico TS occupa il supporto di trasmissione.
- **Excess Usage Events**: numero di volte in cui il client ha superato il tempo del supporto stabilito per la sua TSPEC. Violazioni minori e meno frequenti vengono ignorate.
- **VAP MAC Address**: l'indirizzo MAC dell'access point virtuale.

Statistiche:

- **Network Interface**: l'interfaccia radio utilizzata dal client.
- **Station**: l'indirizzo MAC della stazione client.
- **TS Identifier**: l'identificatore della sessione di traffico TSPEC; i valori possibili sono compresi nell'intervallo da 0 a 7.
- **Access Category**: la categoria di accesso TS (voce o video).
- **Direction**: la direzione del traffico del TS. È possibile scegliere una delle direzioni seguenti:
  - uplink: dal client al dispositivo;
  - downlink: dal dispositivo al client;
  - bidirectional.
- **From Station**: mostra il numero di pacchetti e byte ricevuti dal client wireless e il numero di pacchetti e byte eliminati dopo essere stati ricevuti.
  - **Packets**: il numero di pacchetti in eccesso per una TSPEC consentita.
  - **Bytes**: il numero di byte quando non è stata stabilita alcuna TSPEC ed è richiesta l'ammissione da parte del dispositivo WAP.
- **To Station**: il numero di pacchetti e byte trasmessi dal dispositivo WAP al client wireless e il numero di pacchetti e byte eliminati durante la trasmissione.
  - **Packets**: il numero di pacchetti in eccesso per una TSPEC consentita.

- **Bytes**: il numero di byte per i quali non è stata stabilita alcuna TSPEC quando è richiesta l'ammissione da parte del dispositivo WAP.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Stato e statistiche TSPEC

Nella pagina TSPEC Status and Statistics vengono mostrate le seguenti informazioni:

- Informazioni di riepilogo sulle sessioni TSPEC via radio.
- Informazioni di riepilogo sulle sessioni TSPEC via VAP.
- Statistiche di trasmissione e ricezione in tempo reale per l'interfaccia radio e le interfacce di rete.

Tutte le statistiche di trasmissione e ricezione mostrate rappresentano il totale dall'ultimo avvio del dispositivo WAP. Se si riavvia il dispositivo WAP, questi dati indicheranno i totali di trasmissione e ricezione dal riavvio.

Per visualizzare lo stato e le statistiche TSPEC, selezionare **Status and Statistics > TSPEC Status and Statistics** nel riquadro di spostamento.

Nella pagina TSPEC Status and Statistics vengono mostrate le seguenti informazioni di stato per le interfacce WLAN (radio) e VAP:

- **Network Interface**: il nome dell'interfaccia Radio o VAP. Sui dispositivi WAP561, WLAN0 rappresenta l'interfaccia radio 1, mentre WLAN1 rappresenta l'interfaccia radio 2.
- **Access Category**: la categoria di accesso attuale associata al flusso di traffico (voce o video).
- **Status**: se la sessione TSPEC è attivata (up) o disattivata (down) per la categoria di accesso corrispondente.

  NOTA Lo stato si riferisce allo stato della configurazione e non rappresenta necessariamente l'attività della sessione corrente.
- **Active Traffic Stream**: il numero di flussi di traffico TSPEC attivi per l'interfaccia radio e la categoria di accesso.
- **Traffic Stream Clients**: il numero di client TS associati all'interfaccia radio e alla categoria di accesso.

- **Medium Time Admitted**: tempo assegnato a questa categoria di accesso sul supporto di trasmissione per trasmettere i dati. Questo valore deve essere minore o uguale alla larghezza di banda massima consentita sul supporto per questo TS.
- **Medium Time Unallocated**: tempo di larghezza di banda inutilizzata per questa categoria di accesso.

Queste statistiche vengono visualizzate separatamente per i percorsi di trasmissione e ricezione sull'interfaccia radio wireless:

- **Access Category**: la categoria di accesso associata al flusso di traffico (voce o video).
- **Total Packets**: il numero totale di pacchetti TS inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dall'interfaccia radio per la categoria di accesso specificata.
- **Total Bytes**: il numero totale di byte ricevuti nella categoria di accesso specificata.

Queste statistiche vengono visualizzate separatamente per i percorsi di trasmissione e ricezione sulle interfacce di rete (VAP):

- **Total Voice Packets**: il numero totale di pacchetti vocali TS inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP per il VAP.
- **Total Voice Bytes**: totale di byte vocali TS inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP per il VAP.
- **Total Video Packets**: il numero totale di pacchetti video TS inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP per il VAP.
- **Total Video Bytes**: totale di byte video TS inviati, indicati nella tabella Transmit, o ricevuti, indicati nella tabella Received, dal dispositivo WAP per il VAP.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Statistiche AP TSPEC

Nella pagina TSPEC AP Statistics vengono fornite informazioni sui flussi di traffico vocali e video accettati e rifiutati dal dispositivo WAP. Per visualizzare questa pagina, selezionare **Status and Statistics > TSPEC AP Statistics** nel riquadro di spostamento.

- **TSPEC Statistics Summary for Voice ACM**: il numero totale di flussi di traffico vocali accettati e di quelli rifiutati.
- **TSPEC Statistics Summary for Video ACM**: il numero totale di flussi di traffico video accettati e di quelli rifiutati.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Statistiche radio

È possibile utilizzare la pagina Radio Statistics per mostrare le statistiche a livello di pacchetti e di byte per ciascuna interfaccia radio wireless. Per visualizzare la pagina Radio Statistics, selezionare **Status and Statistics > Radio Statistics** nel riquadro di spostamento.

Per il dispositivo WAP561, selezionare l'interfaccia radio di cui si desidera visualizzare le statistiche.

- **Packets Received**: pacchetti totali ricevuti dal dispositivo WAP.
- **Packets Transmitted**: pacchetti totali trasmessi dal dispositivo WAP.
- **Bytes Received**: byte totali ricevuti dal dispositivo WAP.
- **Bytes Transmitted**: byte totali trasmessi dal dispositivo WAP.
- **Packets Receive Dropped**: il numero di pacchetti ricevuti dal dispositivo WAP e che sono stati persi.
- **Packets Transmit Dropped**: il numero di pacchetti trasmessi dal dispositivo WAP e che sono stati persi.
- **Bytes Receive Dropped**: il numero di byte ricevuti dal dispositivo WAP e che sono stati persi.
- **Bytes Transmit Dropped**: il numero di byte trasmessi dal dispositivo WAP e che sono stati persi.

- **Fragments Received**: il numero di frame frammentati ricevuti dal dispositivo WAP.
- **Fragments Transmitted**: il numero di frame frammentati inviati dal dispositivo WAP.
- **Multicast Frames Received**: il numero di frame MSDU ricevuti con il bit multicast impostato nell'indirizzo MAC di destinazione.
- **Multicast Frames Transmitted**: il numero di frame MSDU trasmessi correttamente in cui il bit multicast era impostato nell'indirizzo MAC di destinazione.
- **Duplicate Frame Count**: il numero di volte in cui un frame è stato ricevuto e nel campo Sequence Control è stato segnalato che era un duplicato.
- **Failed Transmit Count**: il numero di volte in cui un MSDU non è stato trasmesso correttamente perché è stato superato il limite di tentativi breve o lungo impostato.
- **FCS Error Count**: il numero di errori FCS rilevati in un frame MPDU ricevuto.
- **Transmit Retry Count**: il numero di volte in cui un MSDU è stato trasmesso correttamente dopo uno o più tentativi.
- **ACK Failure Count**: il numero di frame ACK non ricevuti quando era previsto.
- **RTS Failure Count**: il numero di frame CTS non ricevuti in risposta a un frame RTS.
- **WEP Undecryptable Count**: il numero di frame eliminati perché non è stato possibile decodificarli tramite l'interfaccia radio. I frame possono essere eliminati perché non è stato possibile decodificarli oppure perché è stata utilizzata per la crittografia un'opzione di privacy non supportata dal dispositivo WAP.
- **RTS Success Count**: il numero di frame CTS ricevuti in risposta a un frame RTS.
- **Multiple Retry Count**: il numero di volte in cui un MSDU è stato trasmesso correttamente dopo più tentativi.
- **Frames Transmitted Count**: il numero di ogni MSDU trasmesso correttamente.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Stato relativo agli avvisi tramite e-mail

Nella pagina Email Alert Status vengono fornite informazioni sugli avvisi inviati tramite e-mail in base ai messaggi syslog generati dal dispositivo WAP. Per visualizzare questa pagina, selezionare **Status and Statistics > Email Alert Status** nel riquadro di spostamento.

- **Email Alert Status**: lo stato configurato per gli avvisi tramite e-mail. Lo stato può essere Enabled o Disabled. L'impostazione predefinita è Disabled.
- **Number of Emails Sent**: il numero totale di messaggi e-mail inviati. L'intervallo è un numero intero senza segno a 32 bit. L'impostazione predefinita è 0.
- **Number of Emails Failed**: il numero totale di messaggi e-mail con errori. L'intervallo è un numero intero senza segno a 32 bit. L'impostazione predefinita è 0.
- **Time Last Email Sent**: il giorno, la data e l'ora in cui è stato inviato l'ultimo messaggio e-mail.

È possibile fare clic su **Refresh** per visualizzare le informazioni aggiornate.

Log

Nella pagina Log viene mostrato un elenco di eventi di sistema che hanno generato una voce di log, ad esempio tentativi di login e modifiche della configurazione. Il log viene cancellato in caso di riavvio e può essere eliminato da un amministratore. È possibile visualizzare fino a 512 eventi. Le voci meno recenti vengono rimosse dall'elenco in base alle necessità per fare spazio a nuovi eventi.

Per visualizzare la pagina Log, selezionare **Status and Statistics > Log** nel riquadro di spostamento.

- **Time Stamp**: l'ora di sistema in cui si è verificato l'evento.
- **Severity**: se l'evento è dovuto a un errore (err) o è di tipo informativo (info).
- **Service**: il componente software associato all'evento.
- **Description**: una descrizione dell'evento.

È possibile fare clic su **Refresh** per aggiornare la schermata e visualizzare le informazioni attuali.

Per cancellare tutte le voci di log, fare clic su **Cancella tutto**.

3

Amministrazione

In questo capitolo viene descritto come configurare le impostazioni globali di sistema ed eseguire operazioni di diagnostica.

Vengono trattati i seguenti argomenti:

- **Impostazioni di sistema**
- **Account utente**
- **Impostazioni relative all'ora**
- **Impostazioni del log**
- **Avvisi tramite e-mail**
- **Servizio HTTP/HTTPS**
- **Controllo degli accessi per la gestione**
- **Firmware di gestione**
- **Download/backup del file di configurazione**
- **Proprietà dei file di configurazione**
- **Copia/Salvataggio della configurazione**
- **Riavvio**
- **Rilevamento - Bonjour**
- **Acquisizione dei pacchetti**
- **Informazioni di supporto**

Impostazioni di sistema

Nella pagina System Settings vengono configurate le informazioni che identificano il dispositivo WAP all'interno della rete.

Per configurare le impostazioni di sistema, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **System Settings**.

PASSAGGIO 2 Immettere i seguenti parametri:

- **Host Name**: il nome assegnato dall'amministratore al dispositivo WAP. Per convenzione, viene utilizzato il nome di dominio completo del nodo. Il nome host predefinito è **wap**, concatenato con le ultime 6 cifre esadecimali dell'indirizzo MAC del dispositivo WAP. Le etichette dei nomi host possono contenere solo lettere, cifre e trattini, ma non possono iniziare o finire con un trattino. Non sono consentiti altri simboli, segni di punteggiatura o spazi bianchi. Il nome host può essere composto da 1 a 63 caratteri.
- **System Contact**: la persona di riferimento per il dispositivo WAP. La voce System Contact può contenere da 0 a 255 caratteri e includere spazi e caratteri speciali.
- **System Location**: la descrizione della posizione fisica del dispositivo WAP. La voce System Location può contenere da 0 a 255 caratteri e includere spazi e caratteri speciali.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Account utente

Sul dispositivo WAP è configurato per impostazione predefinita un utente di gestione:

- Nome utente: **cisco**
- Password: **cisco**

Utilizzare la pagina User Accounts per configurare massimo quattro utenti aggiuntivi e modificare la password di un utente.

Per aggiungere un nuovo utente, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **User Accounts**.

Nella tabella User Account vengono visualizzati gli utenti attualmente configurati. L'utente **cisco** è preconfigurato nel sistema con privilegi di lettura/scrittura.

Tutti gli altri utenti hanno accesso in sola lettura, non in lettura/scrittura.

PASSAGGIO 2 Fare clic su **Aggiungi**. Viene visualizzata una nuova riga di caselle di testo.

PASSAGGIO 3 Selezionare la casella del nuovo utente e fare clic su **Modifica**.

PASSAGGIO 4 Nel campo **User Name**, immettere un nome composto da 1-32 caratteri alfanumerici. Per i nomi utente sono consentiti solo i numeri da 0 a 9 e le lettere dalla a alla z (maiuscole e minuscole).

PASSAGGIO 5 Nel campo **New Password**, immettere una nuova password composta da 1-64 caratteri; immettere poi la stessa password nel campo **Confirm New Password**.

Durante l'inserimento della password, il numero e il colore delle barre verticali cambia indicando la complessità:

- Rosso: la password non soddisfa i requisiti minimi di complessità.
- Arancione: la password soddisfa i requisiti minimi di complessità, ma è debole.
- Verde: la password è sicura.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare un utente, selezionare la casella accanto al nome utente e fare clic su **Elimina**. Per confermare definitivamente l'eliminazione, fare clic su **Salva**.

Per modificare la password di un utente, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **User Accounts**.

Nella tabella User Account vengono visualizzati gli utenti attualmente configurati. L'utente **cisco** è preconfigurato nel sistema con privilegi di lettura/scrittura. È possibile modificare la password per l'utente **cisco**.

PASSAGGIO 2 Selezionare l'utente da configurare e fare clic su **Modifica**.

PASSAGGIO 3 Nel campo **New Password**, immettere una nuova password composta da 1-64 caratteri; immettere poi la stessa password nel campo **Confirm New Password**.

Durante l'inserimento della password, il numero e il colore delle barre verticali cambia indicando la complessità.

- Rosso: la password non soddisfa i requisiti minimi di complessità.
- Arancione: la password soddisfa i requisiti minimi di complessità, ma è debole.
- Verde: la password è sicura.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Se si modifica la password, è necessario accedere di nuovo al sistema.

Impostazioni relative all'ora

Per fornire un servizio di timestamp sincronizzato in rete per gli eventi software, come i log dei messaggi, viene utilizzato un orologio di sistema. È possibile configurare l'orologio di sistema manualmente o configurare il dispositivo WAP come NTP (Network Time Protocol), che ricava i dati sull'ora da un server.

Utilizzare la pagina Time Settings per impostare l'ora di sistema manualmente o per configurare il sistema in modo che acquisisca le impostazioni sull'ora da un server NTP preconfigurato. Per impostazione predefinita, il dispositivo WAP ricava l'ora da un elenco predefinito di server NTP.

L'ora del sistema corrente viene visualizzata nella parte superiore della pagina, insieme all'opzione System Clock Source.

Per utilizzare NTP in modo che il dispositivo WAP acquisisca automaticamente le impostazioni relative all'ora, attenersi alla seguente procedura:

PASSAGGIO 1 Nel campo System Clock Source, selezionare **Network Time Protocol (NTP)**.

PASSAGGIO 2 Configurare i parametri seguenti:

- **NTP Server/IPv4/IPv6 Address Name**: specificare l'indirizzo IPv4, l'indirizzo IPv6 o il nome host di un server NTP. Viene visualizzato un server NTP predefinito.

Un nome host può essere composto da una o più etichette, formate a loro volta da un numero massimo di 63 caratteri alfanumerici. Se un nome host include più etichette, queste saranno separate da un punto (.). La lunghezza massima dell'intera serie di etichette (punti compresi) è di 253 caratteri.

- **Time Zone**: selezionare il fuso orario della propria località.

PASSAGGIO 3 Selezionare **Adjust Time for Daylight Savings** se nella propria zona è applicata l'ora legale. Se si seleziona l'ora legale, configurare i seguenti campi:

- **Daylight Savings Start**: selezionare la settimana, il giorno, il mese e l'ora di inizio dell'ora legale.
- **Daylight Savings End**: selezionare la settimana, il giorno, il mese e l'ora di fine dell'ora legale.
- **Daylight Savings Offset**: specificare il numero di minuti di cui portare avanti l'orologio all'entrata in vigore dell'ora legale e indietro al ritorno all'ora solare.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Per configurare manualmente le impostazioni relative all'ora, attenersi alla seguente procedura:

PASSAGGIO 1 Nel campo System Clock Source, selezionare **Manually**.

PASSAGGIO 2 Configurare i parametri seguenti:

- **System Date**: selezionare la data attuale nel formato mese, giorno e anno dagli elenchi a discesa.
- **System Time**: selezionare l'ora e i minuti correnti nel formato 24 ore, ad esempio 22:00:00 per le 22.
- **Time Zone**: selezionare il fuso orario della propria località.

PASSAGGIO 3 Selezionare **Adjust Time for Daylight Savings** se nella propria zona è applicata l'ora legale. Se si seleziona l'ora legale, configurare i seguenti campi:

- **Daylight Savings Start**: selezionare la settimana, il giorno, il mese e l'ora di inizio dell'ora legale.
- **Daylight Savings End**: selezionare la settimana, il giorno, il mese e l'ora di fine dell'ora legale.
- **Daylight Savings Offset**: specificare il numero di minuti di cui portare avanti l'orologio all'entrata in vigore dell'ora legale e indietro al ritorno all'ora solare.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Impostazioni del log

Utilizzare la pagina Log Settings per salvare i messaggi di log nella memoria permanente. È inoltre possibile inviare i log a un host remoto.

Se il sistema viene riavviato in maniera inaspettata, i messaggi di log possono essere utili per diagnosticare la causa del riavvio. Tuttavia, se non si avvia la registrazione permanente, i messaggi di log vengono cancellati al riavvio del sistema.

ATTENZIONE L'attivazione del log permanente può esaurire la memoria flash (non volatile) e incidere negativamente sulle prestazioni della rete. Abilitare questa funzione solo per il debug di un problema e ricordarsi di disabilitarla al termine del debug.

Per configurare il log permanente, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Log Settings**.

PASSAGGIO 2 Configurare i seguenti parametri:

- **Persistence**: fare clic su **Enable** per salvare i log di sistema nella memoria non volatile, in modo che vengano conservati al riavvio del dispositivo WAP. Nella memoria non volatile è possibile salvare fino a 128 messaggi di log. Al raggiungimento del limite di 128, il messaggio di log meno recente verrà sovrascritto da quello più recente. Disattivare questo campo per salvare i log di sistema nella memoria volatile. I log nella memoria volatile vengono cancellati al riavvio del sistema.
- **Severity**: la gravità minima che un evento deve avere affinché venga scritto nel log della memoria non volatile. Se, ad esempio, si specifica 2 (evento critico), nella memoria non volatile verranno registrati gli eventi critici, di allerta e di emergenza. I messaggi di errore con un livello di gravità compreso fra 3 e 7 verranno scritti nella memoria volatile.
- **Depth**: il numero massimo di messaggi, fino a 512, memorizzati nella memoria volatile. Una volta raggiunto il numero configurato in questo campo, l'evento di log meno recente verrà sovrascritto dal più recente. Il numero

massimo di messaggi di log che è possibile memorizzare nella memoria non volatile (log permanente) è di 128 e non è possibile modificare questa impostazione.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Il log del kernel contiene un elenco completo degli eventi di sistema (mostrati nel log di sistema) e di messaggi del kernel, ad esempio condizioni di errore.

Non è possibile visualizzare i messaggi del log del kernel direttamente dall'interfaccia Web. È necessario configurare prima un server di log remoto che riceva e acquisisca i log. Successivamente è possibile configurare il dispositivo WAP per accedere al server di log remoto.

La raccolta dei server di log remoto per i messaggi SYSLOG del dispositivo WAP offre le funzioni seguenti:

- Consente l'aggregazione di messaggi SYSLOG da più AP.
- Memorizza una cronologia di messaggi più estesa rispetto a quella memorizzata su un singolo dispositivo WAP.
- Attiva operazioni di gestione e allerta definite tramite script.

Per specificare l'host della rete che svolge funzioni di server di log remoto, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Log Settings**.

PASSAGGIO 2 Configurare i seguenti parametri:

- **Remote Log**: consente al dispositivo WAP di inviare messaggi di log a un host remoto. Se questa opzione è disattivata, tutti i messaggi di log verranno conservati sul sistema locale.
- **Server IPv4/IPv6 Address/Name**: l'indirizzo IPv4 o IPv6 o il nome host del server di log remoto.

  Un nome host può essere composto da una o più etichette, formate a loro volta da un numero massimo di 63 caratteri alfanumerici. Se un nome host include più etichette, queste saranno separate da un punto (.). La lunghezza massima dell'intera serie di etichette (punti compresi) è di 253 caratteri.
- **UDP Port**: il numero di porta logica per il processo SYSLOG sull'host remoto. L'intervallo è compreso tra 1 e 65535. La porta predefinita è 514.

Si consiglia di utilizzare la porta predefinita. Se si desidera utilizzare una porta di log diversa, assicurarsi che il numero di porta assegnato a SYSLOG sia disponibile.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Se è stato attivato un host di log remoto, fare clic su **Salva** per attivare la registrazione remota. Il dispositivo WAP invia messaggi del kernel in tempo reale che verranno visualizzati sul monitor del server di log remoto, salvati in un file di log del kernel specificato o memorizzati in un altro percorso, a seconda della configurazione.

Se l'host di log remoto viene disattivato, fare clic su **Salva** per disattivare la registrazione remota.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Avvisi tramite e-mail

Utilizzare la funzione Email Alert per inviare messaggi agli indirizzi e-mail configurati quando si verificano determinati eventi di sistema.

Questa funzione supporta la configurazione dei server di posta, l'impostazione della gravità dei messaggi e fino a tre indirizzi e-mail per l'invio di avvisi urgenti o meno.

SUGGERIMENTO Non utilizzare l'indirizzo e-mail personale, poiché si divulgherebbero inutilmente le credenziali di accesso personali. Utilizzare un account di posta separato. È importante ricordare, inoltre, che molti account di posta conservano per impostazione predefinita una copia di tutti i messaggi inviati. Chiunque abbia accesso a questo account potrà, quindi, consultare anche tutti i messaggi inviati. Controllare le impostazioni della posta elettronica per assicurarsi che i criteri di privacy siano configurati correttamente.

Per configurare il dispositivo WAP per l'invio di avvisi tramite e-mail, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Email Alert**.

PASSAGGIO 2 Nella sezione Global Configuration, configurare i parametri seguenti:

- **Administrative Mode**: scegliere se attivare la funzione di avvisi tramite e-mail a livello globale.
- **From Email Address**: immettere l'indirizzo da visualizzare come mittente del messaggio. L'indirizzo è una stringa di 255 caratteri; sono consentiti solo caratteri stampabili. Non è configurato un indirizzo predefinito.
- **Log Duration**: scegliere la frequenza di invio dei messaggi pianificati. L'intervallo è compreso tra 30 e 1440 minuti. Il valore predefinito è 30 minuti.
- **Scheduled Message Severity**: i messaggi di log di gravità pari o superiore a quella impostata in questo campo vengono raggruppati e inviati all'indirizzo e-mail configurato alla frequenza specificata nel campo Log Duration. Scegliere tra i valori seguenti: None, Emergency, Alert, Critical, Error, Warning, Notice, Info e Debug. Se si seleziona None, non verranno inviati messaggi di gravità pianificati. La gravità predefinita è Warning.
- **Urgent Message Severity**: i messaggi di log con questo livello di gravità o superiore vengono inviati immediatamente all'indirizzo e-mail configurato. Scegliere tra i valori seguenti: None, Emergency, Alert, Critical, Error, Warning, Notice, Info e Debug. Se si seleziona None, i messaggi urgenti non verranno inviati. L'impostazione predefinita è Alert.

PASSAGGIO 3 Nell'area Mail Server Configuration, configurare i parametri seguenti:

- **Server IPv4 Address/Name**: immettere l'indirizzo IP o il nome host del server SMTP in uscita. Per conoscere il nome host, contattare il provider di posta. L'indirizzo del server deve essere un nome host valido o un indirizzo IPv4 il cui formato deve essere simile a xxx.xxx.xxx.xxx (192.0.2.10).

  Un nome host può essere composto da una o più etichette, formate a loro volta da un numero massimo di 63 caratteri alfanumerici. Se un nome host include più etichette, queste saranno separate da un punto (.). La lunghezza massima dell'intera serie di etichette (punti compresi) è di 253 caratteri.
- **Data Encryption**: specificare la modalità di protezione degli avvisi tramite e-mail in uscita. Gli avvisi possono essere inviati tramite il protocollo TLS o il protocollo aperto predefinito. Con il protocollo sicuro TLSv1 è possibile prevenire eventuali accessi non autorizzati e manomissioni durante la comunicazione attraverso la rete pubblica.

- **Port**: immettere il numero di porta SMTP da utilizzare per i messaggi e-mail in uscita. L'intervallo è un numero di porta valido compreso fra 0 e 65535. La porta predefinita è 465. Il numero di porta dipende, in genere, dalla modalità utilizzata dal provider di posta.
- **Username**: immettere il nome utente dell'account di posta utilizzato per inviare i messaggi. Il nome utente corrisponde spesso all'indirizzo e-mail completo, dominio compreso, ad esempio, nome@esempio.com. L'account specificato verrà utilizzato come indirizzo e-mail del mittente. Il nome utente può contenere da 1 a 64 caratteri alfanumerici.
- **Password**: immettere la password per l'account di posta che verrà utilizzato per inviare i messaggi. La password può contenere da 1 a 64 caratteri.

PASSAGGIO 4 Configurare gli indirizzi e-mail e l'oggetto dei messaggi.

- **To Email Address 1/2/3**: immettere massimo tre indirizzi per la ricezione degli avvisi. È necessario specificare indirizzi validi.
- **Email Subject**: immettere il testo che verrà visualizzato nell'oggetto del messaggio. È possibile immettere un massimo di 255 caratteri alfanumerici.

PASSAGGIO 5 Fare clic su **Test Mail** per inviare un messaggio di prova e convalidare l'account configurato.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Negli esempi seguenti viene mostrato come impostare i parametri di configurazione del server di posta:

```
Gmail
Nome/Indirizzo server IPv4 = smtp.gmail.com
Crittografia dati = TLSv1
Porta = 465
Nome utente = indirizzo e-mail completo che è possibile utilizzare per
accedere all'account di posta associato al server
Password = xxxxxxxx, password valida per l'account di posta configurato
E-mail di destinazione 1 = miaemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail raccomanda le seguenti impostazioni:
Crittografia dati: TLSv1
Server SMTP: smtp.live.com
Porta SMTP: 587
Nome utente: l'indirizzo e-mail completo, ad esempio mioNome@hotmail.com
oppure mioNome@mioDominio.com
Password: la password dell'account Windows Live.
```

```
Yahoo! Mail
Per questo tipo di servizio è necessario un account a pagamento. Yahoo
raccomanda le seguenti impostazioni:
Crittografia dati: TLSv1
Server SMTP: plus.smtp.mail.yahoo.com
Porta SMTP: 465 o 587
Nome utente: l'indirizzo e-mail senza il nome di dominio, ad esempio mioNome
(senza @yahoo.com)
Password: la password dell'account Yahoo!
```

Nell'esempio seguente viene mostrato il formato di un normale messaggio di log:

```
From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME           PriorityProcess Id          Message
Sep 8 03:48:25 info    login[1457]         root login on ttyp0
Sep 8 03:48:26 info    mini_http-ssl[1175] Max concurrent connections of 20
reached
```

Servizio HTTP/HTTPS

Utilizzare la pagina HTTP/HTTPS Service per attivare e configurare le connessioni di gestione sul Web. Se si sceglie HTTPS per le sessioni di gestione sicura, è possibile utilizzare la pagina HTTP/HTTPS Service per gestire i certificati SSL necessari.

Per configurare i servizi HTTP e HTTPS, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **HTTP/HTTPS Service**.

PASSAGGIO 2 Configurare le impostazioni generali seguenti:

- **Maximum Sessions**: il numero di sessioni Web, sia HTTP che HTTPS, che è possibile attivare contemporaneamente.

  Ogni volta che un utente accede all'utilità di configurazione del dispositivo WAP viene creata una sessione che rimane attiva fino a quando l'utente non si disconnette o quando viene raggiunto il valore di timeout della sessione. L'intervallo è compreso tra 1 e 10 sessioni. L'impostazione predefinita è 5. Se è stato raggiunto il numero massimo di sessioni, quando un utente cerca di accedere all'utilità di configurazione verrà visualizzato un messaggio di errore.

- **Session Timeout**: l'intervallo di tempo massimo, espresso in minuti, durante il quale un utente che ha effettuato l'accesso all'utilità di configurazione del dispositivo WAP rimane inattivo. Quando viene raggiunto il limite di timeout impostato, l'utente viene disconnesso automaticamente. L'intervallo è compreso tra 1 e 60 minuti. Il valore predefinito è 10 minuti.

PASSAGGIO 3 Configurare i servizi HTTP e HTTPS:

- **HTTP Server**: consente l'accesso tramite HTTP. L'accesso HTTP è abilitato per impostazione predefinita. Se si disattiva questa opzione, tutte le connessioni in corso che utilizzano questo protocollo saranno disconnesse.
- **HTTP Port**: il numero di porta logica da utilizzare per le connessioni HTTP. L'intervallo consentito è compreso fra 1025 e 65535. Il numero di porta predefinito per le connessioni HTTP è il ben noto numero di porta IANA 80.
- **HTTP Server**: consente l'accesso tramite HTTP protetto. L'accesso HTTPS è abilitato per impostazione predefinita. Se si disattiva questa opzione, tutte le connessioni in corso che utilizzano questo protocollo saranno disconnesse.
- **HTTPS Port**: il numero di porta logica da utilizzare per le connessioni HTTP. L'intervallo consentito è compreso fra 1025 e 65535. Il numero di porta predefinito per le connessioni HTTP è il ben noto numero di porta IANA 443.
- **Redirect HTTP to HTTPS**: reindirizza i tentativi di accesso alla porta HTTP di gestione dalla porta HTTP alla porta HTTPS. Questo campo è disponibile solo se l'accesso HTTP è disabilitato.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Per utilizzare i servizi HTTPS, il dispositivo WAP deve disporre di un certificato SSL valido. Il dispositivo WAP può generare un certificato o, in alternativa, è possibile scaricarlo dalla rete o da un server TFTP.

Per generare il certificato con il dispositivo WAP, fare clic su **Generate SSL Certificate.** Prima di eseguire questa operazione, il dispositivo WAP deve acquisire un indirizzo IP per assicurarsi che il nome comune del certificato corrisponda all'indirizzo IP del dispositivo WAP. Se si genera un nuovo certificato SSL, il server Web sicuro viene riavviato. La connessione protetta sarà attiva dopo che il nuovo certificato viene accettato dal browser.

Nell'area Certificate File Status, è possibile vedere se sul dispositivo WAP esiste già un certificato e visualizzare le informazioni seguenti:

- Presenza del file del certificato

- Data di scadenza del certificato
- Nome comune dell'autorità che ha rilasciato il certificato

Se sul dispositivo WAP è presente un certificato SSL (con estensione .pem), è possibile scaricarlo sul proprio computer come copia di backup. Nell'area Download SSL Certificate (From Device to PC), selezionare **HTTP** o **TFTP** nel campo **Download Method**, quindi fare clic su **Download**.

- Se si seleziona HTTP, verrà chiesto di confermare il download e di selezionare il percorso di salvataggio del file sulla rete.
- Se si seleziona TFTP, verranno visualizzati campi aggiuntivi in cui inserire il nome da assegnare al file scaricato e l'indirizzo del server TFTP in cui il file verrà scaricato.

È inoltre possibile caricare un file di certificato (con estensione .pem) dal computer al dispositivo WAP. Nell'area Upload SSL Certificate (From PC to Device), selezionare **HTTP** o **TFTP** nel campo **Upload Method**.

- Se si sceglie HTTP, selezionare il percorso di rete, selezionare il file e fare clic su **Upload**.
- Se si sceglie TFTP, riportare nel campo **File Name** il nome del file così come appare sul server TFTP e immettere l'indirizzo IPv4 del server TFTP nel campo **TFTP Server IPv4 Address**, quindi fare clic su **Upload**. Il nome del file non può contenere i seguenti caratteri: spazi, <, >, |, \, : , (,), &, ; , #, ? , * e due o più punti consecutivi.

Al termine dell'upload verrà visualizzato un messaggio di conferma

Controllo degli accessi per la gestione

È possibile creare un elenco di controllo degli accessi (ACL, Access Control List) che contiene massimo cinque host IPv4 e cinque host IPv6 autorizzati ad accedere all'utilità di configurazione del dispositivo WAP. Se questa funzione è disattivata, chiunque fornisca il nome utente e la password corretti per il dispositivo WAP potrà accedere all'utilità di configurazione da qualsiasi client di rete.

Se l'ACL di gestione è abilitato, l'accesso tramite Web e SNMP sarà limitato agli host IP specificati.

ATTENZIONE Verificare ogni indirizzo IP inserito. Se un indirizzo IP non corrisponde al computer di amministrazione, l'accesso all'interfaccia di configurazione verrà interrotto. Per il computer di amministrazione, si consiglia vivamente di impostare un indirizzo IP statico, in modo che non cambi nel tempo.

Per creare un elenco di controllo degli accessi, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Management Access Control**.

PASSAGGIO 2 Selezionare **Enable** per **Management ACL Mode**.

PASSAGGIO 3 Immettere fino a cinque indirizzi IPv4 e cinque indirizzi IPv6 che potranno effettuare l'accesso.

PASSAGGIO 4 Assicurarsi che gli indirizzi IP siano corretti.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Firmware di gestione

Il dispositivo WAP mantiene due immagini firmware, una attiva e l'altra inattiva. Se l'immagine attiva non viene caricata durante l'avvio, viene caricata quella inattiva, che diventa a sua volta attiva. È inoltre possibile scambiare l'immagine primaria e quella secondaria.

Quando viene rilasciata una nuova versione del firmware del dispositivo WAP, è possibile effettuare l'aggiornamento sui dispositivi per poter utilizzare le nuove funzionalità e i miglioramenti apportati. Il dispositivo WAP utilizza un client TFTP o HTTP per gli aggiornamenti del firmware.

Dopo avere caricato il nuovo firmware e riavviato il sistema, il firmware aggiornato diventerà l'immagine primaria. Se l'aggiornamento non viene completato, verrà utilizzato come immagine primaria il firmware originale.

NOTA Quando si aggiorna il firmware, l'access point mantiene i dati di configurazione esistenti.

Scambio dell'immagine del firmware

Per cambiare l'immagine del firmware attivo sull'AP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Manage Firmware**.

PASSAGGIO 2 Fare clic su **Swap Active Image**.

Viene visualizzata una finestra di conferma dello scambio di immagine del firmware e del successivo riavvio.

PASSAGGIO 3 Fare clic su **OK** per continuare.

La procedura potrebbe richiedere alcuni minuti; durante questa operazione l'access point non è disponibile. Non spegnere l'access point mentre è in corso il cambio dell'immagine. Al termine del cambio di immagine, l'access point verrà riavviato. L'AP riprende a funzionare normalmente con le medesime impostazioni di configurazione attive prima dell'aggiornamento.

Per aggiornare il firmware su un access point mediante TFTP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Manage Firmware**.

Verranno visualizzati l'ID del prodotto (PID VID) e la versioni del firmware attivo e di quello inattivo.

PASSAGGIO 2 Selezionare TFTP come metodo di trasferimento.

PASSAGGIO 3 Immettere un nome (da 1 a 256 caratteri) per il file di immagine nel campo **Source File Name**, incluso il percorso alla directory che contiene l'immagine da caricare.

Ad esempio, per caricare l'immagine ap_upgrade.tar, collocata nella directory /share/builds/ap, immettere: */share/builds/ap/ap_upgrade.tar*

Il file di aggiornamento del firmware deve avere estensione tar. I file bin o di altri formati non funzionano.

Il nome del file non può contenere i seguenti caratteri: spazi, <, >, |, \, : , (,), &, ; , #, ? , * e due o più punti consecutivi.

PASSAGGIO 4 Immettere l'indirizzo IPv4 del server TFTP nel rispettivo campo e fare clic su **Upgrade**.

L'upload del nuovo software può richiedere alcuni minuti. Non aggiornare la pagina o passare a un'altra pagina durante l'upload del nuovo software; in caso contrario, l'upload verrà interrotto. Al termine della procedura, l'access point verrà riavviato, riprendendo il normale funzionamento.

PASSAGGIO 5 Per verificare che l'aggiornamento del firmware sia stato completato correttamente, accedere all'interfaccia utente, aprire la pagina Upgrade Firmware e visualizzare la versione del firmware attiva.

Per eseguire l'aggiornamento tramite HTTP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare HTTP come metodo di trasferimento.

PASSAGGIO 2 Se si conosce il nome e il percorso del nuovo file, immetterlo nel campo **Source File Name**. In caso contrario, fare clic sul pulsante **Browse** e selezionare il file di immagine del firmware sulla rete.

Il file di aggiornamento del firmware deve avere estensione tar. I file bin o di altri formati non funzionano.

PASSAGGIO 3 Fare clic su **Upgrade** per applicare la nuova immagine del firmware.

L'upload del nuovo software può richiedere alcuni minuti. Non aggiornare la pagina o passare a un'altra pagina durante l'upload del nuovo software; in caso contrario, l'upload verrà interrotto. Al termine della procedura, l'access point verrà riavviato, riprendendo il normale funzionamento.

PASSAGGIO 4 Per verificare che l'aggiornamento del firmware sia stato completato correttamente, accedere all'interfaccia utente, aprire la pagina Upgrade Firmware e visualizzare la versione del firmware attiva.

Download/backup del file di configurazione

I file di configurazione del dispositivo WAP sono in formato XML e contengono tutte le informazioni relative alle impostazioni del dispositivo WAP. È possibile eseguire il backup (upload) dei file di configurazione su un host di rete o un server TFTP per modificarne manualmente i contenuti o creare delle copie. Dopo avere modificato un file di configurazione di cui è stato eseguito il backup, sarà possibile scaricarlo sull'access point per modificarne la configurazione.

Il dispositivo WAP conserva i seguenti file di configurazione:

- **Startup Configuration**: il file di configurazione salvato nella memoria flash.
- **Backup Configuration**: un file di configurazione aggiuntivo salvato sul dispositivo WAP come copia di backup.
- **Mirror Configuration**: se la configurazione di avvio non viene modificata per almeno 24 ore, viene salvata automaticamente in un file di configurazione mirror. Questo file contiene l'istantanea di una configurazione di avvio precedente. La configurazione mirror viene mantenuta anche in seguito al ripristino delle impostazioni predefinite; in questo modo sarà possibile copiare la configurazione mirror nella configurazione di avvio per recuperare una configurazione di sistema dopo tale ripristino.

NOTA Oltre a scaricare e caricare tali file su un altro sistema, è possibile copiarli in tipi di file diversi sul dispositivo WAP. Vedere la sezione **Copia/Salvataggio della configurazione**.

Per eseguire il backup (upload) del file di configurazione su un host di rete o un server TFTP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Download/Backup Configuration File**.

PASSAGGIO 2 Selezionare **Via TFTP** o **Via HTTP/HTTPS** nel campo **Transfer Method**.

PASSAGGIO 3 Selezionare **Backup (AP to PC)** nel campo **Save Action**.

PASSAGGIO 4 Solo per backup tramite TFTP, immettere un nome nel campo **Destination File Name** con estensione .xml. Includere, inoltre, il percorso del file sul server e l'indirizzo IPv4 del server TFTP nel rispettivo campo.

Il nome del file non può contenere i seguenti caratteri: spazi, <, >, |, \, : , (,), &, ; , #, ? , * e due o più punti consecutivi.

PASSAGGIO 5 Solo per il backup tramite TFTP, immettere l'indirizzo IPv4 del server TFTP nel rispettivo campo.

PASSAGGIO 6 Selezionare il file di configurazione di cui si desidera eseguire il backup:

- **Startup Configuration**: il tipo di file di configurazione utilizzato all'avvio del dispositivo WAP. Questo file non include le modifiche alla configurazione applicate, ma non ancora salvate sul dispositivo WAP.
- **Backup Configuration**: il tipo di file di configurazione per il backup salvato sul dispositivo WAP.

- **Mirror Configuration**: se la configurazione di avvio non viene modificata per almeno 24 ore, viene salvata automaticamente in un file di configurazione mirror. Questo file contiene l'istantanea di una configurazione di avvio precedente. La configurazione mirror viene mantenuta anche in seguito al ripristino delle impostazioni predefinite; in questo modo sarà possibile copiare la configurazione mirror nella configurazione di avvio per recuperare una configurazione di sistema dopo tale ripristino.

PASSAGGIO 7 Fare clic su **Salva** per avviare il backup. Per i backup tramite HTTP viene visualizzata una finestra in cui è possibile selezionare il percorso desiderato per il salvataggio del file.

È possibile scaricare un file sul dispositivo WAP per aggiornare la configurazione o ripristinare una configurazione di cui è stato eseguito il backup in precedenza.

Per scaricare un file di configurazione sul dispositivo WAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Download/Backup Configuration File**.

PASSAGGIO 2 Selezionare **Via TFTP** o **Via HTTP/HTTPS** nel campo **Transfer Method**.

PASSAGGIO 3 Selezionare **Download (PC to AP)** nel campo **Save Action**.

PASSAGGIO 4 Solo per il download tramite TFTP, immettere un nome con estensione .xml nel campo **Source File Name**. Includere, inoltre, il percorso del file sul server e l'indirizzo IPv4 del server TFTP nel rispettivo campo.

Il nome del file non può contenere i seguenti caratteri: spazi, <, >, |, \, : , (,), &, ; , #, ? , * e due o più punti consecutivi.

PASSAGGIO 5 Sul dispositivo WAP, selezionare il file di configurazione che si desidera sostituire con il file scaricato, ovvero il file della **configurazione di avvio** o quello della **configurazione di backup**.

Se il file scaricato sovrascrive il file della configurazione di avvio e supera un controllo di validità, al successivo riavvio del dispositivo WAP verrà applicata la configurazione scaricata.

PASSAGGIO 6 Fare clic su **Salva** per avviare l'aggiornamento o il backup. Per i download tramite HTTP viene visualizzata una finestra in cui è possibile selezionare il file da scaricare. Al termine del download verrà visualizzata una finestra di conferma.

ATTENZIONE Assicurarsi che il dispositivo WAP rimanga acceso per tutta la durata del download del file di configurazione. Se si verifica un'interruzione di corrente durante il download, il file di configurazione andrà perso e sarà necessario ripetere la procedura.

Proprietà dei file di configurazione

Nella pagina Configuration Files Properties è possibile cancellare il file della configurazione di avvio o di backup. Se si cancella il file della configurazione di avvio, al successivo avvio del dispositivo WAP diventerà attivo il file della configurazione di backup.

Per eliminare il file della configurazione di avvio o di backup, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Configuration Files Properties**.

PASSAGGIO 2 Selezionare il tipo di file: **Startup Configuration** o **Backup Configuration**.

PASSAGGIO 3 Fare clic su **Clear Files**.

Copia/Salvataggio della configurazione

Nella pagina Copy/Save Configuration è possibile copiare i file nel file system del dispositivo WAP. Ad esempio, è possibile copiare il file della configurazione di backup nel file della configurazione di avvio in modo che venga utilizzato al successivo avvio del dispositivo WAP.

Per copiare un file in un altro tipo di file, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Copy/Save Configuration**.

PASSAGGIO 2 Selezionare il nome del file di origine nel rispettivo campo:

- **Startup Configuration**: il tipo di file di configurazione utilizzato all'avvio del dispositivo WAP. Questo file non include le modifiche alla configurazione applicate, ma non ancora salvate sul dispositivo WAP.
- **Backup Configuration**: il tipo di file di configurazione per il backup salvato sul dispositivo WAP.
- **Mirror Configuration**: se la configurazione di avvio non viene modificata per almeno 24 ore, viene salvata automaticamente in un file di configurazione mirror. Questo file contiene l'istantanea di una configurazione di avvio precedente. La configurazione mirror viene mantenuta anche in seguito al ripristino delle impostazioni predefinite; in questo modo sarà possibile copiare la configurazione mirror nella configurazione di avvio per recuperare una configurazione di sistema dopo tale ripristino.

PASSAGGIO 3 Nel campo **Destination File Name**, selezionare il tipo di file da sovrascrivere con il file copiato:

PASSAGGIO 4 Fare clic su **Salva** per avviare la copia.

Al termine della procedura viene visualizzata una finestra di conferma dell'operazione.

Riavvio

Utilizzare la pagina Reboot per riavviare il dispositivo WAP.

PASSAGGIO 1 Per riavviare il dispositivo WAP, selezionare **Administration** > **Reboot** nel riquadro di spostamento.

PASSAGGIO 2 Selezionare una delle seguenti opzioni:

- **Reboot**: riavvia il dispositivo WAP utilizzando la configurazione di avvio.
- **Reboot to Factory Default**: riavvia il dispositivo WAP utilizzando il file di configurazione con le impostazioni predefinite di fabbrica. Tutte le impostazioni personalizzate andranno perse.

Viene visualizzata una finestra che consente di confermare o annullare il riavvio. La sessione di gestione corrente potrebbe essere interrotta.

PASSAGGIO 3 Fare clic su **OK** per riavviare.

Rilevamento - Bonjour

Bonjour consente di rilevare il dispositivo WAP e i relativi servizi tramite DNS multicast (mDNS). Bonjour dichiara i servizi alla rete e risponde alle richieste dei tipi di servizio supportati, semplificando la configurazione di rete nelle piccole imprese.

Il dispositivo WAP dichiara i seguenti tipi di servizi:

- **Cisco-specific device description** (csco-sb): servizio che permette ai client di rilevare i dispositivi WAP Cisco e altri prodotti distribuiti in reti di piccole aziende.
- **Management user interfaces**: questo servizio individua le interfacce di gestione disponibili sul dispositivo WAP (HTTP e SNMP).

Quando un dispositivo WAP che supporta Bonjour viene collegato a una rete, i client Bonjour possono rilevarlo e ottenere l'accesso all'utilità di configurazione senza previa configurazione.

Un amministratore di sistema può utilizzare un plug-in di Internet Explorer installato per rilevare il dispositivo WAP. L'utilità di configurazione basata sul Web viene visualizzata come scheda del browser.

Bonjour funziona sia sulle reti IPv4 che IPv6.

Bonjour è attivo per impostazione predefinita. Per modificare lo stato amministrativo, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Administration** > **Discovery - Bonjour**.

PASSAGGIO 2 Fare clic su **Enable** per attivare Bonjour oppure deselezionare **Enable** per disattivarlo.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Acquisizione dei pacchetti

La funzione di acquisizione dei pacchetti wireless consente di acquisire e memorizzare i pacchetti ricevuti e trasmessi dal dispositivo WAP. I pacchetti acquisiti possono poi essere analizzati da uno strumento di analisi dei protocolli di rete per la risoluzione dei problemi o l'ottimizzazione delle prestazioni. Sono disponibili due metodi di acquisizione dei pacchetti:

- Metodo di acquisizione locale: i pacchetti acquisiti vengono memorizzati in un file sul dispositivo WAP. Il dispositivo WAP può trasferire il file su un server TFTP. Il file è in formato pcap e può essere esaminato utilizzando strumenti come Wireshark e OmniPeek.
- Metodo di acquisizione remoto: i pacchetti acquisiti vengono reindirizzati in tempo reale a un computer esterno su cui viene eseguito lo strumento Wireshark.

Il dispositivo WAP può acquisire i tipi di pacchetti seguenti:

- Pacchetti 802.11 ricevuti e trasmessi su interfacce radio. I pacchetti acquisiti su interfacce radio includono l'intestazione 802.11.
- Pacchetti 802.3 ricevuti e trasmessi sull'interfaccia Ethernet.
- Pacchetti 802.3 ricevuti e trasmessi sulle interfacce logiche interne, come VAP e WDS.

Fare clic su **Administration > Packet Capture** per visualizzare la pagina Packet Capture. In questa pagina è possibile eseguire le operazioni seguenti:

- Configurare i parametri di acquisizione dei pacchetti.
- Avviare l'acquisizione locale o remota dei pacchetti.
- Visualizzare lo stato corrente dell'acquisizione dei pacchetti.
- Scaricare un file di acquisizione dei pacchetti.

Nell'area Packet Capture Configuration, è possibile configurare i parametri e avviare l'acquisizione dei pacchetti.

Per configurare l'acquisizione dei pacchetti, attenersi alla seguente procedura:

PASSAGGIO 1 Configurare i parametri seguenti:

- **Capture Beacons**: abilita o disabilita l'acquisizione di beacon 802.11 rilevati o trasmessi dall'interfaccia radio.

- **Promiscuous Capture**: abilita o disabilita la modalità promiscua quando è attiva l'acquisizione.

  In modalità promiscua, l'interfaccia radio riceve tutto il traffico sul canale, incluso il traffico non destinato al dispositivo WAP. Quando è attiva la modalità promiscua, l'interfaccia radio continua a servire i client associati. I pacchetti non destinati al dispositivo WAP non vengono inoltrati.

  Al termine dell'acquisizione, l'interfaccia radio torna a operare in modalità non promiscua.

- **Radio Client Filter**: attiva o disattiva il filtro del client WLAN per acquisire soltanto i frame trasmessi a/ricevuti da un client WLAN con indirizzo MAC specifico.

- **Client Filter MAC Address**: specifica l'indirizzo MAC per il filtraggio del client WLAN.

  NOTA Il filtro MAC è attivo soltanto quando si esegue l'acquisizione su un'interfaccia 802.11.

- **Packet Capture Method**: selezionare una delle opzioni seguenti:

  - **Local file**: i pacchetti acquisiti sono memorizzati in un file sul dispositivo WAP.

  - **Remote**: i pacchetti acquisiti vengono reindirizzati in tempo reale a un computer esterno su cui viene eseguito lo strumento Wireshark.

PASSAGGIO 2 A seconda del metodo selezionato, fare riferimento alla procedura descritta nella sezione relativa all'acquisizione di pacchetti locale remota per continuare.

NOTA Le modifiche ai parametri di configurazione dell'acquisizione di pacchetti vengono applicate al riavvio dell'acquisizione di pacchetti. La modifica dei parametri durante l'acquisizione dei pacchetti non incide sulla sessione di acquisizione in corso. Per iniziare a utilizzare i nuovi parametri, è necessario interrompere e riavviare una sessione di acquisizione dei pacchetti in corso.

Per avviare l'acquisizione dei pacchetti locale, attenersi alla seguente procedura:

PASSAGGIO 1 Assicurarsi che nel campo **Packet Capture Method** sia selezionato **Local File**.

PASSAGGIO 2 Configurare i parametri seguenti:

- **Capture Interface**: immettere un tipo di interfaccia di acquisizione dei pacchetti:

- **radio1**: traffico 802.11 sull'interfaccia Radio 1.
- **radio2**: traffico 802.11 sull'interfaccia Radio 2 (solo WAP561).
- **eth0**: traffico 802.3 sulla porta Ethernet.
- **VAP0** o **WLAN0:VAP0**: traffico VAP0. Per WAP 561, verrà mostrato WLAN0:VAP0, laddove WLAN0 rappresenta Radio 1.
- **WLAN1:VAP0**: traffico VAP0 su Radio 2 (solo per dispositivi WAP561).
- **Da VAP1** a **VAP15**, se configurati: traffico sul VAP specificato. Per WAP561, i nomi dell'interfaccia sono preceduti da WLAN0: o WLAN1:, laddove WLAN0 rappresenta Radio 1 e WLAN1 rappresenta Radio 2.
- **brtrunk**: interfaccia Linux sul dispositivo WAP.

- **Capture Duration**: immettere la durata dell'acquisizione in secondi. L'intervallo è compreso tra 10 e 3600. L'impostazione predefinita è 60.
- **Max Capture File Size**: immettere le dimensioni massime consentite per il file di acquisizione in KB. L'intervallo è compreso tra 64 e 4096. L'impostazione predefinita è 1024.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

PASSAGGIO 4 Fare clic su **Start Capture**.

In modalità Packet File Capture, il dispositivo WAP memorizza i pacchetti acquisiti nel file system della RAM. All'attivazione, l'acquisizione dei pacchetti procede fino a quando non si verifica uno degli eventi seguenti:

- Viene raggiunta la durata configurata per l'acquisizione.
- Vengono raggiunte le dimensioni massime del file di acquisizione.
- L'amministratore interrompe l'acquisizione.

Nell'area Packet Capture Status della pagina viene mostrato lo stato dell'acquisizione dei pacchetti, se sul dispositivo WAP è attiva un'acquisizione.

- **Current Capture Status**: indica se l'acquisizione dei pacchetti è in corso o interrotta.
- **Packet Capture Time**: il tempo di acquisizione trascorso.
- **Packet Capture File Size**: le dimensioni attuali del file di acquisizione.

Fare clic su **Refresh** per visualizzare i dati aggiornati del dispositivo WAP.

NOTA Per interrompere l'acquisizione di un file di pacchetto, fare clic su **Stop Capture**.

La funzione di acquisizione dei pacchetti remota consente di specificare una porta remota come destinazione dell'acquisizione. Questa funzione opera in combinazione con lo strumento di analisi della rete Wireshark per Windows. Sul dispositivo WAP viene eseguito un server di acquisizione dei pacchetti che invia i pacchetti acquisiti tramite una connessione TCP allo strumento Wireshark. Wireshark è uno strumento open source disponibile gratuitamente sul sito http://www.wireshark.org.

Un computer su cui viene eseguito Microsoft Windows con Wireshark consente di visualizzare, registrare e analizzare il traffico acquisito. L'acquisizione dei pacchetti remota è una funzione standard dello strumento Wireshark per Windows. La versione Linux non può essere usata con dispositivi WAP.

Se è attiva la modalità di acquisizione remota, i dati acquisiti non vengono memorizzati localmente nel file system del dispositivo WAP.

Se tra il computer con Wireshark e il dispositivo WAP è installato un firewall, è necessario autorizzare il passaggio del traffico su tali porte attraverso il firewall. È necessario, inoltre, configurare il firewall in modo da consentire al computer con Wireshark di stabilire una connessione TCP verso il dispositivo WAP.

Per avviare un'acquisizione remota su un dispositivo WAP, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Administration** > **Packet Capture**.

PASSAGGIO 2 Attivare l'opzione **Promiscuous Capture**.

PASSAGGIO 3 In **Packet Capture Method**, selezionare **Remote**.

PASSAGGIO 4 In **Remote Capture Port**, utilizzare la porta predefinita (2002) o, se si utilizza una porta diversa, immettere il numero della porta desiderata per collegare Wireshark al dispositivo WAP. L'intervallo valido è compreso tra 1025 e 65530.

PASSAGGIO 5 Se si desidera salvare le impostazioni per il futuro, fare clic su **Salva**.

PASSAGGIO 6 Fare clic su **Start Capture**.

Per avviare lo strumento di analisi della rete Wireshark per Microsoft Windows, attenersi alla seguente procedura:

PASSAGGIO 1 Sullo stesso computer, avviare Wireshark.

PASSAGGIO 2 Nel menu, selezionare **Capture** > **Options**. Viene visualizzata una finestra.

PASSAGGIO 3 In **Interface**, selezionare **Remote**. Viene visualizzata una finestra.

PASSAGGIO 4 In **Host**, immettere l'indirizzo IP del dispositivo WAP.

PASSAGGIO 5 In **Port**, immettere il numero di porta del dispositivo WAP. Ad esempio, immettere 2002 se si utilizza la porta predefinita oppure immettere il numero della porta desiderata, se diversa dalla predefinita.

PASSAGGIO 6 Fare clic su **OK**.

PASSAGGIO 7 Selezionare l'interfaccia da cui si desidera acquisire i pacchetti. Nella finestra popup di Wireshark, accanto all'indirizzo IP viene visualizzato un menu a discesa con l'elenco delle interfacce disponibili. Di seguito sono riportate le interfacce disponibili:

Interfaccia bridge Linux sul dispositivo WAP
`--rpcap://[192.168.1.220]:2002/brtrunk`
Interfaccia LAN cablata
`-- rpcap://[192.168.1.220]:2002/eth0`
Traffico VAP0 su radio 1
`-- rpcap://[192.168.1.220]:2002/wlan0`
Traffico 802.11
`-- rpcap://[192.168.1.220]:2002/radio1`
Su WAP561, traffico VAP1 ~ VAP7
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
Su WAP561, traffico VAP1 ~ VAP3
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3`

Sul dispositivo WAP è possibile tracciare fino a quattro interfacce contemporaneamente. Per ogni interfaccia sarà tuttavia necessario avviare una sessione separata di Wireshark. Per avviare altre sessioni di acquisizione remota, ripetere la procedura di Wireshark; sul dispositivo WAP non sarà necessaria alcuna configurazione.

NOTA Il sistema utilizza quattro numeri di porta consecutivi, partendo dalla porta configurata per le sessioni di acquisizione dei pacchetti remota. Assicurarsi che siano disponibili quattro numeri di porta consecutivi. Se non si utilizza la porta predefinita, si consiglia di utilizzare un numero di porta maggiore di 1024.

Durante l'acquisizione di dati sull'interfaccia radio, è possibile disabilitare l'acquisizione dei beacon, anche se altri frame di controllo 802.11 verranno comunque inviati a Wireshark. È possibile impostare un filtro in modo da visualizzare soltanto i dati seguenti:

- Frame di dati nella traccia
- Traffico su BSSID (Basic Service Set ID) specifici
- Traffico tra due client

Alcuni esempi d filtri di visualizzazione utili:

- Escludere i beacon e i frame ACK/RTS/CTS:

  !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- Soli frame di dati:

  wlan.fc.type == 2

- Traffico su un BSSID specifico:

  wlan.bssid == 00:02:bc:00:17:d0

- Tutto il traffico da e verso un client specifico:

  wlan.addr == 00:00:e8:4e:5f:8e

In modalità di acquisizione remota, i dati vengono inviati al computer su cui viene eseguito Wireshark attraverso una delle interfacce di rete. A seconda della posizione di Wireshark, i dati possono essere inviati tramite un'interfaccia Ethernet o una delle interfacce radio. Per evitare un flusso di dati eccessivo dovuto al tracciamento dei pacchetti, sul dispositivo WAP viene installato automaticamente un filtro di acquisizione per escludere tutti i pacchetti destinati all'applicazione Wireshark. Ad esempio, se la porta IP per Wireshark è configurata su 58000, allora tale filtro verrà installato automaticamente sul dispositivo WAP:

not portrange 58000-58004

Per questioni legate alla sicurezza e alle prestazioni, la modalità di acquisizione dei pacchetti non viene salvata nella NVRAM del dispositivo WAP; se il dispositivo WAP viene reimpostato, la modalità di acquisizione viene disabilitata e sarà necessario riattivarla per riprendere l'acquisizione dei dati. I parametri di acquisizione dei pacchetti, ad eccezione della modalità, sono salvati nella NVRAM.

L'abilitazione della funzione di acquisizione dei pacchetti può generare un problema di sicurezza: alcuni client non autorizzati, infatti, potrebbero essere in grado di collegarsi al dispositivo WAP e tracciare i dati utente. L'acquisizione dei pacchetti rallenta anche le prestazioni del dispositivo WAP; tale impatto continua, in misura minore, anche quando non sono attive sessioni di Wireshark. Per ridurre al minimo l'impatto sulle prestazioni del dispositivo WAP durante l'acquisizione di traffico, installare filtri di acquisizione che limitino i dati inviati a Wireshark. Durante l'acquisizione di traffico 802.11, buona parte dei frame acquisiti è composta da

beacon, inviati normalmente ogni 100 ms da tutti gli AP. Sebbene Wireshark supporti un filtro di visualizzazione dei frame beacon, non supporta un filtro di acquisizione che impedisca al dispositivo WAP di inoltrare i pacchetti di beacon a Wireshark. Per ridurre l'impatto dell'acquisizione di beacon 802.11 sulle prestazioni, disabilitare la modalità di acquisizione beacon.

È possibile scaricare un file di acquisizione tramite TFTP su un server TFTP configurato o tramite HTTP(S) su un computer. All'avvio del comando di download del file di acquisizione, il processo di acquisizione in corso viene interrotto automaticamente.

Poiché il file di acquisizione si trova nel file system della RAM, verrà eliminato se si reimposta il dispositivo WAP.

Per scaricare un file di acquisizione dei pacchetti tramite TFTP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Use TFTP to download the capture file**.

PASSAGGIO 2 Se il nome del file è diverso da quello predefinito, inserirlo nel campo **TFTP Server Filename**. I pacchetti acquisiti vengono memorizzati per impostazione predefinita nel file /tmp/apcapture.pcap sul dispositivo WAP.

PASSAGGIO 3 Specificare l'indirizzo IPv4 del server TFTP nel relativo campo.

PASSAGGIO 4 Fare clic su **Download**.

Per scaricare un file di acquisizione dei pacchetti tramite HTTP, attenersi alla seguente procedura:

PASSAGGIO 1 Disattivare la casella **Use TFTP to download the captured file**.

PASSAGGIO 2 Fare clic su **Download**. Viene visualizzata una finestra di conferma.

PASSAGGIO 3 Fare clic su **OK**. Viene visualizzata una finestra di dialogo in cui è possibile selezionare il percorso di rete per il salvataggio del file.

Informazioni di supporto

Nella pagina Support Information è possibile scaricare un file di testo con le informazioni dettagliate di configurazione relative all'AP. Il file comprende informazioni sulla versione hardware e software, gli indirizzi MAC e IP, lo stato operativo e amministrativo di funzioni, impostazioni configurate dall'utente, statistiche sul traffico e altro. Il file di testo può essere inviato al personale del supporto tecnico per ricevere assistenza nella risoluzione dei problemi.

Per visualizzare la pagina Support Information, selezionare **Administration > Support Information** nel riquadro di spostamento.

Fare clic su **Download** per generare il file basato sulle impostazioni di sistema correnti. Dopo alcuni istanti viene visualizzata una finestra di salvataggio del file sul computer.

4

LAN

In questo capitolo vengono descritte le modalità di configurazione delle impostazioni per porta, rete e orologio dei dispositivi WAP.

Vengono trattati i seguenti argomenti:

- **Impostazioni della porta**
- **Impostazioni dell'indirizzo IPv4 e della VLAN**
- **Indirizzi IPv6**
- **Tunnel IPv6**

Impostazioni della porta

La finestra Port Settings consente di visualizzare e configurare le impostazioni della porta che connette fisicamente il dispositivo WAP a una rete LAN.

Per visualizzare e configurare le impostazioni LAN, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'area di navigazione, selezionare **LAN** > **Port Settings**.

Nell'area Operational Status viene visualizzato il tipo di porta LAN e le caratteristiche del collegamento configurati nell'area Administrative Settings. Se durante la configurazione o la negoziazione automatica le impostazioni vengono modificate, è possibile fare clic su **Refresh** per visualizzare le ultime impostazioni.

PASSAGGIO 2 Attivare o disattivare la funzione **Auto Negotiation**.

- Se attivata, viene eseguita una negoziazione fra la porta e il suo partner di collegamento per impostare la velocità di connessione massima e la modalità duplex.
- Se è disattivata, è possibile configurare manualmente la velocità della porta e la modalità duplex.

PASSAGGIO 3 Se la negoziazione automatica è disattivata, selezionare un valore nel campo **Port Speed** (10/100/1000 Mb/s) e la modalità duplex (half-duplex o full-duplex).

PASSAGGIO 4 Attivare o disattivare la modalità Green Ethernet. Se attivata, il dispositivo WAP entra automaticamente in modalità a risparmio energetico in caso di assenza di energia sulla linea e riprende il funzionamento normale quando viene rilevata energia.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Impostazioni dell'indirizzo IPv4 e della VLAN

È possibile utilizzare la pagina VLAN and IPv4 Address Settings per configurare le impostazioni dell'interfaccia LAN, compresa l'assegnazione di un indirizzo IPv4 statico o dinamico.

Per configurare le impostazioni LAN, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'area di navigazione, selezionare **LAN** > **VLAN and IPv4 Address**.

Nella pagina vengono mostrare le impostazioni generali e le impostazioni IPv4. Nell'area Global Settings viene mostrato l'indirizzo MAC della porta di interfaccia LAN. Il campo è di sola lettura.

PASSAGGIO 2 Configurare le impostazioni generali seguenti:

- **Untagged VLAN**: consente di attivare o disattivare i tag della VLAN. Se la casella è attivata (impostazione predefinita), tutto il traffico sarà contrassegnato con un ID VLAN.

  Tutto il traffico dell'access point utilizza per impostazione predefinita la VLAN 1, la VLAN predefinita senza tag. Ciò significa che se la VLAN senza tag non viene disattivata e non vengono modificati l'ID VLAN del traffico senza tag o l'ID VLAN di un VAP o il client che utilizza RADIUS, tutto il traffico non presenterà alcun tag.

- **Untagged VLAN ID**: indica un numero da 1 a 4094 per l'ID VLAN senza tag. Il valore predefinito è 1. Quando viene inoltrato alla rete, il traffico sulla VLAN specificato in questo campo non viene contrassegnato con un ID VLAN.

  VLAN 1 coincide sia con la VLAN senza tag predefinita che con la VLAN di gestione predefinita. Se si desidera separare il traffico di gestione dal traffico VLAN senza tag, configurare il nuovo ID VLAN sul router, quindi utilizzare il nuovo ID VLAN sul dispositivo WAP.

- **Management VLAN ID**: la VLAN associata all'indirizzo IP utilizzato per accedere al dispositivo WAP. Immettere un numero da 1 a 4094 per l'ID VLAN di gestione. Il valore predefinito è 1.

  Questa VLAN è anche la VLAN senza tag predefinita. Se sulla rete è già stata configurata una VLAN di gestione con un ID VLAN diverso, è necessario modificare l'ID VLAN della VLAN di gestione sul dispositivo WAP.

PASSAGGIO 3 Configurare le impostazioni IPv4 seguenti:

- **Connection Type**: per impostazione predefinita, il client DHCP dell'access point Cisco WAP551 e WAP561 trasmette automaticamente le richieste relative alle informazioni di rete. Se si desidera utilizzare un indirizzo IP statico, è necessario disabilitare il client DHCP e configurare manualmente l'indirizzo IP e le altre informazioni di rete.

  Selezionare uno dei valori seguenti dall'elenco:

  - **DHCP**: il dispositivo WAP acquisisce l'indirizzo IP da un server DHCP sulla LAN.
  - **Static IP**: viene configurato manualmente l'indirizzo IPv4, il cui formato deve essere simile a xxx.xxx.xxx.xxx (192.0.2.10).

- **Static IP Address, Subnet Mask, and Default Gateway**: se si intende assegnare un indirizzo IP statico, immettere le informazioni IP.

- **Domain Name Servers**: selezionare un'opzione dall'elenco:

  - **Dynamic**: il dispositivo WAP acquisisce gli indirizzi dei server DNS da un server DHCP sulla LAN.
  - **Manual**: vengono configurati manualmente uno o più indirizzi del server DNS. Immettere fino a due indirizzi IP nelle caselle di testo.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Indirizzi IPv6

È possibile utilizzare la pagina IPv6 Addresses per configurare il dispositivo WAP e utilizzare gli indirizzi IPv6.

Per configurare le impostazioni degli indirizzi IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'area di navigazione, selezionare **LAN** > **IPv6 Addresses**.

PASSAGGIO 2 Configurare le seguenti impostazioni:

- **IPv6 Connection Type**: scegliere il metodo di acquisizione dell'indirizzo IPv6 da parte del dispositivo WAP:
  - **DHCPv6**: l'indirizzo IPv6 viene assegnato da un server DHCPv6.
  - **Static IPv6**: viene configurato manualmente l'indirizzo IPv6, il cui formato deve essere simile a xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).
- **IPv6 Administration Mode**: consente l'accesso alla gestione di IPv6.
- **IPv6 Auto Configuration Administration Mode**: consente la configurazione automatica dell'indirizzo IPv6 sul dispositivo WAP.

  Se è attivata, il dispositivo WAP acquisisce il gateway e gli indirizzi IPv6 elaborando gli annunci del router ricevuti sulla porta LAN. Il dispositivo WAP può avere più indirizzi IPv6 configurati automaticamente.
- **Static IPv6 Address**: l'indirizzo IPv6 statico. Il dispositivo WAP può avere un indirizzo IPv6 statico anche se gli indirizzi sono già stati configurati automaticamente.
- **Static IPv6 Address Prefix Length**: la lunghezza del prefisso dell'indirizzo statico, che corrisponde a un numero intero compreso nell'intervallo da 0 a 128. Il valore predefinito è 0.
- **Static IPv6 Address Status**: visualizza uno dei seguenti valori:
  - **Operational**: l'indirizzo IP è stato verificato come univoco sulla LAN e può essere utilizzato nell'interfaccia.
  - **Tentative**: quando viene assegnato un indirizzo IP, il dispositivo WAP avvia automaticamente una procedura di rilevamento degli indirizzi duplicati (DAD, Duplicate Address Detection). Durante la verifica dell'univocità dell'indirizzo IPv6 sulla rete, lo stato è "provvisorio". Tale stato non consente l'utilizzo dell'indirizzo IPv6 per trasmettere o ricevere traffico ordinario.

  - **Vuoto (nessun valore)**: non viene assegnato alcun indirizzo IP oppure l'indirizzo assegnato non è operativo.

- **IPv6 Autoconfigured Global Addresses**: vengono elencati gli indirizzi IPv6 eventualmente assegnati automaticamente al dispositivo WAP.
- **IPv6 Link Local Address**: l'indirizzo IPv6 utilizzato dal collegamento fisico locale. Questo indirizzo non può essere configurato e viene assegnato tramite la procedura di rilevamento degli indirizzi IPv6 adiacenti.
- **Default IPv6 Gateway**: il gateway IPv6 predefinito configurato in modo statico.
- **IPv6 DNS Nameservers**: selezionare uno dei seguenti valori:
  - **Dynamic**: i server dei nomi DNS vengono acquisiti in modo dinamico tramite DHCPv6.
  - **Manual**: specificare fino a due server dei nomi DNS IPv6 nei rispettivi campi.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Tunnel IPv6

I dispositivi WAP551 e WAP561 supportano il protocollo ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), che consente al dispositivo WAP di trasmettere tramite LAN i pacchetti IPv6 incapsulati nei pacchetti IPv4. Questo protocollo permette al dispositivo WAP di comunicare con gli host IPv6 remoti anche quando la LAN che li collega non supporta IPv6.

Il dispositivo WAP funge anche da client ISATAP. È necessario che nella LAN sia presente un host o un router ISATAP. L'indirizzo IP o il nome host del router viene configurato sul dispositivo WAP (per impostazione predefinita, è isatap). Se è configurato come nome host, il dispositivo WAP comunica con un server DNS per risolvere il nome in uno o più indirizzi di router ISATAP. In seguito, il dispositivo WAP

invia messaggi di sollecitazione al router. Quando un router ISATAP risponde con un messaggio di annuncio, il router e il dispositivo WAP stabiliscono il tunnel. All'interfaccia tunnel vengono assegnati un indirizzo del collegamento locale e un indirizzo IPv6 globale, che fungono da interfacce IPv6 virtuali sulla rete IPv4.

Quando gli host IPv6 avviano la comunicazione con il dispositivo WAP connesso tramite il router ISATAP, i pacchetti IPv6 vengono incapsulati nei pacchetti IPv4 dal router ISATAP.

Per configurare un tunnel IPv6 tramite ISATAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'area di navigazione, selezionare **LAN** > **IPv6 Tunnel**.

PASSAGGIO 2 Configurare i seguenti parametri:

- **ISATAP Status**: consente di attivare o disattivare la modalità amministrativa di ISATAP sul dispositivo WAP.
- **ISATAP Capable Host**: il nome DNS o l'indirizzo IP del router ISATAP. Il valore predefinito è isatap.
- **ISATAP Query Interval**: specifica la frequenza con cui il dispositivo WAP dovrebbe inviare le query al server DNS per tentare di risolvere il nome host ISATAP in un indirizzo IP. Il dispositivo WAP invia le query DNS solo se l'indirizzo IP di un router ISATAP risulta sconosciuto. L'intervallo valido è compreso tra 120 e 3600 secondi.
- **ISATAP Solicitation Interval**: specifica la frequenza con cui il dispositivo WAP dovrebbe inviare messaggi di richiesta del router ai router ISATAP di cui viene a conoscenza tramite i messaggi di query DNS. Il dispositivo WAP invia messaggi di richiesta del router solo in assenza di router ISATAP attivi. L'intervallo valido è compreso tra 120 e 3600 secondi.

PASSAGGIO 3 Fare clic su **Salva**. Le impostazioni vengono salvate nella configurazione di avvio.

Una volta stabilito il tunnel, nella pagina vengono visualizzati l'**indirizzo locale del collegamento IPv6 ISATAP** e l'**indirizzo globale IPv6 ISATAP**. Sono indirizzi di interfacce IPv6 virtuali sulla rete IPv4.

5

Wireless

In questo capitolo viene descritto come configurare le proprietà del funzionamento delle interfacce radio wireless.

Vengono trattati i seguenti argomenti:

- **Radio**
- **Rilevamento di AP non autorizzati**
- **Reti**
- **Strumento di programmazione**
- **Associazione dello strumento di programmazione**
- **Utilizzo della larghezza di banda**
- **Filtraggio MAC**
- **Bridge WDS**
- **WorkGroup Bridge**
- **QoS**
- **Configurazione WPS**
- **Processo WPS**

Radio

Le impostazioni radio controllano direttamente il comportamento dell'interfaccia radio nel dispositivo WAP e la sua interazione con il supporto fisico, ovvero il tipo di segnale emesso dal dispositivo WAP e il metodo di emissione.

Per configurare le impostazioni radio, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **Radio**.

PASSAGGIO 2 Nell'area Global Settings, configurare il campo **TSPEC Violation Interval**, ovvero l'intervallo di tempo in secondi entro il quale il dispositivo WAP deve segnalare i client associati che non sono conformi alle procedure obbligatorie di controllo delle ammissioni. La segnalazione avviene attraverso il log di sistema e i trap SNMP. Immettere un valore compreso tra 0 e 900 secondi. L'impostazione predefinita è 300 secondi.

PASSAGGIO 3 Per i dispositivi WAP561, selezionare l'interfaccia **Radio** da configurare (Radio 1 o Radio 2).

PASSAGGIO 4 Nella sezione Basic Settings, configurare le seguenti impostazioni:

NOTA Le normative locali potrebbero vietare l'uso di determinate modalità radio. Non tutte le modalità sono disponibili in tutti i Paesi. Inoltre, per il dispositivo WAP561 a doppia radio, l'interfaccia Radio 1 supporta la banda a 2,4 GHz (opzione predefinita) oppure quella a 5 GHz, mentre l'interfaccia Radio 2 supporta soltanto la banda 5 GHz. La singola radio sul dispositivo WAP551 può supportare una qualunque delle due bande.

- **Radio**: attiva o disattiva l'interfaccia radio. Questa interfaccia è disattivata per impostazione predefinita.
- **MAC Address**: immettere l'indirizzo MAC (Media Access Control) dell'interfaccia. L'indirizzo MAC è assegnato dal produttore e non è possibile modificarlo.
- **Mode**: lo standard IEEE 802.11 e la frequenza utilizzata dall'interfaccia radio. Per ciascuna interfaccia radio, selezionare una delle modalità disponibili:
  - 802.11a: soltanto i client 802.11a possono collegarsi al dispositivo WAP.
  - 802.11b/g: soltanto i client 802.11b e 802.11g possono collegarsi al dispositivo WAP.
  - 802.11a/n: i client 802.11a e 802.11n che operano nella frequenza 5 GHz possono collegarsi al dispositivo WAP.
  - 802.11b/g/n (predefinito): i client 802.11b, 802.11g e 802.11n che operano nella frequenza 2,4 GHz possono collegarsi al dispositivo WAP.
  - 5 GHz 802.11n: solo i client 802.11n che operano nella frequenza 5 GHz possono collegarsi al dispositivo WAP.

  - 2,4 GHz 802.11n: solo i client 802.11n che operano nella frequenza 2,4 GHz possono collegarsi al dispositivo WAP.

- **Channel Bandwidth**: la specifica 802.11n consente un canale a 20/40 MHz coesistente oltre al canale a 20 MHz disponibile con altri modelli precedenti. Il canale a 20/40 MHz consente velocità di trasmissione dei dati superiori, ma lascia a disposizione un minor numero di canali per l'uso da parte di altri dispositivi a 2,4 GHz e 5 GHz.

  Per impostazione predefinita, se la modalità radio include 802.11n, la larghezza di banda del canale è impostata su 20/40 MHz per attivare entrambe le larghezze di canale. Impostare il campo su 20 MHz per limitare l'uso della larghezza di banda a un canale a 20 MHz.

- **Primary Channel** (soltanto modalità 802.11n con larghezza di banda a 20/40 MHz): un canale a 40 MHz può essere considerato come due canali contigui a 20 MHz nel dominio di frequenza. Questi due canali a 20 MHz sono spesso definiti come canale primario e secondario. Il canale primario è utilizzato per i client 802.11n che supportano soltanto una larghezza di banda del canale a 20 MHz e per i client di vecchia generazione.

  Selezionare una delle seguenti opzioni:

  - **Upper**: imposta il canale primario come canale 20 MHz superiore nella banda 40 MHz.
  - **Lower**: imposta il canale primario come canale 20 MHz inferiore nella banda 40 MHz. Questa è l'opzione predefinita.

- **Channel**: la parte dello spettro radio utilizzato per trasmettere e ricevere dati.

  La gamma di canali disponibili è determinata dalla modalità dell'interfaccia radio e dall'impostazione del codice paese. Se per l'impostazione del canale si seleziona **Auto**, il dispositivo WAP esamina i canali disponibili e seleziona il canale in cui rileva la minore quantità di traffico.

  Ciascuna modalità offre un numero di canali a seconda delle licenze dello spettro da parte delle autorità nazionali e transnazionali, quali la Federal Communications Commission (FCC) o l'International Telecommunication Union (ITU-R).

PASSAGGIO 5 Nella sezione Advanced Settings, configurare le seguenti opzioni:

- **Short Guard Interval Supported**: questo campo è disponibile soltanto se la modalità radio selezionata include 802.11n.

  L'intervallo di guardia è il tempo morto, espresso in nanosecondi, tra simboli OFDM. L'intervallo di guardia impedisce l'interferenza inter-simbolo e inter-carrier (ISI, ICI). La modalità 802.11n consente una riduzione in questo intervallo di guardia rispetto alla definizione a e g da 800 a 400 nanosecondi. La riduzione dell'intervallo di guardia può consentire un miglioramento del 10% nel throughput dei dati.

  Anche il client con il quale il dispositivo WAP sta comunicando deve supportare l'intervallo di guardia breve.

  Selezionare una delle seguenti opzioni:

  - **Yes**: il dispositivo WAP trasmette dati utilizzando un intervallo di guardia di 400 nanosecondi quando comunica con client che supportano anch'essi l'intervallo di guardia breve. Questa è l'impostazione predefinita.
  - **No**: il dispositivo WAP trasmette dati utilizzando un intervallo di guardia di 800 nanosecondi.

- **Protection**: la funzionalità di protezione contiene regole per garantire che le trasmissioni 802.11 non causino interferenze con stazioni o applicazioni di vecchia generazione. La protezione è attiva per impostazione predefinita (Auto). Con questa opzione attiva, verrà richiesta la protezione se dispositivi di vecchia generazione rientrano nell'intervallo del dispositivo WAP.

  È possibile disattivare la protezione (Off); tuttavia, i client o i dispositivi WAP di vecchia generazione nell'intervallo saranno influenzati dalle trasmissioni 802.11n. La protezione è disponibile anche quando è attiva la modalità 802.11b/g. In questo caso vengono protetti i client e i dispositivi WAP 802.11b dalle trasmissioni 802.11g.

  NOTA Questa impostazione non influenza la capacità del client di effettuare l'associazione al dispositivo WAP.

- **Beacon Interval**: l'intervallo tra due trasmissioni di frame beacon. Il dispositivo WAP trasmette questi frame a intervalli regolari per annunciare l'esistenza della rete wireless. Per impostazione predefinita viene inviato un frame beacon ogni 100 millisecondi (o 10 al secondo).

  Immettere un numero intero compreso tra 20 e 2000 millisecondi. L'intervallo predefinito è di 100 millisecondi.

- **DTIM Period**: il periodo DTIM (Delivery Traffic Indication Map). Immettere un numero intero compreso tra 1 e 255 beacon. Il valore predefinito è 2 beacon.

  Il messaggio DTIM è un elemento incluso in alcuni frame beacon. Indica per quali stazioni client, attualmente in modalità di sospensione a risparmio energetico, sono presenti dati nel buffer del dispositivo WAP in attesa di essere prelevati.

  Il periodo DTIM specificato indica la frequenza con la quale i client associati al dispositivo WAP devono controllare i dati presenti nel buffer del dispositivo WAP in attesa di essere prelevati.

  I dati vengono misurati in beacon. Ad esempio, se si imposta questo campo su 1, i client controllano i dati presenti nel buffer del dispositivo WAP a ogni beacon. Se si imposta questo campo su 10, i client effettuano il controllo ogni 10 beacon.

- **Fragmentation Threshold**: la soglia di dimensioni del frame espressa in byte. Immettere in questo campo un numero intero valido pari e compreso tra 256 e 2346. Il valore predefinito è 2346.

  La soglia di frammentazione rappresenta un modo per limitare le dimensioni dei pacchetti (frame) trasmessi sulla rete. Se un pacchetto supera la soglia, viene attivata la funzione di frammentazione e il pacchetto viene inviato sotto forma di più frame 802.11.

  Se il pacchetto trasmesso non supera la soglia impostata, la funzione di frammentazione non viene utilizzata. L'impostazione della soglia sul valore massimo (2346 byte, l'impostazione predefinita) consente di disattivare la frammentazione.

  La frammentazione comporta un maggiore sovraccarico sia a causa del lavoro aggiuntivo richiesto, legato alla divisione e al riassemblaggio dei frame, sia per l'aumento del traffico di messaggi sulla rete. Tuttavia, la frammentazione, se configurata correttamente, può contribuire a migliorare le prestazioni di rete e l'affidabilità.

  L'invio di frame più piccoli, utilizzando una soglia di frammentazione inferiore, aiuta a evitare alcuni problemi di interferenza, ad esempio con i forni microonde.

  La frammentazione è disattivata per impostazione predefinita. Si raccomanda di utilizzare la frammentazione solo se si sospetta che siano presenti interferenze radio. Le intestazioni aggiuntive applicate a ciascun frammento aumentano il sovraccarico sulla rete e possono ridurre notevolmente il throughput.

- **RTS Threshold**: valore della soglia RTS (Request to Send). Immettere un numero intero valido compreso tra 0 e 2347. Il valore predefinito è 2347 ottetti.

  La soglia RTS indica il numero di ottetti in un MPDU al di sotto del quale non viene eseguito l'handshake RTS/CTS.

  La modifica della soglia RTS può contribuire a controllare il flusso di traffico attraverso il dispositivo WAP, soprattutto in caso di molti client. Se si specifica un valore di soglia basso, i pacchetti RTS vengono inviati con maggiore frequenza, consumando maggiore larghezza di banda e riducendo il throughput del pacchetto. Tuttavia, l'invio di più pacchetti RTS può favorire il recupero della rete dopo interferenze o collisioni che possono verificarsi su una rete occupata o con interferenze elettromagnetiche.

- **Maximum Associated Clients**: il numero massimo di stazioni che possono accedere a ciascuna interfaccia radio del dispositivo WAP in qualsiasi momento. È possibile immettere un numero intero compreso tra 0 e 200. L'impostazione predefinita è 200 stazioni. Di conseguenza, il dispositivo WAP551 a singola radio può supportare fino a 200 client, mentre il dispositivo WAP561 a doppia radio può supportare un totale di 400 client.

- **Transmit Power**: un valore percentuale per il livello di potenza di trasmissione del dispositivo WAP.

  Il valore predefinito di 100% è più efficiente in termini di costo rispetto a una percentuale inferiore poiché consente al dispositivo WAP di ottenere la massima distanza di trasmissione e riduce il numero di access point necessari.

  Per aumentare la capacità della rete, posizionare i dispositivi WAP più vicini tra loro e ridurre il valore della potenza di trasmissione. Ciò contribuisce a ridurre la sovrapposizione e l'interferenza tra access point. L'impostazione di una potenza di trasmissione inferiore può inoltre rendere più sicura la rete poiché è meno probabile che segnali wireless più deboli vengano propagati al di fuori della posizione fisica della rete.

  Alcune combinazioni di intervalli di canali e codici Paese hanno una potenza di trasmissione massima relativamente bassa. Se si cerca di impostare una potenza di trasmissione su intervalli inferiori, ad esempio 25% o 12%, il calo atteso nella potenza potrebbe non verificarsi poiché alcuni amplificatori di potenza hanno requisiti di potenza di trasmissione minima.

- **Fixed Multicast Rate**: la velocità di trasmissione in Mbps per i pacchetti multicast e broadcast. Questa impostazione può essere utile negli ambienti in cui si verifica streaming video multicast wireless, a condizione che i client wireless siano in grado di gestire la velocità configurata.

  Se si seleziona l'impostazione **Auto**, il dispositivo WAP sceglie la velocità migliore per i client associati. L'intervallo di valori validi è determinato dalla modalità radio configurata.

- **Legacy Rate Sets**: le velocità sono espresse in megabit al secondo.

  Il campo Supported Rate Sets indica le velocità supportate dal dispositivo WAP. È possibile selezionare più velocità; selezionare la casella di una velocità per attivarla o disattivarla. Il dispositivo WAP sceglie automaticamente la velocità più efficiente in base a fattori quali frequenze di errore e distanza delle stazioni client dal dispositivo WAP.

  Il campo Basic Rate Sets indica le velocità che il dispositivo WAP dichiara alla rete per impostare la comunicazione con altri access point e stazioni client sulla rete. È generalmente più efficiente avere un dispositivo WAP che trasmette un subset di velocità supportate.

- **MCS (Data Rate) Settings**: i valori dell'indice MCS (Modulation and Coding Scheme) dichiarati dal dispositivo WAP. MCS può potenziare il throughput per i client wireless 802.11n.

  Selezionare la casella sotto il numero dell'indice MCS per attivarlo oppure deselezionarla per disattivarlo. Non è possibile disattivare tutti gli indici contemporaneamente.

  Il dispositivo WAP supporta gli indici MCS da 0 a 23. L'indice MSC 23 consente una velocità di trasmissione massima di 450 Mbps. Se non viene selezionato alcun indice MCS, l'interfaccia radio funziona all'indice MCS 0, che consente una velocità di trasmissione massima di 15 Mbps.

  È possibile configurare le impostazioni MCS soltanto se la modalità radio include il supporto 802.11n.

- **Broadcast/Multicast Rate Limiting**: la limitazione della velocità multicast e broadcast può migliorare le prestazioni di rete generali limitando il numero di pacchetti trasmessi sulla rete.

  La limitazione della velocità di multicast/broadcast è disattivata per impostazione predefinita. I campi seguenti diventano disponibili solo dopo aver attivato la limitazione della velocità di multicast/broadcast.

- **Rate Limit**: il limite di velocità per il traffico multicast e broadcast. Il limite deve essere maggiore di 1, ma minore di 50 pacchetti al secondo. Il traffico al di sotto di tale limite di velocità sarà sempre conforme e sarà trasmesso alla destinazione appropriata. L'impostazione predefinita è di 50 pacchetti al secondo, ovvero il valore massimo.
- **Rate Limit Burst**: la quantità di traffico, misurato in byte, consentito nella trasmissione di un burst temporaneo, anche se supera la velocità massima specificata. L'impostazione predefinita è di 75 pacchetti al secondo, ovvero il valore massimo.

- **TSPEC Mode**: regola la modalità TSPEC generale del dispositivo WAP. La modalità TSPEC è disattivata per impostazione predefinita. Sono disponibili le seguenti opzioni:
  - **On**: il dispositivo WAP gestisce le richieste TSPEC in base alle impostazioni TSPEC configurate nella pagina Radio. Utilizzare questa impostazione se il dispositivo WAP gestisce il traffico da dispositivi che supportano il servizio QoS, ad esempio un telefono con certificazione Wi-Fi.
  - **Off**: il dispositivo WAP ignora le richieste TSPEC dalle stazioni client. Selezionare questa opzione se non si desidera utilizzare TSPEC per assegnare ai dispositivi che supportano il servizio QoS la priorità per il traffico con esigenze temporali.
- **TSPEC Voice ACM Mode**: regola le procedure obbligatorie di controllo delle ammissioni (ACM) per la categoria di accesso vocale. La modalità TSPEC Voice ACM è disattivata per impostazione predefinita. Sono disponibili le seguenti opzioni:
  - **On**: per poter ricevere o inviare un flusso di traffico vocale, è necessario che una stazione invii una richiesta TSPEC di larghezza di banda al dispositivo WAP. Il dispositivo WAP risponde con il risultato della richiesta, che include il tempo medio assegnato se è stata ammessa la TSPEC.
  - **Off**: una stazione può inviare e ricevere traffico vocale prioritario senza richiedere una TSPEC ammessa; il dispositivo WAP ignora le richieste TSPEC vocali provenienti dalle stazioni client.
- **TSPEC Voice ACM Limit**: il limite massimo della quantità di traffico che il dispositivo WAP tenta di trasmettere sul supporto wireless utilizzando un AC vocale per ottenere l'accesso. Il limite predefinito è pari al 20% del traffico totale.

- **TSPEC Video ACM Mode**: regola le procedure obbligatorie di controllo delle ammissioni per la categoria di accesso video. La modalità TSPEC Video ACM è disattivata per impostazione predefinita. Sono disponibili le seguenti opzioni:
  - **On**: per poter ricevere o inviare un flusso di traffico video, è necessario che una stazione invii una richiesta TSPEC di larghezza di banda al dispositivo WAP. Il dispositivo WAP risponde con il risultato della richiesta, che include il tempo medio assegnato se è stata ammessa la TSPEC.
  - **Off**: una stazione può inviare e ricevere traffico video prioritario senza richiedere una TSPEC ammessa; il dispositivo WAP ignora le richieste TSPEC video provenienti dalle stazioni client.
- **TSPEC Video ACM Limit**: il limite massimo della quantità di traffico che il dispositivo WAP tenta di trasmettere sul supporto wireless utilizzando un AC video per ottenere l'accesso. Il limite predefinito è pari al 15% del traffico totale.
- **TSPEC AP Inactivity Timeout**: l'intervallo di inattività su un dispositivo WAP dopo il quale una specifica del traffico downlink viene eliminata. È possibile immettere un numero intero compreso tra 0 e 120 secondi; il valore predefinito è 30 secondi.
- **TSPEC Station Inactivity Timeout**: l'intervallo di inattività su un dispositivo WAP dopo il quale una specifica del traffico uplink viene eliminata. È possibile immettere un numero intero compreso tra 0 e 120 secondi; il valore predefinito è 30 secondi.
- **TSPEC Legacy WMM Queue Map Mode**: attiva o disattiva la presenza di traffico precedente sulle code che operano come ACM. Questa modalità è disattivata per impostazione predefinita.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

ATTENZIONE Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Rilevamento di AP non autorizzati

Un AP non autorizzato è un access point che è stato installato su una rete sicura senza l'autorizzazione esplicita di un amministratore di sistema. Gli access point non autorizzati rappresentano una minaccia per la sicurezza poiché chiunque abbia accesso alla postazione può installare in maniera inconsapevole o con intenti malevoli un dispositivo WAP wireless poco costoso che potrebbe consentire a utenti non autorizzati di accedere alla rete.

Il dispositivo WAP esegue una scansione RF su tutti i canali di ciascuna interfaccia radio per rilevare tutti gli AP nelle vicinanze della rete. Eventuali AP non autorizzati rilevati vengono mostrati nella pagina Rogue AP Detection. Se un AP indicato come non autorizzato è legittimo, è possibile aggiungerlo all'elenco di AP noti.

NOTA L'elenco degli AP non autorizzati rilevati e quello degli AP attendibili forniscono informazioni che è possibile utilizzare per adottare ulteriori misure. L'AP non ha alcun controllo sugli AP non autorizzati inclusi negli elenchi e non può applicare criteri di protezione agli AP rilevati attraverso la scansione RF.

Se il rilevamento degli AP è attivato, l'interfaccia radio passa periodicamente dal canale operativo alla scansione degli altri canali nella stessa banda.

È possibile attivare e disattivare il rilevamento degli AP non autorizzati. Per attivare la raccolta di informazioni sugli AP non autorizzati attraverso l'interfaccia radio, fare clic su **Enable** accanto ad **AP Detection** per Radio 1 (o Radio 2 sui dispositivi WAP561), quindi fare clic su **Salva**.

Vengono visualizzate informazioni sugli access point rilevati e non autorizzati attendibili. È possibile fare clic su **Refresh** per aggiornare la schermata e mostrare le informazioni attuali:

- **Action**: se l'AP si trova nell'elenco degli AP non autorizzati rilevati, fare clic su **Trust** per spostarlo nell'elenco degli AP attendibili.

  Se l'AP si trova nell'elenco degli AP attendibili, fare clic su **Untrust** per spostarlo in quello degli AP rilevati non autorizzati.

  NOTA L'elenco degli AP rilevati non autorizzati e quello degli AP attendibili forniscono varie informazioni. Il dispositivo WAP non ha alcun controllo sugli AP inclusi nell'elenco e non può applicare criteri di protezione agli AP rilevati attraverso la scansione RF.

- **Indirizzo MAC:** l'indirizzo MAC dell'AP non autorizzato.

- **Beacon Interval**: l'intervallo di frequenza del beacon utilizzato dall'AP non autorizzato.

I frame beacon vengono trasmessi da un AP a intervalli regolari per annunciare l'esistenza della rete wireless. Per impostazione predefinita viene inviato un frame beacon ogni 100 millisecondi (o 10 al secondo).

NOTA L'intervallo beacon viene impostato nella pagina **Radio**.

- **Tipo**: il tipo di dispositivo:
  - AP indica che il dispositivo non autorizzato è un AP che supporta gli standard IEEE 802.11 per reti wireless in modalità Infrastructure.
  - Ad hoc indica una stazione non autorizzata in modalità Ad hoc. Le stazioni impostate sulla modalità Ad hoc comunicano direttamente, senza l'utilizzo di un AP tradizionale. La modalità ad hoc è un framework per reti wireless IEEE 802.11 noto anche come modalità peer-to-peer o IBSS (Independent Basic Service Set).
- **SSID**: il SSID (Service Set Identifier) del dispositivo WAP.

  Il SSID è una stringa alfanumerica di un massimo di 32 caratteri che identifica in modo univoco una LAN wireless. Viene chiamato anche nome di rete.
- **Privacy**: indica se sul dispositivo non autorizzato sono disponibili opzioni di protezione:
  - Off indica che la modalità di protezione sul dispositivo non autorizzato è impostata su None (nessuna protezione).
  - On indica che sul dispositivo non autorizzato sono presenti alcune opzioni di protezione.

  NOTA È possibile utilizzare la pagina **Reti** per configurare le opzioni di protezione sull'AP.
- **WPA**: determina se la protezione WPA è attivata o disattivata per l'AP non autorizzato.
- **Band**: la modalità IEEE 802.11 utilizzata sull'AP non autorizzato, ad esempio IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.

  Il numero visualizzato indica la modalità:
  - 2.4 indica la modalità IEEE 802.11b, 802.11g o 802.11n (o una combinazione di modalità).
  - 5 indica la modalità IEEE 802.11a o 802.11n (o entrambe le modalità).
- **Channel**: il canale su cui l'AP non autorizzato sta trasmettendo.

Il canale definisce la parte dello spettro radio utilizzata dall'interfaccia radio per trasmettere e ricevere dati.

NOTA Utilizzare la pagina **Radio** per impostare il canale.

- **Rate**: la velocità in megabit al secondo alla quale l'AP non autorizzato sta trasmettendo.

  La velocità attuale è sempre una delle velocità indicate nella casella Supported Rates.

- **Signal**: l'intensità del segnale radio emesso dall'AP non autorizzato. Se si posiziona il puntatore del mouse sulle barre, viene visualizzato un numero che rappresenta la forza in decibel (dB).

- **Beacon**: il numero totale di beacon ricevuti dall'AP non autorizzato a partire dalla prima rilevazione.

- **Last Beacon**: data e ora dell'ultimo beacon ricevuto dall'AP non autorizzato.

- **Rates**: velocità supportate e di base (dichiarate) per l'AP non autorizzato. Le velocità sono indicate in megabit al secondo (Mbps).

  Sono elencate tutte le velocità supportate, con quelle di base in grassetto. Le velocità vengono definite nella pagina **Radio**.

Per creare un elenco di AP attendibili e salvarlo in un file, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'elenco degli AP rilevati non autorizzati, fare clic su **Trust** per gli AP noti. Gli AP attendibili vengono spostati nel relativo elenco.

PASSAGGIO 2 Nell'area Download/Backup Trusted AP List, selezionare **Backup (AP to PC)**.

PASSAGGIO 3 Fare clic su **Salva**.

L'elenco contiene gli indirizzi MAC di tutti gli AP che sono stati aggiunti all'elenco di AP noti. Il nome del file è Rogue2.cfg per impostazione predefinita. È possibile utilizzare un editor di testo o un browser Web per aprire il file e visualizzarne i contenuti.

È possibile importare un elenco di AP noti da un elenco salvato. L'elenco può essere acquisito da un altro AP o creato da un file di testo. Se l'indirizzo MAC di un AP è incluso nell'elenco degli AP attendibili, non viene rilevato come non autorizzato.

Per importare un elenco di AP da un file, attenersi alla seguente procedura:

PASSAGGIO 1 Nell'area Download/Backup Trusted AP List, selezionare **Download (PC to AP)**.

PASSAGGIO 2 Fare clic su **Sfoglia** per selezionare il file da importare.

Il file importato deve essere un file di testo normale con estensione .txt o .cfg. Le voci del file sono indirizzi MAC in formato esadecimale con ciascun ottetto separato da due punti, ad esempio 00:11:22:33:44:55. È necessario separare le voci con un solo spazio. Per poter essere accettato dall'AP, è necessario che il file contenga solo indirizzi MAC.

PASSAGGIO 3 Scegliere se sostituire l'elenco esistente di AP attendibili o aggiungere le voci nel file importato all'elenco stesso.

a. Selezionare **Sostituisci** per importare l'elenco e sostituire i contenuti dell'elenco di AP noti.

b. Selezionare **Unisci** per importare l'elenco e aggiungere gli AP nel file importato a quelli attualmente visualizzati nell'elenco degli AP noti.

PASSAGGIO 4 Fare clic su **Salva**.

Al termine dell'importazione, la schermata viene aggiornata e gli indirizzi MAC degli AP nel file importato vengono visualizzati nell'elenco degli AP noti.

Reti

I Virtual Access Point (VAP) segmentano la LAN wireless in più domini di trasmissione che sono l'equivalente wireless delle VLAN Ethernet. I VAP simulano più access point in un dispositivo WAP fisico. Il dispositivo WAP supporta fino a 16 VAP.

Ogni VAP può essere attivato o disattivato in modo indipendente, ad eccezione del VAP0, ovvero l'interfaccia radio fisica, che resta attiva fin quando la radio è attiva. Per disattivare il funzionamento di VAP0, è necessario disattivare l'interfaccia radio.

Ciascun VAP è identificato da un SSID (Service Set Identifier) configurato dall'utente. Non è possibile assegnare lo stesso nome SSID a più VAP. È possibile attivare o disattivare le trasmissioni SSID in modo indipendente su ogni VAP. La trasmissione SSID è attivata per impostazione predefinita.

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

Il SSID, che fa distinzione tra maiuscole e minuscole, è una voce alfanumerica costituita da un minimo di 2 a un massimo di 32 caratteri. Sono consentiti i caratteri stampabili più lo spazio (ASCII 0x20); i caratteri seguenti, invece, non sono consentiti:

?, ", $, [, \,] e +.

I seguenti caratteri sono consentiti:

ASCII 0x20, 0x21, 0x23, da 0x25 a 0x2A, da 0x2C a 0x3E, da 0x40 a 0x5A, da 0x5E a 0x7E.

Inoltre, i tre caratteri seguenti non possono essere utilizzati come primo carattere:

!, # e ; (ASCII 0x21, 0x23 e 0x3B rispettivamente).

Gli spazi iniziali e finali (ASCII 0x20) non sono consentiti.

NOTA Ciò significa che all'interno del SSID sono consentiti gli spazi, ma non come primo o ultimo carattere, e il punto "." (ASCII 0x2E) è consentito.

Ogni VAP è associato a una VLAN, identificata da un ID VLAN (VID). Un VID può essere un valore compreso tra 1 e 4094. I dispositivi WAP551 e WAP561 supporta 17 VLAN attive (16 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 predefinito senza tag. Se il VID di gestione è lo stesso del VID assegnato a un VAP, i client WLAN associati al VAP specifico potranno amministrare il dispositivo WAP. Se necessario, è possibile creare un elenco di controllo degli accessi (ACL) per disabilitare l'amministrazione da parte dei client WLAN.

Per configurare i VAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **Networks**.

PASSAGGIO 2 Per i dispositivi WAP561, selezionare l'interfaccia **Radio** su cui si desidera configurare i VAP (**Radio 1** o **Radio 2**).

PASSAGGIO 3 Selezionare la casella **Enabled** per il VAP che si desidera configurare.

—Oppure—

Se VAP0 è l'unico VAP configurato sul sistema e si desidera aggiungere un VAP, fare clic su **Aggiungi**. Quindi, selezionare il VAP e fare clic su **Modifica**.

PASSAGGIO 4 Configurare i seguenti parametri:

- **VLAN ID**: il VID della VLAN da associare al VAP.

ATTENZIONE Inserire un ID VLAN che sia configurato correttamente sulla rete. Se il VAP associa client wireless a una VLAN configurata in maniera errata possono verificarsi dei problemi di rete.
Quando un client wireless si connette al dispositivo WAP attraverso il VAP, il dispositivo WAP tagga tutto il traffico dal client wireless con l'ID VLAN inserito in questo campo a meno che si inserisca l'ID VLAN della porta o si utilizzi un server RADIUS per assegnare un client wireless a una VLAN. L'intervallo per l'ID VLAN è compreso tra 1 e 4094.

NOTA Se si modifica l'ID VLAN su un ID diverso dall'attuale ID VLAN di gestione, i client WLAN associati al VAP specifico non potranno amministrare il dispositivo. Verificare la configurazione degli ID VLAN di gestione e senza tag nella pagina LAN. Per ulteriori informazioni, vedere la sezione **Impostazioni dell'indirizzo IPv4 e della VLAN**.

- **SSID Name**: nome della rete wireless. Il SSID è una stringa alfanumerica costituita da massimo 32 caratteri. Selezionare un SSID univoco per ogni VAP.

  NOTA Se si è connessi come client wireless allo stesso dispositivo WAP che si sta amministrando, la reimpostazione del SSID causerà la perdita di connettività al dispositivo WAP. In questo caso sarà necessario riconnettersi al nuovo SSID dopo aver salvato la nuova impostazione.

- **Broadcast SSID**: attiva e disattiva la trasmissione del SSID.

  Specificare se consentire o meno al dispositivo WAP di trasmettere il SSID nei suoi frame beacon. Il parametro Broadcast SSID è attivato per impostazione predefinita. Quando il VAP non trasmette il suo SSID, il nome di rete non viene mostrato nell'elenco delle reti disponibili su una stazione client. In questo caso, è necessario immettere manualmente il nome di rete esatto nell'utilità di connessione wireless sul client in modo che possa connettersi.

La disattivazione della trasmissione del SSID impedisce che i client si connettano accidentalmente alla rete, ma non impedisce anche i più semplici tentativi da parte di un pirata informatico di connettersi o di monitorare il traffico non crittografato. L'eliminazione della trasmissione del SSID offre un livello minimo di protezione su una rete altrimenti esposta, ad esempio una rete guest, laddove è necessario semplificare in primo luogo la connessione per i client e non sono disponibili informazioni sensibili.

- **Security**: il tipo di autenticazione richiesta per l'accesso al VAP:
  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

  Se si seleziona una modalità di protezione diversa da None, saranno visualizzati campi aggiuntivi.

  NOTA Si raccomanda di utilizzare WPA Personal o WPA Enterprise come tipo di autenticazione poiché forniscono una maggiore protezione. Utilizzare Static WEP o Dynamic WEP soltanto per computer o dispositivi wireless di precedente generazione che non supportano WPA Personal/Enterprise. Se è necessario selezionare l'opzione Static WEP o Dynamic WEP, configurare la Radio in modalità 802.11a o 802.11b/g (vedere **Radio**). La modalità 802.11n limita l'utilizzo delle opzioni Static o Dynamic WEP come modalità di protezione.
- **MAC Filtering**: specifica se le stazioni che possono accedere a questo VAP sono limitate a un elenco globale configurato di indirizzi MAC. È possibile selezionare uno dei seguenti tipi di filtro MAC:
  - **Disabled**: non utilizzare il filtro MAC.
  - **Local**: utilizzare l'elenco di autenticazione MAC configurato nella pagina **Filtraggio MAC**.
  - **RADIUS**: utilizzare l'elenco di autenticazione MAC su un server RADIUS esterno.
- **Channel Isolation**: attiva e disattiva l'isolamento della stazione.
  - Se questa opzione è disattivata, i client wireless possono comunicare fra di loro normalmente inviando traffico attraverso il dispositivo WAP.

- Se attivata, il dispositivo WAP blocca la comunicazione tra i client wireless sullo stesso VAP. Il dispositivo WAP consente comunque il traffico dati tra i suoi client wireless e i dispositivi cablati sulla rete attraverso un collegamento WDS e con altri client wireless associati a un VAP diverso, ma non tra client wireless.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

ATTENZIONE Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

NOTA Per eliminare un VAP, selezionarlo e fare clic su **Elimina**. Per confermare l'eliminazione, fare clic su **Salva** al termine dell'operazione.

In queste sezioni vengono descritte le impostazioni di protezione che è possibile configurare a seconda dell'opzione selezionata nell'elenco Security della pagina Networks.

Se si seleziona **None** come modalità di protezione, non è possibile configurare altre impostazioni di protezione per il dispositivo WAP. In questo caso tutti i dati trasferiti da e verso il dispositivo WAP non sono crittografati. Questa modalità di protezione può essere utile durante la configurazione di rete iniziale o per la risoluzione dei problemi, ma non è raccomandata per l'uso regolare sulla rete interna poiché non è sicura.

Wired Equivalent Privacy (WEP) è un protocollo di crittografia dei dati per reti wireless 802.11. Tutte le stazioni e gli access point wireless della rete sono configurati con una chiave condivisa statica a 64 bit (chiave segreta da 40 bit + vettore di inizializzazione, VI, da 24 bit) o 128 bit (chiave segreta da 104 bit + vettore di inizializzazione, VI, da 24 bit) per la crittografia dei dati.

La modalità Static WEP non è l'opzione più sicura, ma offre maggiore protezione rispetto all'impostazione dell'opzione None (Plain-text), poiché impedisce che un soggetto esterno intercetti facilmente il traffico wireless non crittografato.

Il protocollo WEP crittografa i dati in movimento sulla rete wireless in base a una chiave statica. L'algoritmo di crittografia è una cifratura a flusso chiamata RC4.

I parametri per la configurazione della modalità Static WEP sono i seguenti:

- **Transfer Key Index**: un elenco dell'indice delle chiavi. Sono disponibili indici delle chiavi da 1 a 4. L'impostazione predefinita è 1.

  Il valore di questo campo indica la chiave WEP utilizzata dal dispositivo WAP per crittografare i dati trasmessi.

- **Key Length**: la lunghezza della chiave. Selezionare una delle opzioni seguenti:

  - 64 bit
  - 128 bit

- **Key Type**: il tipo di chiave. Selezionare una delle opzioni seguenti:

  - ASCII
  - Hex

- **WEP Keys**: è possibile specificare fino a quattro chiavi WEP. In ciascuna casella di testo, immettere una stringa di caratteri per ciascuna chiave. Le chiavi inserite dipendono dal tipo di chiave selezionata:

  - ASCII: include lettere alfabetiche maiuscole e minuscole, numeri e caratteri speciali quali @ e #.
  - Hex: include cifre comprese tra 0 e 9 e lettere dalla A alla F.

  Utilizzare lo stesso numero di caratteri per ogni chiave come specificato nel campo Characters Required. Si tratta delle chiavi WEP RC4 condivise con le stazioni che utilizzano il dispositivo WAP.

  È necessario configurare ogni stazione client per utilizzare una di queste chiavi WEP nello stesso slot come specificato sul dispositivo WAP.

- **Characters Required**: il numero di caratteri immessi nei campi WEP Key è determinato dalla lunghezza e dal tipo di chiave selezionata. Ad esempio, se si utilizzano chiavi ASCII a 128 bit, la chiave WEP deve contenere 26 caratteri. Il numero di caratteri obbligatori cambia automaticamente a seconda dell'impostazione della lunghezza e del tipo di chiave.

- **802.1X Authentication**: l'algoritmo di autenticazione definisce il metodo utilizzato per determinare se una stazione client ha l'autorizzazione a effettuare l'associazione con il dispositivo WAP quando è attiva la modalità di protezione Static WEP.

Per specificare l'algoritmo di autenticazione che si desidera utilizzare, scegliere una delle seguenti opzioni:

- **Open System**: l'autenticazione consente a qualsiasi stazione client di effettuare l'associazione con il dispositivo WAP indipendentemente dal fatto che la stazione client abbia o meno la chiave WEP corretta. Questo algoritmo è utilizzato nelle modalità di testo normale, IEEE 802.1X e WPA. Se l'algoritmo di autenticazione è impostato su Open System, qualsiasi client può effettuare l'associazione al dispositivo WAP.

  NOTA La possibilità di effettuare l'associazione, però, non garantisce che la stazione client possa scambiare dati con un dispositivo WAP. Per poter accedere e decodificare i dati dal dispositivo WAP e per trasmettere dati leggibili al dispositivo WAP, infatti, è necessario che una stazione disponga della chiave WEP corretta.

- Se si seleziona l'opzione **Shared Key**, la stazione client deve disporre della chiave WEP corretta per effettuare l'associazione al dispositivo WAP. Nella modalità Shared Key, una stazione con una chiave WEP errata non può effettuare l'associazione al dispositivo WAP.

- **Open System** e **Shared Key**. Se si selezionano entrambi gli algoritmi di autenticazione, le stazioni client configurate per l'utilizzo del protocollo WEP in modalità chiave condivisa devono avere una chiave WEP valida per poter effettuare l'associazione al dispositivo WAP. Le stazioni client configurate per l'utilizzo di WEP in modalità Open System (modalità Shared Key non attivata), invece, possono effettuare l'associazione al dispositivo WAP anche se non dispongono della chiave WEP corretta.

Se si utilizza l'impostazione Static WEP, vengono applicate le seguenti regole:

- Su tutte le stazioni client è necessario impostare la protezione LAN wireless (WLAN) su WEP e tutti i client devono disporre di una delle chiavi WEP specificate sul dispositivo WAP per decodificare le trasmissioni dati dall'AP alla stazione.
- Il dispositivo WAP deve avere tutte le chiavi utilizzate dai client per la trasmissione dalla stazione all'AP in modo che possa decodificare le trasmissioni della stazione.
- La stessa chiave deve occupare lo stesso slot su tutti i nodi (AP e client). Ad esempio, se il dispositivo WAP definisce la chiave abc123 come chiave WEP 3, tutte le stazioni client devono definire la stessa stringa come chiave WEP 3.

- Le stazioni client possono utilizzare chiavi diverse per trasmettere dati all'access point. In alternativa, possono utilizzare tutte la stessa chiave, ma tale impostazione è meno sicura poiché significa che una stazione può decodificare i dati inviati da un'altra.
- Su alcuni software client wireless, è possibile configurare più chiavi WEP e definire un indice di chiavi di trasferimento della stazione client e, successivamente, impostare le stazioni per crittografare i dati trasmessi utilizzando chiavi diverse. Ciò garantisce che gli access point vicini non possano decodificare le trasmissioni di altri access point.
- Non è possibile combinare chiavi WEP a 64 bit e 128 bit tra l'access point e le relativi stazioni client.

Dynamic WEP fa riferimento alla combinazione della tecnologia 802.1x e del protocollo Extensible Authentication Protocol (EAP). Con la modalità di protezione Dynamic WEP, le chiavi WEP vengono modificate dinamicamente.

I messaggi EAP sono inviati su una rete wireless IEEE 802.11 tramite un protocollo chiamato EAPOL (EAP Encapsulation Over LAN). IEEE 802.1X fornisce chiavi generate dinamicamente che vengono aggiornate periodicamente. Per crittografare il corpo del frame viene utilizzata una cifratura a flusso RC4 e il CRC (Cyclic Redundancy Checking) di ciascun frame 802.11.

Per questa modalità è necessario utilizzare un server RADIUS esterno per l'autenticazione degli utenti. Il dispositivo WAP richiede un server RADIUS che supporti EAP, ad esempio Microsoft Internet Authentication Server. Per lavorare con i client Microsoft Windows, il server di autenticazione deve supportare Protected EAP (PEAP) e MSCHAP V2.

È possibile utilizzare i vari metodi di autenticazione supportati dalla modalità IEEE 802.1X, inclusi certificati, il protocollo Kerberos e l'autenticazione con chiave pubblica. È necessario configurare le stazioni client per utilizzare lo stesso metodo di autenticazione utilizzato dal dispositivo WAP.

I parametri per la configurazione della modalità Dynamic WEP sono i seguenti:

- **Use Global RADIUS Server Settings**: per impostazione predefinita, ciascun VAP utilizza le impostazioni globali RADIUS definite per il dispositivo WAP (vedere **Server RADIUS**). Tuttavia, è possibile configurare ciascun VAP in modo da utilizzare una serie diversa di server RADIUS.

  Per utilizzare le impostazioni globali del server RADIUS, assicurarsi che questa casella sia selezionata.

Per utilizzare un server RADIUS separato per il VAP, deselezionare questa casella, quindi immettere l'indirizzo IP del server RADIUS e la chiave nei campi seguenti:

- **Server IP Address Type**: la versione IP utilizzata dal server RADIUS.

  È possibile alternare tipi di indirizzi diversi per configurare le impostazioni degli indirizzi globali RADIUS IPv4 e IPv6, ma il dispositivo WAP contatta soltanto i server RADIUS associati al tipo di indirizzo selezionato in questo campo.

- **Server IP Address 1** o **Server IPv6 Address 1**: l'indirizzo del server RADIUS primario per questo VAP.

  Quando il primo client wireless tenta di effettuare l'autenticazione con il dispositivo WAP, quest'ultimo invia una richiesta di autenticazione al server primario. Se il server primario risponde alla richiesta di autenticazione, il dispositivo WAP continua a utilizzare questo server RADIUS come server primario e le richieste di autenticazione sono inviate all'indirizzo specificato.

  L'indirizzo IPv4 deve essere nel formato seguente: xxx.xxx.xxx.xxx (192.0.2.10). L'indirizzo IPv6 deve essere nel formato seguente: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

- Da **Server IP Address 2** fino a **4** o da **Server IPv6 Address 2** fino a **4**: fino a tre indirizzi del server RADIUS di backup IPv4 o IPv6.

  Se l'autenticazione con il server primario ha esito negativo, si prova in sequenza con ciascun server di backup configurato.

- **Key**: la chiave segreta condivisa utilizzata dal dispositivo WAP per eseguire l'autenticazione con il server primario RADIUS.

  È possibile immettere massimo 63 caratteri alfanumerici standard e speciali. La chiave fa distinzione tra maiuscole e minuscole e deve corrispondere a quella configurata sul server RADIUS. Il testo immesso viene mostrato come una serie di asterischi.

- Da **Key 2** a **Key 4**: la chiave RADIUS associata ai server RADIUS di backup configurati. Il server indicato nel campo Server IP (IPv6) Address 2 utilizza la chiave specificata nel campo Key 2, il server indicato in Server IP (IPv6) Address 3 utilizza la chiave del campo Key 3 e così via.

- **Enable RADIUS Accounting**: consente di rilevare e misurare le risorse utilizzate da un determinato utente, ad esempio l'ora di sistema, la quantità di dati trasmessi e ricevuti e così via.

Se selezionata, la funzione di accounting RADIUS viene abilitata per il server RADIUS primario e per tutti i server di backup.

- **Active Server**: attiva la selezione amministrativa del server RADIUS attivo, invece di far sì che il dispositivo WAP tenti di contattare ciascun server configurato in sequenza e scelga il primo server attivo.
- **Broadcast Key Refresh Rate**: l'intervallo di aggiornamento della chiave (gruppo) di trasmissione per i client associati al VAP.

  L'impostazione predefinita è 300. L'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di trasmissione non viene aggiornata.
- **Session Key Refresh Rate**: l'intervallo di aggiornamento delle chiavi (unicast) di sessione da parte del dispositivo WAP per i client associati al VAP.

  L'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di trasmissione non viene aggiornata.

WPA Personal è uno standard Wi-Fi Alliance IEEE 802.11i che include la crittografia AES-CCMP e TKIP. La versione Personal di WPA utilizza una chiave precondivisa (PSK) invece di utilizzare IEEE 802.1X ed EAP come nella modalità di protezione Enterprise WPA. Il sistema PSK è utilizzato esclusivamente per un controllo iniziale delle credenziali. La modalità WPA Personal viene definita anche WPA-PSK.

Questa modalità di protezione è compatibile con le versioni precedenti per i client wireless che supportano la modalità WPA originale.

I parametri per la configurazione della modalità WPA Personal sono i seguenti:

- **WPA Versions**: i tipi di stazioni client da supportare:
  - **WPA**: la rete presenta stazioni client che supportano la modalità WPA originale, ma non supportano la più recente modalità WPA2.
  - **WPA2**: tutte le stazioni client della rete supportano WPA2. Questa versione del protocollo fornisce la migliore protezione per lo standard IEEE 802.11i.

  Se la rete è composta da una combinazione di client che supportano WPA2 e la modalità WPA originale, selezionare entrambe le caselle. Ciò consente sia alle stazioni client WPA che WPA2 di effettuare l'associazione e l'autenticazione, ma utilizza la modalità WPA2 più potente per i client che la supportano. Questa configurazione WPA consente maggiore interoperabilità in cambio di parte della protezione.

- **Cipher Suites**: la suite di cifratura che si desidera utilizzare:
  - TKIP
  - CCMP (AES)

  È possibile selezionare una delle due o entrambe. Sia i client TKIP che AES possono eseguire l'associazione al dispositivo WAP. Per poter effettuare l'associazione al dispositivo WAP, i client WPA devono disporre di una delle chiavi seguenti:
  - Una chiave TKIP valida
  - Una chiave AES-CCMP valida

  I client non configurati per l'utilizzo di WPA Personal non possono eseguire l'associazione al dispositivo WAP.
- **Key**: la chiave segreta condivisa per la protezione WPA Personal. Immettere una stringa di 8-63 caratteri. I caratteri accettabili includono lettere alfabetiche maiuscole e minuscole, numeri e caratteri speciali quali @ e #.
- **Key Strength Meter**: il dispositivo WAP controlla la chiave in base a criteri di complessità quali il numero di tipi diversi di caratteri (lettere alfabetiche maiuscole e minuscole, numeri e caratteri speciali) utilizzati e la lunghezza della stringa. Se il controllo della complessità WPA-PSK è attivato, la chiave viene accettata solo se rispetta i requisiti minimi. Per informazioni sulla configurazione del controllo di complessità, vedere **Complessità WPA-PSK**.
- **Broadcast Key Refresh Rate**: l'intervallo di aggiornamento della chiave (gruppo) di trasmissione per i client associati al VAP. L'impostazione predefinita è 300 secondi e l'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di trasmissione non viene aggiornata.

WPA Enterprise con RADIUS è un'implementazione dello standard Wi-Fi Alliance IEEE 802.11i che include la crittografia CCMP (AES) e TKIP. La modalità Enterprise richiede l'uso di un server RADIUS per l'autenticazione degli utenti.

Questa modalità di protezione è compatibile con le versioni precedenti per i client wireless che supportano la modalità WPA originale.

I parametri per la configurazione della modalità WPA Enterprise sono i seguenti:

- **WPA Versions**: i tipi di stazioni client da supportare:

- **WPA**: se tutte le stazioni client della rete supportano la modalità WPA originale, ma nessuna supporta la modalità più recente WPA2, selezionare WPA.
- **WPA2**: se tutte le stazioni client della rete supportano WPA2, si consiglia di utilizzare questa modalità, perché offre la migliore protezione in base allo standard IEEE 802.11i.
- **WPA e WPA2**: se la rete è composta da una combinazione di client che supportano WPA2 e la modalità WPA originale, selezionare sia WPA che WPA2. Questa impostazione consente sia alle stazioni client WPA che WPA2 di effettuare l'associazione e l'autenticazione, ma utilizza la modalità WPA2 più potente per i client che la supportano. Questa configurazione WPA consente maggiore interoperabilità in cambio di parte della protezione.

- **Enable pre-authentication**: se per le versioni WPA si seleziona soltanto WPA2 o sia WPA che WPA2, è possibile attivare la pre-autenticazione per i client WPA2.

  Fare clic su **Enable pre-authentication** se si desidera che i client wireless WPA2 inviino pacchetti di pre-autenticazione. Le informazioni di pre-autenticazione sono inoltrate dal dispositivo WAP utilizzato dal client al dispositivo WAP di destinazione. L'attivazione di questa funzionalità può contribuire a velocizzare l'autenticazione per i client in roaming che si connettono a più access point.

  Questa opzione non si applica se il campo WPA Versions è stato impostato su WPA, poiché la modalità WPA originale non supporta questa funzionalità.

- **Cipher Suites**: la suite di cifratura che si desidera utilizzare:
  - TKIP
  - CCMP (AES)
  - TKIP e CCMP (AES)

  Per impostazione predefinita sono selezionate sia TKIP che CCMP. Se sono selezionate entrambe, le stazioni client configurate per l'utilizzo di WPA con RADIUS devono avere uno di questi indirizzi e chiavi:
  - Un indirizzo IP RADIUS TKIP valido e una chiave RADIUS
  - Un indirizzo IP CCMP (AES) valido e una chiave RADIUS

- **Use Global RADIUS Server Settings**: per impostazione predefinita, ciascun VAP utilizza le impostazioni globali RADIUS definite per il dispositivo WAP (vedere **Server RADIUS**). Tuttavia, è possibile configurare ciascun VAP in modo da utilizzare una serie diversa di server RADIUS.

  Per utilizzare le impostazioni globali del server RADIUS, assicurarsi che questa casella sia selezionata.

  Per utilizzare un server RADIUS separato per il VAP, deselezionare questa casella, quindi immettere l'indirizzo IP del server RADIUS e la chiave nei campi seguenti:

- **Server IP Address Type**: la versione IP utilizzata dal server RADIUS.

  È possibile alternare tipi di indirizzi diversi per configurare le impostazioni degli indirizzi globali RADIUS IPv4 e IPv6, ma il dispositivo WAP contatta soltanto i server RADIUS associati al tipo di indirizzo selezionato in questo campo.

- **Server IP Address 1** o **Server IPv6 Address 1**: l'indirizzo del server RADIUS primario per questo VAP.

  Se si seleziona **IPv4** nel campo **Server IP Address Type**, immettere l'indirizzo IP del server RADIUS che tutti i VAP utilizzeranno per impostazione predefinita, ad esempio 192.168.10.23. Se si seleziona **IPv6**, immettere l'indirizzo IPv6 del server globale RADIUS primario, ad esempio 2001:DB8:1234::abcd.

- Da **Server IP Address 2** a **4** o da **Server IPv6 Address 2** a **4**: fino a tre indirizzi IPv4 e/o IPv6 da utilizzare come server RADIUS di backup per questo VAP.

  Se l'autenticazione con il server primario ha esito negativo, si prova in sequenza con ciascun server di backup configurato.

- **Key 1**: la chiave segreta condivisa per il server RADIUS globale. È possibile immettere massimo 63 caratteri alfanumerici standard e speciali. La chiave fa distinzione tra maiuscole e minuscole ed è necessario configurare la stessa chiave sul dispositivo WAP e sul server RADIUS. Il testo immesso viene mostrato come una serie di asterischi per impedire che altri vedano la chiave RADIUS mentre la si digita.

- Da **Key 2** a **Key 4**: la chiave RADIUS associata ai server RADIUS di backup configurati. Il server indicato nel campo **Server IP (IPv6) Address 2** utilizza la chiave specificata nel campo **Key 2**, il server indicato nel campo **Server IP (IPv6) Address 3** utilizza la chiave del campo **Key 3** e così via.

- **Enable RADIUS Accounting**: rileva e misura le risorse utilizzate da un determinato utente, ad esempio l'ora di sistema, la quantità di dati trasmessi e ricevuti e così via.

  Se selezionata, la funzione di accounting RADIUS viene abilitata per il server RADIUS primario e per tutti i server di backup.

- **Active Server**: attiva la selezione amministrativa del server RADIUS attivo, invece di far sì che il dispositivo WAP tenti di contattare ciascun server configurato in sequenza e scelga il primo server attivo.

  Broadcast Key Refresh Rate: l'intervallo di aggiornamento della chiave (gruppo) di trasmissione per i client associati al VAP.

  L'impostazione predefinita è 300 secondi. L'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di trasmissione non viene aggiornata.

- **Session Key Refresh Rate**: l'intervallo di aggiornamento delle chiavi (unicast) di sessione da parte del dispositivo WAP per i client associati al VAP.

  L'intervallo valido è compreso tra 0 e 86400 secondi. Il valore 0 indica che la chiave di sessione non è aggiornata.

Strumento di programmazione

Lo strumento di programmazione radio e VAP consente di configurare una regola che attivi o disattivi automaticamente i VAP o le interfacce radio in base a un intervallo specificato.

È possibile utilizzare questa funzionalità per programmare l'interfaccia radio in modo che funzioni soltanto durante l'orario lavorativo, garantendo così la protezione e riducendo il consumo energetico. È inoltre possibile utilizzare lo strumento di programmazione per consentire ai client wireless di accedere ai VAP soltanto in orari specifici del giorno.

Il dispositivo WAP supporta fino a 16 profili. Al profilo vengono aggiunte soltanto regole valide. È possibile raggruppare fino a 16 regole per formare un profilo di programmazione. Le voci orarie periodiche che appartengono allo stesso profilo non possono sovrapporsi.

È possibile creare fino a 16 nomi di profili di programmazione. Per impostazione predefinita, non vengono creati profili.

Per visualizzare lo stato dello strumento di programmazione e aggiungere un profilo, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **Scheduler**.

PASSAGGIO 2 Accertarsi che l'opzione **Administrative Mode** sia attiva. Per impostazione predefinita, è disattivata.

Nell'area Scheduler Operational Status viene indicato lo stato di funzionamento corrente dello strumento di programmazione:

- **Status**: lo stato operativo dello strumento di programmazione. Le opzioni disponibili sono Up o Down. L'impostazione predefinita è Down.
- **Reason**: la motivazione dello stato operativo dello strumento di programmazione. È possibile scegliere fra i valori seguenti:
  - IsActive: lo strumento di programmazione è attivato in modalità amministrativa.
  - Administrative Mode is disabled: lo stato operativo è Down poiché la configurazione globale è disattivata.

PASSAGGIO 3 Per aggiungere un profilo, immettere il nome nella casella di testo **Scheduler Profile Configuration** e fare clic su **Aggiungi**. Il nome del profilo può contenere un massimo di 32 caratteri alfanumerici.

È possibile configurare fino a 16 regole per un profilo. Ogni regola specifica l'ora di inizio, l'ora di fine e il giorno (o i giorni) della settimana in cui l'interfaccia radio o il VAP possono essere operativi. Le regole sono di tipo periodico e vengono ripetute ogni settimana. Una regola valida deve contenere tutti i parametri (giorni della settimana, ora e minuti) per l'ora di inizio e l'ora di fine. Non possono esistere conflitti fra le regole; ad esempio, è possibile configurare una regola che venga avviata ogni giorno lavorativo e un'altra che venga avviata ogni giorno del weekend, ma non è possibile configurare una regola che venga avviata tutti i giorni e un'altra che venga avviata nei weekend.

Per configurare una regola per un profilo, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare il profilo dall'elenco **Select a Profile Name**.

PASSAGGIO 2 Fare clic su **Add Rule**.

La nuova regola viene visualizzata nella tabella delle regole.

PASSAGGIO 3 Selezionare la casella accanto a **Profile Name** e fare clic su **Modifica**.

PASSAGGIO 4 Nel menu **Day of the Week** , selezionare la programmazione ricorrente per la regola. È possibile impostare la regola in modo che venga eseguita ogni giorno, ogni giorno lavorativo, ogni giorno del weekend (sabato e domenica) o qualsiasi giorno della settimana.

PASSAGGIO 5 Impostare l'ora di inizio e di fine:

- **Start Time**: l'ora in cui viene attivato il funzionamento dell'interfaccia radio o del VAP. L'ora è espressa nel formato HH:MM a 24 ore. L'intervallo è <00-23>:<00-59>. L'impostazione predefinita è 00:00.
- End Time: l'ora in cui viene disattivato il funzionamento dell'interfaccia radio o del VAP. L'ora è espressa nel formato HH:MM a 24 ore. L'intervallo è <00-23>:<00-59>. L'impostazione predefinita è 00:00.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per poter applicare un profilo di programmazione è necessario associarlo a un'interfaccia radio o a un VAP. Vedere la sezione **Associazione dello strumento di programmazione**.

NOTA Per eliminare una regola, selezionare il profilo nella colonna **Profile Name**, quindi fare clic su **Elimina**.

Associazione dello strumento di programmazione

Per poter utilizzare i profili di programmazione è necessario associarli all'interfaccia WLAN o a un'interfaccia VAP. Per impostazione predefinita, non vengono creati profili di programmazione e all'interfaccia radio o VAP non sono associati profili.

È possibile associare un solo profilo di programmazione all'interfaccia WLAN o a ciascun VAP. È possibile associare lo stesso profilo a più VAP. Se il profilo di programmazione associato a un VAP o all'interfaccia WLAN viene eliminato, l'associazione viene rimossa.

Per associare un profilo di programmazione all'interfaccia WLAN o a un VAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **Scheduler Association**. Per i dispositivi WAP561, selezionare l'interfaccia **Radio** da associare a un profilo di programmazione (**Radio 1** o **Radio 2**).

PASSAGGIO 2 Per l'interfaccia WLAN o un VAP, selezionare il profilo nell'elenco **Profile Name**.

Nella colonna **Interface Operational Status** viene indicato se l'interfaccia è attualmente attivata o disattivata.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Utilizzo della larghezza di banda

Utilizzare la pagina Bandwidth Utilization per configurare la larghezza di banda radio che è possibile utilizzare prima di bloccare nuove associazioni client al dispositivo WAP. Questa funzione è attivata per impostazione predefinita.

Per modificare le impostazioni di utilizzo della larghezza di banda, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **Bandwidth Utilization**.

PASSAGGIO 2 Fare clic su **Enable** per attivare **l'utilizzo della larghezza di banda** oppure deselezionare **Enable** per disattivare questa funzione.

PASSAGGIO 3 Se questa opzione è attivata, nella casella **Maximum Utilization Threshold** immettere la percentuale di utilizzo della larghezza di banda di rete consentita sull'interfaccia radio prima di bloccare nuove associazioni client al dispositivo WAP.

È possibile immettere numeri interi da 0 a 100 percento. L'impostazione predefinita è 70 percento. Se questo campo è impostato su 0, tutte le nuove associazioni sono consentite, a prescindere dalla percentuale di utilizzo.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Filtraggio MAC

È possibile utilizzare il filtraggio MAC (Media Access Control) per consentire l'autenticazione all'access point soltanto alle stazioni client autorizzate. È possibile attivare e disattivare l'autenticazione MAC per singolo VAP nella pagina **Reti**. A seconda della configurazione del VAP, il dispositivo WAP può fare riferimento a un elenco di filtri MAC archiviato su un server RADIUS esterno o un elenco archiviato localmente sul dispositivo WAP.

Il dispositivo WAP supporta un solo elenco locale di filtri MAC; questo significa che lo stesso elenco si applica a tutti i VAP abilitati all'utilizzo dell'elenco locale. È possibile configurare il filtro in modo da concedere o negare l'accesso soltanto agli indirizzi MAC inclusi nei rispettivi elenchi.

È possibile aggiungere fino a 512 indirizzi MAC all'elenco di filtri.

Per configurare il filtraggio MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **MAC Filtering**.

PASSAGGIO 2 Selezionare la modalità di utilizzo dell'elenco di filtri da parte del dispositivo WAP:

- **Allow only stations in the list**: l'accesso alla rete tramite il dispositivo WAP viene consentito solo ed esclusivamente alle stazioni elencate.
- **Block all stations in the list**: le stazioni incluse nell'elenco non possono accedere alla rete tramite il dispositivo WAP. Tutte le altre stazioni, invece, possono accedere.

  NOTA L'impostazione del filtro si applica anche all'elenco di filtraggio MAC archiviato sul server RADIUS, se presente.

PASSAGGIO 3 Nel campo **MAC Address**, immettere l'indirizzo MAC da consentire o bloccare e fare clic su **Aggiungi**.

L'indirizzo MAC viene visualizzato nel campo **Stations List**.

PASSAGGIO 4 Immettere tutti gli indirizzi MAC da includere nell'elenco, quindi fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare un indirizzo MAC dall'elenco delle stazioni, selezionarlo e fare clic su **Rimuovi**.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Se uno o più VAP devono utilizzare un filtro MAC archiviato su un server di autenticazione RADIUS, è necessario configurare l'elenco delle stazioni sul server RADIUS. Nella tabella seguente viene mostrato il formato dell'elenco:

Attributo del server RADIUS	Descrizione	Valore
User-Name (1)	Indirizzo MAC della stazione client.	Indirizzo MAC Ethernet valido.
User-Password (2)	Una password globale fissa utilizzata per cercare una voce MAC client.	NOPASSWORD

Bridge WDS

Il Wireless Distribution System (WDS) consente di connettere più dispositivi WAP551 e WAP561. Con il sistema WDS, gli access point comunicano tra di loro senza cavi. Questa funzionalità è fondamentale per fornire un'esperienza ottimale ai client in roaming e per gestire più reti wireless. Può inoltre semplificare l'infrastruttura di rete riducendo la quantità di cavi necessari. È possibile configurare il dispositivo WAP in modalità bridge point-to-point o point-to-multipoint in base al numero di collegamenti da connettere.

Nella modalità point-to-point, il dispositivo WAP accetta associazioni client e comunica con client wireless e altri ripetitori. Il dispositivo WAP inoltra tutto il traffico indirizzato all'altra rete sul tunnel stabilito tra access point. Il bridge non è incluso nel numero di hop. Funziona come semplice dispositivo di rete OSI Layer 2.

Nella modalità bridge point-to-multipoint, un dispositivo WAP agisce da collegamento comune tra più access point. In questa modalità, il dispositivo WAP centrale accetta associazioni client e comunica con i client e altri ripetitori. Tutti gli altri access point vengono associati soltanto al dispositivo WAP centrale che inoltra i pacchetti al bridge wireless appropriato a scopi di routing.

Il dispositivo WAP può anche fungere da ripetitore. In questa modalità, il dispositivo WAP funge da collegamento tra due dispositivi WAP che potrebbero essere troppo distanti per rientrare nell'intervallo tra celle. Se svolge funzioni di ripetitore, il dispositivo WAP non è connesso alla LAN via cavo e ripete i segnali utilizzando la connessione wireless. Per utilizzare il dispositivo WAP come ripetitore non sono necessarie configurazioni speciali e non sono presenti impostazioni per la modalità ripetitore. I client wireless possono comunque connettersi a un dispositivo WAP che funziona da ripetitore.

Prima di configurare il sistema WDS sul dispositivo WAP, prendere nota delle seguenti linee guida:

- Il sistema WDS funziona soltanto con i dispositivi Cisco WAP551 e Cisco WAP561.
- Tutti i dispositivi WAP Cisco in un collegamento WDS devono presentare gli stessi valori per le impostazioni seguenti:
  - Radio
  - Modalità IEEE 802.11
  - Larghezza di banda canale
  - Canale (l'impostazione Auto è sconsigliata)

  NOTA Se si esegue il bridging nella banda 802.11n a 2,4 GHz, impostare la larghezza di banda del canale su 20 MHz invece che sull'impostazione predefinita 20/40 MHz. Nella banda a 2,4 GHz 20/40 MHz, la larghezza di banda operativa può passare da 40 MHz a 20 MHz se si rilevano dispositivi WAP da 20 MHz nell'area. Una mancata corrispondenza con la larghezza di banda del canale può causare la disconnessione del collegamento.

  Per informazioni sulla configurazione di queste impostazioni, vedere **Radio** (impostazioni di base).

- Il sistema WDS deve essere configurato su entrambi i dispositivi WAP che partecipano al collegamento WDS.
- È possibile avere un solo collegamento WDS tra una coppia di dispositivi WAP. Questo significa che un indirizzo MAC remoto può essere visualizzato solo una volta nella pagina WDS di un determinato dispositivo WAP.

Per configurare un bridge WDS, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **WDS Bridge**.

PASSAGGIO 2 Selezionare **Enable** per **Spanning Tree Mode**. La modalità STP, se attivata, contribuisce a evitare il loop switching. La modalità STP è raccomandata se si configurano collegamenti WDS. Per i dispositivi WAP561, selezionare **Radio 1** o **Radio 2** per ciascun collegamento WDS configurato.

PASSAGGIO 3 Selezionare **Enable** per **WDS Interface**.

PASSAGGIO 4 Configurare i parametri rimanenti:

- **Remote MAC Address**: specifica l'indirizzo MAC del dispositivo WAP di destinazione, ovvero il dispositivo WAP all'altra estremità del collegamento WDS a cui sono inviati o consegnati i dati e da cui si ricevono dati.

SUGGERIMENTO È possibile trovare l'indirizzo MAC nella pagina Status and Statistics > Network Interface.

- **Encryption**: il tipo di crittografia da utilizzare sul collegamento WDS; non deve necessariamente corrispondere al VAP per cui si crea il bridge. Le impostazioni di crittografia WDS sono univoche del bridge WDS. Le opzioni sono None, WEP e WPA Personal.

  Se non si è interessati ai problemi di sicurezza del collegamento WDS, è possibile decidere di non impostare alcun tipo di crittografia. Se, invece, si è preoccupati per la sicurezza, è possibile scegliere tra Static WEP e WPA Personal. In modalità WPA Personal, il dispositivo WAP utilizza WPA2-PSK con crittografia CCMP (AES) sul collegamento WDS. Per ulteriori informazioni sulle opzioni di crittografia, vedere **WEP su collegamenti WDS** o **WPA/PSK su collegamenti WDS** di seguito.

PASSAGGIO 5 Ripetere questi passaggi per un massimo di tre interfacce WDS aggiuntive.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

PASSAGGIO 7 Ripetere la procedura sugli altri dispositivi che devono connettersi al bridge.

SUGGERIMENTO Per verificare se il collegamento del bridge è attivo, visualizzare la pagina Status and Statistics > Network Interface. Nella tabella Interface Status, lo stato WLAN0:WDS(x) deve indicare Up.

ATTENZIONE Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Questi campi aggiuntivi vengono visualizzati quando si seleziona WEP come tipo di crittografia.

- **Key Length**: se è attiva la crittografia WEP, specificare la lunghezza della chiave WEP come **64 bit** o **128 bit**.
- **Key Type**: se è attiva la crittografia WEP, specificare il tipo di chiave WEP: **ASCII** o **Hex**.
- **WEP Key**: se è stato selezionato il tipo **ASCII**, immettere una combinazione di numeri da 0 a 9, di lettere da a a z o da A a Z. Se è stato selezionato il tipo **Hex**, immettere cifre esadecimali (una combinazione di numeri da 0 a 9 e di lettere da a a f o da A a F). Si tratta delle chiavi di crittografia RC4 condivise con le stazioni che utilizzano il dispositivo WAP.

  Il numero di caratteri richiesto è indicato a destra del campo e cambia in base alle opzioni selezionate nei campi **Key Type** e **Key Length**.

Questi campi aggiuntivi vengono visualizzati quando si seleziona WPA/PSK come tipo di crittografia.

- **WDS ID**: immettere un nome appropriato per il nuovo collegamento WDS creato. È importante che lo stesso ID WDS venga immesso anche all'altra estremità del collegamento WDS. Se gli ID WDS non corrispondono, i due dispositivi WAP sul collegamento WDS non potranno comunicare e scambiare dati.

  L'ID WDS è una combinazione alfanumerica.
- **Key**: immettere una chiave condivisa univoca per il bridge WDS. Questa chiave deve essere immessa anche per il dispositivo WAP all'altra estremità del collegamento WDS. Se le chiavi non corrispondono, i due dispositivi WAP non potranno comunicare e scambiare dati.

La chiave WPA-PSK è una stringa di 8-63 caratteri. I caratteri accettabili includono lettere alfabetiche maiuscole e minuscole, numeri e caratteri speciali quali @ e #.

WorkGroup Bridge

La funzionalità WorkGroup Bridge del dispositivo WAP consente al dispositivo WAP di estendere l'accessibilità di una rete remota. In modalità WorkGroup Bridge, il dispositivo WAP funge da stazione wireless (STA) sulla LAN wireless. Può fungere da bridge per il traffico tra una rete cablata remota o i client wireless associati e la LAN wireless collegata utilizzando la modalità WorkGroup Bridge.

La funzionalità WorkGroup Bridge attiva il supporto per il funzionamento simultaneo in modalità STA e AP. Il dispositivo WAP può operare in un BSS (Basic Service Set) come dispositivo STA e in un altro BSS come dispositivo WAP. Se la modalità WorkGroup Bridge è attiva, il dispositivo WAP supporta un solo BSS per i client wireless associati e un altro BSS con cui il dispositivo WAP si associa come client wireless.

Si raccomanda di utilizzare la modalità WorkGroup Bridge soltanto quando il bridge WDS non può funzionare con un dispositivo WAP di pari livello. WDS è una soluzione migliore ed è preferita rispetto alla soluzione WorkGroup Bridge. Utilizzare WDS per il bridging dei dispositivi Cisco WAP121, WAP321, WAP551 e WAP561. In caso contrario, prendere in considerazione la funzionalità WorkGroup Bridge. Se la funzionalità WorkGroup Bridge è attivata, viene applicata soltanto la configurazione WorkGroup Bridge; le configurazioni VAP vengono ignorate.

NOTA La funzionalità WDS non funziona se sul dispositivo WAP è attiva la modalità WorkGroup Bridge.

In modalità WorkGroup Bridge, il BSS gestito dal dispositivo WAP durante il funzionamento in modalità dispositivo WAP viene indicato come interfaccia Access Point e le stazioni STA associate come STA downstream. Il BSS gestito dall'altro dispositivo WAP, ovvero BSS a cui il dispositivo WAP si associa come stazione STA, viene indicato come interfaccia Infrastructure Client e l'altro dispositivo WAP come AP upstream.

I dispositivi collegati all'interfaccia cablata del dispositivo WAP, oltre alle stazioni downstream associate all'interfaccia Access Point del dispositivo, possono accedere alla rete connessa dall'interfaccia Infrastructure Client. Per consentire il bridging dei pacchetti, la configurazione VLAN per l'interfaccia Access Point e l'interfaccia cablata devono corrispondere a quella dell'interfaccia Infrastructure Client.

La modalità WorkGroup Bridge può essere utilizzata per estendere la portata e consentire al BSS di fornire accesso a reti remote o difficilmente raggiungibili. È possibile configurare una sola interfaccia radio per inoltrare i pacchetti dalle stazioni STA associate a un altro dispositivo WAP nello stesso ESS, senza utilizzare WDS.

Prima di configurare WorkGroup Bridge sul dispositivo WAP, prendere nota delle seguenti linee guida:

- Tutti i dispositivi WAP in un WorkGroup Bridge devono presentare gli stessi valori per le impostazioni seguenti:
  - Radio
  - Modalità IEEE 802.11
  - Larghezza di banda canale
  - Canale (l'impostazione Auto è sconsigliata)

  Per informazioni sulla configurazione di queste impostazioni, vedere **Radio** (impostazioni di base).
- La modalità WorkGroup Bridge supporta attualmente soltanto il traffico IPv4.
- La modalità WorkGroup Bridge non è supportata su un punto di installazione singolo.
- Si sconsiglia di associare un altro AP all'interfaccia downstream del dispositivo WAP che funzioni in modalità WorkGroup Bridge; il concatenamento e il cascading degli AP non sono supportati.

Per configurare la modalità WorkGroup Bridge, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **WorkGroup Bridge**.

PASSAGGIO 2 Selezionare **Enable** per **WorkGroup Bridge Mode**.

PASSAGGIO 3 Per i dispositivi WAP561, selezionare l'interfaccia radio su cui configurare la modalità WorkGroup Bridge (**Radio 1** o **Radio 2**).

PASSAGGIO 4 Configurare questi parametri per l'interfaccia Infrastructure Client (upstream):

- **SSID**: il SSID del BSS.

NOTA Accanto al SSID per la scansione SSID è presente una freccia; questa funzionalità è disattivata per impostazione predefinita ed è attivata soltanto se è attivo il rilevamento degli AP non autorizzati (disattivato per impostazione predefinita).

- **Security**: il tipo di protezione da utilizzare per l'autenticazione come stazione client sul dispositivo WAP upstream. Le opzioni disponibili sono:
  - **None**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise**

- **ID VLAN**: la VLAN associata al BSS.

NOTA L'interfaccia Infrastructure Client sarà associata al dispositivo WAP upstream con le credenziali configurate. Il dispositivo WAP può ottenere il suo indirizzo IP da un server DHCP sul collegamento upstream. In alternativa, è possibile assegnare un indirizzo IP statico. Il campo **Connection Status** indica se il dispositivo WAP è connesso al dispositivo WAP upstream. Fare clic sul pulsante **Refresh** nella parte superiore della pagina per visualizzare lo stato di connessione più recente.

PASSAGGIO 5 Configurare i seguenti campi aggiuntivi per l'interfaccia Access Point:

- **Status**: selezionare **Enable** per l'interfaccia Access Point.
- **SSID**: il SSID dell'interfaccia Access Point non deve essere lo stesso del nome SSID dell'interfaccia Infrastructure Client. Tuttavia, se si tenta di supportare un tipo di scenario roaming, il nome SSID e il tipo di protezione devono essere identici.
- **SSID Broadcast**: selezionare se trasmettere il nome SSID downstream. Questa opzione è attivata per impostazione predefinita.
- **Security**: il tipo di protezione da utilizzare per l'autenticazione. Le opzioni disponibili sono:
  - **None**
  - **Static WEP**
  - **WPA Personal**
- **MAC Filtering**: selezionare una delle seguenti opzioni:

- **Disabled**: la serie di client nel BSS degli AP che possono accedere alla rete upstream non è limitata ai client specificati in un elenco di indirizzi MAC.
- **Local**: la serie di client nel BSS degli AP che possono accedere alla rete upstream è limitata ai client specificati in un elenco di indirizzi MAC locale.
- **RADIUS**: la serie di client nel BSS degli AP che possono accedere alla rete upstream è limitata ai client specificati in un elenco di indirizzi MAC su un server RADIUS.

Se si seleziona Local o RADIUS, vedere **Filtraggio MAC** per istruzioni sulla creazione dell'elenco di filtri MAC.

- **VLAN ID**: configurare l'interfaccia Access Point con lo stesso ID VLAN comunicato sull'interfaccia Infrastructure Client.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

I client downstream associati ora possono connettersi alla rete upstream.

QoS

Le impostazioni QoS (Quality of Service, qualità del servizio) consentono di configurare le code di trasmissione per un throughput ottimizzato e prestazioni migliori quando si gestisce traffico wireless differenziato, come Voice-over-IP (VoIP), altri tipi di audio, video, streaming multimediale e dati IP tradizionali.

Per configurare QoS sul dispositivo WAP, è necessario impostare i parametri delle code di trasmissione per diversi tipi di traffico wireless e specificare i tempi di attesa minimo e massimo (attraverso finestre di contesa) per la trasmissione.

I parametri WAP Enhanced Distributed Channel Access (EDCA) influenzano il flusso del traffico dal dispositivo WAP alla stazione client.

I parametri EDCA della stazione incidono sul flusso del traffico dalla stazione client al dispositivo WAP.

I parametri EDCA della stazione influenzano il flusso del traffico dalla stazione client al dispositivo WAP. La modifica di tali valori influenza la qualità del servizio fornito.

Per configurare i parametri EDCA della stazione e del dispositivo WAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare, **Wireless** > **QoS**. Per i dispositivi WAP561, selezionare l'interfaccia radio su cui configurare le impostazioni QoS (**Radio 1** o **Radio 2**).

PASSAGGIO 2 Selezionare un'opzione nell'elenco **EDCA Template**:

- **WFA Defaults**: imposta i parametri EDCA della stazione e del dispositivo WAP sui valori predefiniti WiFi Alliance, che sono i migliori per il traffico generale misto.
- **Optimized for Voice**: imposta i parametri EDCA della stazione e del dispositivo WAP sui valori ottimali per il traffico vocale.
- **Custom**: consente di scegliere parametri EDCA personalizzati.

Queste quattro code sono definite per i diversi tipi di dati trasmessi dal dispositivo WAP alla stazione. Se si sceglie un modello personalizzato, è possibile configurare i parametri che definiscono le code; in caso contrario, vengono utilizzati i valori predefiniti appropriati per l'opzione scelta. Le quattro code sono:

- Data 0 (Voice): coda ad alta priorità con ritardo minimo. I dati con esigenze temporali, come VoIP e streaming multimediale, vengono inviati automaticamente a questa coda.
- Data 1 (Video): coda ad alta priorità con ritardo minimo. I dati video con esigenze temporali vengono inviati automaticamente a questa coda.
- Data 2 (Best Effort): coda a priorità media con throughput e ritardo di media entità. La maggior parte dei dati IP tradizionali viene inviata a questa coda.
- Data 3 (Background): coda a priorità minima e alto throughput. I dati in blocco che richiedono un throughput molto elevato e non hanno esigenze di risposta rapida, ad esempio i dati FTP, vengono inviati a questa coda.

PASSAGGIO 3 Configurare i seguenti parametri EDCA ed EDCA della stazione:

NOTA È possibile configurare questi parametri se nel passaggio precedente è stata selezionata l'opzione Custom.

- **Arbitration Inter-Frame Space**: tempo di attesa per i frame di dati, misurato in slot. I valori validi per AIFS sono compresi fra 1 e 255.
- **Minimum Contention Window**: input per l'algoritmo che determina il tempo di attesa di backoff casuale iniziale (finestra) per riprovare una trasmissione.

Questo valore è il limite superiore (in millisecondi) di un intervallo da cui si determina il tempo di attesa di backoff casuale iniziale.

Il primo numero casuale generato è un numero compreso tra 0 e il numero specificato qui.

Se il primo intervallo di attesa casuale di backoff scade prima dell'invio del frame di dati, il contatore di nuovi tentativi viene incrementato e il valore di backoff casuale (finestra) viene raddoppiato. Il valore continua a raddoppiare fino a raggiungere il numero definito nel campo Maximum Contention Window.

I valori validi sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1023. Questo valore deve essere minore del valore impostato nel campo Maximum Contention Window.

- **Maximum Contention Window**: il limite superiore (in millisecondi) fino al quale è possibile raddoppiare il valore di backoff casuale. Il valore continua a raddoppiare fino all'invio del frame di dati o al raggiungimento del valore impostato nel campo Maximum Contention Window.

  Quando viene raggiunto il valore del campo Maximum Contention Window, i nuovi tentativi proseguono fino al raggiungimento del numero massimo di tentativi consentiti.

  I valori validi sono 1, 3, 7, 15, 31, 63, 127, 255, 511 o 1023. Questo valore deve essere maggiore del valore impostato nel campo Minimum Contention Window.

- **Maximum Burst** (solo WAP): un parametro EDCA WAP che si applica soltanto al traffico dal dispositivo WAP alla stazione client.

  Questo valore, espresso in millisecondi, specifica la lunghezza massima consentita per il bursting di pacchetti sulla rete wireless. Un burst di pacchetti è un insieme di più frame trasmessi senza informazioni di intestazione. Il minore sovraccarico offre un maggiore throughput e prestazioni migliori.

  I valori validi sono compresi tra 0,0 e 999.

- **Wi-Fi MultiMedia (WMM)**: selezionare **Enable** per attivare le estensioni Wi-Fi MultiMedia (WMM). Questo campo è attivato per impostazione predefinita. Se la modalità WMM è attivata, sono attivi l'assegnazione delle priorità QoS e il coordinamento dell'accesso ai supporti wireless. Con l'opzione WMM attiva, le impostazioni QoS sul dispositivo WAP controllano il traffico downstream dal dispositivo WAP alla stazione client (parametri EDCA dell'AP) e il traffico upstream dalla stazione all'AP (parametri EDCA della stazione).

Se si disattiva la modalità WMM, vengono disattivati anche il controllo QoS dei parametri EDCA della stazione sul traffico upstream dalla stazione client al dispositivo WAP. Se l'opzione WMM è disattivata, è comunque possibile impostare alcuni parametri del traffico downstream dal dispositivo WAP alla stazione client (parametri EDCA dell'AP).

- **TXOP Limit** (solo stazione): il limite TXOP è un parametro EDCA della stazione e si applica soltanto al traffico dalla stazione client al dispositivo WAP. La Transmission Opportunity (TXOP) è l'intervallo di tempo, espresso in millisecondi, in cui una stazione client WME ha il diritto di iniziare le trasmissioni sul supporto wireless (WM, wireless medium) verso il dispositivo WAP. Il valore massimo del limite TXOP è 65535.

PASSAGGIO 4 Configurare le seguenti impostazioni aggiuntive:

- **No Acknowledgement**: selezionare **Enable** per specificare che il dispositivo WAP non deve utilizzare il valore della classe di servizio QosNoAck per confermare i frame.
- **Unscheduled Automatic Power Save Delivery**: selezionare **Enable** per attivare APSD, un metodo di gestione del risparmio energetico. L'opzione APSD è raccomandata se ci sono telefoni VoIP che accedono alla rete attraverso il dispositivo WAP.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

ATTENZIONE Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Configurazione WPS

In questa sezione viene descritto il protocollo WPS (Wi-Fi Protected Setup) e la sua configurazione sul dispositivo WAP.

WPS è uno standard che consente di creare facilmente reti wireless senza compromettere la sicurezza di rete. Grazie a WPS, gli utenti dei client wireless e gli amministratori dei dispositivi WAP non devono conoscere i nomi di rete, le chiavi e molte altre opzioni di configurazione della crittografia.

WPS facilita la configurazione di rete consentendo all'amministratore di utilizzare un tasto o un PIN per creare reti wireless senza dover immettere nomi di rete (SSID) e parametri di protezione wireless manualmente:

- **Tasto**: il tasto WPS si trova sul prodotto oppure è disponibile come pulsante su cui è possibile fare clic nell'interfaccia utente.
- **Personal Identification Number (PIN)**: il PIN può essere visualizzato nell'interfaccia utente del prodotto.

Per garantire la protezione di rete, quando è attiva la modalità WPS gli utenti dei nuovi dispositivi client e gli amministratori delle WLAN devono disporre di accesso fisico ai rispettivi dispositivi o di accesso remoto sicuro a tali dispositivi.

Di seguito vengono riportati i tipici scenari di utilizzo del protocollo WPS:

- Un utente desidera registrare una stazione client su una WLAN con abilitazione WPS. Il dispositivo client da registrare può rilevare la rete e chiedere all'utente di registrarsi, sebbene ciò non sia necessario. L'utente attiva la registrazione premendo un tasto sul dispositivo client. L'amministratore del dispositivo WAP spinge quindi un tasto sul dispositivo WAP. Durante un breve scambio di messaggi di protocollo WPS, il dispositivo WAP fornisce al nuovo client una nuova configurazione di protezione tramite protocollo Extensible Authentication Protocol (EAP). I due dispositivi vengono scollegati e riassociati, quindi effettuano l'autenticazione con le nuove impostazioni.
- Un utente desidera registrare una stazione client su una WLAN con abilitazione WPS fornendo all'amministratore del dispositivo WAP il PIN del dispositivo client. L'amministratore immette il PIN nell'utilità di configurazione del dispositivo WAP e attiva la registrazione del dispositivo. Il nuovo client registrato e il dispositivo WAP si scambiano messaggi WPS, inclusa una nuova configurazione di protezione, quindi vengono scollegati, riassociati e autenticati.
- L'amministratore di un dispositivo WAP acquista un nuovo dispositivo WAP conforme a WPS versione 2.0 (certificato da Wi-Fi Alliance) e desidera aggiungere il dispositivo WAP a una rete esistente (cablata o wireless). L'amministratore accende il dispositivo WAP, quindi accede a un host di rete che supporta il protocollo di registrazione WPS. L'amministratore immette il PIN del dispositivo WAP nell'utilità di configurazione del registrar esterno e attiva il processo di registrazione WPS. Su una LAN cablata, i messaggi di protocollo WPS vengono trasportati attraverso il protocollo Universal Plug and Play o UPnP. L'host registra il dispositivo WAP come nuovo dispositivo di rete e lo configura con le nuove impostazioni di protezione.

- L'amministratore di un dispositivo WAP ha appena aggiunto un nuovo dispositivo WAP a una rete (wireless o cablata) esistente attraverso WPS e desidera concedere l'accesso a un nuovo dispositivo client. Il dispositivo viene registrato attraverso i metodi con PIN o tasto (PBC, Push-Button Control) descritti in precedenza, ma questa volta il dispositivo viene registrato nel registrar esterno e il dispositivo WAP agisce esclusivamente come proxy.
- Un dispositivo wireless che non supporta WPS deve collegarsi alla WLAN con abilitazione WPS. L'amministratore, che in questo caso non può utilizzare WPS, configura manualmente il nome SSID, la chiave condivisa pubblica e le modalità di crittografia del dispositivo WAP con abilitazione WPS sul dispositivo da collegare. Il dispositivo viene così collegato alla rete.

Il PIN può essere un numero a otto cifre che utilizza l'ultima cifra come valore di checksum o un numero a quattro cifre senza checksum. Ciascuno di questi numeri può contenere zeri iniziali.

Lo standard WPS assegna ruoli specifici ai vari componenti della sua architettura:

- **Enrollee**: un dispositivo che può collegarsi alla rete wireless.
- **AP**: un dispositivo che fornisce accesso wireless alla rete.
- **Registrar**: un'entità che emette credenziali di sicurezza agli iscritti e configura gli AP.

I dispositivi WAP agiscono da dispositivi AP e supportano un registrar integrato. Non funzionano come iscritti.

L'amministratore può attivare o disattivare lo standard WPS su un solo VAP. WPS è operativo soltanto se il VAP soddisfa le seguenti condizioni:

- Il dispositivo WAP è configurato per la trasmissione del nome SSID VAP.
- Il filtraggio degli indirizzi MAC è disattivato sul VAP.
- La crittografia WEP è disattivata sul VAP.
- Sul VAP non sono presenti opzioni di protezione oppure è selezionata la modalità WPA Personal. Se è stata selezionata la modalità di crittografia WPA2-PSK, è necessario configurare una chiave pre-condivisa (PSK) valida e attivare la crittografia CCMP (AES).
- Il VAP è attivato dal punto di vista operativo.

Se una di queste condizioni non viene soddisfatta, il WPS è disattivato dal punto di vista operativo sul VAP.

NOTA Anche se la modalità WPS viene disattivata su un VAP, i client autenticati in precedenza tramite WPS su quel VAP rimangono associati.

Non è necessario che i dispositivi WAP gestiscano la registrazione dei client sulla rete. Il dispositivo WAP può utilizzare il registrar integrato o agire da proxy per un registrar esterno. È possibile accedere al registrar esterno attraverso la LAN cablata o wireless. Il registrar esterno può essere utilizzato anche per configurare il nome SSID, la modalità di crittografia e la chiave pubblica condivisa di un BSS con WPS. Questa funzionalità è estremamente utile per distribuzioni out-of-box, ovvero quando un amministratore collega semplicemente un nuovo dispositivo WAP a una LAN per la prima volta.

Se il dispositivo WAP utilizza un registrar integrato, i nuovi client vengono registrati utilizzando la configurazione del VAP associato al servizio WPS, a prescindere dal fatto che la configurazione sia stata effettuata direttamente sul dispositivo WAP o acquisita da un registrar esterno attraverso WPS.

Tasto

Il dispositivo WAP registra i client 802.11 tramite WPS attraverso due metodi: il metodo Push-Button Control (PBC) o il Personal Identification Number (PIN).

Nel primo caso l'utente di un potenziale client preme un tasto sul dispositivo da registrare e l'amministratore del dispositivo WAP con registrar integrato preme un tasto simile (hardware o software) sul suo dispositivo. Questa sequenza avvia il processo di registrazione e il dispositivo client entra in rete. Sebbene i dispositivi WAP Cisco non supportino un tasto hardware vero e proprio, l'amministratore può avviare la registrazione per un particolare VAP utilizzando un pulsante software nell'utilità di configurazione basata sul Web.

NOTA L'ordine di selezione del tasto sul dispositivo client e sul dispositivo WAP non è importante. La registrazione può essere avviata da uno qualunque dei due dispositivi. Tuttavia, se si seleziona il pulsante software sul dispositivo WAP e nessun client tenta di registrarsi dopo 120 secondi, la transazione di registrazione WPS in sospeso sul dispositivo WAP viene terminata.

Controllo tramite PIN

È anche possibile utilizzare un PIN per registrare un client su un registrar. Ad esempio, l'amministratore del dispositivo WAP può immettere il PIN di un client per avviare una transazione di registrazione per un particolare VAP. Quando il client rileva il dispositivo con abilitazione WPS, l'utente può fornire il suo PIN al dispositivo WAP per proseguire il processo di registrazione. Una volta completato il protocollo WPS, il client entra in modo sicuro in rete. Questo processo può essere avviato anche dal client.

Come nel caso del metodo PBC, se il dispositivo WAP avvia la transazione di registrazione e nessun client tenta di registrarsi dopo 120 secondi, la transazione in sospeso sul dispositivo WAP viene terminata.

L'utilizzo del registrar integrato nel dispositivo WAP è facoltativo. Un dispositivo WAP, se configurato da un registrar esterno, agisce da proxy per quel registrar, a prescindere dal fatto che il registrar integrato del dispositivo WAP sia attivato (impostazione predefinita) o meno.

Ciascun dispositivo WAP archivia un PIN dispositivo compatibile con WPS in una RAM non volatile. Questo PIN è necessario se un amministratore desidera consentire a un dispositivo WAP non configurato (ovvero un dispositivo con le impostazioni predefinite in fabbrica, tra cui l'abilitazione WPS su un VAP) di entrare in una rete. In questo scenario, l'amministratore ottiene il valore del PIN dall'utilità di configurazione del dispositivo WAP.

Se l'integrità della rete è stata compromessa, l'amministratore può modificare il PIN. Il dispositivo WAP fornisce, infatti, un metodo per generare un nuovo PIN e memorizzarlo nella NVRAM. Se il valore nella NVRAM è danneggiato, viene cancellato o non è presente, il dispositivo WAP genera un nuovo PIN che viene memorizzato nella NVRAM.

Il metodo di registrazione tramite PIN è potenzialmente vulnerabile agli attacchi. Un intruso nella rete potrebbe presentarsi come registrar esterno sulla LAN wireless e tentare di ricavare il valore del PIN del dispositivo WAP applicando in modo esaustivo tutti i PIN conformi a WPS. Per contrastare questa vulnerabilità, se un registrar sbaglia tre tentativi di immissione del PIN corretto entro 60 secondi, il dispositivo WAP blocca ulteriori tentativi di registrazione al dispositivo WAP sul VAP con abilitazione WPS per 60 secondi. La durata del blocco aumenta in caso di tentativi non riusciti in successione fino a un massimo di 64 minuti. La funzionalità di registrazione dei dispositivi WAP viene bloccata in maniera permanente dopo il decimo tentativo consecutivo non riuscito. Per riavviare la funzionalità di registrazione, è necessario reimpostare il dispositivo.

Tuttavia, durante il periodo di blocco le stazioni client wireless possono registrarsi con il registrar integrato del dispositivo WAP, se attivato. Il dispositivo WAP continua inoltre a fornire servizi proxy per le richieste di registrazione a registrar esterni.

Il dispositivo WAP ha funzionalità di sicurezza aggiuntive per la protezione del PIN dispositivo. Al termine della registrazione del dispositivo WAP con un registrar esterno e della transazione WPS risultante, il PIN dispositivo viene rigenerato automaticamente.

Il protocollo WPS può configurare i seguenti parametri per un VAP con abilitazione WPS su un dispositivo WAP:

- SSID di rete
- Opzioni di gestione delle chiavi (WPA-PSK o WPA-PSK e WPA2-PSK)
- Opzioni di crittografia (CCMP/AES o TKIP e CCMP/AES)
- Chiave di rete (condivisa pubblica)

Se un VAP è abilitato per il protocollo WPS, questi parametri di configurazione sono soggetti a modifica e vengono mantenuti tra due riavvii del dispositivo WAP.

Il dispositivo WAP supporta la registrazione con registrar esterni (ER, External Registrar) WPS sulla LAN cablata e wireless. Sulla WLAN, i registrar esterni dichiarano le loro funzionalità all'interno di Information Elements (IE) specifici per WPS dei loro frame beacon; sulla LAN cablata, i registrar esterni annunciano la loro presenza attraverso UPnP.

Per il protocollo WPS v2.0 non è necessario registrarsi con un ER attraverso l'interfaccia utente. L'amministratore può registrare il dispositivo WAP con un ER nei modi seguenti:

PASSAGGIO 1 Inserimento del PIN ER sul dispositivo WAP.

PASSAGGIO 2 Inserimento del PIN dispositivo WAP sull'interfaccia utente dell'ER.

NOTA Durante il processo di registrazione, il dispositivo WAP può anche essere configurato in base alle impostazioni dell'area VAP Configuration Changes, se negli IE specifici per WPS dei frame beacon o dei messaggi UPnP del dispositivo WAP è stato indicato di richiedere tale configurazione.

Il dispositivo WAP può fungere da proxy per un massimo di tre registrar esterni simultaneamente.

Qualunque VAP sul dispositivo WAP può essere abilitato per WPS. Sul dispositivo WAP può essere attiva una sola transazione WPS alla volta, ad esempio la registrazione e l'associazione di un client 802.11. L'amministratore del dispositivo WAP può terminare la transazione in corso dall'utilità di configurazione dell'access point basata sul Web. Tuttavia, non si dovrebbe modificare la configurazione del VAP durante la transazione né il VAP durante il processo di autenticazione. Questa restrizione è raccomandata ma non obbligatoria sul dispositivo WAP.

Sebbene i dispositivi WAP supportino il protocollo WPS versione 2.0, il dispositivo WAP interagisce con dispositivi registrati e registrar con certificato Wi-Fi Alliance di conformità alla versione 1.0 del protocollo WPS.

Utilizzare la pagina WPS Setup per attivare il dispositivo WAP come dispositivo WPS e configurare le impostazioni di base. Per utilizzare la funzionalità di registrazione di un nuovo dispositivo o aggiungere il dispositivo WAP a una rete abilitata per WPS, visualizzare la pagina **Processo WPS**.

ATTENZIONE Per motivi di sicurezza, si raccomanda (ma non vi è alcun obbligo) di utilizzare una connessione HTTPS all'utilità di configurazione dell'access point basata sul Web quando si configura WPS.

Per configurare il dispositivo WAP come dispositivo WPS, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Wireless** > **WPS Setup**.

Nella pagina WPS Setup vengono mostrati i parametri e lo stato a livello globale e dell'istanza WPS. Un'istanza è un'implementazione del protocollo WPS associata a un VAP sulla rete. Il dispositivo WAP supporta una sola istanza.

PASSAGGIO 2 Configurare i parametri globali:

- **Supported WPS Version**: la versione del protocollo WPS supportata dal dispositivo WAP.
- **WPS Device Name**: il nome predefinito per il dispositivo. È possibile assegnare un nome diverso composto da 1 a 32 caratteri, inclusi spazi e caratteri speciali.
- **WPS Global Operational Status**: mostra se lo stato operativo del protocollo WPS è attivo o inattivo sul dispositivo WAP.
- **WPS Device PIN**: un PIN WPS di otto cifre generato dal sistema per il dispositivo WAP. L'amministratore può utilizzare questo PIN per registrare il dispositivo WAP con un registrar esterno.

  Per generare un nuovo PIN, fare clic su **Generate**. Se l'integrità di rete è stata compromessa, è opportuno generare un nuovo PIN.

PASSAGGIO 3 Configurare i parametri dell'istanza WPS:

- **WPS Instance ID**: identificativo dell'istanza. Poiché esiste una sola istanza, l'unica opzione disponibile è wps1.

- **WPS Mode**: attiva o disattiva l'istanza.
- **WPS Radio**: l'interfaccia radio a cui si applica questa istanza WPS (soltanto dispositivi WAP561).
- **WPS VAP**: il VAP associato a questa istanza WPS.
- **WPS Built-in Registrar**: attiva il registrar integrato. Se si seleziona questa opzione, i dispositivi registrati (solitamente client WLAN) possono eseguire la registrazione al dispositivo WAP. Se disattivata, il registrar sul dispositivo WAP viene disattivato e i dispositivi registrati devono utilizzare un altro registrar della rete. In questo caso, un altro dispositivo della rete agirà da registrar e il dispositivo WAP fungerà da proxy per l'inoltro delle richieste di registrazione client e le risposte del registrar.
- **WPS Configuration State**: specifica se il VAP sarà configurato dal registrar esterno nell'ambito del processo WPS. È possibile scegliere uno dei valori seguenti:
  - **Unconfigured**: le impostazioni VAP sono configurate tramite WPS; al termine della configurazione lo stato diventerà Configured.
  - **Configured**: le impostazioni VAP non sono configurate da un registrar esterno e manterranno la configurazione esistente.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Vengono visualizzati lo stato operativo dell'istanza e la motivazione dello stato. Per informazioni sulle condizioni che possono causare la disattivazione dell'istanza, vedere la sezione relativa all'attivazione o alla disattivazione di WPS su un VAP.

Nell'area Instance Status vengono mostrate le seguenti informazioni sull'istanza WPS selezionata:

- **WPS Operational Status**: mostra se l'istanza WPS è operativa o meno.
- **AP Lockdown Status**: mostra se l'AP è in modalità di blocco, in cui i registrar esterni sono bloccati e non possono effettuare la registrazione con l'AP. In stato di blocco, questo campo riporta l'orario di inizio del blocco, indicando se sia temporaneo o permanente e, se temporaneo, la durata del blocco. Se la modalità di blocco non è attiva, lo stato viene visualizzato come **Disabled**.
- **Failed Attempts with Invalid PIN**: il numero di tentativi di registrazione al dispositivo WAP falliti da un registrar esterno.

In stato di blocco vengono visualizzati i seguenti campi:

- **AP Lockdown Duration**: la durata in minuti del blocco del WAP 1 Se il WAP è bloccato in maniera permanente, questo valore è impostato su –1.
- **AP Lockdown Timestamp**: l'ora in cui il dispositivo WAP è stato bloccato.

Fare clic su **Refresh** per aggiornare la pagina con le informazioni più recenti sullo stato.

Processo WPS

Utilizzare la pagina WPS Process per utilizzare il dispositivo WPA per registrare una stazione client sulla rete. Per registrare un client, è possibile utilizzare un PIN o un tasto, se supportato sulla stazione client.

Per registrare una stazione client tramite il metodo PIN, attenersi alla seguente procedura:

PASSAGGIO 1 Ottenere il PIN dal dispositivo client. Il PIN può essere stampato sul dispositivo o rilevato nell'interfaccia software del dispositivo.

PASSAGGIO 2 Nel riquadro di spostamento, selezionare **Wireless** > **WPS Process**.

PASSAGGIO 3 Immettere il PIN del client nella casella di testo **PIN Enrollment** e fare clic su **Start**.

NOTA Oltre al PIN di otto cifre del dispositivo WPS (che può contenere zeri iniziali), è possibile immettere "stop" nella casella PIN Enrollment per interrompere la registrazione.

PASSAGGIO 4 Entro due minuti, immettere il PIN WAP nell'interfaccia software del dispositivo client. Il PIN WAP viene configurato nella pagina **Configurazione WPS**.

Quando si immette il PIN sul dispositivo client, lo stato operativo del protocollo WPS diventa Adding Enrollee. Al termine del processo di registrazione, lo stato operativo del protocollo WPS diventa Ready, mentre lo stato della transazione diventa Success.

Al termine della registrazione, il registrar integrato del dispositivo WAP o il registrar esterno sulla rete procedono alla configurazione del client con il nome SSID, la modalità di crittografa e la chiave condivisa pubblica di un BSS con abilitazione WPS.

ATTENZIONE La sequenza di registrazione può funzionare anche al contrario; questo significa che è possibile immettere il PIN del dispositivo WAP sulla stazione client per avviare il processo. Tuttavia, questo metodo **è sconsigliato** per motivi di sicurezza poiché consente al client di configurare il nome SSID e le impostazioni di protezione sull'AP. L'amministratore deve condividere il PIN soltanto con dispositivi attendibili.

Per registrare una stazione client tramite tasto, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Start** e selezionare **PCB Enrollment.**

PASSAGGIO 2 Premere il tasto hardware sulla stazione client.

NOTA In alternativa è possibile avviare il processo sulla stazione client e premere il tasto PBC Enrollment Start sul dispositivo WAP.

Quando si preme il tasto sulla stazione client, lo stato operativo del protocollo WPS diventa Adding Enrollee. Al termine del processo di registrazione, lo stato operativo del protocollo WPS diventa Ready, mentre lo stato della transazione diventa Success.

Al termine della registrazione, il registrar integrato del dispositivo WAP o il registrar esterno sulla rete procedono alla configurazione del client con il nome SSID, la modalità di crittografa e la chiave condivisa pubblica di un BSS con abilitazione WPS.

Nella sezione Instance Status vengono mostrate le seguenti informazioni sull'istanza WPS selezionata nell'elenco **WPS Instance ID**:

- **WPS Status**: mostra se l'istanza WPS selezionata è attivata o disattivata.
- **WPS Configuration State**: specifica se il VAP sarà configurato dal registrar esterno nell'ambito del processo WPS.
- **Transaction Status**: lo stato operativo dell'ultima transazione WPS. I valori possibili sono None, Success, WPS Message Error e Timed Out.
- **WPS Operational Status**: lo stato operativo della transazione WPS corrente o più recente. I valori possibili sono Disabled, Ready, Configuring, Proxying e Adding Enrollee. Se non sono state eseguite transazioni WPS dall'attivazione del protocollo WPS, viene visualizzato lo stato Ready.

- **AP Lockdown Status**: mostra se l'istanza è attualmente in stato di blocco.
- **Failed Attempts with Invalid PIN**: numero di tentativi di autenticazione di un registrar esterno falliti a causa di password errata.

Per l'istanza WPS vengono visualizzate le informazioni seguenti:

- **WPS Radio** (solo WAP561)
- **WPS VAP**
- **SSID**
- **Security**
- **Shared Key**

Se il campo WPS Configuration State della pagina WPS Setup è impostato su Unconfigured, i valori SSID e Security sono configurati dal registrar esterno. Se il campo è impostato su Configurato, questi valori sono configurati dall'amministratore.

NOTA Fare clic su **Refresh** per aggiornare la pagina con le informazioni più recenti sullo stato.

6

Sicurezza del sistema

In questo capitolo viene spiegato come configurare le impostazioni di sicurezza sul dispositivo WAP.

Vengono trattati i seguenti argomenti:

- **Server RADIUS**
- **Richiedente 802.1X**
- **Complessità password**
- **Complessità WPA-PSK**

Server RADIUS

Diverse funzioni richiedono la comunicazione con un server di autenticazione RADIUS. Ad esempio, quando si configurano gli access point virtuali (VAP, Virtual Access Point) sul dispositivo WAP, è possibile configurare alcuni metodi di protezione in grado di controllare l'accesso da parte dei client wireless (consultare la pagina **Radio**). I metodi di protezione Dynamic WEP e WPA Enterprise utilizzano un server RADIUS esterno per autenticare i client. La funzione di filtro dell'indirizzo MAC, che consente l'accesso soltanto a un elenco, può essere configurata anche in modo da utilizzare un server RADIUS per controllare gli accessi. Anche la funzione Captive Portal autentica i client tramite RADIUS.

Nella pagina Server RADIUS, è possibile configurare i server RADIUS utilizzati da queste funzioni. È possibile configurare fino a quattro server RADIUS IPv4 o IPv6 disponibili a livello globale; tuttavia, per quanto riguarda i server globali, è necessario scegliere la modalità di funzionamento del client RADIUS: IPv4 o IPv6. Un server funge sempre da server primario, mentre gli altri svolgono la funzione di server di backup.

NOTA Oltre a utilizzare i server RADIUS globali, è anche possibile configurare ciascun VAP in modo che utilizzi un determinato gruppo di server RADIUS. Vedere la pagina **Reti**.

Per configurare i server RADIUS globali, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **System Security** > **RADIUS Server**.

PASSAGGIO 2 Immettere i seguenti parametri:

- **Server IP Address Type**: la versione IP utilizzata dal server RADIUS.

  È possibile passare da un tipo di indirizzo a un altro per configurare le impostazioni dell'indirizzo RADIUS globale IPv4 e IPv6, tuttavia il dispositivo WAP contatta soltanto il server RADIUS o i server del tipo di indirizzo selezionato in questo campo.

- **Server IP Address 1** o **Server IPv6 Address 1**: gli indirizzi del server RADIUS globale primario.

  Quando il primo client wireless cerca di effettuare l'autenticazione con il dispositivo WAP, il dispositivo invia una richiesta di autenticazione al server primario. Se il server primario risponde alla richiesta di autenticazione, il dispositivo WAP continua a utilizzare questo server RADIUS come server primario e le richieste di autenticazione vengono inviate all'indirizzo specificato.

- **Server IP Address (da 2** a **4)** o **Server IPv6 Address (da 2** a **4)**: fino a tre indirizzi server RADIUS IPv4 o IPv6 di backup.

  Se l'autenticazione con il server primario ha esito negativo, si prova in sequenza con ciascun server di backup configurato.

- **Key 1**: la chiave segreta condivisa utilizzata dal dispositivo WAP per l'autenticazione con il server RADIUS primario.

  È possibile utilizzare da 1 a 64 caratteri speciali e alfanumerici standard. La chiave fa distinzione tra maiuscole e minuscole e deve corrispondere a quella configurata sul server RADIUS. Il testo inserito viene visualizzato sotto forma di asterischi.

- **Key (da 2** a **4)**: la chiave RADIUS associata ai server RADIUS di backup configurati. Il server indicato nel campo **Server IP (IPv6) Address 2** utilizza la chiave specificata nel campo **Key 2**; il server indicato nel campo **Server IP (IPv6) Address-3** utilizza, invece, la chiave specificata nel campo **Key 3** e così via.

- **Enable RADIUS Accounting**: consente di rilevare e misurare le risorse utilizzate da un determinato utente, ad esempio l'ora di sistema, la quantità di dati trasmessi e ricevuti e così via.

Se selezionata, la funzione di accounting RADIUS viene abilitata per il server RADIUS primario e per tutti i server di backup.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Richiedente 802.1X

Con l'autenticazione IEEE 802.1X, l'access point può accedere a una rete cablata protetta. È possibile abilitare l'access point come richiedente (client) 802.1X sulla rete cablata. Nome utente e password crittografati con l'algoritmo MD5 possono essere configurati in modo da consentire l'autenticazione dell'access point tramite 802.1X.

Sulle reti che utilizzano il controllo di accesso alla rete basato sulla porta IEEE 802.1X, un richiedente può ottenere l'accesso alla rete solo se concesso dall'autenticatore 802.1X. Se la rete utilizza 802.1X, è necessario configurare le informazioni di autenticazione 802.1X sul dispositivo WAP, in modo tale che vengano fornite all'autenticatore.

La pagina 802.1X Supplicant è suddivisa in tre aree: Supplicant Configuration, Certificate File Status e Certificate File Upload.

Nell'area Supplicant Configuration, è possibile configurare le impostazioni di base e lo stato operativo di 802.1X.

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **System Security** > **802.1X Supplicant**.

PASSAGGIO 2 Fare clic su **Refresh** per aggiornare lo stato del file di certificato.

PASSAGGIO 3 Immettere i seguenti parametri:

- **Administrative Mode**: abilita la funzionalità 802.1X Supplicant.
- **EAP Method**: l'algoritmo da utilizzare per crittografare password e nomi utente utilizzati per l'autenticazione.
  - **MD5**: una funzione di hashing definita in RFC 3748 che fornisce la protezione di base.
  - **PEAP** (Protected Extensible Authentication Protocol): fornisce un livello di protezione più elevato rispetto a MD5 tramite l'incapsulamento in un tunnel TLS.

- **TLS** (Transport Layer Security): uno standard aperto che fornisce un elevato livello di protezione, come definito in RFC 5216.

- **Username**: il dispositivo WAP utilizza questo nome utente quando risponde alle richieste provenienti da un autenticatore 802.1X. Il nome utente può essere composto da un numero di caratteri compreso tra 1 e 64. È possibile utilizzare caratteri stampabili ASCII, che includono lettere maiuscole e minuscole, cifre e qualsiasi carattere speciale tranne le virgolette.
- **Password**: il dispositivo WAP utilizza questa password MD5 quando risponde alle richieste provenienti da un autenticatore 802.1X. La password può essere composta da un numero di caratteri compreso tra 1 e 64. È possibile utilizzare caratteri stampabili ASCII, che includono lettere maiuscole e minuscole, cifre e qualsiasi carattere speciale tranne le virgolette.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Nell'area Certificate File Status viene indicato se esiste un certificato corrente:

- **Certificate File Present**: indica se è presente il file del certificato SSL HTTP. Se presente, nel campo compare la voce Sì. L'impostazione predefinita è No.
- **Certificate Expiration Date**: indica la scadenza del file del certificato SSL HTTP. L'intervallo è una data valida.

L'area Certificate File Upload consente di caricare un file di certificato sul dispositivo WAP:

PASSAGGIO 1 Selezionare **HTTP** o **TFTP** come metodo di trasferimento.

PASSAGGIO 2 Se si seleziona HTTP, fare clic su **Sfoglia** per selezionare il file.

NOTA Per configurare le impostazioni del server HTTPS e HTTP, consultare la sezione **Servizio HTTP/HTTPS**.

Se si seleziona TFTP, immettere il nome del file nel campo **Filename** e l'indirizzo IPv4 del server TFTP. Il nome file non può contenere i seguenti caratteri: spazi, <, >, |, \, : , (,), &, ; , #, ? , * e due o più punti consecutivi.

PASSAGGIO 3 Fare clic su **Upload**.

Viene visualizzata una finestra di conferma, seguita da una barra di avanzamento che indica lo stato del caricamento.

Complessità password

È possibile configurare i requisiti di complessità delle password utilizzate per accedere all'utilità di configurazione del dispositivo WAP. Le password complesse garantiscono una maggiore sicurezza.

Per configurare i requisiti di complessità delle password, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **System Security** > **Password Complexity**.

PASSAGGIO 2 Per l'impostazione **Password Complexity**, selezionare **Enable**.

PASSAGGIO 3 Configurare i seguenti parametri:

- **Password Minimum Character Class**: il numero minimo di classi di caratteri che devono essere rappresentati nella stringa della password. Le quattro classi di caratteri possibili sono: lettere maiuscole, lettere minuscole, numeri e caratteri speciali disponibili sulla tastiera standard.
- **Password Different From Current**: selezionare questa opzione per chiedere agli utenti di immettere una password diversa quando scade quella corrente. Se questa opzione non viene selezionata, gli utenti potranno selezionare nuovamente la stessa password quando scade.
- **Maximum Password Length**: la lunghezza massima della password è compresa tra 64 e 80 caratteri. Il valore predefinito è 64.
- **Minimum Password Length**: la lunghezza minima della password è compresa tra 0 e 32 caratteri. Il valore predefinito è 8.
- **Password Aging Support**: selezionare questa opzione per far sì che le password scadano dopo un determinato periodo di tempo.
- **Password Aging Time**: il numero di giorni (compreso tra 1 e 365) di durata della password creata. Il valore predefinito è 180 giorni.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Complessità WPA-PSK

Quando si configurano i VAP sul dispositivo WAP, è possibile selezionare un metodo per autenticare i client in modo sicuro. Se si seleziona il protocollo WPA Personal (detto anche chiave WPA precondivisa o WPA-PSK) come metodo di protezione per i VAP, è possibile utilizzare la pagina Complessità WPA-PSK per configurare i requisiti di complessità per la chiave utilizzata nella procedura di autenticazione. Le chiavi più complesse garantiscono una maggiore protezione.

Per configurare la complessità di WPA-PSK, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **System Security** > **WPA-PSK Complexity**.

PASSAGGIO 2 Fare clic su **Enable** per l'impostazione **WPA-PSK Complexity** per far sì che il dispositivo WAP verifichi le chiavi WPA-PSK in base ai criteri configurati. Se si deseleziona la casella, non verrà utilizzata alcuna di queste impostazioni. L'opzione WPA-PSK Complexity è disattivata per impostazione predefinita.

PASSAGGIO 3 Configurare i seguenti parametri:

- **WPA-PSK Minimum Character Class**: il numero minimo di classi di caratteri che devono essere rappresentati nella stringa della chiave. Le quattro classi di caratteri possibili sono: lettere maiuscole, lettere minuscole, numeri e caratteri speciali disponibili sulla tastiera standard. Il valore predefinito è tre.
- **WPA-PSK Different From Current**: selezionare una di queste opzioni:
  - **Enable**: alla scadenza della chiave corrente, gli utenti ne devono configurare una diversa.
  - **Disable**: alla scadenza della chiave corrente gli utenti possono continuare a utilizzarla.
- **Maximum WPA-PSK Length**: la lunghezza massima della chiave è compresa tra 32 e 63 caratteri. Il valore predefinito è 63.
- **Minimum WPA-PSK Length**: la lunghezza minima della chiave è compresa tra 8 e 16 caratteri. Il valore predefinito è 8. Selezionare la casella per rendere modificabile il campo e attivare questo requisito.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

7

Qualità del servizio dei client

In questo capitolo viene presentata una panoramica della qualità del servizio (QoS, Quality of Service) dei client e vengono descritte le opzioni disponibili nel menu Client QoS. Vengono trattati i seguenti argomenti:

- **Impostazioni generali di Client QoS**
- **ACL**
- **Mappa delle classi**
- **Mappa dei criteri**
- **Associazione di Client QoS**
- **Stato di Client QoS**

Impostazioni generali di Client QoS

Utilizzare la pagina Client QoS Global Settings per attivare o disattivare la funzionalità QoS sul dispositivo WAP.

Se si disattiva l'opzione **Client QoS Mode**, tutti gli ACL, le limitazioni di velocità e le configurazioni DiffServ vengono disattivati a livello globale.

Se si attiva questa modalità è anche possibile attivare o disattivare la modalità Client QoS su determinati VAP. Vedere l'impostazione **Client QoS Mode** nella sezione *Associazione di Client QoS*.

ACL

Gli ACL sono una raccolta di condizioni di permesso e negazione, dette regole, che garantiscono protezione bloccando gli utenti non autorizzati e consentendo a quelli autorizzati di accedere a risorse specifiche. Gli ACL possono bloccare qualsiasi tentativo ingiustificato di accedere alle risorse di rete.

Il dispositivo WAP supporta fino a 50 ACL IPv4, IPv6 e MAC.

Gli ACL IP classificano il traffico per i livelli 3 e 4.

Ogni ACL è un insieme di massimo 10 regole applicate al traffico inviato o ricevuto dal dispositivo WAP. Ogni regola specifica se utilizzare i contenuti di un determinato campo per consentire o negare l'accesso alla rete. Le regole possono essere basate su diversi criteri e si possono applicare a uno o più campi in un pacchetto, come l'indirizzo IP di origine o di destinazione, la porta di origine o di destinazione o il protocollo contenuto nel pacchetto.

NOTA Al termine di ogni regola creata è presente una negazione implicita. Per evitare la negazione di tutto, si consiglia di aggiungere una regola di autorizzazione all'interno dell'ACL per consentire il traffico.

Gli ACL MAC sono ACL di livello 2. È possibile configurare le regole per esaminare i campi di un frame come l'indirizzo MAC di origine o di destinazione, l'ID VLAN o la classe di servizio. I frame che entrano o escono dalla porta di un dispositivo WAP (a seconda che l'ACL sia applicato in entrata o in uscita) vengono esaminati e confrontati con le regole ACL. Se viene trovata una corrispondenza fra le regole e il contenuto, viene eseguita un'azione di autorizzazione o negazione sul frame.

Utilizzare la pagina ACL Configuration per configurare gli ACL e le regole, quindi applicare le regole al VAP specificato.

Questi passaggi forniscono una descrizione generale della configurazione degli ACL:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Client QoS** > **ACL**.

PASSAGGIO 2 Specificare un nome per l'ACL.

PASSAGGIO 3 Selezionare il tipo di ACL da aggiungere.

PASSAGGIO 4 Aggiungere l'ACL.

PASSAGGIO 5 Aggiungere nuove regole all'ACL.

PASSAGGIO 6 Configurare i criteri di corrispondenza per le regole.

PASSAGGIO 7 Utilizzare la pagina **Associazione di Client QoS** per applicare l'ACL a uno o più VAP.

Questi passaggi forniscono una descrizione dettagliata della configurazione degli ACL:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Client QoS** > **ACL**.

PASSAGGIO 2 Per creare un nuovo ACL, specificare i parametri seguenti:

- **ACL Name**: un nome che identifichi l'ACL. Il nome dell'ACL può contenere da 1 a 31 caratteri alfanumerici e i seguenti caratteri speciali: trattini, caratteri di sottolineatura, barra rovesciata e due punti. Gli spazi non sono consentiti.
- **ACL Type**: il tipo di ACL da configurare:
  - IPv4
  - IPv6
  - MAC

  Gli ACL IPv4 e IPv6 controllano l'accesso alle risorse di rete in base ai criteri di livello 3 e livello 4. Gli ACL MAC controllano l'accesso in base ai criteri di livello 2.

PASSAGGIO 3 Fare clic su **Add ACL**.

Nella pagina vengono mostrati campi aggiuntivi per la configurazione dell'ACL.

PASSAGGIO 4 Configurare i parametri delle regole:

- **ACL Name - ACL Type**: l'ACL da configurare con la nuova regola. L'elenco contiene tutti gli ACL aggiunti nell'area ACL Configuration.
- **Rule**: l'azione da intraprendere:
  - Selezionare **New Rule** per configurare una nuova regola per l'ACL selezionato.
  - Se le regole esistono già (anche se create per altri ACL), è possibile selezionare il numero di regola per aggiungerla all'ACL selezionato o per modificarla.

  Se l'ACL ha più di una regola, le regole vengono applicate al pacchetto o al frame nell'ordine in cui vengono aggiunte all'ACL. La regola finale è una regola implicita che nega tutto.

- **Action**: se la regola ACL consente o nega un'azione.

  Se si seleziona Permit, la regola consente tutto il traffico che soddisfa i criteri della regola per entrare o uscire dal dispositivo WAP (in base alla direzione dell'ACL selezionato). Il traffico che non soddisfa i criteri viene eliminato.

  Se si seleziona Deny, la regola impedisce a tutto il traffico che soddisfa i criteri della regola di entrare o uscire dal dispositivo WAP (in base alla direzione dell'ACL selezionato). Il traffico che non soddisfa i criteri viene inoltrato, a meno che si tratti della regola finale. Poiché al termine di ogni ACL è presente una regola implicita che nega tutto, il traffico che non viene esplicitamente consentito viene eliminato.

- **Match Every Packet**: se selezionata, la regola, che ha un'azione di autorizzazione o negazione, utilizza il frame o il pacchetto per la corrispondenza indipendentemente dal contenuto.

  Se si seleziona questo campo non è possibile configurare criteri di corrispondenza aggiuntivi. L'opzione Match Every Packet è selezionata per impostazione predefinita per le nuove regole. Per configurare altri campi di corrispondenza è necessario disattivare questa opzione.

Per gli ACL IPv4, configurare i seguenti parametri:

- **Protocol**: selezionare il campo Protocol per utilizzare una condizione di corrispondenza del protocollo di livello 3 o livello 4 in base al valore del campo IP Protocol nei pacchetti IPv4 o del campo Next Header nei pacchetti IPv6.

  Se si seleziona Protocol, scegliere una delle seguenti opzioni:

  - **Select From List**: selezionare uno dei protocolli seguenti: IP, ICMP, IGMP, TCP o UDP.
  - **Match to Value**: immettere l'ID di un protocollo standard assegnato da IANA compreso tra 0 e 255. Scegliere questo metodo per identificare un protocollo che non compare nell'elenco del campo Select From List.

- **Source IP Address**: l'indirizzo IP di origine del pacchetto deve corrispondere all'indirizzo elencato qui. Per applicare questo criterio, immettere un indirizzo IP nel campo appropriato.

- **Wild Card Mask**: la maschera di controllo di accesso per l'indirizzo IP di origine.

La maschera di controllo di accesso definisce i bit che vengono utilizzati e quelli che vengono ignorati. La maschera 255.255.255.255 indica che nessun bit è importante, mentre la maschera 0.0.0.0 indica che tutti i bit sono importanti. Se si seleziona l'opzione Source IP Address, questo campo è obbligatorio.

Una maschera di controllo di accesso è sostanzialmente il contrario di una subnet mask. Ad esempio, per la corrispondenza dei criteri a un singolo indirizzo host, utilizzare la maschera di controllo di accesso 0.0.0.0. Per far corrispondere i criteri a una sottorete a 24 bit, ad esempio 192.168.10.0/24, utilizzare la maschera di controllo di accesso 0.0.0.255.

- **Source Port**: include una porta di origine nella condizione di corrispondenza per la regola. La porta di origine è identificata nell'intestazione del datagramma.

  Se si seleziona Source Port, scegliere il nome della porta o inserire il relativo numero.

  - **Select From List**: la parola chiave associata alla porta di origine da associare: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Ognuna di queste parole chiave viene convertita nel numero di porta equivalente.

  - **Match to Port**: il numero di porta IANA che deve corrispondere alla porta di destinazione identificata nell'intestazione del datagramma. L'intervallo di porte è compreso tra 0 e 65535 e comprende tre diversi tipi di porte:

    Da 0 a 1023: porte comuni

    Da 1024 a 49151: porte registrate

    Da 49152 a 65535: porte dinamiche e/o private

- **Destination IP Address**: è necessario che un indirizzo IP di destinazione del pacchetto corrisponda all'indirizzo elencato qui. Per applicare questo criterio, immettere un indirizzo IP nel campo appropriato.
- **Wild Card Mask**: la maschera di controllo di accesso per l'indirizzo IP di destinazione.

  La maschera di controllo di accesso definisce i bit che vengono utilizzati e quelli che vengono ignorati. La maschera 255.255.255.255 indica che nessun bit è importante, mentre la maschera 0.0.0.0 indica che tutti i bit sono importanti. Se si seleziona l'opzione Source IP Address, questo campo è obbligatorio.

Una maschera di controllo di accesso è sostanzialmente il contrario di una subnet mask. Ad esempio, per associare i criteri a un singolo indirizzo host, utilizzare la maschera di controllo di accesso 0.0.0.0. Per associare i criteri a una sottorete a 24 bit, ad esempio 192.168.10.0/24, utilizzare la maschera di controllo di accesso 0.0.0.255.

- **Destination Port**: include una porta di destinazione nella condizione di corrispondenza per la regola. La porta di destinazione è identificata nell'intestazione del datagramma.

  Se si seleziona Destination Port, scegliere il nome della porta o immettere il relativo numero.

  - **Select From List**: selezionare la parola chiave associata alla porta di destinazione da associare: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Ognuna di queste parole chiave viene convertita nel numero di porta equivalente.

  - **Match to Port**: il numero di porta IANA da associare alla porta di destinazione identificata nell'intestazione del datagramma. L'intervallo delle porte è compreso tra 0 e 65535 e comprende tre diversi tipi:

    Da 0 a 1023: porte comuni

    Da 1024 a 49151: porte registrate

    Da 49152 a 65535: porte dinamiche e/o private

- **IP DSCP**: utilizza il valore IP DSCP dei pacchetti per la corrispondenza.

  Se si seleziona IP DSCP, scegliere una delle opzioni seguenti come criterio di corrispondenza:

  - **Select From List**: valori DSCP Assured Forwarding (AS), Class of Service (CoS) o Expedited Forwarding (EF).

  - **Match to Value**: un valore DSCP personalizzato, da 0 a 63.

- **IP Precedence**: utilizza il valore di precedenza IP dei pacchetti per la corrispondenza. Se si seleziona questa opzione, immettere un valore di precedenza IP compreso tra 0 e 7.

- **IP TOS Bits**: specifica un valore che consente di utilizzare i bit Type of Service del pacchetto nell'intestazione IP come criterio di corrispondenza.

Per definizione, il campo IP TOS in un pacchetto corrisponde agli otto bit dell'ottetto Service Type nell'intestazione IP. Il valore IP TOS Bits è un numero esadecimale a due cifre compreso tra 00 e ff.

I tre bit di ordine elevato rappresentano il valore di precedenza IP. I sei bit di ordine elevato rappresentano il valore IP DSCP (Differentiated Services Code Point).

- **IP TOS Mask**: immettere un valore IP TOS Mask che consente di identificare le posizioni dei bit nel valore IP TOS Bits utilizzati per il confronto con il campo IP TOS in un pacchetto.

  Il valore IP TOS Mask è un numero esadecimale a due cifre compreso tra 00 e FF, che rappresenta una maschera invertita, ovvero una maschera di controllo di accesso. I bit pari a zero in IP TOS Mask indicano le posizioni dei bit nel valore IP TOS Bits utilizzati per il confronto con il campo IP TOS di un pacchetto. Ad esempio, per trovare un valore IP TOS con i bit 7 e 5 impostati e il bit 1 cancellato, dove il bit 7 è il più significativo, utilizzare un valore IP TOS Bits pari a 0 e un IP TOS Mask pari a 00.

Per gli ACL IPv6, configurare i seguenti parametri:

- **Protocol**: selezionare il campo Protocol per utilizzare una condizione di corrispondenza del protocollo di livello 3 o livello 4 in base al valore del campo IP Protocol nei pacchetti IPv4 o del campo Next Header nei pacchetti IPv6.

  Se si seleziona questo campo, scegliere il protocollo per la corrispondenza in base alla parola chiave o all'ID protocollo.

- **Source IPv6 Address**: selezionare questo campo per richiedere che un indirizzo IPv6 di origine del pacchetto corrisponda all'indirizzo elencato qui. Per applicare questo criterio, immettere un indirizzo IPv6 nel campo appropriato.

- **Source IPv6 Prefix Length**: immettere la lunghezza del prefisso dell'indirizzo IPv6 di origine.

- **Source Port**: selezionare questa opzione per includere una porta di origine nella condizione di corrispondenza per la regola. La porta di origine è identificata nell'intestazione del datagramma. Se si seleziona questa opzione, scegliere il nome della porta o inserire il relativo numero.

- **Destination IPv6 Address**: selezionare questo campo per richiedere che un indirizzo IPv6 di destinazione del pacchetto corrisponda all'indirizzo elencato qui. Per applicare questo criterio, immettere un indirizzo IPv6 nel campo appropriato.

- **Destination IPv6 Prefix Length**: immettere la lunghezza del prefisso dell'indirizzo IPv6 di destinazione.
- **Destination Port**: selezionare questa opzione per includere una porta di destinazione nella condizione di corrispondenza per la regola. La porta di destinazione è identificata nell'intestazione del datagramma. Se si seleziona questa opzione, scegliere il nome della porta o inserire il relativo numero.
- **IPv6 Flow Label**: un numero a 20 bit univoco per un pacchetto IPv6. Questo numero viene utilizzato dalle stazioni terminali per indicare la gestione di QoS nei router (intervallo tra 0 e 1048575).
- **IP DSCP**: utilizza il valore IP DSCP dei pacchetti per la corrispondenza. Se si seleziona questa opzione, scegliere una delle opzioni seguenti come criterio di corrispondenza:
  - **Select From List**: valori DSCP Assured Forwarding (AS), Class of Service (CoS) o Expedited Forwarding (EF).
  - **Match to Value**: un valore DSCP personalizzato, da 0 a 63.

Per un ACL MAC, configurare i seguenti parametri:

- **EtherType**: selezionare questo parametro per confrontare i criteri di corrispondenza con il valore nell'intestazione di un frame Ethernet.

  Selezionare una parola chiave EtherType oppure immettere un valore EtherType per specificare i criteri di corrispondenza.
  - **Select From List**: selezionare uno dei seguenti tipi di protocollo: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.
  - **Match to Value**: immettere un identificatore di protocollo personalizzato a cui devono corrispondere i pacchetti. Il valore immesso in questo campo è un numero esadecimale a quattro cifre compreso tra 0600 e FFFF.
- **Class of Service**: selezionare questo campo e immettere una priorità utente 802.1p per il confronto con un frame Ethernet.

  L'intervallo valido è compreso tra 0 e 7. Questo campo si trova nel primo/unico tag VLAN 802.1Q.
- **Source MAC Address**: selezionare questo campo e immettere l'indirizzo MAC di origine per il confronto con un frame Ethernet.
- **Source MAC Mask**: selezionare questo campo e immettere la maschera dell'indirizzo MAC di origine per specificare quali bit nel MAC di destinazione sono da confrontare con un frame Ethernet.

Per ogni posizione bit nella maschera MAC, uno 0 indica che il bit dell'indirizzo corrispondente è importante e un 1 indica che il bit dell'indirizzo viene ignorato. Ad esempio, per verificare soltanto i primi quattro ottetti di un indirizzo MAC viene utilizzata la maschera MAC 00:00:00:00:ff:ff. La maschera MAC 00:00:00:00:00:00 verifica tutti i bit dell'indirizzo e viene utilizzata per la corrispondenza con un singolo indirizzo MAC.

- **Destination MAC Address**: selezionare questo campo e immettere l'indirizzo MAC di destinazione da confrontare con un frame Ethernet.
- **Destination MAC Mask**: immettere la maschera dell'indirizzo MAC di destinazione per specificare quali bit nel MAC di destinazione sono da confrontare con un frame Ethernet.

  Per ogni posizione bit nella maschera MAC, uno 0 indica che il bit dell'indirizzo corrispondente è importante e un 1 indica che il bit dell'indirizzo viene ignorato. Ad esempio, per verificare soltanto i primi quattro ottetti di un indirizzo MAC viene utilizzata la maschera MAC 00:00:00:00:ff:ff. La maschera MAC 00:00:00:00:00:00 verifica tutti i bit dell'indirizzo e viene utilizzata per la corrispondenza con un singolo indirizzo MAC.
- **VLAN ID**: selezionare questo campo e immettere l'ID VLAN specifico per il confronto con un frame Ethernet.

  Questo campo si trova nel primo/unico tag VLAN 802.1Q.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare un ACL, selezionarlo nell'elenco **ACL Name-ACL Type**, selezionare **Delete ACL** e fare clic su **Salva**.

Mappa delle classi

La funzione Client QoS supporta DiffServ (Differentiated Services) che consente di classificare il traffico in flussi e di dargli un certo trattamento QoS in base ai comportamenti per-hop definiti.

Le reti standard basate su IP sono concepite per fornire un servizio di trasferimento dati basato sul massimo impegno. Questo servizio implica che la rete trasmette i dati in maniera tempestiva, ma non vi è alcuna garanzia che lo farà. Durante i periodi di congestione, i pacchetti possono essere ritardati, inviati sporadicamente oppure eliminati. Per le applicazioni Internet comuni, come la

posta elettronica e il trasferimento di file, una riduzione minima delle prestazioni del servizio è accettabile e, in molti casi, impercettibile. Tuttavia, nel caso di applicazioni con requisiti temporali vincolanti, come quelle vocali o multimediali, anche la minima riduzione delle prestazioni può avere effetti indesiderati.

Per configurare il servizio DiffServ si definiscono prima le mappe delle classi, che classificano il traffico in base al loro protocollo IP o ad altri criteri. Ogni mappa delle classi può poi essere associata a una mappa di criteri, che stabilisce come gestire la classe di traffico. Le classi che includono traffico con esigenze temporali possono essere assegnate a mappe di criteri che diano la precedenza sull'altro traffico.

È possibile utilizzare la pagina Class Map per definire le classi di traffico. Utilizzare la pagina *Mappa dei criteri* per definire i criteri e associarli alle mappe delle classi.

Per aggiungere una mappa di classi, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Client QoS** > **Class Map**.

PASSAGGIO 2 Immettere un nome nel campo **Class Map Name**. Il nome può contenere da 1 a 31 caratteri alfanumerici e i seguenti caratteri speciali: trattini, caratteri di sottolineatura, barra rovesciata e due punti. Gli spazi non sono consentiti.

PASSAGGIO 3 Selezionare un valore dall'elenco **Match Layer 3 Protocol**:

- **IPv4**: la mappa delle classi viene applicata soltanto al traffico IPv4 sul dispositivo WAP.
- **IPv6**: la mappa delle classi viene applicata soltanto al traffico IPv6 sul dispositivo WAP.

Nella pagina Class Map vengono visualizzati campi aggiuntivi in base al protocollo di livello 3 selezionato:

Utilizzare i campi nell'area Match Criteria Configuration per verificare la corrispondenza dei pacchetti a una classe. Selezionare la casella accanto a ciascun campo da utilizzare come criterio per una classe e immettere i dati nel campo corrispondente. Una classe può contenere più criteri di corrispondenza.

I campi dei criteri di corrispondenza disponibili dipendono dal tipo di mappa delle classi, ovvero IPv4 o IPv6.

Per configurare una mappa di classi, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare la mappa di classi dall'elenco **Class Map Name**.

PASSAGGIO 2 Configurare i parametri seguenti (le opzioni disponibili soltanto per le mappe di classi IPv4 o IPv6 sono indicate):

- **Match Every Packet**: la condizione di corrispondenza è vera per tutti i parametri in un pacchetto di livello 3.

  Se si seleziona questa opzione, tutti i pacchetti di livello 3 soddisfano la condizione.

- **Protocol**: utilizzare una condizione di corrispondenza del protocollo di livello 3 o livello 4 in base al valore del campo IP Protocol nei pacchetti IPv4 o del campo Next Header nei pacchetti IPv6.

  Se si seleziona questo campo, scegliere il protocollo per verificare la corrispondenza in base alla parola chiave o immettere un ID protocollo.

  - **Select From List**: utilizzare il protocollo selezionato per la corrispondenza: IP, ICMP, IPv6, ICMPv6, IGMP, TCP, UDP.
  - **Match to Value**: utilizzare per la corrispondenza un protocollo che non è elencato in base al nome. Immettere l'ID protocollo (un valore standard assegnato da IANA). L'intervallo è compreso tra 0 e 255.

- **Source IP Address** o **Source IPv6 Address**: è necessario che un indirizzo IP di origine del pacchetto corrisponda all'indirizzo elencato qui. Selezionare la casella e immettere un indirizzo IP.

- **Source IP Mask** (soltanto IPv4): la maschera per l'indirizzo IP di origine.

  La maschera per DiffServ è una maschera di bit di tipo rete in formato IP decimale puntato che indica le parti dell'indirizzo IP di destinazione da utilizzare per la corrispondenza con il contenuto dei pacchetti.

  Una maschera DiffServ 255.255.255.255 indica che tutti i bit sono importanti, mentre una maschera 0.0.0.0 indica che nessun bit è importante. Con una maschera di controllo di accesso ACL è vero l'opposto. Ad esempio, per la corrispondenza dei criteri a un singolo indirizzo host, utilizzare la maschera 255.255.255.255. Per la corrispondenza dei criteri a una sottorete a 24 bit, ad esempio 192.168.10.0/24, utilizzare la maschera 255.255.255.0.

- **Source IPv6 Prefix Length** (soltanto IPv6): la lunghezza del prefisso dell'indirizzo IPv6 di origine.

- **Destination IP Address** o **Destination IPv6 Address**: è necessario che un indirizzo IP di destinazione del pacchetto corrisponda all'indirizzo elencato qui. Per applicare questo criterio, immettere un indirizzo IP nel campo appropriato.
- **Destination IP Mask** (soltanto IPv4): la maschera per l'indirizzo IP di destinazione.

  La maschera per DiffServ è una maschera di bit di tipo rete in formato IP decimale puntato che indica le parti dell'indirizzo IP di destinazione da utilizzare per la corrispondenza con il contenuto dei pacchetti.

  Una maschera DiffServ 255.255.255.255 indica che tutti i bit sono importanti, mentre una maschera 0.0.0.0 indica che nessun bit è importante. Con una maschera di controllo di accesso ACL è vero l'opposto. Ad esempio, per la corrispondenza dei criteri a un singolo indirizzo host, utilizzare la maschera 255.255.255.255. Per la corrispondenza dei criteri a una sottorete a 24-bit, ad esempio 192.168.10.0/24, utilizzare la maschera 255.255.255.0.
- **Destination IPv6 Prefix Length** (soltanto IPv6): la lunghezza del prefisso dell'indirizzo IPv6 di destinazione.
- **IPv6 Flow Label** (soltanto IPv6): un numero a 20 bit univoco per un pacchetto IPv6. Questo numero viene utilizzato dalle stazioni terminali per indicare la gestione di QoS nei router (intervallo tra 0 e 1048575).
- **IP DSCP**: vedere la descrizione nel campo Service Type.
- **Source Port**: include una porta di origine nella condizione di corrispondenza per la regola. La porta di origine è identificata nell'intestazione del datagramma.

  Se si seleziona questo campo, scegliere il nome della porta o inserire il relativo numero.

  - **Select From List**: utilizza una parola chiave associata alla porta di origine per la corrispondenza: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Ognuna di queste parole chiave viene convertita nel numero di porta equivalente.

  - **Match to Port**: utilizza il numero della porta di origine nell'intestazione del datagramma per la corrispondenza con un numero di porta IANA specificato. L'intervallo della porta è compreso tra 0 e 65535 e comprende tre diversi tipi di porte:

    Da 0 a 1023: porte comuni

Da 1024 a 49151: porte registrate

Da 49152 a 65535: porte dinamiche e/o private

- **Destination Port**: include una porta di destinazione nella condizione di corrispondenza per la regola. La porta di destinazione è identificata nell'intestazione del datagramma.

  Se si seleziona questo campo, scegliere il nome della porta o inserire il relativo numero.

  - **Select From List**: utilizza la porta di destinazione nell'intestazione del datagramma per la corrispondenza con la parola chiave selezionata: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Ognuna di queste parole chiave viene convertita nel numero di porta equivalente.

  - **Match to Port**: utilizza la porta di destinazione nell'intestazione del datagramma per la corrispondenza con un numero di porta IANA specificato. L'intervallo della porta è compreso tra 0 e 65535 e comprende tre diversi tipi di porte:

    Da 0 a 1023: porte comuni

    Da 1024 a 49151: porte registrate

    Da 49152 a 65535: porte dinamiche e/o private

- **EtherType**: confronta i criteri di corrispondenza con il valore nell'intestazione di un frame Ethernet.

  Selezionare una parola chiave EtherType oppure immettere un valore EtherType per specificare i criteri di corrispondenza.

  - **Select From List**: utilizza il tipo di connessione Ethernet nell'intestazione del datagramma per la corrispondenza con i tipi di protocollo selezionati: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.

  - **Match to Value**: utilizza il tipo di connessione Ethernet nell'intestazione del datagramma per la corrispondenza con un identificatore di protocollo personalizzato specificato. Il valore immesso in questo campo è un numero esadecimale a quattro cifre compreso tra 0600 e FFFF.

- **Class of Service**: un valore di priorità utente di classe di servizio 802.1p per la corrispondenza con i pacchetti. L'intervallo valido è compreso tra 0 e 7.

- **Source MAC Address**: un indirizzo MAC di origine per il confronto con un frame Ethernet.

- **Source MAC Mask**: la maschera dell'indirizzo MAC di origine che specifica i bit nel MAC di destinazione per il confronto con un frame Ethernet.

  Per ogni posizione bit nella maschera MAC, uno 0 indica che il bit dell'indirizzo corrispondente è importante e un 1 indica che il bit dell'indirizzo viene ignorato. Ad esempio, per verificare soltanto i primi quattro ottetti di un indirizzo MAC viene utilizzata la maschera MAC 00:00:00:00:ff:ff. La maschera MAC 00:00:00:00:00:00 verifica tutti i bit dell'indirizzo e viene utilizzata per la corrispondenza con un singolo indirizzo MAC.

- **Destination MAC Address**: un indirizzo MAC di destinazione per il confronto con un frame Ethernet.

- **Destination MAC Mask**: la maschera dell'indirizzo MAC di destinazione che specifica i bit nel MAC di destinazione per il confronto con un frame Ethernet.

  Per ogni posizione bit nella maschera MAC, uno 0 indica che il bit dell'indirizzo corrispondente è importante e un 1 indica che il bit dell'indirizzo viene ignorato. Ad esempio, per verificare soltanto i primi quattro ottetti di un indirizzo MAC viene utilizzata la maschera MAC 00:00:00:00:ff:ff. La maschera MAC 00:00:00:00:00:00 verifica tutti i bit dell'indirizzo e viene utilizzata per la corrispondenza con un singolo indirizzo MAC.

- **VLAN ID**: un ID VLAN per la corrispondenza con i pacchetti. L'intervallo valido per gli ID VLAN è compreso tra 0 e 4095.

I Service Type seguenti sono disponibili soltanto per IPv4. È possibile specificare un tipo di servizio da utilizzare nella corrispondenza dei pacchetti con i criteri di classe.

- **IP DSCP**: un valore DSCP (Differentiated Services Code Point) da utilizzare come criterio di corrispondenza:
  - **Select from List**: un elenco di tipi di DSCP.
  - **Match to Value**: un valore DSCP personalizzato, da 0 a 63.
- **IP Precedence** (soltanto IPv4): utilizza il valore di precedenza IP del pacchetto per la corrispondenza con il valore di precedenza IP del criterio di classe. L'intervallo della precedenza IP è compreso tra 0 e 7.
- **IP TOS Bits** (soltanto IPv4): utilizza i bit Type of Service del pacchetto nell'intestazione IP come criterio di corrispondenza.

  Il valore dei bit IP TOS è compreso tra (00 e FF). I tre bit di ordine elevato rappresentano il valore della precedenza IP. I sei bit di ordine elevato rappresentano il valore IP DSCP (Differentiated Services Code Point).

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare una mappa delle classi, selezionarla nell'elenco **Class Map Name** e fare clic su **Elimina**. Se la mappa delle classi è già collegata a un criterio, non è possibile eliminarla.

Mappa dei criteri

I pacchetti vengono classificati ed elaborati in base a criteri definiti. I criteri di classificazione sono definiti in base alla classe nella pagina *Mappa delle classi*. L'elaborazione è definita in base agli attributi di un criterio nella pagina Policy Map. Gli attributi del criterio possono essere definiti in base alle singole classi e determinano come viene gestito il traffico che corrisponde ai criteri di classe.

Il dispositivo WAP supporta fino a 50 mappe dei criteri. Una mappa dei criteri può contenere fino a 10 mappe di classe.

Per aggiungere e configurare una mappa dei criteri, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Client QoS** > **Policy Map**.

PASSAGGIO 2 Immettere un nome nel campo **Policy Map Name**. Il nome può contenere da 1 a 31 caratteri alfanumerici e i seguenti caratteri speciali: trattini, caratteri di sottolineatura, barra rovesciata e due punti. Gli spazi non sono consentiti.

PASSAGGIO 3 Fare clic su **Add Policy Map**. La pagina viene aggiornata e vengono visualizzati campi aggiuntivi per la configurazione della mappa dei criteri.

PASSAGGIO 4 Nell'area Policy Class Definition, assicurarsi che la mappa di criteri appena creata sia visualizzata nell'elenco **Policy Map Name**.

PASSAGGIO 5 Nell'elenco **Class Map Name** selezionare la mappa delle classi cui applicare questo criterio.

PASSAGGIO 6 Configurare i seguenti parametri:

- **Police Simple**: stabilisce lo stile di monitoraggio del traffico per la classe. La forma semplice di monitoraggio utilizza una singola velocità dati e dimensione burst, producendo due risultati: conforme e non conforme. Se si seleziona questo campo, configurare uno dei campi seguenti:

  - **Committed Rate**: la velocità riservata, in Kbps, che deve essere rispettata dal traffico. L'intervallo è compreso tra 1 e 1000000 Kbps.
  - **Committed Burst**: la dimensione del burst impegnata, in byte, che deve essere rispettata dal traffico. L'intervallo è compreso tra 1 e 204800000 byte.
- **Send**: se vengono soddisfatti i criteri della mappa di classi, tutti i pacchetti del flusso di traffico associato devono essere inoltrati.
- **Drop**: se vengono soddisfatti i criteri della mappa di classi, tutti i pacchetti del flusso di traffico associato devono essere eliminati.
- **Mark Class of Service**: contrassegna tutti i pacchetti del flusso di traffico associato con il valore di classe di servizio specificato nel campo della priorità dell'intestazione 802.1p. Se il pacchetto non contiene ancora questa intestazione, ne viene inserita una. Il valore CoS è un numero intero compreso tra 0 e 7.
- **Mark IP DSCP**: contrassegna tutti i pacchetti del flusso di traffico associato con il valore IP DSCP selezionato dall'elenco o specificato.
  - **Select from List**: un elenco di tipi di DSCP.
  - **Match to Value**: un valore DSCP specificato. Il valore è un numero intero compreso tra 0 e 63.
- **Mark IP Precedence**: contrassegna tutti i pacchetti del flusso di traffico associato con il valore di precedenza IP specificato. Il valore di precedenza IP è un numero intero compreso tra 0 e 7.
- **Disassociate Class Map**: rimuove la classe selezionata nell'elenco Class Map Name dal criterio selezionato nell'elenco Policy Map Name.
- **Member Classes**: elenca tutte le classi DiffServ attualmente definite come membri del criterio selezionato. Se al criterio non sono associate classi, il campo è vuoto.

PASSAGGIO 7 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare una mappa di criteri, selezionarla nell'elenco **Policy Map Name** e fare clic su **Elimina**.

Associazione di Client QoS

La pagina Client QoS Association fornisce un controllo aggiuntivo di alcuni aspetti QoS dei client wireless che si collegano alla rete, come la quantità di larghezza di banda disponibile per un singolo client per inviare e ricevere dati. Per controllare le categorie di traffico generali, come il traffico HTTP o il traffico di una sottorete specifica, è possibile configurare gli ACL e assegnarli a uno o più VAP.

Oltre a controllare le categorie di traffico generali, Client QoS permette di configurare condizioni di microflussi per i singoli client mediante Differentiated Services (DiffServ). I criteri DiffServ rappresentano uno strumento utile per stabilire una definizione generale di microflussi e caratteristiche di trattamento che è possibile applicare a ciascun client wireless, sia in entrata che in uscita, quando effettua l'autenticazione sulla rete.

Per configurare i parametri delle associazioni Client QoS, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Client QoS** > **Client QoS Association**.

PASSAGGIO 2 Soltanto sui dispositivi WAP561, selezionare l'interfaccia radio sulla quale si desidera configurare l'associazione (**Radio 1** o **Radio 2**).

PASSAGGIO 3 Nell'elenco VAP, selezionare il VAP sul quale si desiderano configurare i parametri di Client QoS.

PASSAGGIO 4 Selezionare **Enable** per **Client QoS Global** per attivare questa funzione.

PASSAGGIO 5 Configurare i parametri seguenti per il VAP selezionato:

- **Client QoS Mode**: selezionare **Enable** per attivare la funzionalità Client QoS sul VAP selezionato.
- **Bandwidth Limit Down**: la velocità di trasmissione massima consentita dal dispositivo WAP al client in bit al secondo (bps). L'intervallo valido è compreso tra 0 e 300 Mbps.
- **Bandwidth Limit Up**: la velocità di trasmissione massima consentita dal client al dispositivo WAP in bit al secondo (bps). L'intervallo valido è compreso tra 0 e 300 Mbps.
- **ACL Type Down**: il tipo di ACL da applicare al traffico in uscita (da dispositivo WAP a client); è possibile scegliere uno dei valori seguenti:
  - IPv4: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv4.
  - IPv6: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv6.

  - MAC: l'ACL cerca corrispondenze con le regole ACL nei frame di livello 2.
- **ACL Name Down**: il nome dell'ACL applicato al traffico in uscita.

  Dopo aver trasferito il pacchetto o il frame all'interfaccia di uscita, vengono cercate eventuali corrispondenze nelle regole ACL. Se autorizzato, il pacchetto o il frame viene trasmesso; in caso contrario viene eliminato.
- **ACL Type Up**: il tipo di ACL da applicare al traffico in ingresso (da client a dispositivo WAP); è possibile scegliere uno dei valori seguenti:
  - IPv4: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv4.
  - IPv6: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv6.
  - MAC: l'ACL cerca corrispondenze con le regole ACL nei frame di livello 2.
- **ACL Name Up**: il nome dell'ACL applicato al traffico in entrata sul dispositivo WAP.

  Quando il dispositivo WAP riceve un pacchetto o un frame, vengono cercate eventuali corrispondenze nelle regole ACL. Se autorizzato, il pacchetto o il frame viene elaborato; in caso contrario viene eliminato.
- **DiffServ Policy Down**: il nome del criterio DiffServ applicato al traffico dal dispositivo WAP in uscita (da dispositivo WAP a client).
- **DiffServ Policy Up**: il nome del criterio DiffServ applicato al traffico inviato al dispositivo WAP in entrata (da client a dispositivo WAP).

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Stato di Client QoS

Nella pagina Client QoS Status vengono mostrate le impostazioni di Client QoS applicate a ciascun client attualmente associato al dispositivo WAP.

Per visualizzare la pagina Client QoS Status, selezionare **Client QoS** > **Client QoS Status** nel riquadro di spostamento.

Utilizzare i campi seguenti per configurare lo stato di Client QoS:

- **Station**: questa casella contiene l'indirizzo MAC di ciascun client attualmente associato con il dispositivo WAP. Per visualizzare le impostazioni QoS applicate a un client, selezionare il relativo indirizzo MAC dall'elenco.

- **Global QoS Mode**: indica se la funzione QoS è attivata a livello globale sul dispositivo WAP. Questo stato viene configurato nella pagina *Associazione di Client QoS*.
- **Client QoS Mode**: indica se la funzione QoS è attivata sul VAP associato. Questo stato viene configurato nella pagina *Associazione di Client QoS*.
- **Bandwidth Limit Down**: la velocità di trasmissione massima consentita dal dispositivo WAP al client in bit al secondo (bps). L'intervallo valido è compreso tra 0 e 4294967295 bps.
- **Bandwidth Limit Up**: la velocità di trasmissione massima consentita dal client al dispositivo WAP in bit al secondo (bps). L'intervallo valido è compreso tra 0 e 4294967295 bps.
- **ACL Type Up**: il tipo di ACL da applicare al traffico in ingresso (da client a dispositivo WAP); è possibile scegliere uno dei valori seguenti:
  - IPv4: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv4.
  - IPv6: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv6.
  - MAC: l'ACL cerca corrispondenze con le regole ACL nei frame di livello 2.
- **ACL Name Up**: il nome dell'ACL applicato al traffico in entrata sul dispositivo WAP. Quando il dispositivo WAP riceve un pacchetto o un frame, vengono cercate eventuali corrispondenze nelle regole ACL. Se autorizzato, il pacchetto o il frame viene elaborato; in caso contrario viene eliminato.
- **ACL Type Down**: il tipo di ACL da applicare al traffico in uscita (da dispositivo WAP a client); è possibile scegliere uno dei valori seguenti:
  - IPv4: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv4.
  - IPv6: l'ACL cerca corrispondenze con le regole ACL nei pacchetti IPv6.
  - MAC: l'ACL cerca corrispondenze con le regole ACL nei frame di livello 2.
- **ACL Name Down**: il nome dell'ACL applicato al traffico in uscita. Dopo aver trasferito il pacchetto o il frame all'interfaccia di uscita, vengono cercate eventuali corrispondenze nelle regole ACL. Se autorizzato, il pacchetto o il frame viene trasmesso; in caso contrario viene eliminato.
- **DiffServ Policy Up**: il nome del criterio DiffServ applicato al traffico inviato al dispositivo WAP in entrata (da client a dispositivo WAP).
- **DiffServ Policy Down**: il nome del criterio DiffServ applicato al traffico dal dispositivo WAP in uscita (da dispositivo WAP a client).

8

Protocollo SNMP

In questo capitolo viene descritto come configurare il protocollo SNMP (Simplified Network Management Protocol) per l'esecuzione di attività di configurazione e raccolta delle statistiche.

Vengono trattati i seguenti argomenti:

- **Impostazioni SNMP generali**
- **Viste**
- **Gruppi**
- **Utenti**
- **Target**

Impostazioni SNMP generali

Utilizzare la pagina General per abilitare SNMP e configurare le impostazioni di base del protocollo.

Per configurare le impostazioni SNMP generali, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **SNMP** > **General**.

PASSAGGIO 2 Selezionare **Enabled** per l'impostazione **SNMP**. La modalità SNMP è disattivata per impostazione predefinita.

PASSAGGIO 3 Nel campo **UDP Port**, immettere una porta per il traffico SNMP.

Per impostazione predefinita, un agente SNMP ascolta solo le richieste della porta 161. Tuttavia, è possibile configurarlo in modo che ascolti anche le richieste di un'altra porta. L'intervallo valido è compreso tra 1025 e 65535.

PASSAGGIO 4 Configurare le impostazioni di SNMPv2:

- **Read-only Community**: il nome della comunità per l'accesso di sola lettura tramite SNMPv2. È possibile immettere da 1 a 256 caratteri alfanumerici e speciali.

  Il nome della comunità agisce da semplice funzione di autenticazione per limitare i computer della rete che possono richiedere dati all'agente SNMP. Il nome funziona da password, quindi se il mittente conosce la password la richiesta è considerata autentica.

- **Read-write Community**: il nome della comunità da utilizzare per l'accesso in lettura e scrittura per le richieste di impostazione SNMP. È possibile immettere da 1 a 256 caratteri alfanumerici e speciali.

  L'impostazione del nome della comunità è simile all'impostazione di una password. Vengono accettate solo le richieste provenienti dai computer che accedono con il nome della comunità specificato in questo campo.

- **Management Station**: consente di stabilire quali stazioni possono accedere al dispositivo WAP tramite SNMP. Selezionare una delle seguenti opzioni:

  - **All**: non vengono applicati limiti al gruppo di stazioni che può accedere al dispositivo WAP tramite SNMP.

  - **User Defined**: sono consentite soltanto le richieste SNMP specificate.

- **NMS, IPv4 Address/Name**: l'indirizzo IP IPv4, il nome host DNS, la sottorete del sistema di gestione della rete (NMS, Network Management System) o il gruppo di computer che può eseguire richieste di tipo get e set sui dispositivi gestiti.

  Un nome host DNS può essere composto da una o più etichette, formate a loro volta da un numero massimo di 63 caratteri alfanumerici. Se un nome host include più etichette, queste saranno separate da un punto (.). La lunghezza massima dell'intera serie di etichette (punti compresi) è di 253 caratteri.

  Come per i nomi della comunità, questa impostazione fornisce un livello di protezione alle impostazioni SNMP. L'agente SNMP accetta solo le richieste provenienti dall'indirizzo IP, dal nome host o dalla sottorete specificata in questo campo.

  Per specificare una sottorete, immettere uno o più intervalli di indirizzi di sottorete nel formato *indirizzo/lunghezza_maschera*, dove *indirizzo* indica l'indirizzo IP e *lunghezza_maschera* indica il numero di bit della maschera. Sono supportati entrambi i formati *indirizzo/maschera* e

indirizzo/lunghezza_maschera. Ad esempio, l'intervallo 192.168.1.0/24 specifica una sottorete con indirizzo 192.168.1.0 e una subnet mask con indirizzo 255.255.255.0.

L'intervallo di indirizzi viene utilizzato per specificare la sottorete del sistema di gestione della rete designato. Solo i computer con indirizzi IP che rientrano in questo intervallo sono autorizzati a eseguire le richieste di tipo get e set sul dispositivo gestito. Se si considera l'esempio precedente, i computer con indirizzi da 192.168.1.1 a 192.168.1.254 possono eseguire i comandi SNMP sul dispositivo. L'indirizzo identificato dal suffisso .0 in un intervallo della sottorete è sempre riservato all'indirizzo della sottorete, mentre l'indirizzo identificato da .255 nell'intervallo è sempre riservato all'indirizzo di broadcast.

Un altro esempio: se si inserisce un intervallo di 10.10.1.128/25, i computer con indirizzi IP da 10.10.1.129 a 10.10.1.254 possono eseguire le richieste SNMP sui dispositivi gestiti. In questo esempio, 10.10.1.128 rappresenta l'indirizzo di rete, mentre 10.10.1.255 è l'indirizzo di broadcast. In questo caso verrebbero designati, in totale, 126 indirizzi.

- **NMS IPv6 Address/Name**: l'indirizzo IPv6, il nome host DNS o la sottorete dei computer che possono eseguire le richieste di tipo get e set sui dispositivi gestiti. L'indirizzo IPv6 deve essere nel formato seguente: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

  Un nome host può essere composto da una o più etichette, formate a loro volta da un numero massimo di 63 caratteri alfanumerici. Se un nome host include più etichette, queste saranno separate da un punto (.). La lunghezza massima dell'intera serie di etichette (punti compresi) è di 253 caratteri.

PASSAGGIO 5 Configurare le impostazioni trap di SNMPv2:

- **Trap Community**: una stringa della comunità globale associata ai trap SNMP. I trap inviati dal dispositivo forniscono questa stringa come nome della comunità. È possibile immettere da 1 a 60 caratteri alfanumerici e speciali.
- **Trap Destination Table**: un elenco che comprende fino a tre indirizzi IP o nomi host che ricevono i trap SNMP. Selezionare questa casella e scegliere un tipo di indirizzo IP host (IPv4 or IPv6) nel rispettivo campo prima di aggiungere il nome host/l'indirizzo IP.

  Un esempio di nome host DNS è snmptraps.foo.com. Poiché i trap SNMP vengono inviati in maniera casuale dall'agente SNMP, è necessario specificare l'esatta destinazione dei trap. È possibile specificare massimo

tre nomi host DNS. Assicurarsi di aver selezionato la casella di controllo **Enabled**, quindi selezionare l'opzione appropriata nel campo **Host IP Address Type**.

Leggere anche la nota relativa ai nomi host nel passaggio precedente.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Dopo aver salvato le nuove impostazioni, i processi corrispondenti potrebbero essere interrotti e riavviati. In questo caso, il dispositivo WAP potrebbe perdere la connessione. Si consiglia di modificare le impostazioni del dispositivo WAP quando l'eventuale perdita di connessione avrebbe un impatto minimo sui client wireless.

Viste

Una vista MIB SNMP è una famiglia di strutture secondarie della vista nella gerarchia MIB. Una struttura secondaria è identificata dall'associazione di un valore di struttura secondaria OID (identificatore oggetto) al valore maschera di una stringa di bit. Ogni vista MIB viene definita da due set di strutture secondarie, incluse o escluse dalla vista MIB. È possibile creare viste MIB per controllare l'intervallo OID a cui gli utenti SNMPv3 possono accedere.

Su un dispositivo WAP sono supportate massimo 16 viste.

Di seguito vengono presentate alcune delle linee guida più importanti relative alla configurazione delle viste SNMPv3. Leggere tutte le note prima di proseguire.

NOTA All'interno del sistema viene creata per impostazione predefinita una vista MIB denominata "all". Questa vista contiene tutti gli oggetti di gestione supportati dal sistema.

NOTA Sul dispositivo WAP vengono create per impostazione predefinita le viste SNMPv3 "view-all" e "view-none". Queste viste non possono essere eliminate o modificate.

Per aggiungere e configurare una vista SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **SNMP** > **Views**.

PASSAGGIO 2 Fare clic su **Aggiungi** per creare una nuova riga nella tabella delle viste SNMPv3.

PASSAGGIO 3 Selezionare la casella nella nuova riga e fare clic su **Modifica**.

- **View Name**: immettere un nome che identifichi la vista MIB. I nomi delle viste possono contenere fino a 32 caratteri alfanumerici.
- **Type**: scegliere se includere o escludere la struttura secondaria o la famiglia di strutture secondarie dalla vista MIB.
- **OID**: immettere una stringa OID per la struttura secondaria da includere o escludere dalla vista.

  Ad esempio, la struttura secondaria di sistema è specificata dalla stringa OID .1.3.6.1.2.1.1.
- **Mask**: immettere una maschera OID. La stringa della maschera è composta da 47 caratteri. Il formato della maschera OID è xx.xx.xx (.)... o xx:xx:xx.... (:), per una lunghezza di 16 ottetti. Ogni ottetto è composto da due caratteri esadecimali separati da un punto (.) o due punti (:). In questo campo è possibile immettere solo caratteri esadecimali.

  Ad esempio, la maschera OID FA.80 è 11111010.10000000.

  Per definire una famiglia di strutture secondarie della vista, viene utilizzata una maschera famiglia. La maschera famiglia indica quali identificatori secondari della stringa OID famiglia associata sono importanti per la definizione della famiglia. Una famiglia di strutture secondarie della vista consente di controllare in maniera efficiente l'accesso a una riga in una tabella.

PASSAGGIO 4 Fare clic su **Salva**. La vista viene aggiunta all'elenco di viste SNMPv3 e le modifiche vengono salvate nella configurazione di avvio.

NOTA Per rimuovere una vista, selezionarla nell'elenco, quindi fare clic su **Elimina**.

Gruppi

I gruppi SNMPv3 consentono di unire gli utenti in gruppi di autorizzazioni e privilegi di accesso. Ogni gruppo è associato a uno dei tre livelli di protezione:

- noAuthNoPriv
- authNoPriv
- authPriv

Per controllare l'accesso alle MIB, a ogni gruppo viene associata una MIB per accesso in lettura o scrittura, separatamente.

Il dispositivo WAP dispone, per impostazione predefinita, di due gruppi:

- **RO**: un gruppo in sola lettura che utilizza l'autenticazione e la crittografia dei dati. Gli utenti in questo gruppo utilizzano una chiave o password MD5 per l'autenticazione e una chiave o password DES per la crittografia. È necessario definire sia le chiavi/password MD5 che DES. Per impostazione predefinita, gli utenti di questo gruppo hanno accesso in lettura alla vista MIB all predefinita.
- **RW**: un gruppo in lettura e scrittura che utilizza l'autenticazione e la crittografia dei dati. Gli utenti in questo gruppo utilizzano una chiave o password MD5 per l'autenticazione e una chiave o password DES per la crittografia. È necessario definire sia le chiavi/password MD5 che DES. Per impostazione predefinita, gli utenti di questo gruppo hanno accesso in lettura e scrittura alla vista MIB all predefinita.

NOTA Non è possibile eliminare i gruppi predefiniti RO e RW.

NOTA Su un dispositivo WAP sono supportati massimo otto gruppi.

Per aggiungere e configurare un gruppo SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **SNMP** > **Groups**.

PASSAGGIO 2 Fare clic su **Aggiungi** per creare una nuova riga nella tabella dei gruppi SNMPv3.

PASSAGGIO 3 Selezionare la casella del nuovo gruppo e fare clic su **Modifica**.

PASSAGGIO 4 Configurare i seguenti parametri:

- **Group Name**: nome che identifica il gruppo. I nomi dei gruppi predefiniti sono RO e RW.

  I nomi dei gruppi possono contenere fino a 32 caratteri alfanumerici.

- **Security Level**: consente di impostare il livello di protezione del gruppo. È possibile scegliere una delle opzioni seguenti:

  - **noAuthentication-noPrivacy**: nessuna autenticazione e nessuna crittografia dei dati (nessuna protezione).
  - **Authentication-noPrivacy**: autenticazione, ma nessuna crittografia dei dati. Con questo livello di protezione, gli utenti inviano messaggi SNMP che utilizzano una chiave o password MD5 per l'autenticazione, ma non una chiave o password DES per la crittografia.

- **Authentication-Privacy**: autenticazione e crittografia dei dati. Con questo livello di protezione, gli utenti inviano una chiave o password MD5 per l'autenticazione e una chiave o password DES per la crittografia.

  È necessario definire le chiavi o password MD5 e DES nella pagina SNMP Users per i gruppi che richiedono l'autenticazione, la crittografia o entrambe.

- **Write Views**: l'accesso in scrittura alle MIB da parte del gruppo. È possibile scegliere una delle opzioni seguenti:
  - **view-all**: il gruppo può creare, modificare ed eliminare le MIB.
  - **view-none**: il gruppo non può creare, modificare o eliminare le MIB.
- **Read Views**: l'accesso in lettura alle MIB da parte del gruppo:
  - **view-all**: il gruppo è autorizzato a visualizzare e leggere tutte le MIB.
  - **view-none**: il gruppo non può visualizzare o leggere le MIB.

PASSAGGIO 5 Fare clic su **Salva**. Il gruppo viene aggiunto all'elenco dei gruppi SNMPv3 e le modifiche vengono salvate nella configurazione di avvio.

NOTA Per rimuovere un gruppo, selezionarlo nell'elenco, quindi fare clic su **Elimina**.

Utenti

Utilizzare la pagina SNMP Users per definire gli utenti, associare un livello di protezione a ciascun utente e configurare le chiavi di sicurezza per ogni utente.

Ogni utente viene associato a un gruppo SNMPv3 da un gruppo predefinito o definito dall'utente. È anche possibile configurare le opzioni di autenticazione e crittografia per un utente. L'unico tipo di autenticazione supportato è MD5. L'unico tipo di crittografia supportato è DES. Non sono presenti utenti SNMPv3 predefiniti sul dispositivo WAP ed è possibile aggiungere massimo otto utenti.

Per aggiungere utenti SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **SNMP** > **Users**.

PASSAGGIO 2 Fare clic su **Aggiungi** per creare una nuova riga nella tabella degli utenti SNMPv3.

PASSAGGIO 3 Selezionare la casella nella nuova riga e fare clic su **Modifica**.

PASSAGGIO 4 Configurare i seguenti parametri:

- **User Name**: nome che identifica l'utente SNMPv3. I nomi utente possono contenere fino a 32 caratteri alfanumerici.
- **Group**: il gruppo associato all'utente. I gruppi predefiniti sono RWAuth, RWPriv e RO. È possibile definire gruppi aggiuntivi nella pagina SNMP Groups.
- **Authentication Type**: il tipo di autenticazione da utilizzare per le richieste SNMPv3 provenienti dell'utente. È possibile selezionare una delle opzioni seguenti:
  - **MD5**: richiede l'autenticazione MD5 per le richieste SNMP provenienti dall'utente.
  - **None**: per le richieste SNMPv3 da parte dell'utente non è richiesta l'autenticazione.
- **Authentication Pass Phrase**: se si seleziona MD5 come tipo di autenticazione, immettere in questo campo una frase che consenta all'agente SNMP di autenticare le richieste inviate dall'utente. La frase deve contenere da 8 a 32 caratteri.
- **Encryption Type**: il tipo di privacy da utilizzare per le richieste SNMP provenienti dall'utente. È possibile selezionare una delle opzioni seguenti:
  - **DES**: utilizza la crittografia DES per le richieste SNMPv3 provenienti dall'utente.
  - **None**: per le richieste SNMPv3 da parte dell'utente non sono richieste impostazioni di privacy.
- **Encryption Pass Phrase**: se si seleziona DES come tipo di privacy, immettere in questo campo una frase da utilizzare per crittografare le richieste SNMP. La frase deve contenere da 8 a 32 caratteri.

PASSAGGIO 5 Fare clic su **Salva**. L'utente viene aggiunto all'elenco degli utenti SNMPv3 e le modifiche vengono salvate nella configurazione di avvio.

NOTA Per rimuovere un utente, selezionarlo nell'elenco, quindi fare clic su **Elimina**.

Target

I target SNMPv3 inviano le notifiche SNMP a SNMP Manager tramite messaggi Inform. Per i target SNMPv3 vengono inviati solo messaggi Inform; non vengono inviati trap. I trap vengono inviati per le versioni 1 e 2 di SNMP. Ciascun target è definito da un indirizzo IP destinatario, una porta UDP e un nome utente SNMPv3.

NOTA Per proseguire con la configurazione dei target, è necessario completare prima la configurazione degli utenti SNMPv3; vedere la pagina **Utenti**.

NOTA Su un dispositivo WAP sono supportati massimo otto target.

Per aggiungere target SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **SNMP** > **Targets**.

PASSAGGIO 2 Fare clic su **Aggiungi**. Viene creata una nuova riga nella tabella.

PASSAGGIO 3 Selezionare la casella nella nuova riga e fare clic su **Modifica**.

PASSAGGIO 4 Configurare i seguenti parametri:

- **IP Address**: immettere l'indirizzo IPv4 del dispositivo SNMP Manager remoto che riceverà il target.
- **UDP Port**: immettere la porta UDP da utilizzare per l'invio dei target SNMPv3.
- **Users**: immettere il nome dell'utente SNMP da associare al target. Per configurare gli utenti SNMP, vedere la pagina **Utenti**.

PASSAGGIO 5 Fare clic su **Salva**. L'utente viene aggiunto all'elenco dei target SNMPv3 e le modifiche vengono salvate nella configurazione di avvio.

NOTA Per rimuovere un target SNMP, selezionarlo nell'elenco, quindi fare clic su **Elimina**.

9

Captive Portal

In questo capitolo viene descritta la funzione Captive Portal (CP), che consente ai client wireless di accedere alla rete solo dopo aver verificato l'identità dell'utente. È possibile configurare la verifica CP in modo da consentire l'accesso sia agli utenti ospiti che agli utenti autenticati.

NOTA La funzione Captive Portal è disponibile sui dispositivi WAP5xx e sul dispositivo Cisco WAP321.

Per poter accedere, gli utenti autenticati devono essere convalidati a fronte di un database di gruppi o utenti Captive Portal autorizzati. Il database può essere memorizzato a livello locale sul dispositivo WAP o su un server RADIUS.

Captive Portal è costituito da due istanze CP. Ciascuna istanza può essere configurata in modo indipendente, con metodi di verifica diversi per ogni VAP o SSID. I dispositivi Cisco WAP551 e WAP561 funzionano in concomitanza con alcuni VAP configurati per l'autenticazione CP e altri configurati per i normali metodi di autenticazione wireless, quali WPA o WPA Enterprise.

In questo capitolo sono trattati gli argomenti seguenti:

- **Configurazione globale di Captive Portal**
- **Configurazione delle istanze**
- **Associazione delle istanze**
- **Personalizzazione del portale Web**
- **Gruppi locali**
- **Utenti locali**
- **Client autenticati**
- **Autenticazione client non riuscita**

Configurazione globale di Captive Portal

Utilizzare la pagina Global CP Configuration per controllare lo stato amministrativo della funzione CP e configurare le impostazioni generali di tutte le istanze Captive Portal configurate sul dispositivo WAP.

Per configurare le impostazioni generali CP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal** > **Global Configuration**.

PASSAGGIO 2 Configurare i seguenti parametri:

- **Captive Portal Mode**: abilita la funzione CP sul dispositivo WAP.
- **Authentication Timeout**: per accedere alla rete tramite un portale, è necessario inserire prima le informazioni di autenticazione in una pagina Web. In questo campo viene specificato il numero di secondi in cui il dispositivo WAP mantiene aperta una sessione di autenticazione con il client wireless associato. Se il client non inserisce le credenziali di autenticazione entro il periodo di timeout consentito, potrebbe essere necessario aggiornare la pagina di autenticazione. Il timeout di autenticazione predefinito è 300 secondi. È possibile immettere un valore compreso tra 60 e 600 secondi.
- **Additional HTTP Port**: il traffico HTTP utilizza la porta di gestione HTTP (porta 80 per impostazione predefinita). È possibile configurare una porta aggiuntiva per il traffico HTTP. Inserire un numero di porta compreso tra 1025 e 65535 oppure 80. Le porte HTTP e HTTPS devono essere diverse.
- **Additional HTTPS Port**: il traffico HTTPS (HTTP over SSL) utilizza la porta di gestione HTTPS (porta 443 per impostazione predefinita). È possibile configurare una porta aggiuntiva per il traffico HTTPS. Inserire un numero di porta compreso tra 1025 e 65535 o 443. Le porte HTTP e HTTPS devono essere diverse.

Nell'area Captive Portal Configuration Counters sono contenute informazioni relative a CP in sola lettura:

- **Instance Count**: il numero di istanze CP attualmente configurate sul dispositivo WAP. È possibile configurare massimo due istanze.
- **Group Count**: il numero di gruppi CP attualmente configurati sul dispositivo WAP. È possibile configurare massimo due gruppi. Default Group è predefinito e non può essere eliminato.

- **User Count**: il numero di utenti CP attualmente configurati sul dispositivo WAP. È possibile configurare massimo 128 utenti.

PASSAGGIO 3 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Configurazione delle istanze

È possibile configurare fino a due istanze Captive Portal; ogni istanza CP rappresenta un set definito di parametri. Le istanze possono essere associate a uno o più VAP. È possibile configurare diverse istanze che rispondano in modo diverso quando gli utenti cercano di accedere al VAP associato.

NOTA Prima di creare un'istanza, controllare i punti seguenti:

- Se è necessario aggiungere un nuovo VAP, passare alla sezione **Reti** per indicazioni su come procedere.
- Se è necessario aggiungere un nuovo gruppo, passare alla sezione **Gruppi locali** per indicazioni su come procedere.
- Se è necessario aggiungere un nuovo utente, passare alla sezione **Utenti locali** per indicazioni su come procedere.

Per creare un'istanza CP e configurarne le relative impostazioni, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal** > **Instance Configuration**.

PASSAGGIO 2 Assicurarsi che nell'elenco **Captive Port Instances** sia selezionato **Create**.

PASSAGGIO 3 Immettere un nome nella casella **Instance Name** e fare clic su **Salva**. Il nome dell'istanza può contenere 1-32 caratteri alfanumerici e il trattino di sottolineatura.

PASSAGGIO 4 Selezionare il nome dell'istanza dall'elenco **Captive Portal Instances**.

Verranno visualizzati di nuovo i campi Captive Portal Instance Parameters con opzioni aggiuntive.

PASSAGGIO 5 Configurare i seguenti parametri:

- **Instance ID**: l'ID dell'istanza. Non è possibile modificare questo campo.
- **Administrative Mode**: attiva e disattiva l'istanza CP.

- **Protocol**: specifica HTTP o HTTPS come protocollo per l'istanza CP da utilizzare nella procedura di verifica.
  - **HTTP**: non utilizza la crittografia durante la verifica.
  - **HTTPS**: utilizza la funzione Secure Socket Layer (SSL), che richiede un certificato per applicare la crittografia.

    Il certificato viene fornito all'utente al momento della connessione.
- **Verification**: il metodo di autenticazione CP da utilizzare per identificare i client:
  - **Guest**: non è necessaria l'autenticazione dell'utente a fronte di un database.
  - **Local**: il dispositivo WAP utilizza un database locale per autenticare gli utenti.
  - **RADIUS**: il dispositivo WAP utilizza un database su un server RADIUS remoto per autenticare gli utenti.
- **Redirect**: indica che il client autenticato deve essere reindirizzato da CP all'URL configurato. Se questa opzione è disattivata, dopo l'autenticazione verrà visualizzata la pagina iniziale dell'area geografica dell'utente.
- **Redirect URL**: se è stata attivata l'opzione Redirect, immettere l'URL (incluso http:// o https://) al quale il client autenticato verrà reindirizzato. L'intervallo è compreso tra 0 e 256 caratteri.
- **Away Timeout**: periodo in cui un utente rimane nell'elenco di client CP autenticati dopo la disassociazione dal WAP. Se l'intervallo specificato in questo campo scade prima che il client esegua di nuovo l'autenticazione, la relativa voce verrà rimossa dall'elenco dei client autenticati. L'intervallo è compreso tra 0 e 1440 minuti. Il valore predefinito è 60 minuti.

  NOTA Anche per ogni utente viene configurato un valore di timeout. Vedere la pagina **Utenti locali**. Il valore di timeout impostato nella pagina Local Users prevale sul valore configurato qui, a meno che il valore impostato non sia 0 (predefinito). Il valore 0 indica di utilizzare il valore di timeout dell'istanza.
- **Session Timeout**: tempo rimanente, espresso in secondi, alla scadenza della sessione CP. Quando il contatore arriva a zero, l'autenticazione del client scade. L'intervallo è compreso tra 0 e 1440 minuti. Il valore predefinito è 0.

- **Maximum Bandwidth Upstream**: la velocità massima di upload dei dati da parte del client tramite Captive Portal, espressa in megabit al secondo. Il valore di questo campo limita la larghezza di banda per l'invio dei dati in rete da parte del client. L'intervallo è compreso tra 0 e 300 Mbps. Il valore predefinito è 0.
- **Maximum Bandwidth Downstream**: la velocità massima di download dei dati da parte del client tramite Captive Portal, espressa in megabit al secondo. Il valore di questo campo limita la larghezza di banda per la ricezione dei dati dalla rete. L'intervallo è compreso tra 0 e 300 Mbps. Il valore predefinito è 0.
- **User Group Name**: se la modalità di verifica è impostata su Local o RADIUS, assegna un gruppo utente esistente all'istanza CP. Tutti gli utenti che appartengono al gruppo possono accedere alla rete tramite il portale.
- **RADIUS IP Network**: la versione IP utilizzata dal server RADIUS. Anche se è possibile alternare i tipi di indirizzo per configurare le impostazioni degli indirizzi RADIUS IPv4 e IPv6, il dispositivo WAP contatterà esclusivamente i server RADIUS del tipo di indirizzo selezionato in questo campo.
- **Global RADIUS**: questo campo è disponibile se la modalità di verifica è impostata su RADIUS. L'istanza CP utilizza per impostazione predefinita i parametri RADIUS globali definiti per il dispositivo WAP; vedere **Server RADIUS**. Tuttavia, è possibile configurare ogni istanza perché utilizzi un set di server RADIUS diverso. Per utilizzare le impostazioni globali del server RADIUS, assicurarsi che questa casella sia selezionata. Per utilizzare un server RADIUS separato per l'istanza CP, deselezionare questa casella, quindi immettere i valori nei campi Server IP Address e Key che seguono.
- **RADIUS Accounting**: consente di rilevare e misurare le risorse utilizzate da un determinato utente, ad esempio l'ora di sistema e la quantità di dati trasmessi e ricevuti. Se selezionata, la funzione di accounting RADIUS viene abilitata per il server RADIUS primario, per tutti i server di backup e per i server configurati a livello globale o locale.
- **Server IP Address 1** o **Server IPv6 Address 1**: l'indirizzo del server RADIUS primario per l'istanza CP. Quando il primo client wireless tenta di effettuare l'autenticazione con il dispositivo WAP, quest'ultimo invia una richiesta di autenticazione al server primario. Se il server primario risponde alla richiesta di autenticazione, il dispositivo WAP continua a utilizzare questo server RADIUS come server primario e le richieste di autenticazione sono inviate all'indirizzo specificato. L'indirizzo IPv4 deve essere nel formato seguente: xxx.xxx.xxx.xxx (192.0.2.10). L'indirizzo IPv6 deve essere nel formato seguente: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

- **Server IP Address 2-4** o **Server IPv6 Address 2-4**: fino a tre indirizzi del server RADIUS di backup IPv4 o IPv6. Se l'autenticazione con il server primario ha esito negativo, si prova in sequenza con ciascun server di backup configurato.
- **Key 1**: la chiave segreta condivisa utilizzata dal dispositivo WAP per l'autenticazione con il server RADIUS primario. È possibile immettere massimo 63 caratteri alfanumerici standard e speciali. La chiave fa distinzione tra maiuscole e minuscole e deve corrispondere a quella configurata sul server RADIUS. Il testo immesso viene mostrato come una serie di asterischi.
- **Key 2**-**Key 4**: la chiave RADIUS associata ai server RADIUS di backup configurati. Il server indicato nel campo Server IP (IPv6) Address 2 utilizza la chiave specificata nel campo Key 2, il server indicato in Server IP (IPv6) Address 3 utilizza la chiave del campo Key 3 e così via.
- **Locale Count**: il numero di impostazioni regionali associate all'istanza. Utilizzare la pagina Web Customization per creare e assegnare le impostazioni regionali per ogni istanza CP; è possibile definire massimo tre impostazioni per istanza.
- **Delete Instance**: cancella l'istanza attuale.

PASSAGGIO 6 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Associazione delle istanze

Utilizzare la pagina Instance Association per associare un'istanza CP creata a un VAP. Le impostazioni dell'istanza CP associata si applicano agli utenti che effettuano l'autenticazione sul VAP.

Per associare un'istanza a un VAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal** > **Instance Association**.

PASSAGGIO 2 Per i dispositivi WAP561, selezionare l'interfaccia radio su cui si desidera configurare l'associazione di un'istanza.

PASSAGGIO 3 Selezionare il nome dell'istanza per ogni VAP cui si desidera associarla.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Personalizzazione del portale Web

Dopo aver associato l'istanza CP a un VAP, è necessario creare un'impostazione regionale (una pagina Web di autenticazione) e associarla all'istanza CP. Quando un utente accede a un VAP associato a un'istanza di Captive Portal, viene visualizzata la pagina di autenticazione. Utilizzare la pagina Web Portal Customization per creare pagine specifiche delle varie impostazioni regionali sulla rete e personalizzare testi e immagini delle pagine.

Per creare e personalizzare una pagina di autenticazione CP, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal > Web Portal Customization**.

PASSAGGIO 2 Selezionare **Create** nell'elenco **Captive Portal Web Locale**.

È possibile creare fino a tre pagine di autenticazione diverse con impostazioni regionali diverse sulla rete.

PASSAGGIO 3 Immettere un nome per la pagina nel campo **Web Locale Name**. Il nome può contenere 1-32 caratteri alfanumerici e il trattino di sottolineatura.

PASSAGGIO 4 Nell'elenco **Captive Portal Instances**, selezionare l'istanza CP associata all'impostazione regionale.

È possibile associare più impostazioni regionali alla medesima istanza. Quando un utente accede a un determinato VAP associato a un'istanza CP, nella pagina di autenticazione vengono visualizzati i collegamenti alle impostazioni regionali associate all'istanza. L'utente può selezionare un collegamento per passare alle relative impostazioni regionali.

PASSAGGIO 5 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

PASSAGGIO 6 Nell'elenco **Captive Portal Web Locale**, selezionare le impostazioni regionali create.

Nella pagina vengono mostrati campi aggiuntivi per la modifica delle impostazioni regionali. I campi **Locale ID** e **Instance Name** non possono essere modificati. Nei campi modificabili vengono visualizzati valori predefiniti.

PASSAGGIO 7 Configurare i seguenti parametri:

- **Background Image Name**: l'immagine da visualizzare come sfondo della pagina. Fare clic su **Upload/Delete Custom Image** per caricare delle immagini per le istanze Captive Portal. Vedere Caricamento ed eliminazione di immagini.
- **Logo Image Name**: il file di immagine visualizzato nell'angolo superiore sinistro della pagina. Questa immagine viene utilizzata per scopi di branding, ad esempio il logo della società. Se è stata caricata l'immagine di un logo personalizzato sul dispositivo WAP, è possibile selezionarla dall'elenco.
- **Foreground color**: il codice HTML del colore di primo piano in formato esadecimale a 6 cifre. L'intervallo è compreso tra 1 e 32 caratteri. L'impostazione predefinita è #999999.
- **Background color**: il codice HTML del colore di sfondo in formato esadecimale a 6 cifre. L'intervallo è compreso tra 1 e 32 caratteri. L'impostazione predefinita è #BFBFBF.
- **Separator**: il codice HTML del colore della linea orizzontale spessa che separa l'intestazione dal corpo della pagina, in formato esadecimale a 6 cifre. L'intervallo è compreso tra 1 e 32 caratteri. L'impostazione predefinita è #BFBFBF.

Local Label: un'etichetta descrittiva delle impostazioni regionali; la lunghezza dell'etichetta è compresa tra 1 e 32 caratteri. L'etichetta deve essere conforme al Language Subtag Registry IANA e a eventuali codici regionali. Ad esempio, *en* per l'inglese, *fr* per il francese, *zh-TW* per il taiwanese. La lingua predefinita è l'inglese.

- **Locale**: abbreviazione delle impostazioni regionali, da 1 a 32 caratteri. L'impostazione predefinita è en.
- **Account Image**: il file di immagine da visualizzare sopra il campo di accesso, ad indicare un utente autenticato.
- **Account Label**: il testo che chiede all'utente di immettere un nome utente. L'intervallo è compreso tra 1 e 32 caratteri.
- **User Label**: l'etichetta della casella di testo del nome utente. L'intervallo è compreso tra 1 e 32 caratteri.
- **Password Label**: l'etichetta della casella di testo della password utente. L'intervallo è compreso tra 1 e 64 caratteri.
- **Button Label**: l'etichetta del pulsante su cui l'utente deve fare clic per inviare il nome utente e la password per l'autenticazione. L'intervallo è compreso tra 2 e 32 caratteri. La versione predefinita è Connect.

- **Fonts**: il nome del tipo di carattere utilizzato per il testo della pagina CP. È possibile immettere i nomi di più tipi di carattere, separati da una virgola. Se il primo tipo di carattere non è disponibile sul sistema client, verrà utilizzato il successivo e così via. I nomi di tipi di carattere che contengono spazi devono essere inseriti tra virgolette. L'intervallo è compreso tra 1 e 512 caratteri. L'impostazione predefinita è MS UI Gothic, Arial, sans-serif.
- **Browser Title**: il testo da visualizzare nella barra del titolo del browser. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Captive Portal.
- **Browser Content**: il testo visualizzato nell'intestazione della pagina, a destra del logo. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Welcome to the Wireless Network.
- **Content**: il testo con le istruzioni visualizzato nel corpo della pagina sotto i campi relativi al nome utente e alla password. L'intervallo è compreso tra 1 e 256 caratteri. L'impostazione predefinita è To start using this service, enter your credentials and click the connect button.
- **Acceptance Use Policy**: il testo visualizzato nella casella Acceptance Use Policy. L'intervallo è compreso tra 1 e 4096 caratteri. L'impostazione predefinita è Acceptance Use Policy.
- **Accept Label**: testo che indica all'utente di selezionare l'apposita casella per confermare di avere letto e accettato i termini di utilizzo. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Check here to indicate that you have read and accepted the Acceptance Use Policy.
- **No Accept Text**: testo visualizzato in una finestra popup quando un utente inserisce le credenziali di accesso senza selezionare la casella di accettazione dei termini di utilizzo. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Error: You must acknowledge the Acceptance Use Policy before connecting!
- **Work In Progress Text**: testo visualizzato durante l'autenticazione. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Connecting, please be patient...
- **Denied Text**: testo visualizzato in caso di autenticazione fallita. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Error Invalid Credentials, please try again!
- **Welcome Title**: testo visualizzato quando il client viene autenticato sul VAP. L'intervallo è compreso tra 1 e 128 caratteri. L'impostazione predefinita è Congratulations!

- **Welcome Content**: testo visualizzato una volta che il client si è connesso alla rete. L'intervallo è compreso tra 1 e 256 caratteri. L'impostazione predefinita è You are now authorized and connected to the network.
- **Delete Locale**: elimina le impostazioni regionali correnti.

PASSAGGIO 8 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

PASSAGGIO 9 Fare clic su **Anteprima** per visualizzare la pagina aggiornata.

NOTA Fare clic su **Anteprima** per visualizzare il testo e le immagini già salvati nella configurazione di avvio. In caso di modifiche, fare clic su **Salva**, quindi su **Anteprima** per vedere i contenuti aggiornati.

Quando un utente accede a un VAP associato a un'istanza Captive Portal, viene visualizzata una pagina di autenticazione, che è possibile personalizzare con il proprio logo o altre immagini.

È possibile caricare fino a 18 immagini (ipotizzando sei impostazioni regionali, tre immagini per ognuna). Tutte le immagini devono avere una dimensione massima di 5 kilobyte ed essere in formato GIF o JPG.

Le immagini vengono ridimensionate per adattarle alle dimensioni specifiche. Per ottenere risultati ottimali, il logo e le immagini dell'account dovrebbero avere proporzioni simili a quelle predefinite, ovvero:

Tipo di immagine	Uso	Larghezza e altezza predefinite
Sfondo	Viene mostrata come sfondo della pagina.	10 x 800 pixel
Logo	Viene mostrata nell'angolo superiore sinistro della pagina per fornire informazioni sul marchio.	168 x 78 pixel
Account	Viene mostrata sopra il campo di accesso ad indicare un utente autenticato.	295 x 55 pixel

Per caricare file di immagine binari sul dispositivo WAP, attenersi alla seguente procedura:

PASSAGGIO 1 Nella pagina Web Portal Customization, fare clic su **Upload/Delete Custom Image** accanto ai campi **Background Image Name**, **Logo Image Name** o **Account Image**.

Viene visualizzata la pagina Web Portal Custom Image.

PASSAGGIO 2 Selezionare l'immagine.

PASSAGGIO 3 Fare clic su **Upload**.

PASSAGGIO 4 Fare clic su **Back** per tornare alla pagina Web Portal Custom Image.

PASSAGGIO 5 Selezionare le impostazioni regionali Web di Captive Portal da configurare.

PASSAGGIO 6 Nei campi **Background Image Name**, **Logo Image Name** o **Account Image**, selezionare l'immagine appena caricata.

PASSAGGIO 7 Fare clic su **Salva**.

NOTA Per eliminare un'immagine, nella pagina Web Portal Custom Image, selezionarla nell'elenco **Delete Web Customization image** e fare clic su **Elimina**. Non è possibile eliminare le immagini predefinite.

Gruppi locali

Ogni utente locale viene assegnato a un gruppo utenti. Ogni gruppo è assegnato a un'istanza CP. Il gruppo facilita la gestione dell'assegnazione di utenti alle istanze CP.

Il gruppo di utenti Default è predefinito e non può essere eliminato. È possibile creare massimo due gruppi aggiuntivi di utenti.

Per aggiungere gruppi di utenti locali, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal** > **Local Groups**.

PASSAGGIO 2 Immettere un nome nel campo **Nome Gruppo** e fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

NOTA Per eliminare un gruppo, selezionarlo nell'elenco **Captive Portal Groups**, selezionare la casella **Delete Group** e fare clic su **Salva**.

Utenti locali

È possibile configurare un'istanza Captive Portal destinata sia agli utenti ospiti che agli utenti autorizzati. Agli utenti ospiti non vengono assegnati nome utente e password.

Gli utenti autorizzati, invece, devono inserire un nome utente e una password che verranno convalidati a fronte di un database locale o di un server RADIUS. Gli utenti autorizzati sono assegnati in genere a un'istanza CP associata a un VAP diverso da quello degli utenti ospiti.

Utilizzare la pagina Local Users per configurare massimo 128 utenti autorizzati nel database locale.

Per aggiungere e configurare un utente locale, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Captive Portal** > **Local Users**.

PASSAGGIO 2 Immettere un nome utente nel rispettivo campo e fare clic su **Salva**.

Verranno visualizzati campi aggiuntivi per la configurazione dell'utente.

PASSAGGIO 3 Immettere i seguenti parametri:

- **User Password**: immettere la password; la lunghezza della password è compresa tra 8 e 64 caratteri e sono consentiti caratteri alfanumerici e speciali. Per accedere alla rete tramite Captive Portal, l'utente deve inserire la password.
- **Show Password as Clear Text**: se si seleziona questa opzione, il testo digitato sarà visibile. Se disattivata, il testo verrà nascosto durante la digitazione.
- **Away Timeout**: periodo in cui un utente rimane nell'elenco di client CP autenticati dopo la disassociazione dall'AP. Se l'intervallo specificato in questo campo scade prima che il client esegua di nuovo l'autenticazione, la relativa voce verrà rimossa dall'elenco dei client autenticati. L'intervallo è compreso tra 0 e 1440 minuti. Il valore predefinito è 60. Il valore di timeout impostato in questo campo prevale sul valore configurato per l'istanza Captive Portal, a meno che il valore utente non sia impostato su 0. In tal caso, verrà utilizzato il valore di timeout configurato per l'istanza CP.
- **Group Name**: il gruppo di utenti assegnato. Ogni istanza CP è configurata per supportare un particolare gruppo di utenti.

- **Maximum Bandwidth Up**: la velocità massima di upload dei dati da parte del client tramite Captive Portal, espressa in megabit al secondo. Il valore di questo campo limita la larghezza di banda per l'invio dei dati in rete. L'intervallo è compreso tra 0 e 300 Mbps. L'impostazione predefinita è 0.
- **Maximum Bandwidth Down**: la velocità massima di download dei dati da parte del client tramite Captive Portal, espressa in megabit al secondo. Il valore di questo campo limita la larghezza di banda per la ricezione dei dati dalla rete. L'intervallo è compreso tra 0 e 300 Mbps. L'impostazione predefinita è 0.
- **Delete User**: elimina l'utente corrente.

PASSAGGIO 4 Fare clic su **Salva**. Le modifiche vengono salvate nella configurazione di avvio.

Client autenticati

Nella pagina Authenticated Clients vengono fornite informazioni sui client che hanno effettuato l'autenticazione su un'istanza Captive Portal.

Per visualizzare l'elenco dei client autenticati, selezionare **Captive Portal** > **Authenticated Clients** nel riquadro di spostamento.

- **MAC Address**: l'indirizzo MAC del client.
- **IP Address**: l'indirizzo IP del client.
- **User Name**: il nome utente Captive Portal del client.
- **Protocol**: il protocollo utilizzato dall'utente per stabilire la connessione (HTTP o HTTPS).
- **Verification**: il metodo utilizzato per autenticare l'utente su Captive Portal; è possibile selezionare uno dei valori seguenti:
  - **Guest**: non è necessaria l'autenticazione dell'utente a fronte di un database.
  - **Local**: il dispositivo WAP utilizza un database locale per gli utenti autenticati.
  - **RADIUS**: il dispositivo WAP utilizza un database su un server RADIUS remoto per gli utenti autenticati.

- **VAP ID**: il VAP associato all'utente.
- **Radio ID**: l'ID dell'interfaccia radio. Per il dispositivo WAP551 a singola interfaccia radio, il campo mostra **Radio 1**. Per il dispositivo WAP561 a doppia interfaccia radio, il campo mostra **Radio 1** o **Radio 2**.
- **Captive Portal ID**: l'ID dell'istanza Captive Portal associata all'utente.
- **Session Timeout**: tempo rimanente, espresso in secondi, alla scadenza della sessione CP. Quando il contatore arriva a zero, l'autenticazione del client scade.
- **Away Timeout**: tempo rimanente, espresso in secondi, alla scadenza della voce del client. Il timer viene avviato quando il client si disassocia da CP. Quando il contatore arriva a zero, l'autenticazione del client scade.
- **Received Packets**: il numero di pacchetti IP che il dispositivo WAP riceve dalla stazione dell'utente.
- **Transmitted Packets**: il numero di pacchetti IP trasmessi dal dispositivo WAP alla stazione dell'utente.
- **Received Bytes**: il numero di byte che il dispositivo WAP riceve dalla stazione dell'utente.
- **Transmitted Bytes**: il numero di byte trasmessi dal dispositivo WAP alla stazione dell'utente.

Per visualizzare i dati aggiornati dal dispositivo WAP, fare clic su **Refresh**.

Autenticazione client non riuscita

Nella pagina Authenticated Clients Failed vengono mostrate le informazioni sui client che non è stato possibile autenticare su un'istanza Captive Portal.

Per visualizzare l'elenco dei client che non sono stati autenticati, selezionare **Captive Portal** > **Failed Authentication Clients** nel riquadro di spostamento.

- **MAC Address**: l'indirizzo MAC del client.
- **IP Address**: l'indirizzo IP del client.
- **User Name**: il nome utente Captive Portal del client.
- **Verification**: il metodo utilizzato dal client per eseguire l'autenticazione Captive Portal; è possibile selezionare uno dei valori seguenti:

- **Guest**: non è necessaria l'autenticazione dell'utente a fronte di un database.
- **Local**: il dispositivo WAP utilizza un database locale per gli utenti autenticati.
- **RADIUS**: il dispositivo WAP utilizza un database su un server RADIUS remoto per gli utenti autenticati.

- **VAP ID**: il VAP associato all'utente.
- **Radio ID**: l'ID dell'interfaccia radio. Per il dispositivo WAP551 a singola interfaccia radio, il campo mostra **Radio 1**. Per il dispositivo WAP561 a doppia interfaccia radio, il campo mostra **Radio 1** o **Radio 2**.
- **Captive Portal ID**: l'ID dell'istanza Captive Portal associata all'utente.
- **Failure Time**: l'ora in cui si è verificato l'errore di autenticazione. Questo campo contiene un timestamp che mostra l'ora dell'errore.

Per visualizzare i dati aggiornati dal dispositivo WAP, fare clic su **Refresh**.

10

Punto di installazione singolo

In questo capitolo viene descritta la configurazione del punto di installazione singolo su più dispositivi WAP.

Vengono trattati i seguenti argomenti:

- **Descrizione del punto di installazione singolo**
- **Access point**
- **Sessioni**
- **Gestione dei canali**
- **Risorse wireless**

Descrizione del punto di installazione singolo

I dispositivi WAP551 e WAP561 supportano il punto di installazione singolo. Il punto di installazione singolo offre un metodo centralizzato per amministrare e controllare i servizi wireless fra più dispositivi. È possibile utilizzare il punto di installazione singolo per creare un singolo gruppo, o cluster, di dispositivi wireless. Dopo aver effettuato il clustering dei dispositivi WAP, è possibile visualizzare, distribuire, configurare e proteggere la rete wireless come singola entità. Dopo aver creato un cluster wireless, il punto di installazione singolo semplifica anche la pianificazione dei canali attraverso i servizi wireless consentendo così la riduzione delle interferenze radio e un utilizzo ottimale della larghezza di banda sulla rete wireless.

Durante la configurazione iniziale del dispositivo WAP è possibile utilizzare la procedura guidata per configurare il punto di installazione singolo oppure accedere a un punto di installazione singolo esistente. Se non si desidera utilizzare la procedura guidata, è possibile utilizzare l'utilità di configurazione basata sul Web.

Il punto di installazione singolo consente di creare un cluster, o gruppo, di dispositivi WAP, dinamico e in grado di rilevare la configurazione, nella stessa sottorete di una rete. Un cluster supporta un gruppo di massimo 16 dispositivi WAP551 e WAP561 configurati; non sono consentiti altri modelli nello stesso cluster.

Il punto di installazione singolo permette di gestire più cluster nella stessa sottorete o rete; tuttavia i cluster sono gestiti come singole entità indipendenti. Nella tabella seguente vengono mostrati i limiti dei servizi wireless del punto di installazione singolo.

Tipo di gruppo/ cluster	Dispositivi WAP per punto di installazione singolo	Numero di client attivi per punto di installazione singolo	Numero massimo di client (attivi e inattivi)
WAP5xx	16	480 960 per WAP561 con doppia radio	1024 2048 per WAP561 con doppia radio

È possibile propagare le informazioni sulla configurazione di un cluster, ad esempio impostazioni VAP, parametri di coda QoS e parametri radio. Le impostazioni manuali o predefinite di un dispositivo sul quale viene configurato il punto di installazione singolo vengono propagate agli altri dispositivi che accedono al cluster. Per creare un cluster, assicurarsi che siano soddisfatti i prerequisiti o le condizioni seguenti:

PASSAGGIO 1 Pianificare il cluster con punto di installazione singolo. Accertarsi che i due o più dispositivi WAP che si desidera utilizzare per il cluster siano compatibili tra loro. I dispositivi Cisco WAP551, ad esempio, possono formare un cluster soltanto con altri dispositivi Cisco WAP551 o WAP561.

> **NOTA** Si consiglia di eseguire la versione più recente del firmware su tutti i dispositivi WAP del cluster. Gli aggiornamenti del firmware **non vengono** propagati a tutti i dispositivi WAP in un cluster ed è necessario, quindi, aggiornarli singolarmente.

PASSAGGIO 2 Impostare i dispositivi WAP che formeranno il cluster sulla stessa sottorete IP e verificare che siano interconnessi e accessibili attraverso la rete LAN commutata.

PASSAGGIO 3 Attivare il punto di installazione singolo su tutti i dispositivi WAP. Vedere la sezione **Access point**.

PASSAGGIO 4 Verificare che i dispositivi WAP facciano tutti riferimento allo stesso nome del punto di installazione singolo. Vedere la sezione **Access point**.

NOTA Due dispositivi non devono necessariamente avere lo stesso numero di interfacce radio per essere nello stesso punto di installazione singolo; tuttavia è necessario che le interfacce radio supportino le stesse funzionalità.

Punto di installazione singolo AP a singola e a doppia radio

Un punto di installazione singolo può contenere una combinazione di AP a singola e a doppia radio. Se la configurazione di un dispositivo a singola radio nel cluster cambia, la modifica viene propagata alla prima radio di tutti i membri. La configurazione della seconda radio in qualsiasi AP a doppia radio nel cluster non viene modificata.

Se un punto di installazione singolo contiene soltanto AP a singola radio e un dispositivo a doppia radio accede al cluster, la configurazione del punto di installazione singolo verrà propagata soltanto all'interfaccia radio 1 del dispositivo a doppia radio. L'interfaccia radio 2 mantiene la configurazione precedente. Se, tuttavia, il punto di installazione singolo include già almeno un dispositivo a doppia radio, le impostazioni del cluster vengono propagate anche alla seconda interfaccia radio del dispositivo aggiunto al cluster.

Se su un dispositivo WAP viene abilitato e configurato il punto di installazione singolo, il dispositivo inizia a inviare annunci periodici ogni 10 secondi per annunciare la propria presenza. Se sono presenti altri dispositivi WAP che corrispondono ai criteri del cluster, inizia la negoziazione per determinare il dispositivo WAP che distribuirà la configurazione principale al resto dei membri del cluster.

Per la negoziazione e la creazione del cluster con punto di installazione singolo vengono applicate le regole seguenti:

- Per i cluster con punto di installazione singolo esistenti, ogni volta che l'amministratore aggiorna la configurazione di un cluster, la modifica viene propagata a tutti i membri e il dispositivo WAP configurato assume il controllo del cluster.
- Quando due cluster separati con punto di installazione singolo vengono uniti in un singolo cluster, l'ultimo cluster modificato vince la negoziazione della configurazione e sovrascrive e aggiorna la configurazione di tutti i dispositivi WAP del cluster.

- I dispositivi WAP all'interno di un cluster che non ricevono annunci da un dispositivo WAP per oltre 60 secondi (ad esempio se il dispositivo perde la connessione ad altri dispositivi nel cluster) verranno rimossi dal cluster.
- Se un dispositivo WAP in modalità punto di installazione singolo perde la connessione, non viene rimosso immediatamente dal cluster. Se la connessione viene ripristinata e il dispositivo accede nuovamente al cluster senza essere stato eliminato, eventuali modifiche apportate alla configurazione del dispositivo durante il periodo di perdita di connessione verranno propagate automaticamente agli altri membri del cluster.
- Se un dispositivo WAP all'interno di un cluster perde la connessione, viene rimosso e riaccede successivamente al cluster, eventuali modifiche apportate alla configurazione durante il periodo di perdita di connessione verranno propagate al dispositivo al nuovo accesso. Se sono state apportate modifiche alla configurazione nel dispositivo scollegato e nel cluster, per propagare la configurazione al cluster verrà utilizzato il dispositivo con il maggior numero di modifiche o, a parità di modifiche, quello con la modifica più recente. Questo significa che se il dispositivo WAP1 presenta più modifiche e WAP2 ha la modifica più recente, verrà selezionato WAP1. Se, però, i due dispositivi presentano lo stesso numero di modifiche, verrà selezionato WAP2, perché ha la modifica più recente.

Quando un dispositivo WAP che appartiene a un cluster viene scollegato, vengono applicate le seguenti linee guida:

- La perdita di contatto con il cluster impedisce al dispositivo WAP di ricevere le impostazioni di configurazione più recenti. La disconnessione genera un'interruzione del servizio wireless attraverso la rete di produzione.
- Il dispositivo WAP continua a funzionare con gli ultimi parametri wireless ricevuti dal cluster.
- I client wireless associati al dispositivo WAP che non fa parte del cluster continuano a comunicare con il dispositivo senza interruzione della connessione wireless. In altre parole, la perdita di contatto con il cluster non impedisce necessariamente ai client wireless associati al dispositivo WAP di continuare ad accedere alle risorse di rete.
- Un'eventuale perdita di contatto con il cluster dovuta alla disconnessione fisica o logica dall'infrastruttura LAN potrebbe incidere sui servizi di rete forniti ai client wireless a seconda della causa dell'errore.

Nelle tabelle seguenti viene presentato un riepilogo delle configurazioni condivise e propagate tra tutti i dispositivi WAP nel cluster.

Parametri e impostazioni di configurazione comuni propagati nel punto di installazione singolo	
Captive Portal	Password Complexity
Client QoS	Account utente
Avvisi tramite e-mail	QoS
Servizio HTTP/HTTPS (tranne configurazione certificato SSL)	Impostazioni radio incluse impostazioni TSpec (alcune eccezioni)
Impostazioni del log	Rilevamento AP non autorizzato
Filtraggio MAC	Scheduler
Controllo degli accessi per la gestione	SNMP General e SNMPv3
Reti	Complessità WPA-PSK
Impostazioni relative all'ora	

Parametri e impostazioni di configurazione radio propagati nel punto di installazione singolo
Modalità
Soglia di frammentazione
Soglia RTS
Impostazioni velocità
Canale principale
Protezione
Velocità multicast fissa
Limitazione velocità broadcast o multicast
Larghezza di banda canale
Intervallo di guardia breve supportato

Parametri e impostazioni di configurazione radio non propagati nel punto di installazione singolo
Canale
Intervallo beacon
Periodo DTIM
Stazioni massime
Potenza di trasmissione

Altri parametri e impostazioni di configurazione non propagati nel punto di installazione singolo	
Utilizzo della larghezza di banda	Impostazioni porta
Bonjour	VLAN e IPv4
Indirizzo IPv6	Bridge WDS
Tunnel IPv6	WPS
Acquisizione dei pacchetti	WorkGroup Bridge

Access point

La pagina Access Points consente di attivare o disattivare il punto di installazione singolo su un dispositivo WAP, visualizzare i membri del cluster e configurare la posizione e il nome del cluster per un membro. È inoltre possibile fare clic sull'indirizzo IP di un dispositivo per configurare e visualizzare i relativi dati.

Per configurare la posizione e il nome di un singolo membro del cluster con punto di installazione singolo, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Single Point Setup > Access Points**.

Il punto di installazione singolo è disattivato per impostazione predefinita sul dispositivo WAP. Se disattivato, è visibile il pulsante **Enable Single Point Setup**. Se, invece, è attivato, è visibile il pulsante **Disable Single Point Setup**. È possibile modificare le opzioni del punto di installazione singolo solo se è disattivato.

Le icone sul lato destro della pagina indicano se il punto di installazione singolo è attivato e, in questo caso, il numero di dispositivi WAP che sono attualmente inclusi nel cluster.

PASSAGGIO 2 Con il punto di installazione singolo disattivato, configurare le seguenti informazioni per ogni singolo membro di un cluster con punto di installazione singolo.

- **Location**: immettere una descrizione relativa alla posizione fisica dell'access point, ad esempio Reception. Questo campo è facoltativo.
- **Cluster Name**: immettere il nome del cluster a cui deve accedere il dispositivo WAP, ad esempio Reception_Cluster.

  Il nome del cluster non viene inviato ad altri dispositivi WAP. È necessario configurare lo stesso nome su ogni dispositivo membro. È necessario che il nome del cluster sia univoco per ciascun punto di installazione singolo configurato sulla rete. L'impostazione predefinita è ciscosb-cluster.
- **Clustering IP Version**: specificare la versione IP che i dispositivi WAP nel cluster utilizzano per comunicare con altri membri del cluster. L'impostazione predefinita è IPv4.

  Se si seleziona IPv6, il punto di installazione singolo può utilizzare l'indirizzo locale del collegamento, l'indirizzo globale IPv6 configurato automaticamente e l'indirizzo globale IPv6 configurato staticamente. Se si seleziona IPv6, assicurarsi che tutti i dispositivi WAP nel cluster utilizzino soltanto indirizzi locali di collegamento oppure soltanto indirizzi globali.

  Il punto di installazione singolo funziona soltanto con dispositivi che utilizzano lo stesso tipo di indirizzamento IP. Non funziona con un gruppo di dispositivi WAP in cui alcuni utilizzano indirizzi IPv4 e altri indirizzi IPv6.

PASSAGGIO 3 Fare clic su **Enable Single Point Setup**.

Il dispositivo WAP inizia a cercare nella sottorete altri dispositivi WAP configurati con lo stesso nome del cluster e la stessa versione IP. Un potenziale membro del cluster invia annunci ogni 10 secondi per segnalare la propria presenza.

Durante la ricerca di altri membri del cluster, nello stato viene indicata l'applicazione della configurazione. Aggiornare la pagina per visualizzare la nuova configurazione.

Se uno o più dispositivi WAP sono già stati configurati con le stesse impostazioni del cluster, il dispositivo WAP accede al cluster e le informazioni su ciascun membro vengono visualizzate in una tabella.

PASSAGGIO 4 Ripetere questi passaggi sui dispositivi WAP aggiuntivi che si desidera inserire nel punto di installazione singolo.

Se il punto di installazione singolo è attivato, il dispositivo WAP forma automaticamente un cluster con gli altri dispositivi WAP che presentano la stessa configurazione. Nella pagina Access Points è presente una tabella in cui vengono elencati i dispositivi WAP rilevati e vengono visualizzate le seguenti informazioni:

- **Location**: descrizione della posizione fisica dell'access point.
- **MAC Address**: indirizzo MAC (Media Access Control) dell'access point. Si tratta dell'indirizzo MAC per il bridge (br0) con il quale il dispositivo WAP è noto all'esterno ad altre reti.
- **IP Address**: l'indirizzo IP dell'access point.

Sul lato destro della pagina vengono mostrati graficamente lo stato del punto di installazione singolo e il numero di dispositivi WAP.

Per aggiungere un nuovo access point che si trova attualmente in modalità indipendente in un cluster con punto di installazione singolo, attenersi alla seguente procedura:

PASSAGGIO 1 Visualizzare l'utilità di configurazione basata sul Web sull'access point indipendente.

PASSAGGIO 2 Nel riquadro di spostamento, selezionare **Single Point Setup > Access Points**.

PASSAGGIO 3 Nel campo **Cluster name** immettere lo stesso nome configurato per i membri del cluster.

PASSAGGIO 4 (Facoltativo) Nel campo Location immettere una descrizione relativa alla posizione fisica dell'access point, ad esempio Reception.

PASSAGGIO 5 Fare clic su **Enable Single Point Setup**.

L'access point viene inserito automaticamente nel punto di installazione singolo.

Per rimuovere un access point dal cluster con punto di installazione singolo, attenersi alla seguente procedura:

PASSAGGIO 1 Nella tabella che mostra i dispositivi rilevati, fare clic sull'indirizzo IP del dispositivo WAP da rimuovere.

Viene visualizzata l'utilità di configurazione basata sul Web relativa al dispositivo WAP selezionato.

PASSAGGIO 2 Nel riquadro di spostamento, selezionare **Single Point Setup > Access Points**.

PASSAGGIO 3 Fare clic su **Disable Single Point Setup**.

Nel campo di stato **Single Point Setup** relativo all'access point rimosso verrà mostrato ora **Disabled**.

Tutti i dispositivi WAP in un cluster con punto di installazione singolo rispecchiano la stessa configurazione, ammesso che gli elementi configurabili possano essere propagati. Le modifiche apportate alla configurazione su qualsiasi dispositivo WAP all'interno del cluster vengono propagate agli altri membri, a prescindere dal dispositivo WAP a cui ci si collega per l'amministrazione.

Tuttavia, in alcune situazioni si desidera visualizzare o gestire le informazioni su un particolare dispositivo WAP. Ad esempio si desidera controllare le informazioni sullo stato, come le associazioni dei client o gli eventi di un access point. In questo caso, fare clic sull'indirizzo IP nella tabella della pagina Access Points per visualizzare l'utilità di configurazione basata sul Web relativa all'access point selezionato.

Per accedere all'utilità di configurazione basata sul Web di un dispositivo WAP specifico, è anche possibile immettere l'indirizzo IP dell'access point come URL direttamente nella barra degli indirizzi di un browser Web, come mostrato di seguito:

http://*IndirizzoIPAccessPoint* (se si usa HTTP)

https://IndirizzoIPAccessPoint (se si usa HTTPS)

Sessioni

La pagina Sessions mostra informazioni sui client WLAN associati ai dispositivi WAP all'interno del cluster con punto di installazione singolo. Ciascun client WLAN è identificato dal suo indirizzo MAC, insieme alla posizione del dispositivo da cui si collega.

NOTA Nella pagina Sessions vengono mostrati massimo 20 client per interfaccia radio sui dispositivi WAP del cluster. Per visualizzare tutti i client WLAN associati a un particolare dispositivo WAP, accedere alla pagina Status > Associated Clients del dispositivo in questione.

Per visualizzare una particolare statistica relativa alla sessione di un client WLAN, selezionare un elemento dall'elenco Display e fare clic su **Go**. È possibile visualizzare informazioni sui periodi di inattività, sulla velocità di trasmissione dei dati e sulla potenza del segnale.

In questo contesto una sessione corrisponde al periodo in cui un utente su un dispositivo client (stazione) con un indirizzo MAC univoco mantiene la connessione con la rete wireless. La sessione inizia quando il client WLAN accede alla rete e termina quando il client WLAN si disconnette intenzionalmente oppure perde la connessione per altri motivi.

NOTA La sessione non deve essere confusa con l'associazione; quest'ultima descrive, infatti, la connessione di un client WLAN a un particolare access point. L'associazione di un client WLAN può passare da un access point nel cluster a un altro all'interno della stessa sessione.

Per visualizzare le sessioni associate al cluster, selezionare **Single Point Setup > Sessions** nel riquadro di spostamento.

Per ogni sessione di client WLAN con un punto di installazione singolo vengono visualizzati i seguenti dati.

- **AP Location**: la posizione dell'access point.

  La posizione viene ricavata dalla posizione specificata nella pagina Administration > System Settings.

- **User MAC**: l'indirizzo MAC del client wireless.

  Un indirizzo MAC è un indirizzo hardware che identifica in maniera univoca ciascun nodo di una rete.

- **Idle**: il periodo in cui il client WLAN è rimasto inattivo.

  Un client WLAN è considerato inattivo quando non riceve o non trasmette dati.

- **Rate**: la velocità di trasmissione dei dati negoziata. Le velocità di trasferimento effettive possono variare in base al sovraccarico.

  La velocità di trasmissione dei dati è misurata in megabit al secondo (Mbps). Il valore deve essere compreso nell'intervallo di velocità dichiarato per la modalità in uso sull'access point. Ad esempio, da 6 a 54 Mbps per 802.11a.

- **Signal**: la potenza del segnale di radiofrequenza (RF) che il client WLAN riceve dall'access point. La misurazione è nota come RSSI (Received Signal Strength Indication) ed è un valore compreso tra 0 e 100.
- **Receive Total**: il numero di pacchetti totali ricevuti dal client WLAN durante la sessione attuale.
- **Transmit Total**: il numero di pacchetti totali trasmessi al client WLAN durante la sessione.
- **Error Rate**: la percentuale di frame temporali persi durante la trasmissione su questo access point.

Per ordinare le informazioni mostrate nelle tabelle secondo un particolare indicatore, fare clic sull'etichetta della colonna desiderata. Ad esempio, se si desidera visualizzare le righe della tabella ordinate in base alla potenza del segnale, fare clic sull'etichetta Signal.

Gestione dei canali

Nella pagina Channel Management vengono mostrate le assegnazioni di canale attuali e programmate per i dispositivi WAP in un cluster con punto di installazione singolo.

Se la gestione dei canali è attivata, il dispositivo WAP assegna automaticamente i canali radio utilizzati dai dispositivi WAP in un cluster con punto di installazione singolo. L'assegnazione automatica dei canali riduce l'interferenza reciproca o con altri dispositivi WAP all'esterno del cluster e ottimizza la larghezza di banda Wi-Fi in modo da garantire una comunicazione efficiente sulla rete wireless.

La funzione di assegnazione automatica dei canali è disattivata per impostazione predefinita. Lo stato della gestione dei canali, ovvero attivato o disattivato, viene propagato agli altri dispositivi del cluster con punto di installazione singolo.

Dopo un intervallo specificato, il gestore dei canali, ovvero il dispositivo che ha fornito la configurazione al cluster, associa tutti i dispositivi WAP nel cluster a diversi canali e misura i livelli di interferenza dei membri del cluster. Se viene rilevata un'interferenza significativa, il gestore dei canali riassegna automaticamente alcuni o tutti i dispositivi a nuovi canali mediante un algoritmo di efficienza o una programmazione automatica dei canali. Se il gestore dei canali stabilisce che è necessaria una modifica, tutti i membri del cluster ricevono le informazioni di riassegnazione. Viene generato, inoltre, un messaggio syslog che indica il dispositivo di origine, insieme alla nuova assegnazione dei canali e a quella precedente.

Per configurare e visualizzare l'assegnazione dei canali per i membri con punto di installazione singolo, attenersi alla seguente procedura:

PASSAGGIO 1 Nel riquadro di spostamento, selezionare **Single Point Setup** > **Channel Management**.

Nella pagina Channel Management è possibile visualizzare le assegnazioni dei canali per tutti i dispositivi WAP nel cluster e interrompere o avviare la gestione automatica dei canali. È inoltre possibile utilizzare le impostazioni avanzate per modificare il potenziale di riduzione delle interferenze che attiva la riassegnazione dei canali, cambiare la programmazione degli aggiornamenti automatici e riconfigurare il set di canali utilizzato per le assegnazioni.

PASSAGGIO 2 Per avviare l'assegnazione automatica dei canali, fare clic su **Start**.

La funzione di gestione dei canali annulla il comportamento predefinito del cluster, che prevede la sincronizzazione dei canali radio di tutti i dispositivi WAP membri del cluster. Se la gestione dei canali è attivata, il canale radio non è sincronizzato con gli altri dispositivi del cluster.

Se l'assegnazione automatica dei canali è attivata, il gestore dei canali analizza periodicamente i canali radio utilizzati dai dispositivi WAP in un cluster con punto di installazione singolo e, se necessario, li riassegna per ridurre l'interferenza con i membri del cluster o con dispositivi all'esterno dello stesso. Il criterio dei canali per l'interfaccia radio è impostato automaticamente sulla modalità statica e l'opzione **Auto** non è disponibile nel campo **Channel** della pagina Wireless > Radio.

Per informazioni sull'assegnazione dei canali attuale e su quella proposta, consultare Visualizzazione dell'assegnazione dei canali e blocco impostazioni.

PASSAGGIO 3 Per interrompere l'assegnazione automatica dei canali, fare clic su **Stop**.

In questo caso non verranno effettuate l'analisi dell'utilizzo dei canali o le riassegnazioni. Soltanto gli aggiornamenti manuali incideranno sull'assegnazione dei canali.

Se la gestione dei canali è attivata, nella pagina viene mostrata una tabella con le assegnazioni dei canali correnti e una tabella con le assegnazioni dei canali proposti.

Nella tabella con le assegnazioni dei canali correnti viene mostrato un elenco di tutti i dispositivi WAP nel cluster con punto di installazione singolo, ordinati per indirizzo IP.

Nella tabella sono inclusi i seguenti dettagli sulle assegnazioni dei canali correnti.

- **Location**: la posizione fisica del dispositivo.
- **IP Address**: l'indirizzo IP dell'access point.
- **Radio interface**: se il dispositivo è collegato tramite l'interfaccia Radio 1 (WLAN0) o Radio 2 (WLAN1). L'opzione Radio 2 viene utilizzata solo per i dispositivi WAP561.
- **Wireless Radio**: l'indirizzo MAC dell'interfaccia radio.
- **Band**: la banda sulla quale sta trasmettendo l'access point.
- **Channel**: il canale radio sul quale sta trasmettendo l'access point.
- **Locked**: obbliga l'access point a rimanere sul canale attuale.
- **Status**: mostra lo stato dell'interfaccia radio wireless nel dispositivo. Alcuni dispositivi WAP possono avere più interfacce radio wireless; ogni interfaccia viene visualizzata su una riga separata della tabella. Lo stato dell'interfaccia radio è up (operativo) o down (non operativo).

Nell'ambito della strategia di ottimizzazione, le programmazioni di gestione automatica dei canali, se selezionate per un access point, non riassegnano i dispositivi WAP a un canale differente. Al contrario, i dispositivi WAP con canali bloccati sono inclusi come requisito per la programmazione.

Fare clic su **Salva** per aggiornare le impostazioni bloccate. Per i dispositivi bloccati viene mostrato lo stesso canale nella tabella delle assegnazioni dei canali correnti e in quella delle assegnazioni dei canali proposti. I dispositivi bloccati mantengono i loro canali attuali.

Nella tabella delle assegnazioni dei canali proposti vengono mostrati i canali proposti da assegnare a ciascun dispositivo WAP al momento dell'aggiornamento successivo. I canali bloccati non vengono riassegnati. L'ottimizzazione della distribuzione dei canali tra i dispositivi tiene conto del fatto che i dispositivi bloccati devono rimanere sui loro canali attuali. I dispositivi WAP che non sono bloccati possono essere assegnati a canali diversi rispetto a quelli usati in precedenza, a seconda dei risultati della programmazione.

Per ciascun dispositivo WAP nel punto di installazione singolo, nella tabella delle assegnazioni dei canali proposti vengono mostrati la posizione, l'indirizzo IP e l'interfaccia radio wireless, come nella tabella delle assegnazioni dei canali correnti. Viene mostrato, inoltre, il canale proposto, ossia il canale radio al quale sarebbe riassegnato il dispositivo WAP in caso di applicazione della programmazione dei canali.

L'area Advanced Settings consente di personalizzare e programmare la programmazione dei canali per il punto di installazione singolo.

Per impostazione predefinita, i canali vengono riassegnati automaticamente ogni ora, ma solo se è possibile ridurre l'interferenza di almeno 25%. I canali vengono riassegnati anche se la rete è occupata. Le impostazioni predefinite soddisfano la maggior parte degli scenari nei quali è necessario implementare la gestione dei canali.

È possibile modificare le impostazioni avanzate seguenti in base alle proprie esigenze:

- **Change channels if interference is reduced by at least**: la percentuale minima di riduzione dell'interferenza che è necessario raggiungere per applicare una programmazione proposta. L'impostazione predefinita è 75%. Selezionare una percentuale tra 5% e 75% dal menu a discesa. Questa impostazione consente di impostare una soglia di guadagno in termini di efficienza per la riassegnazione dei canali, in modo che la rete non venga continuamente interrotta per guadagni minimi di efficienza.

  Ad esempio, se è necessario ridurre l'interferenza dei canali del 75% e le assegnazioni di canali proposte la ridurrebbero soltanto del 30%, i canali non verranno riassegnati. Se, invece, il guadagno di interferenza minimo dei canali viene reimpostato a 25% e si fa clic su **Salva**, la programmazione dei canali proposti verrà implementata e i canali saranno riassegnati come necessario.

- **Determine if there is better set of channels every**: la programmazione degli aggiornamenti automatici. Viene fornita una serie di intervalli, da 30 minuti a sei mesi.

L'impostazione predefinita è un'ora. Questo significa che l'utilizzo dei canali viene ricalcolato ogni ora e viene applicata la programmazione dei canali risultante.

Se si modificano queste impostazioni, fare clic su **Salva**. Le modifiche vengono salvate nella configurazione attiva e nella configurazione di avvio.

Risorse wireless

Nella pagina Wireless Neighborhood vengono mostrati fino a 20 dispositivi per interfaccia radio nell'intervallo di ciascuna interfaccia radio wireless nel cluster. Ad esempio, se un dispositivo WAP ha due interfacce radio wireless, nel cluster vengono visualizzati 40 dispositivi. Nella pagina Wireless Neighborhood vengono indicati anche i dispositivi membri del cluster e quelli che non vi appartengono.

La visualizzazione Wireless Neighborhood è utile nelle situazioni seguenti:

- Individuare e localizzare dispositivi sconosciuti o non autorizzati in un dominio wireless, in modo da poter intervenire e limitare i rischi associati.
- Verificare le aspettative di copertura. Valutando quali dispositivi WAP sono visibili da altri dispositivi e con quale potenza del segnale, è possibile verificare che la distribuzione soddisfi gli obiettivi previsti.
- Rilevare guasti. Modifiche inaspettate nella copertura sono evidenziate nella tabella a colori.

Per visualizzare i dispositivi adiacenti, selezionare **Single Point Setup** > **Wireless Neighborhood** nel riquadro di spostamento. Per vedere tutti i dispositivi rilevati su un determinato punto di installazione singolo, passare all'interfaccia Web di un membro e selezionare **Wireless** > **Rogue AP Detection** nel riquadro di spostamento.

Per ogni access point adiacente vengono mostrate le seguenti informazioni:

- **Display Neighboring APs**: selezionare uno dei seguenti pulsanti di scelta per cambiare la visualizzazione:
  - **In cluster**: soltanto i dispositivi WAP adiacenti che sono membri del cluster.
  - **Not in cluster**: soltanto i dispositivi WAP adiacenti che non sono membri del cluster.
  - **Both**: mostra tutti i dispositivi WAP adiacenti (membri e non membri del cluster).

NOTA Per un AP rilevato che è anche membro del cluster, soltanto gli SSID del VAP predefinito (VAP0) vengono visualizzati come In cluster. I VAP non predefiniti sull'AP risultano come Not in cluster.

- **Cluster**: nell'elenco nella parte superiore della tabella vengono mostrati gli indirizzi IP di tutti i dispositivi WAP raggruppati insieme nel cluster. Questo elenco è uguale all'elenco dei membri nella pagina **Single Point Setup** > **Access Points**.

  Se è presente un solo dispositivo WAP nel cluster, viene visualizzata una colonna con un solo indirizzo IP; questo indica che il dispositivo WAP è raggruppato con se stesso.

  È possibile fare clic su un indirizzo IP per visualizzare ulteriori dettagli su un determinato dispositivo WAP.

- **Neighbors**: i dispositivi adiacenti a uno o più dispositivi del cluster vengono elencati nella colonna a sinistra in base al nome della rete (SSID).

Anche un dispositivo rilevato come adiacente può essere membro del cluster. I dispositivi adiacenti che sono anche membri del cluster vengono sempre visualizzati nella parte superiore dell'elenco con una barra spessa sopra e includono un indicatore della posizione.

Le barre colorate a destra di ogni dispositivo WAP nell'elenco dei dispositivi adiacenti indicano la potenza del segnale di ciascun dispositivo WAP adiacente, come rilevato dal membro del cluster corrispondente all'indirizzo IP visualizzato nella parte superiore della colonna.

Il colore della barra indica la potenza del segnale:

- Barra blu scuro: una barra blu scuro e un numero elevato di potenza del segnale, ad esempio 50, indicano una buona potenza del segnale rilevata dal dispositivo adiacente, come visualizzato dal dispositivo corrispondente all'indirizzo IP elencato sopra a quella colonna.
- Barra blu chiaro: una barra blu chiaro e un numero basso di potenza del segnale, ad esempio 20 o un valore inferiore, indicano una potenza del segnale media o debole dal dispositivo adiacente, come visualizzato dal dispositivo corrispondente all'indirizzo IP elencato sopra a quella colonna.
- Barra bianca: una barra bianca e il numero 0 indicano che un dispositivo adiacente rilevato da uno dei membri del cluster non può essere individuato dal dispositivo corrispondente all'indirizzo IP elencato sopra a quella colonna.

- Barra grigio chiaro: una barra grigio chiaro e nessun numero di potenza del segnale indicano che non è stato rilevato alcun segnale dal dispositivo adiacente, ma quest'ultimo potrebbe essere stato rilevato da altri membri del cluster.
- Barra grigio scuro: una barra grigio scuro e nessun numero di potenza del segnale indicano il dispositivo WAP corrispondente all'indirizzo IP elencato sopra. Viene visualizzata una potenza di segnale pari a zero poiché la potenza del segnale del dispositivo stesso non viene misurata.

Per visualizzare i dettagli di un membro del cluster, fare clic sull'indirizzo IP del dispositivo desiderato nella parte superiore della pagina.

Sotto all'elenco dei dispositivi adiacenti vengono mostrati i seguenti dettagli relativi al dispositivo selezionato.

- **SSID**: SSID (Service Set Identifier) dell'access point adiacente.
- **MAC Address**: l'indirizzo MAC dell'access point adiacente.
- **Channel**: il canale sul quale sta trasmettendo l'access point.
- **Rate**: la velocità in megabit al secondo alla quale sta trasmettendo l'access point. La velocità attuale è sempre una delle velocità indicate nella casella Supported Rates.
- **Signal**: la potenza del segnale radio rilevata dall'access point, misurata in decibel (dB).
- **Beacon Interval**: l'intervallo di frequenza del beacon usato dall'access point.
- **Beacon Age**: la data e l'ora dell'ultimo beacon ricevuto dall'access point.

A

Codici relativi alle cause di annullamento dell'autenticazione

Quando un client annulla l'autenticazione al dispositivo WAP, viene inviato al log di sistema un messaggio con un codice che potrebbe aiutare a determinare la causa di tale annullamento. Per visualizzare i messaggi del log, fare clic su **Status and Statistics > Log**.

Per ulteriori informazioni, vedere:

- **Tabella dei codici relativi alle cause dell'annullamento dell'autenticazione**

Tabella dei codici relativi alle cause dell'annullamento dell'autenticazione

Nella tabella seguente sono descritti i codici relativi alle cause dell'annullamento dell'autenticazione.

Codice causa	Significato
0	Riservato
1	Causa non specificata
2	Autenticazione precedente non più valida
3	Annullamento dell'autenticazione dovuto al fatto che la stazione di invio (STA) sta per abbandonare o ha abbandonato l'IBSS (Independent Basic Service Set) o l'ESS
4	Annullamento dell'associazione dovuto a inattività

Codice causa	Significato
5	Annullamento dell'associazione dovuto al fatto che il dispositivo WAP non è in grado di gestire tutte le STA attualmente associate
6	Ricezione di un frame di classe 2 da una STA non autenticata
7	Ricezione di un frame di classe 3 da una STA non associata
8	Annullamento dell'associazione dovuto al fatto che la STA di invio sta per abbandonare o ha abbandonato il BSS (Basic Service Set)
9	La STA che richiede la riassociazione non è autenticata con la STA che risponde
10	Annullamento dell'associazione dovuto al fatto che le informazioni dell'elemento Power Capability non sono accettabili
11	Annullamento dell'associazione dovuto al fatto che le informazioni dell'elemento Supported Channels non sono accettabili
12	Annullamento dell'associazione dovuto a BSS Transition Management
13	Elemento non valido, ad esempio un elemento definito in questo standard i cui contenuti non soddisfano le specifiche del messaggio 8
14	Errore MIC (Message Integrity Code)
15	Timeout handshake 4-Way
16	Timeout handshake Group Key
17	Elemento handshake 4-Way diverso da frame (Re)Association Request/Probe Response/Beacon
18	Cifratura gruppo non valida
19	Cifratura a coppia non valida
20	AKMP non valido
21	Versione RSNE non supportata

Codice causa	Significato
22	Funzionalità RSNE non valide
23	Errore di autenticazione IEEE 802.1X
24	Cifratura rifiutata a causa dei criteri di sicurezza

B

Risorse aggiuntive

Cisco fornisce un'ampia gamma di risorse per aiutare l'utente e i clienti a ottenere il massimo dall'access point Cisco WAP551 e WAP561.

Assistenza	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Assistenza e risorse di Cisco Small Business	www.cisco.com/go/smallbizhelp
Contatti del supporto telefonico	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Download del firmware di Cisco Small Business	www.cisco.com/go/smallbizfirmware Selezionare un collegamento per scaricare il firmware relativo ai prodotti Cisco Small Business. Non sono necessari dati di accesso. I download per tutti gli altri prodotti Cisco Small Business, inclusi i sistemi di memorizzazione di rete, sono disponibili nell'area Download su Cisco.com al sito www.cisco.com/go/software (richiede la registrazione/l'immissione di dati di accesso).
Richieste Open Source Cisco Small Business	www.cisco.com/go/smallbiz_opensource_request
Documentazione relativa al prodotto	
Guida all'amministrazione e guida di riferimento rapido dell'access point wireless N Cisco WAP551 e WAP561 di Cisco Small Business	http://www.cisco.com/go/100_wap_resources o http://www.cisco.com/go/300_wap_resources

Cisco Small Business	
Cisco Partner Central per Small Business (richiede l'immissione di dati di accesso da parte dei partner)	www.cisco.com/web/partners/sell/smb
Home page di Cisco Small Business	www.cisco.com/smb

78-20594-01