Cisco WAP581 Wireless-AC/N Dual Radio Access Point mit 2,5 GbE LAN

Erste Veröffentlichung: 23 November 2016

Letzte Änderung: 16 Juli 2018

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

DIE BESTIMMUNGEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN OHNE VORHERIGE ANKÜNDIGUNG GEÄNDERT WERDEN. ALLE ANWEISUNGEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH SIND GENAU RECHERCHIERT, WERDEN JEDOCH OHNE JEGLICHE GARANTIE, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, VORGELEGT. DIE BENUTZER TRAGEN DIE VOLLE VERANTWORTUNG FÜR DEN UMGANG MIT SÄMTLICHEN PRODUKTEN.

DIE SOFTWARELIZENZ UND EINGESCHRÄNKTE GARANTIE FÜR DAS ERWORBENE PRODUKT WERDEN IM INFORMATIONSPAKET, DAS IM LIEFERUMFANG DIESES PRODUKTS ENTHALTEN IST, DARGELEGT UND GELTEN HIERMIT ALS BESTANDTEIL DIESER VEREINBARUNG. WENN SIE DIE SOFTWARELIZENZ ODER EINGESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, WENDEN SIE SICH AN EINEN VERTRETER VON CISCO, UM EINE KOPIE ZU ERHALTEN.

Die Cisco Implementierung der TCP-Headerkomprimierung ist eine Adaption eines Programms, das an der University of California, Berkeley (UCB) als Teil der Public-Domain-Version der UCB für das UNIX-Betriebssystem entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Verwaltungsrat der University of California.

UNGEACHTET JEGLICHER ANDERER HIERIN ENTHALTENEN GARANTIEBESTIMMUNG WERDEN ALLE DOKUMENTDATEIEN UND DIE SOFTWARE DIESER LIEFERANTEN„ WIE BESEHEN“ UND OHNE GARANTIE AUF FEHLERFREIHEIT ZUR VERFÜGUNG GESTELLT. CISCO UND ALLE ZUVOR GENANNTEN LIEFERANTEN VERZICHTEN AUF SÄMTLICHE GARANTIEN, AUSDRÜCKLICH ODER STILLSCHWEIGEND; EINSCHLIEßLICH, OHNE BESCHRÄNKUNG, DERJENIGEN IN BEZUG AUF HANDLUNGSFÄHIGKEIT, FITNESS FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG ODER SOLCHEN, DIE AUS DEM HANDELN, BENUTZEN ODER DURCH VERKAUFSAKTIVITÄTEN AUFKOMMEN.

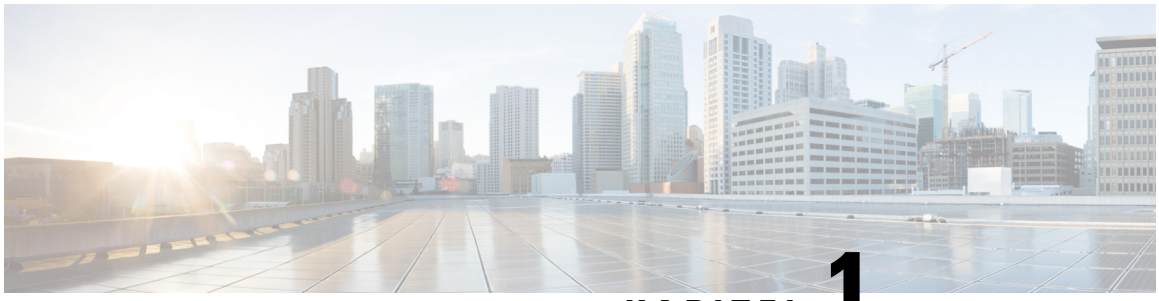
IN KEINEM FALL SIND CISCO ODER SEINE ZULIEFERER HAFTBAR FÜR INDIREKTE, SPEZIELLE UND ZUFÄLLIGE SCHÄDEN ODER FOLGESCHÄDEN JEGLICHER ART, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, SCHÄDEN AUS ENTGANGENEM GEWINN ODER DATENVERLUST AUFGRUND DER VERWENDUNG ODER NICHT MÖGLICHEN VERWENDUNG DIESES HANDBUCHS. DIES GILT AUCH FÜR DEN FALL, DASS CISCO ODER SEINE ZULIEFERER AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN AUFMERKSAM GEMACHT WURDEN.

Sämtliche in diesem Dokument verwendeten IP-Adressen und Telefonnummern sind als Beispiele zu verstehen und beziehen sich nicht auf tatsächlich existierende Adressen und Telefonnummern. Die in diesem Dokument enthaltenen Beispiele, Befehlsausgaben, Netzwerktopologie-Diagramme und anderen Abbildungen dienen lediglich zur Veranschaulichung. Die Verwendung tatsächlicher IP-Adressen oder Telefonnummern in diesem Zusammenhang ist zufällig und nicht beabsichtigt.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken der Cisco Systems, Inc. und/oder ihrer Partnerunternehmen in den USA und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter: https://www.cisco.com/go/trademarks. Erwähnte Marken anderer Anbieter sind das Eigentum ihrer jeweiligen Besitzer. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1721R)


Das Java-Logo ist eine Marke oder eingetragene Marke von Sun Microsystems, Inc. in den Vereinigten Staaten oder anderen Ländern.

INHALTSVERZEICHNIS



KAPITEL 1

Erste Schritte

In diesem Kapitel werden die folgenden Themen behandelt:

Erste Konfigurationsschritte

In diesem Abschnitt werden die Systemanforderungen und der Zugriff auf das webbasierte Konfigurationsdienstprogramm beschrieben.

Unterstützte Browser

Bevor Sie das Konfigurationsdienstprogramm verwenden, vergewissern Sie sich, dass auf Ihrem Computer Internet Explorer 9, Firefox 46, Chrome 49 oder Safari 5.0 oder eine jeweils neuere Version installiert ist.

Browsereinschränkungen

- Konfigurieren Sie die folgenden Sicherheitseinstellungen, falls Sie Internet Explorer 9 verwenden:
  - Wählen Sie **Tools Internetoptionen** und dann die Registerkarte **Sicherheit** aus.
  - Wählen Sie **Lokales Intranet** und **Standorte** aus.
  - Wählen Sie **Erweitert** und dann **Hinzufügen**. Fügen Sie die Intranetadresse für das WAP-Gerät `http://<IP-Adresse>` zur lokalen Intranetzone hinzu. Sie können die IP-Adresse auch als Subnetz-IP-Adresse angeben, sodass alle Adressen im Subnetz zur lokalen Intranetzone hinzugefügt werden.
- Wenn die Verwaltungsstation über mehrere IPv6-Schnittstellen verfügt, verwenden Sie die globale IPv6-Adresse anstelle der lokalen IPv6-Adresse, um über den Browser auf das WAP-Gerät zuzugreifen.

Starten des webbasierten Konfigurationsdienstprogramms

Führen Sie diese Schritte aus, um das Konfigurationsdienstprogramm auf Ihrem Computer zu starten und das WAP-Gerät zu konfigurieren:

1. Verbinden Sie das WAP-Gerät mit dem Netzwerk (oder IP-Subnetz) des PCs. Die IP-Adresse des WAP-Geräts wird standardmäßig über DHCP konfiguriert. Vergewissern Sie sich, dass der DHCP-Server aktiv und erreichbar ist.
2. Ermitteln Sie die IP-Adresse des WAP-Geräts.
    1. Sie können mit dem Cisco FindIT Network Discovery Utility auf das WAP-Gerät zugreifen und Verwaltungsvorgänge durchführen. Mit diesem Hilfsprogramm können Sie automatisch alle unterstützten Cisco-Geräte erkennen, die sich im gleichen lokalen Netzwerksegment befinden wie Ihr Computer. Sie können eine Übersicht aller Geräte anzeigen oder das Konfigurationsprogramm starten, um die Einstellungen anzuzeigen und zu konfigurieren. Weitere Informationen finden Sie unter http://www.cisco.com/go/findit.
    2. Das WAP-Gerät ist Bonjour-fähig, sendet automatisch seine Dienste und horcht auf von anderen Bonjour-fähigen Geräten gesendete Dienste. Wenn Sie über einen Bonjour-fähigen Browser verfügen, z.B. Microsoft Internet Explorer mit Bonjour-Plug-in oder Apple Mac Safari, können Sie das WAP-Gerät im lokalen Netzwerk auch ohne IP-Adresse ermitteln.

       Sie können Bonjour für Microsoft Internet Explorer von der folgenden Apple-Website herunterladen: http://www.apple.com/bonjour/ .
    3. Ermitteln Sie die vom DHCP-Server zugewiesene IP-Adresse, indem Sie auf den Router oder DHCP-Server zugreifen. Weitere Informationen finden Sie in den Anweisungen zu Ihrem DHCP-Server.
3. Starten Sie einen Webbrowser, z.B. Microsoft Internet Explorer.
4. Geben Sie die Standard-DHCP-Adresse in das Adressfeld ein, und drücken Sie die **Eingabetaste**.
5. Geben Sie den Standard-Benutzernamen und das Kennwort ein: `cisco` in die Felder **Benutzername** und **Passwort**.
6. Klicken Sie auf **Anmelden**. Der **Einrichtungsassistent für Access Points** wird geöffnet.

Folgen Sie den Anweisungen des Einrichtungsassistenten, um die Installation abzuschließen. Es wird dringend empfohlen, den Setup-Assistenten für die Erstinstallation zu verwenden. Weitere Informationen finden Sie unter Verwenden des Einrichtungsassistenten für Access Points, auf Seite 2.

Abmelden

Standardmäßig meldet sich das Konfigurationshilfsprogramm nach zehn Minuten Inaktivität ab. Anweisungen zum Ändern des Standard-Timeouts finden Sie unter Management, auf Seite 26.

Zum Abmelden klicken Sie in der rechten oberen Ecke des Konfigurationshilfsprogramms auf **Logout**.

Verwenden des Einrichtungsassistenten für Access Points

Bei der ersten Anmeldung beim Access Point (oder nach dem Zurücksetzen des Geräts auf die Werkseinstellungen) wird der Einrichtungsassistent für Access Points angezeigt, um Sie bei der Erstkonfiguration zu unterstützen. Führen Sie diese Schritte aus, um den Assistenten zu verwenden:

Hinweis Wenn Sie auf **Abbrechen** klicken, um den Assistenten zu umgehen, wird die Seite **Kennwort ändern** angezeigt. Sie können das Standardkennwort und den Standardbenutzernahmen für die Anmeldung ändern. Unter Kennwort ändern, auf Seite 6 finden Sie weitere Informationen.

Nach dem Ändern des Kennworts müssen Sie sich erneut anmelden.

Schritt 1 Klicken Sie auf der **Willkommensseite** des Assistenten auf **Weiter**.

Schritt 2 Klicken Sie im Fenster **Firmware-Upgrade** auf **Upgrade**, um die Firmware zu aktualisieren.

Hinweis Sobald die Firmware aktualisiert wurde, führt das Gerät automatisch einen Neustart aus und ruft die Anmeldeseite auf.

Schritt 3 Klicken Sie auf **Überspringen**. Das Fenster Konfiguration wiederherstellen wird angezeigt.

Schritt 4 Wählen Sie die Konfigurationsdatei aus, die Sie anwenden möchten, und klicken Sie auf **Speichern**.

Hinweis Klicken Sie auf **Speichern**. Das Gerät wendet die relevante Konfiguration an, führt automatisch einen Neustart aus und ruft die Anmeldeseite auf.

Schritt 5 Klicken Sie auf **Überspringen**. Das Fenster **Gerät konfigurieren—IP-Adresse** wird angezeigt.

Schritt 6 Klicken Sie auf **Dynamische IP-Adresse (DHCP) (Empfohlen)**, um eine IP-Adresse von einem DHCP-Server zu erhalten, oder klicken Sie auf **Statische IP-Adresse**, um die IP-Adresse manuell zu konfigurieren. Eine Beschreibung dieser Felder finden Sie unter IPv4-Konfiguration.

Schritt 7 Klicken Sie auf **Weiter**. Das Fenster **Single Point Setup — Set A Cluster** wird angezeigt. Eine Beschreibung von Single Point Setup finden Sie unter Single Point Setup – Übersicht.

Schritt 8 Zum Erstellen eines neuen Single Point Setups für WAP-Geräte klicken Sie auf **Neuer Cluster-Name**, und geben Sie einen neuen Namen an. Wenn Sie die Geräte mit dem gleichen Cluster-Namen konfigurieren und den Single Point Setup-Modus auf anderen WAP-Geräten aktivieren, treten diese Geräte automatisch der Gruppe bei.

Wenn im Netzwerk bereits ein Cluster vorhanden ist, können Sie das Gerät hinzufügen, indem Sie auf **Zu vorhandenem Cluster hinzufügen** klicken und in **Bestehender Cluster-Name** den Namen des vorhandenen Clusters eingeben.

Wenn das Gerät zurzeit nicht Bestandteil eines Single Point Setups sein soll, klicken Sie auf **Single Point Setup nicht aktivieren**.

Optional können Sie den Access Point-Standort im Feld **AP-Standort** angeben, um den physischen Standort des WAP-Geräts anzugeben.

Wenn Sie **Zu vorhandenem Cluster hinzufügen** gewählt haben, konfiguriert das WAP die übrigen Einstellungen dem Cluster entsprechend. Klicken Sie auf **Weiter** und bestätigen Sie das Hinzufügen zum Cluster. Klicken Sie auf **Senden**für das Hinzufügen zum Cluster. Nach Abschluß der Konfiguration klicken Sie auf **Beenden**, um den Einrichtungsassistenten zu beenden.

Schritt 9 Klicken Sie auf **Weiter**. Das Fenster **Gerät konfigurieren – Systemdatum und -zeit festlegen** wird angezeigt.

Schritt 10 Wählen Sie die Zeitzone aus, und stellen Sie dann die Systemzeit automatisch über eine NTP-Server bzw. manuell ein. Eine Beschreibung dieser Optionen finden Sie unter Uhrzeit, auf Seite 18.

Schritt 11 Klicken Sie auf **Weiter**. Das Fenster **Gerät konfigurieren – Kennwort festlegen** wird angezeigt.

Schritt 12 Geben Sie ein **Neues Kennwort** ein und geben Sie es im Feld **Kennwort bestätigen** erneut ein.

Hinweis Deaktivieren Sie die Option **Kennwortstärke**, um die Sicherheitsregeln für Kennwörter zu deaktivieren. Es wird jedoch dringend empfohlen, die Regeln für die Kennwortsicherheit aktiviert zu lassen. Weitere Informationen zu Kennwörtern finden Sie unter Security, auf Seite 34.

Schritt 13 Klicken Sie auf **Weiter**. Das Fenster „Funkmodul 1 konfigurieren – WLAN benennen“ wird angezeigt.

Schritt 14 Geben Sie in **Netzwerkname** einen Netzwerknamen ein. Dieser Name dient als SSID für das Standard-WLAN.

Schritt 15 Klicken Sie auf **Weiter**. Das Fenster „Funkmodul 1 konfigurieren – WLAN sichern“ wird angezeigt.

Schritt 16 Wählen Sie einen Sicherheitsverschlüsselungstyp aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter Konfigurieren von Sicherheitseinstellungen, auf Seite 50.

Schritt 17 **Klicken Sie auf „Weiter“**. Das Fenster „Funkmodul 1 konfigurieren – VLAN-ID für WLAN zuweisen“ wird angezeigt.

Schritt 18 Wählen Sie die **VLAN-ID** für den im WLAN empfangenen Verkehr aus.

Wir empfehlen, für WLAN-Verkehr eine andere VLAN-ID als den Standardwert (1) zuzuweisen, damit dieser Verkehr vom Verwaltungsverkehr in VLAN1 getrennt wird.

Schritt 19 Klicken Sie auf **Weiter**. Wiederholen Sie die Schritte 13 bis 18, um die Einstellungen für das Funkmodul 2 zu konfigurieren.

Schritt 20 Klicken Sie auf **Weiter**. Das Fenster „Captive-Portal aktivieren – Gastnetzwerk erstellen“ wird angezeigt.

Schritt 21 Wählen Sie aus, ob Sie ein Authentifizierungsverfahren für Gäste im Netzwerk einrichten möchten, und klicken Sie auf **Weiter**.

Wenn Sie auf **Nein** klicken, fahren Sie mit Schritt 29 fort.

Wenn Sie auf **Ja** klicken, wird das Fenster „Captive-Portal aktivieren – Gastnetzwerk benennen“ angezeigt.

Schritt 22 Geben Sie einen **Namen des Gastnetzwerks** an.

Schritt 23 Klicken Sie auf **Weiter**. Das Fenster „Captive-Portal aktivieren – Gastnetzwerk sichern“ wird angezeigt.

Schritt 24 Wählen Sie einen Sicherheitsverschlüsselungstyp für das Gastnetzwerk aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter Konfigurieren von Sicherheitseinstellungen, auf Seite 50.

Schritt 25 Klicken Sie auf **Weiter**. Das Fenster „Captive-Portal aktivieren – VLAN-ID zuweisen“ wird angezeigt.

Schritt 26 Geben Sie eine VLAN-ID für das Gastnetzwerk an. Die VLAN-ID des Gastnetzwerks sollte nicht mit der Verwaltungs-VLAN-ID identisch sein.

Schritt 27 Klicken Sie auf **Weiter**. Das Fenster **Captive-Portal aktivieren – Weiterleitungs-URL aktivieren** wird angezeigt.

Schritt 28 Aktivieren Sie die Option **Weiterleitungs-URL aktivieren**, und geben Sie einen vollständigen Domänennamen (FQDN) oder eine IP-Adresse im Feld **Weiterleitungs-URL** ein (einschließlich „http://“). Wenn angeben, werden Benutzer des Gastnetzwerks nach der Authentifizierung an die angegebene URL umgeleitet.

Schritt 29 Klicken Sie auf **Weiter**. Das Fenster „Zusammenfassung – Einstellungen bestätigen“ wird angezeigt.

Schritt 30 Überprüfen Sie die konfigurierten Einstellungen. Klicken Sie auf **Zurück**, um eine oder mehrere Einstellungen neu zu konfigurieren. Wenn Sie auf **Abbrechen** klicken, werden alle Einstellungen auf die vorherigen Werte oder auf die Standardwerte zurückgesetzt.

Schritt 31 Wenn die Einstellungen richtig sind, klicken Sie auf **Absenden**. Die Einrichtungseinstellungen werden gespeichert, und es wird ein Bestätigungsfenster angezeigt.

Schritt 32 Klicken Sie auf **Fertigstellen**.

Das WAP-Gerät wurde erfolgreich konfiguriert. Sie werden aufgefordert, sich mit dem neuen Kennwort erneut anzumelden.

Verwenden des Access Point-Einrichtungsassistenten für Mobilgeräte

Bei der ersten Anmeldung beim Access Point mit Ihrem tragbaren Gerät (oder nach dem Zurücksetzen des Geräts auf die Werkseinstellung) wird der Access Point-Einrichtungsassistent für Mobilgeräte angezeigt, um Sie bei der Erstkonfiguration zu unterstützen. Zur Konfiguration von Access Points mithilfe des Assistenten führen Sie die folgenden Schritte aus:

Hinweis Die werkseitig eingerichtete Standard-SSID lautet **CiscoSB-Setup**. Verbinden Sie Ihr Gerät mit dem Access Point mit dieser SSID und dem Pre-Shared Key, **cisco123**. Öffnen Sie einen Browser und geben Sie eine beliebige IP-Adresse oder einen beliebigen Domänennamen ein,. Eine Website mit Anmeldefeldern wird angezeigt. Geben Sie den standardmäßigen Benutzernamen und das standardmäßige Kennwort ein: **cisco**. Klicken Sie auf **Anmelden**. Die Seite **Access Point Setup Wizard** wird angezeigt.

Schritt 1 Klicken Sie auf der **Willkommensseite** des Assistenten auf **Weiter**. Das Fenster **IP-Adresse konfigurieren** wird angezeigt.

Schritt 2 Für den Empfang von IP-Adressen von einem DHCP-Server ist standardmäßig das Dynamic Host Configuration Protocol (empfohlen) konfiguriert. Um die IP-Adresse manuell zu konfigurieren, klicken Sie auf **Statisch**. Eine Beschreibung dieser Felder finden Sie unter **IPv4-Konfiguration**.

Schritt 3 Klicken Sie auf **Weiter**. Das Fenster **Single Point Setup konfigurieren** wird angezeigt.

Schritt 4 Klicken Sie auf **Überspringen**. Gehen Sie zu Schritt 6.

Schritt 5 Zum Hinzufügen zu einem vorhandenen Clister, geben Sie den Cluster-Gruppennamen ein und klicken Sie auf **Weiter**. Eine Zusammenfassung der Cluster-Informationen wird angezeigt. Bestätigen Sie die Daten und klicken Sie auf **Senden**.

Hinweis Zum Erstellen eines neuen Clusters klicken Sie auf **Erstellen**, geben einen Cluster-Namen ein und gehen Sie zu Schritt 6.

Schritt 6 Geben Sie im Fenster **Gerät konfigurieren—Kennwort festlegen** ein neues Kennwort ein; wiederholen Sie den Vorgang im Feld **Kennwort bestätigen**.

Schritt 7 Klicken Sie auf **Weiter**. Das Fenster **WLAN-Netzwerk konfigurieren** wird angezeigt.

a) Geben Sie einen Netzwerknamen ein, der als SSID für das standardmäßige WLAN-Netzwerk dient.
b) Geben Sie einen Sicherheitsschlüssel ein (Sicherheitstyp, WPA2 Personal – AES ist standardmäßig eingestellt).
c) Geben Sie die VLAN-ID für im WLAN-Netzwerk empfangenen Datenverkehr ein.

Hinweis Aktivieren Sie das Kästchen, um dieselbe Konfiguration an Radio 2 vorzunehmen oder wechseln Sie zu einem anderen Radio-Reiter und wiederholen Sie Schritt 7 zur erneuten Konfiguration.

Schritt 8 Klicken Sie auf **Weiter**. Das Fenster **Captive Portal einrichten** wird angezeigt.

Schritt 9 Klicken Sie auf **Überspringen**. Gehen Sie zu Schritt 12.

Schritt 10 Klicken Sie auf **Ja**. Das Fenster **Konfiguration von Captive Portal** wird angezeigt.

Schritt 11 Wählen Sie **Funkmodul 1 (5 GHz)** oder **Funkmodul 2 (2,4 GHz)** aus.

a) Geben Sie einen Gastnetzwerknamen an.
b) Geben Sie einen Sicherheitsschlüssel ein (Sicherheitstyp, WPA2 Personal – AES ist standardmäßig eingestellt).
c) Geben Sie eine VLAN-ID für das Gastnetzwerk ein.

d) Optional können Sie eine Umleitungs-URL mit einem vollständig qualifizierten Domänennamen eingeben, um Benutzer nach der Authentifizierung zur festgelegten URL umzuleiten.

Schritt 12 Klicken Sie auf **Weiter**. Das Fenster **Zusammenfassung** wird angezeigt.

Schritt 13 Überprüfen Sie die konfigurierten Einstellungen. Klicken Sie auf **Zurück**, um eine oder mehrere Einstellungen neu zu konfigurieren.

Schritt 14 Stellen Sie sicher, dass die Angaben korrekt sind, und klicken Sie auf **Senden**, um die Einstellungen zu speichern.

Schritt 15 Das WAP-Gerät wurde erfolgreich konfiguriert. Melden Sie sich jetzt mit dem neuen Kennwort erneut an.

Kennwort ändern

Aus Sicherheitsgründen müssen Sie das Administratorkennwort in regelmäßigen Abständen ändern. Nach Ablauf der Passwortablaufzeit werden Sie aufgefordert, diese Seite zu besuchen.

Die Passwortkomplexität ist standardmäßig aktiviert. Die Mindestanforderungen für die Passwortkomplexität werden auf der Seite „Passwort ändern“ angezeigt. Das neue Kennwort muss die Kennwortkomplexitätsregeln erfüllen. Alternativ können Sie diese Regeln unter der Option **Kennwortkomplexität** vorübergehend deaktivieren. Weitere Informationen finden Sie unter Security, auf Seite 34.

Konfigurieren Sie die folgenden Felder, um das Standardpasswort zu ändern:

- **Benutzername**: Geben Sie einen neuen Benutzernamen ein. Der Standardname ist „cisco“.
- **Altes Kennwort**: Geben Sie das aktuelle Kennwort (Standard: cisco) ein.
- **Neues Passwort**: Geben Sie ein neues Passwort ein.
- **Kennwort bestätigen**: Geben Sie das neue Kennwort zur Bestätigung erneut ein.
- **Kennwortsicherheitsmessung**: Zeigt die Sicherheit des neuen Passworts an.
- **Passwortkomplexität**: Die Passwortkomplexität ist standardmäßig aktiviert und legt fest, dass das neue Passwort die folgenden Kriterien erfüllen muss:
  - Das neue Passwort muss sich vom Benutzernamen unterscheiden.
  - Das neue Passwort muss sich vom aktuellen Passwort unterscheiden.
  - Das neue Passwort muss eine Mindestlänge von acht Zeichen haben.
  - Das neue Passwort muss Zeichen aus mindestens drei Zeichenklassen enthalten (Großbuchstaben, Kleinbuchstaben, Zahlen und auf einer Standardtastatur verfügbare Sonderzeichen).

Hinweis Klicken Sie auf **Deaktivieren**, um die Regeln für die Passwortkomplexität zu deaktivieren. Es wird jedoch dringend empfohlen, die Regeln für die Passwortkomplexität aktiviert zu lassen.

TCP/UDP-Service

In der Tabelle „TCP/UDP-Service“ werden grundlegende Informationen zu den auf dem WAP verwendeten Protokollen und Diensten angezeigt.

- **Dienst**: Der Dienstname.
- **Protokoll**: Das vom Dienst verwendete zugrunde liegende Transportprotokoll (TCP oder UDP).
- **IP-Adresse**: Die IP-Adresse des verbundenen Geräts. Alle bedeutet, dass jede IP-Adresse im Gerät diesen Dienst verwenden kann.
- **Lokaler Port**: Die lokale Portnummer.
- **Remote-IP-Adresse**: Die IP-Adresse eines Remotehosts, der diesen Dienst verwendet. Alle bedeutet, dass der Dienst für alle Remotehosts verfügbar ist, die auf das System zugreifen können.
- **Remote-Port**: Die Portnummer eines Remotegeräts, das mit diesem Service kommuniziert
- **Verbindungsstatus**: Der Status des Diensts. Für UDP werden in der Tabelle nur Verbindungen mit dem Status „Aktiv“ oder „Verbunden“ angezeigt. Die TCP-Status lauten:
  - **Mithören**: Der Dienst hört Verbindungsanfragen mit.
  - **Aktiv**: Eine Verbindungssitzung ist hergestellt, und es werden Pakete gesendet und empfangen.
  - **Verbunden**: Eine Verbindungssitzung ist zwischen dem WAP-Gerät und einem Server oder Client hergestellt.
  - **Wartezeit**: Die Schlusssequenz wurde initiiert, und das WAP-Gerät wartet vor dem Schließen der Verbindung einen vom System definierten Zeitraum ab (in der Regel 60 Sekunden).

Hinweis Sie können die Reihenfolge in der Tabelle TCP/UDP-Service bearbeiten. Sie können auf **Aktualisieren** klicken, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

Sie können Parameter bezüglich Dienst, Protokoll und anderer Details angeben, um die angezeigten TCP/UDP-Services zu filtern.

Klicken Sie auf **Zurück**, um zur Seite **Erste Schritte** zurückzukehren.

Systemstatus

Auf der Seite „Systemstatus“ werden Hardwaremodell, Softwareversion sowie verschiedene Konfigurationsparameter angezeigt, darunter:

- **PID-VID**: Hardwaremodell und Version des WAP-Geräts.
- **Seriennummer**: Die Seriennummer des WAP-Geräts.
- **Hostname**: Der Hostname des WAP-Geräts.
- **MAC-Adresse**: Die MAC-Adresse des IP-Geräts.

- **IPv4-Adresse**: Die IP-Adresse des WAP-Geräts.
- **IPv6-Adresse**: Die IPv6-Adresse des WAP-Geräts.
- **ETH0/PD-Port**: Der Status der Ethernet-Schnittstelle.
- **ETH1-Port**: Der Status der ETH1-Schnittstelle.
- **Funkmodul 1 (5 GHz)**: Gibt an, ob der 5 GHz-Modus für die Funkschnittstelle 1 aktiviert oder deaktiviert ist.
- **Funkmodul 2 (2,4 GHz)**: Gibt an, ob der 2,4 GHz-Modus für die Funkschnittstelle 2 aktiviert oder deaktiviert ist.
- **Stromquelle**: Das System wird entweder mit einem Netzteil betrieben oder erhält Strom per Power over Ethernet (PoE), inklusive der zwei Stromversorgungsmodi 802.3.af und 802.3at von einem PSE (Power Sourcing Equipment).

  Wenn die Stromversorgung nicht ausreicht (802.3af), behält das WAP-Gerät die folgenden Konfigurationsinformationen bei.

  - Das Funkmodul 1 (5 GHz) ist deaktiviert.
  - Die Antenne von Funkmodul 2 (2,4 GHz) wechselt von 3x3 zu 2x2, der TX-Strom wird auf 18 dBm reduziert.
  - Die Geschwindigkeit des ETH0/PD-Ports wird auf 1 Gbit/s reduziert.
  - Der ETH1-Port wird abgeschaltet.

- **Systembetriebszeit**: Die seit dem letzten Neustart verstrichene Zeit.
- **Systemzeit**: Die aktuelle Systemzeit.
- **Firmware-Version (aktives Image)**: Die Firmwareversion des aktiven Images.
- **Firmware-MD5-Prüfsumme (aktives Image)**: Die Prüfsumme des aktiven Images.
- **Firmware-Version (inaktives Image)**: Die Firmwareversion des Backup-Images.
- **Firmware-MD5 Prüfsumme (inaktives Image)**: Die Prüfsumme des Backup-Images.

QuickStart-Konfiguration

Zur Vereinfachung der Gerätekonfiguration finden Sie auf der Seite **Erste Schritte** Links zum Ausführen allgemeiner Aufgaben. Nach dem Start wird standardmäßig die Seite **Erste Schritte** angezeigt.

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite

Schnellzugang	Einrichtungsassistent	Verwenden des Einrichtungsassistenten für Access Points, auf Seite 2
	Kontokennwort ändern	Hinzufügen eines Benutzers, auf Seite 25
	Konfiguration sichern/wiederherstellen	Konfigurationsdateien, auf Seite 117
	Gerätefirmware aktualisieren	Firmware, auf Seite 115
Erweiterte Konfiguration	WLAN-Einstellungen	Funk, auf Seite 41
	Verwaltungseinstellung	Management, auf Seite 26
	Single Point Setup konfigurieren	Konfigurieren des WAP-Geräts für Single Point Setup, auf Seite 75
	LAN-Einstellung	IPv4-Konfiguration, auf Seite 11
	Gastzugang	Gastzugang, auf Seite 97
Weitere Informationen	Dashboard	Dashboard
	TCP/UDP-Service	TCP/UDP-Service, auf Seite 7
	Systemprotokoll anzeigen	LED-Anzeige, auf Seite 19
	Verkehrsstatistik	Verkehrsstatistik, auf Seite 110

Weitere Informationen zum Gerät finden Sie auf der Produkt-Supportseite oder in der Cisco Support Community:

- Klicken Sie auf **Support**, um die Produkt-Supportseite zu öffnen.
- Klicken Sie auf **Foren**, um die Seite der Cisco Support Community zu öffnen.
- Klicken Sie auf **Weitere Informationen zu FindIT**, um Informationen zum Dienstprogramm FindIT anzuzeigen.
- Klicken Sie auf **FindIT herunterladen**, um das Dienstprogramm FindIT herunterzuladen.

Fensternavigation

Mit den Navigationsschaltflächen können Sie die einzelnen Bereiche der grafischen Benutzeroberfläche des WAP-Geräts aufrufen.

Header des Konfigurationsdienstprogramms

Der Header des Konfigurationsdienstprogramms enthält Standardinformationen und wird oben auf jeder Seite angezeigt. Der Header bietet folgende Schaltflächen:

Schaltflächenname	Beschreibung
(Benutzer)	Der Kontoname (Administrator oder Gast) des auf dem WAP-Gerät angemeldeten Benutzers. Der werksseitige Standardbenutzername lautet **cisco**.

(Sprache)	Bewegen Sie den Mauszeiger über die Schaltfläche und wählen Sie eine Sprache aus. Standardmäßig ist Englisch als Sprache voreingestellt.
	Klicken Sie auf diese Schaltfläche, um sich vom Konfigurationshilfsprogramm abzumelden.
	Klicken Sie auf diese Schaltfläche, um Typ und Versionsnummer des WAP-Geräts anzuzeigen.
	Klicken Sie auf diese Schaltfläche, um die kontextgebundene Onlinehilfe anzuzeigen. Die Onlinehilfe ist für die Anzeige in Browsern mit UTF-8-Codierung gedacht. Wenn in der Onlinehilfe falsche Zeichen angezeigt werden, vergewissern Sie sich, dass in den Codierungseinstellungen im Browser UTF-8 festgelegt ist.

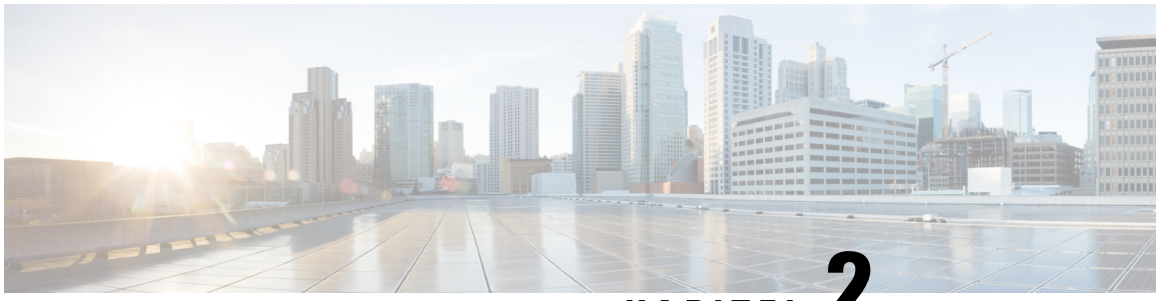
Navigationsbereich

Links auf jeder Seite befindet sich ein Navigationsbereich oder Hauptmenü. Der Navigationsbereich enthält eine Liste der Funktionen der obersten Ebene des WAP-Geräts. Wenn einem Hauptmenüelement ein Pfeil vorangestellt ist, wählen Sie den Pfeil aus, um die Gruppe zu erweitern und das jeweilige Untermenü anzuzeigen. Dann können Sie das gewünschte Untermenüelement auswählen, um die zugehörige Seite zu öffnen.

Verwaltungsschaltflächen

In der folgenden Tabelle werden die am häufigsten verwendeten Schaltflächen beschrieben, die auf den verschiedenen Seiten des Systems zur Verfügung stehen.

Schaltflächenname	**Beschreibung**
Hinzufügen	Fügt der Tabelle oder Datenbank einen neuen Eintrag hinzu.
Abbrechen	Verwirft die auf der Seite vorgenommenen Änderungen.
Alle löschen	Löscht alle Einträge in einer Protokolltabelle.
Löschen	Löscht einen Eintrag in einer Tabelle.
Bearbeiten	Bearbeitet einen vorhandenen Eintrag.
Aktualisieren	Lädt die aktuelle Seite mit den neuesten Daten.
Speichern	Speichert die Einstellungen oder die Konfiguration.
Aktualisieren	Aktualisiert die Startkonfiguration mit den neuen Informationen.



KAPITEL 2

Systemkonfiguration

In diesem Kapitel wird das Konfigurieren globaler Systemeinstellungen und das Ausführen von Diagnosen beschrieben. Das Kapitel enthält die folgenden Themen:

LAN

In diesem Abschnitt wird die Konfiguration von Port, VLAN, IPv4- und IPv6-Einstellungen des WAP-Geräts beschrieben.

IPv4-Konfiguration

Auf der Seite „IPv4-Einstellung“ können Sie die IPv4-Adresse konfigurieren.

Schritt 1 Wählen Sie **LAN > IPv4-Konfiguration** aus.

Schritt 2 Konfigurieren Sie die folgenden IPv4-Einstellungen:

- **Verbindungstyp**: Standardmäßig überträgt der DHCP-Client auf dem WAP-Gerät automatisch die Anfragen zu Netzwerkinformationen. Wenn Sie eine statische IP-Adresse verwenden möchten, müssen Sie den DHCP-Client deaktivieren und die IP-Adresse sowie weitere Netzwerkinformationen manuell konfigurieren.

  Wählen Sie eine der folgenden Optionen aus:

  - **DHCP**: Das WAP-Gerät bezieht seine IP-Adresse von einem DHCP-Server im LAN.
  - **Statische IP**: Manuelle Konfiguration der IPv4-Adresse. Geben Sie die IPv4-Adresse im Format xxx.xxx.xxx.xxx (172.17.144.170) ein.

- **Statische IP-Adresse, Subnetzmaske und Standardgateway**: Geben Sie die Statische IP-Adresse, die Subnetzmaske und das Standardgateway ein.

- **Domänen-Nameserver**: Wählen Sie eine der folgenden Optionen:
  - **Dynamisch**: Das WAP-Gerät bezieht DNS-Serveradressen von einem DHCP-Server im LAN.
  - **Manuell**: Geben sie bis zu zwei IP-Adressen in die entsprechenden Felder ein.

Schritt 3 Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Einstellungen für automatische DHCP-Konfiguration

- **Optionen für automatische DHCP-Konfiguration**: Diese Option ist standardmäßig aktiviert. Wenn ein AP mit Werkseinstellungen eingeschaltet wird, versucht er zunächst, sich mit den DHCP-Optionen automatisch zu konfigurieren.

  Während der automatischen Konfiguration geschieht Folgendes:

  - Der Access Point wird mit aktivierter Ethernet-Schnittstelle und mit deaktivierten WLAN-Schnittstellen gestartet.
  - Für den Benutzer stehen keine Services zur Verfügung (außer Benutzeroberflächen).
  - „Optionen für automatische DHCP-Konfiguration“ wird nach Ablauf der festgelegten Wartezeit oder nach dem TFTP-Upload einer Konfigurationsdatei (je nachdem, was zuerst eintritt) automatisch deaktiviert.
  - Durch Deaktivieren des DHCP-Clients (d. h. Konfiguration mit statischer IP-Adresse) oder durch sofortiges Deaktivieren von „Optionen für automatische DHCP-Konfiguration“ wird die automatische Konfiguration sofort abgebrochen.

  Der DHCP-Client sendet automatisch Anfragen für die DHCP-Optionen 66 und 67. Wenn „DHCP“ und „Optionen für automatische DHCP-Konfiguration“ aktiviert sind, wird der Access Point beim nächsten Neustart automatisch konfiguriert, wobei die vom DHCP-Server für DHCP-Anfragen empfangenen Informationen berücksichtigt werden.

Hinweis Beim Hochladen einer Konfiguration durch den Benutzer oder durch Cisco wird die automatische Konfiguration außer Kraft gesetzt, und die ausgewählte Konfigurationsdatei erhält Vorrang. Bei jedem anderen Neustart des AP (Firmware-Upgrade, Neustart usw.) wird die vorhandene automatische Konfigurationseinstellung beibehalten.

- **IPv4-Adresse/Hostname des TFTP-Servers**: Wenn Sie die Adresse des TFTP-Servers konfigurieren, wird diese verwendet, falls die Datei von anderen TFTP-Servern nicht abgerufen werden kann, die vom DHCP-Server bei der automatischen Konfiguration angegeben wurden. Geben Sie die IPv4-Adresse oder den Hostnamen ein. Wenn Sie einen Hostnamen eingeben, muss der DNS-Server verfügbar sein, um den Hostnamen in eine IP-Adresse zu übersetzen.

Dieser Wert wird beim nächsten Startvorgang für die automatische Konfiguration verwendet.

- **Name der Konfigurationsdatei**: Wenn Sie den Namen der Konfigurationsdatei angeben, wird diese während der automatischen AP-Konfiguration vom TFTP-Server abgerufen, falls der Name der Bootdatei

nicht vom DHCP-Server empfangen wird. Wenn dieser Wert nicht vorhanden ist, wird „config.xml“ verwendet. Die Datei muss mit der Erweiterung „.xml“ angegeben werden.

Dieser Wert wird beim nächsten Startvorgang für die automatische Konfiguration verwendet.

- **Wartezeit**: Sofern konfiguriert, wird der Access Point mit der lokalen Konfiguration aktiv und stellt die aktivierten Services nach der Wartezeit dem Benutzer zur Verfügung. Der Access Point bricht die automatische Konfiguration ab, wenn die TFTP-Transaktion nicht innerhalb dieser angegebenen Zeit initiiert wird.

Dieser Wert wird beim nächsten Startvorgang für die automatische Konfiguration verwendet.

- **Statusprotokoll**: In diesem Feld wird der Grund für den Abschluss oder Abbruch der automatischen Konfiguration angezeigt.

IPv6-Konfiguration

Auf der Seite „IPv6-Einstellungen“ können Sie die IPv6-Adresse mit den folgenden Schritten konfigurieren:

Schritt 1 Wählen Sie **LAN > IPv6-Konfiguration** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **IPv6-Verbindungstyp**: Wählen Sie eine der folgenden Optionen aus:
  - **DHCPv6**: Die IPv6-Adresse wird von einem DHCPv6-Server zugewiesen.
  - **Statisches IPv6**: Konfigurieren Sie die IPv6-Adresse manuell. Geben Sie die IPv6-Adresse im Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) ein.
- **Administrativer IPv6-Modus**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den administrativen IPv6-Modus zu aktivieren.
- **Administrativen IPv6-Modus automatisch konfigurieren**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, die automatische IPv6-Adresskonfiguration zu aktivieren.

  Wenn die automatische IPv6-Adresskonfiguration aktiviert ist, erkennt das WAP-Gerät seine IPv6-Adressen und das Gateway durch die Verarbeitung der am LAN-Anschluss empfangenen Routerankündigungen. Das WAP-Gerät kann mehrere automatisch konfigurierte IPv6-Adressen haben.
- **Statische IPv6-Adresse**: Geben Sie die statische IPv6-Adresse ein. Das WAP-Gerät kann auch dann eine statische IPv6-Adresse haben, wenn die Adressen automatisch konfiguriert wurden.
- **Präfixlänge der statischen IPv6-Adresse**: Geben Sie die Präfixlänge der statischen Adresse ein, eine Ganzzahl im Bereich von 0 bis 128. Die Standardeinstellung ist 0.
- **Status der statischen IPv6-Adresse**: Wählen Sie eine der folgenden Optionen:
  - **Einsatzbereit**: Die Eindeutigkeit der IP-Adresse wurde überprüft, und die IP-Adresse kann an der LAN-Schnittstelle verwendet werden.
  - **Vorläufig**: Das WAP-Gerät initiiert den Erkennungsprozess für doppelte Adressen (Duplicate Address Detection, DAD) automatisch, wenn eine statische IP-Adresse zugewiesen wird. Diese IPv6-Adresse ist vorläufig, da sie noch im Netzwerk überprüft wird, und kann nicht zum Versenden oder Empfangen von Daten verwendet werden.

- **Leer (kein Wert)**: Es wurde keine IP-Adresse zugewiesen.

- **Automatisch konfigurierte globale IPv6-Adressen**: Eine Liste der für das Gerät automatisch konfigurierten globalen IPv6-Adressen.
- **IPv6-Link Local-Adresse**: Die IPv6-Adresse, die von der lokalen physischen Verbindung verwendet wird. Die Link-Local-Adresse ist nicht konfigurierbar und wird mit dem IPv6-Nachbarerkennungsprozess zugewiesen.
- **IPv6-Standardgateway**: Das statisch konfigurierte IPv6-Standardgateway
- **IPv6-Domänen-Nameserver**: Wählen Sie eine der folgenden Optionen aus:
  - **Dynamisch**: Die DNS-Server werden per DHCPv6 dynamisch erkannt.
  - **Manuell**: Mit dieser Option können Sie bis zu zwei IPv6-DNS-Server manuell angeben.

Port-Einstellungen

In der Tabelle „Port-Einstellungen“ können Sie Einstellungen für den Port anzeigen und konfigurieren, über den das WAP-Gerät mit einem LAN verbunden ist.

Schritt 1 Wählen Sie **LAN** > **Mehr** > **Tabelle der Porteinstellungen** aus.

In der **Tabelle der Porteinstellungen** werden die folgenden Statusmeldungen und Konfigurationen für die LAN-Schnittstelle angezeigt:

- **Link-Aggregation**: Aktiviert die Link-Aggregationsgruppe (LAG).
- **LAG-Modus**: Enthält die folgenden Optionen:
  - **Standard-LAG**: Wenn die zwischen zwei Ethernet-Schnittstellen ausgehandelten Geschwindigkeiten unterschiedlich sind, wird das neuere Plug-In gesperrt.
  - **BW-Vorrang**: Wenn die zwischen zwei Ethernet-Schnittstellen ausgehandelten Geschwindigkeiten unterschiedlich sind, wird die niedrigere der beiden Geschwindigkeiten gesperrt.
  - **Vorrang für Redundanz und Energie**: Die beiden Ethernet-Schnittstellen werden für die Bindung auf dieselbe Geschwindigkeit angepasst. Dies ist der Standardmodus.

Hinweis WAP581 unterstützt statisches LAG und ist nicht mit dem LACP kompatibel. Vergewissern Sie sich, dass das LAG mit dem WAP581-Gerät funktioniert. Auf diese Weise können Benutzer das LAG vom Standardmodus in andere Modi versetzen.

In der **Tabelle der Porteinstellungen** werden die folgenden Statusmeldungen und Konfigurationen für eine Schnittstelle (LAN) angezeigt:

- **Schnittstellen**: Gibt die LAN-Schnittstelle an.
- **Linkstatus**: Zeigt den aktuellen Verbindungsstatus des Anschlusses an.
- **Portgeschwindigkeit**: Im Überprüfungsmodus wird hier die aktuelle Portgeschwindigkeit angezeigt. Wählen Sie, sofern die automatische Aushandlung deaktiviert ist, im Bearbeitungsmodus eine Portgeschwindigkeit

wie 100 Mbit/s oder 10 Mbit/s aus. Bei aktivierter automatischer Aushandlung wird nur die Geschwindigkeit 1000 Mbit/s unterstützt.

- **Duplexmodus**: Im Überprüfungsmodus wird hier der aktuelle Duplexmodus für den Port angezeigt. Wählen Sie, sofern die automatische Aushandlung deaktiviert ist, im Bearbeitungsmodus den Duplexmodus **Halb** oder **Voll** aus.
- **Automatische Aushandlung**: Wenn die Option aktiviert ist, handelt der Anschluss mit seinem Verbindungspartner die höchste verfügbare Verbindungsgeschwindigkeit und den höchsten verfügbaren Duplexmodus aus. Wenn die Option deaktiviert ist, können Sie die Portgeschwindigkeit und den Duplexmodus manuell konfigurieren.
- **Green Ethernet**: Der Green-Ethernet-Modus unterstützt sowohl eine automatische Abschaltung als auch den EEE-Modus (Energy Efficient Ethernet, IEEE 802.3az). Der Green-Ethernet-Modus funktioniert nur, wenn die automatische Aushandlung für den Port aktiviert ist. Die Leistung des Chips wird automatisch reduziert, wenn kein Signal von einem Verbindungspartner vorhanden ist. Das WAP-Gerät wechselt automatisch in einen Energiesparmodus, wenn die Leitung nicht genug Strom führt, und nimmt den Normalbetrieb wieder auf, wenn Strom anliegt. Der EEE-Modus unterstützt RUHIGE Zeiten während niedriger Verbindungsauslastung und ermöglicht es so beiden Seiten einer Verbindung, Komponenten der PHY-Platine zu deaktivieren, um Strom zu sparen.

Schritt 2 Klicken Sie auf **Speichern**.

Spanning Tree Protocol

Klicken Sie im Spanning Tree Protocol-Modus auf das Kontrollkästchen **Aktivieren**, um den STP-Modus auf dem Cisco WAP-Gerät zu aktivieren. Wenn STP aktiviert ist, können Switching-Loops vermieden werden. Verwenden Sie nach Möglichkeit STP, wenn Sie WDS-Links konfigurieren.

VLAN-Einstellung

Verwenden Sie die Seite „VLAN-Konfiguration“, um die VLAN-Einstellungen anzuzeigen und zu konfigurieren.

Schritt 1 Wählen Sie **LAN > Mehr > VLAN-Einstellungstabelle**.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **VLAN-ID ohne Tag**: Gibt eine Zahl zwischen 1 und 4094 für die VLAN-ID ohne Tag an. Die Standardeinstellung ist 1. Der Datenverkehr in diesem VLAN, das Sie in diesem Feld angeben, wird nicht mit einer VLAN-ID als Tag versehen, wenn er im Netzwerk weitergeleitet wird.
- **Beschreibung**: Beschreibung des verbundenen VLAN.
- **Management-VLAN**: Das Management-VLAN ist das VLAN, das für den Zugriff auf das WAP-Gerät über Telnet oder die Web-GUI verwendet wird. Es darf nur ein VLAN als Management-VLAN fungieren. Wenn dem Management-VLAN keine Schnittstelle (kabelgebunden oder Wireless) zugeordnet ist, existiert keine Schnittstelle, die der Benutzer für den Zugriff auf das Konfigurationsdienstprogramm verwenden kann.
- **VLAN**: Wählen Sie ein VLAN (**ohne Tag oder mit Tag**) in der Dropdown-Liste aus.

Standardmäßig wird für den gesamten Verkehr des WAP-Geräts das VLAN1 verwendet, das Standard-VLAN ohne Tag. Dies bedeutet, dass der gesamte Verkehr erst mit einem Tag versehen wird, wenn Sie das VLAN ohne Tag deaktivieren, die VLAN-ID für Verkehr ohne Tag ändern oder die VLAN-ID für einen VAP oder Client, der RADIUS verwendet, ändern.

Schritt 3 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Netznachbarerkennung

Bonjour ermöglicht die Erkennung des WAP-Geräts und der zugehörigen Dienste mithilfe von Multicast-DNS (mDNS). Bonjour kündigt Dienste im Netzwerk an und beantwortet Anfragen für die unterstützten Diensttypen, um die Netzwerkkonfiguration in Ihren Umgebungen zu vereinfachen.

Das WAP-Gerät kündigt die folgenden Diensttypen an:

- **Cisco-spezifische Gerätebeschreibung (csco-sb)**: Dieser Dienst ermöglicht Clients die Erkennung von Cisco-WAP-Geräten und anderen Produkten, die in Ihren Netzwerken bereitgestellt sind.
- **Verwaltungsbenutzeroberflächen**: Dieser Dienst identifiziert die im WAP-Gerät verfügbaren Verwaltungsschnittstellen (HTTP und SNMP).

Wenn ein Bonjour-fähiges WAP-Gerät mit einem Netzwerk verbunden ist, können alle Bonjour-Clients ohne vorherige Konfiguration das Konfigurationsdienstprogramm erkennen und auf dieses zugreifen.

Ein Systemadministrator kann das WAP-Gerät mithilfe eines installierten Internet Explorer-Plug-Ins erkennen. Das webbasierte Konfigurationsdienstprogramm wird als Registerkarte im Browser angezeigt.

Hinweis Systemadministratoren könnend die Bonjour-fähigen WAPs mit dem aktuellen Internet Explorer-Plug-In anzeigen (Cisco FindIt). Alle WAP-Geräte in einem Cluster werden nach dem Bonjour-Erkennungsprozess unter dem Clusternamen angezeigt. Administratoren müssen sicherstellen, dass der Name des Clusters im Netzwerk eindeutig ist.

Bonjour kann in IPv4- und IPv6-Netzwerken eingesetzt werden.

Mit den folgenden Schritten können Sie die Erkennung des WAP-Geräts durch Bonjour aktivieren:

Schritt 1 Wählen Sie **LAN > Nachbarerkennung** aus.

Schritt 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Bonjour zu aktivieren.

Schritt 3 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

LLDP

Das LLDP (Link Layer Discovery Protocol) ist im IEEE 802.1AB-Standard definiert und ermöglicht es dem UAP, Informationen zum eigenen Systemnamen, zu Systemfunktionen und Leistungsbedarf anzukündigen. Diese Informationen helfen Ihnen dabei, die Topologie des Systems zu ermitteln und fehlerhafte Konfigurationen im LAN zu erkennen. Der AP unterstützt zudem das LLDP-MED (Link Layer Discovery

Protocol for Media Endpoint Devices), das zusätzliche Informationselemente standardisiert, die Geräte zur Verbesserung des Netzwerkmanagements untereinander austauschen können.

Schritt 1 Wählen Sie **LAN > LLDP** aus, um die LLDP-Einstellungen zu konfigurieren.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **LLDP-Modus**: Klicken Sie auf **Aktivieren**, um LLDP zu aktivieren. Wenn LLDP aktiviert ist, überträgt der Access Point LLDP-Protokolldateneinheiten an benachbarte Geräte.
- **TX-Intervall**: Die Anzahl der Sekunden zwischen den gesendeten LLDP-Mitteilungen. Gültig sind Werte im Bereich von 5 bis 32.768 Sekunden. Der Standardwert liegt bei 30 Sekunden.
- **POE-Priorität**: Wählen Sie die Prioritätsstufe in der Dropdownliste aus (**Kritisch, Hoch, Niedrig oder Unbekannt**). Anhand der PoE-Prioritätsstufe legt das PSE (Power Sourcing Equipment) fest, welchen strombetriebenen Geräten bei der Leistungszuweisung Priorität eingeräumt werden soll, wenn das PSE nicht über ausreichend Kapazität verfügt, um die angeschlossenen Geräte mit Energie zu versorgen.

Schritt 3 Klicken Sie auf **Speichern**.

IPv6 Tunnel

Das WAP-Gerät unterstützt ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Mit ISATAP kann das WAP-Gerät in IPv4-Paketen gekapselte IPv6-Pakete über das LAN senden. Das Protokoll ermöglicht dem WAP-Gerät die Kommunikation mit IPv6-fähigen Remotehosts, auch wenn IPv6 in dem für die Verbindung verwendeten LAN nicht unterstützt wird.

Das WAP-Gerät fungiert als ISATAP-Client. Im LAN muss ein ISATAP-fähiger Host oder Router vorhanden sein. Die IP-Adresse oder der Hostname des Routers wird im WAP-Gerät konfiguriert (der Standardwert lautet „isatap“). Bei der Konfiguration als Hostname kommuniziert das WAP-Gerät mit einem DNS-Server, um den Namen in eine oder mehrere ISATAP-Routeradressen aufzulösen. Anschließend sendet das WAP-Gerät Anfragenachrichten an die Router. Wenn ein ISATAP-fähiger Router mit einer Ankündigungsnachricht antwortet, wird der Tunnel zwischen dem WAP-Gerät und dem Router aufgebaut. Der Tunnelschnittstelle wird eine Link Local-Adresse und eine globale IPv6-Adresse zugewiesen, die als virtuelle IPv6-Schnittstellen im IPv4-Netzwerk dienen.

Wenn IPv6-Hosts die Kommunikation mit dem über den ISATAP-Router verbundenen WAP-Gerät initiieren, werden die IPv6-Pakete vom ISATAP-Router in IPv4-Paketen gekapselt.

- **ISATAP-Status**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um ISATAP auf dem Gerät zu aktivieren.
- **ISATAP-fähiger Host**: Geben Sie die IP-Adresse oder der DNS-Name des ISATAP-Routers ein. Der Standardwert lautet "isatap".
- **ISATAP-Abfrageintervall**: Geben Sie an, wie oft das WAP-Gerät beim Versuch, den ISATAP-Hostnamen in eine IP-Adresse aufzulösen, Abfragen an den DNS-Server senden soll. Gültig sind Werte im Bereich von 120 bis 3.600 Sekunden. Der Standardwert liegt bei 120 Sekunden.
- **ISATAP-Solicitation-Intervall**: Geben Sie an, wie oft das WAP-Gerät die Router Solicitation-Nachrichten an die ISATAP-Router senden soll. Das WAP sendet nur dann Solicitation-Nachrichten, wenn kein aktive ISATAP-Router vorhanden ist. Gültig sind Werte im Bereich von 120 bis 3.600 Sekunden. Der Standardwert liegt bei 120 Sekunden.

- **ISATAP-IPv6-Link-Local-Adresse**: Die IPv6-Adresse, die von der lokalen physischen Verbindung verwendet wird. Die Link-Local-Adresse ist nicht konfigurierbar und wird mit dem IPv6-Nachbarerkennungsprozess zugewiesen.
- **Globale ISATAP-IPv6-Adresse**: Wenn dem WAP-Gerät automatisch eine oder mehrere IPv6-Adressen zugewiesen wurden, werden die Adressen aufgeführt.

Hinweis Wenn der Tunnel aufgebaut wurde, werden die ISATAP-IPv6-Link Local-Adresse und die globale ISATAP-IPv6-Adresse auf der Seite angezeigt. Diese Adressen sind virtuelle IPv6-Schnittstellenadressen.

Klicken Sie auf **Speichern**.

Uhrzeit

Die Systemuhr stellt einen mit dem Netzwerk synchronisierten Zeitstempeldienst für Softwareereignisse wie Nachrichtenprotokolle bereit. Sie können die Systemuhr manuell oder als NTP-Client (Network Time Protocol) konfigurieren, der die Uhrzeitdaten von einem Server bezieht.

Auf der Seite „Zeiteinstellungen“ können Sie die Systemzeit manuell festlegen oder von einem vorkonfigurierten NTP-Server abrufen. Das WAP-Gerät ist standardmäßig so konfiguriert, dass die Uhrzeit von NTP-Servern aus einer vordefinierten Liste bezogen wird.

Die aktuelle Systemzeit wird oben auf der Seite zusammen mit der Option **Systemuhrzeitquelle** angezeigt.

Automatisches Beziehen der Zeiteinstellungen über NTP

Führen Sie die folgenden Schritte aus, um die Zeiteinstellungen automatisch von einem NTP-Server zu beziehen:

Schritt 1 Wählen Sie **Systemkonfiguration > Zeit** aus.

Schritt 2 Klicken Sie im Feld „Systemuhrzeitquelle“ auf **Netzwerkzeitprotokoll (Network Time Protocol, NTP)**.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **NTP-Server (1 bis 4)**: Geben Sie die IPv4- oder IPv6-Adresse oder den Hostnamen eines NTP-Servers ein. Ein Standard-NTP-Server wird aufgeführt.

  Ein Hostname kann aus mindestens einem Label, d. h. einer Gruppe aus bis zu 63 alphanumerischen Zeichen bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Labels durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.

- **Zeitzone**: Wählen Sie die Zeitzone für Ihren Standort aus.
- **Automatisch auf Sommer-/Winterzeit umstellen**: Aktivieren Sie diese Option, um die folgenden Felder zu aktivieren und konfigurieren zu können:
  - **Beginn**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
  - **Ende**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitendes aus.

- **Sommerzeitdifferenz**: Geben Sie die Anzahl der Minuten an, um die die Uhr zu Beginn der Sommerzeit vor- bzw. am Ende der Sommerzeit zurückgestellt werden soll.

Schritt 4 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Manuelle Konfiguration der Zeiteinstellungen:

So konfigurieren Sie die Zeiteinstellungen manuell:

Schritt 1 Wählen Sie **Systemkonfiguration > Zeit** aus.

Schritt 2 Klicken Sie im Feld „Systemuhrzeitquelle“ auf **Manuell**.

Schritt 3 Klicken Sie auf **Uhrzeit mit PC synchronisieren**, um die Zeiteinstellungen von Ihrem lokalen PC zu klonen.

Schritt 4 Außerdem können Sie die folgenden Felder konfigurieren:

- **Systemdatum**: Wählen Sie in den Dropdownlisten das aktuelle Datum (Monat, Tag und Jahr) aus.
- **Systemzeit**: Wählen Sie die aktuelle Uhrzeit (Stunden und Minuten) im 24-Stunden-Format aus.
- **Zeitzone**: Wählen Sie die Zeitzone für Ihren Standort aus.
- **Automatisch auf Sommer-/Winterzeit umstellen**: Aktivieren Sie diese Option und konfigurieren die folgenden Felder, falls Ihre Zeitzone die Sommerzeit verwendet:
  - **Beginn**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
  - **Ende**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitendes aus.
  - **Sommerzeitdifferenz**: Geben Sie die Anzahl der Minuten an, um die die Uhr zu Beginn der Sommerzeit vor- bzw. am Ende der Sommerzeit zurückgestellt werden soll.

Schritt 5 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Klicken Sie auf **Uhrzeit mit PC synchronisieren**, um die Uhrzeit auf dem Gerät mit dem PC abzustimmen.

Benachrichtigung

In diesem Kapitel wird beschrieben, wie Sie die Benachrichtigungen für den Access Point aktivieren und konfigurieren.

LED-Anzeige

Am WAP-Gerät befinden sich zwei Arten von LEDs: System-LED und Ethernet-LED. Auf der Seite „LED-Anzeige“ können Sie sämtliche LEDs konfigurieren.

Sie können die LED-Anzeige mit den folgenden Schritten konfigurieren:

Schritt 1 Wählen Sie **Benachrichtigung > LED-Anzeige** aus.

Schritt 2 Wählen Sie **Aktiviert** aus, um die LEDs zu aktivieren. Wählen Sie **Deaktiviert** aus, um die LEDs zu deaktivieren. Wählen Sie **Planungsmodul zuordnen** aus und fahren Sie mit Schritt 3 fort.

Schritt 3 Wählen Sie in der Dropdownliste „Planungsmodul-LED-Anzeige zuordnen“ einen Profilnamen aus. Den LEDs ist standardmäßig kein Profil zugeordnet. Die Dropdownliste enthält die auf der Seite **Wireless > Planungsmodul** konfigurierten Planungsmodul-Profilnamen.

Wenn die LED einem Planungsmodulprofil zugeordnet ist, zeigt diese Spalte den Status in Abhängigkeit davon an, ob zu dieses Tageszeit eine aktive Profilregel vorliegt oder fehlt.

Schritt 4 Klicken Sie auf **Speichern**.

Protokolleinstellungen

Auf der Seite „Protokolleinstellungen“ können Sie das Speichern von Protokollnachrichten im permanenten Speicher aktivieren. Sie können Protokolle auch an einen Remotehost senden.

Bei einem unerwarteten Neustart des Systems können Protokollmeldungen die Diagnose der Ursache erleichtern. Wenn Sie die dauerhafte Protokollierung jedoch nicht aktivieren, werden Protokollnachrichten beim Neustart des Systems gelöscht.

⚠

Vorsicht Die Aktivierung der dauerhaften Protokollierung kann jedoch zur Abnutzung des (nichtflüchtigen) Flash-Speichers und zur Beeinträchtigung der Netzwerkleistung führen. Aktivieren Sie die dauerhafte Protokollierung nur zum Beheben von Problemen. Deaktivieren Sie die dauerhafte Protokollierung unbedingt, wenn Sie das Problem behoben haben.

Konfigurieren des dauerhaften Protokolls

Schritt 1 Wählen Sie **Benachrichtigung > Protokolleinstellungen** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **Persistenz**: Klicken Sie auf **Aktivieren**, um Systemprotokolle im nichtflüchtigen Datenspeicher zu speichern, damit die Protokolle beim Neustart des WAP-Geräts erhalten bleiben. Sie können bis zu 1000 Protokollnachrichten speichern. Wenn das Limit von 1000 erreicht ist, wird die älteste Protokollnachricht mit der neuesten Nachricht überschrieben. Löschen Sie den Inhalt dieses Felds, um Systemprotokolle im nichtflüchtigen Datenspeicher zu speichern. Protokolle im flüchtigen Datenspeicher werden beim Neustart des Systems gelöscht.
- **Schweregrad**: Wählen Sie den Schweregrad in der Dropdownliste aus (**Notfall, Warnung, Kritisch, Fehler, Warnung, Hinweis, Info oder Debug**), den ein Event mindestens haben muss, um im nichtflüchtigen Speicher abgelegt zu werden. Alle anderen Nachrichten werden im flüchtigen Speicher abgelegt.
- **Tiefe**: Die maximale Anzahl von Nachrichten (bis zu 1000), die im flüchtigen Datenspeicher gespeichert werden kann. Wenn die in diesem Feld konfigurierte Anzahl erreicht ist, wird das älteste Protokollereignis mit dem neuesten Protokollereignis überschrieben.

Schritt 3 Klicken Sie auf **Speichern**.

Remoteprotokollserver

Das Kernel-Protokoll ist eine umfassende Liste von (im Systemprotokoll angezeigten) Systemereignissen und Kernel-Nachrichten.

Die Kernel-Protokollnachrichten können nicht direkt über die Weboberfläche angezeigt werden. Sie müssen zunächst einen Remoteprotokollserver zum Empfangen und Erfassen von Protokollen einrichten. Anschließend können Sie das WAP-Gerät so konfigurieren, dass die Protokolle an den Remoteprotokollserver gesendet werden. Das WAP-Gerät unterstützt bis zu zwei Remoteprotokollserver.

Die Erfassung von Syslog-Nachrichten durch den Remoteprotokollserver ermöglicht Folgendes:

- Aggregation der Syslog-Nachrichten von mehreren APs.
- Speichern eines längeren Verlaufs der Nachrichten als auf einem einzelnen WAP-Gerät.
- Auslösen von skriptgesteuerten Verwaltungsvorgängen und Alarmmeldungen.

So geben Sie einen Host im Netzwerk an, der als Remoteprotokollserver dienen soll:

Schritt 1 Wählen Sie **Benachrichtigung > Protokolleinstellungen** aus.

Schritt 2 Konfigurieren Sie in der Tabelle „Remoteprotokollserver“ die folgenden Parameter:

- **IPv4-Adresse/IPv6-Adresse/Name des Servers**: Geben Sie die IPv4- bzw. IPv6-Adresse oder den Hostnamen des Remoteprotokollservers ein.

  Ein Hostname kann aus mindestens einem Label, d. h. einer Gruppe aus bis zu 63 alphanumerischen Zeichen bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Labels durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.

- **Aktivieren**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Remoteprotokollserver zu aktivieren. Definieren Sie anschließend den Protokollschweregrad und den UDP-Port.
- **Protokollschweregrad**: Wählen Sie die Schweregrade aus, die ein Ereignis aufweisen muss, damit es an den Remoteprotokollserver gesendet wird.
- **UDP-Port**: Geben Sie die Nummer des logischen Ports für den Syslog-Prozess auf dem Remotehost ein. Möglich sind Werte im Bereich von 1 bis 65535. Der Standardwert lautet 514.

  Es wird empfohlen, den Standardport zu verwenden. Wenn Sie den Protokollport neu konfigurieren, müssen Sie sicherstellen, dass die zu Syslog zugewiesene Portnummer verfügbar ist.

Schritt 3 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Wenn Sie einen Remoteprotokollserver aktivieren, können Sie auf **Speichern** klicken, um die Remoteprotokollierung zu aktivieren. Abhängig von der Konfiguration sendet das WAP-Gerät Kernel-Nachrichten in Echtzeit zur Anzeige auf dem Monitor des Remoteprotokollservers, an eine angegebene Kernel-Protokolldatei oder einen anderen Speicherort.

Wenn Sie einen Remoteprotokollserver deaktiviert haben, können Sie auf **Speichern** klicken, um die Remoteprotokollierung zu deaktivieren.

Systemprotokoll anzeigen

Auf der Seite „Systemprotokoll anzeigen“ wird eine Liste der Systemereignisse auf dem Gerät angezeigt. Das Protokoll wird beim Neustart gelöscht und kann von einem Administrator gelöscht werden. Es können bis zu 1000 Ereignisse angezeigt werden. Ältere Einträge werden nach Bedarf aus der Liste entfernt, um Platz für neue Ereignisse freizugeben.

Wählen Sie **Benachrichtigung > Systemprotokoll anzeigen** aus, um die Systemprotokolle anzuzeigen.

Die folgenden Informationen werden angezeigt:

- **Zeitstempel**: Der Zeitpunkt, zu dem das Ereignis aufgetreten ist.
- **Schweregrad**: Der Schweregrad des Ereignisses.
- **Dienst**: Der Dient, zu dem das Ereignis zugeordnet ist.
- **Beschreibung**: Eine Beschreibung des Ereignisses.

Sie können die Einstellungen für die Anzeige des Systemprotokolls filtern oder neu anordnen.

Sie können auf **Aktualisieren** klicken, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

Klicken Sie auf **Alles löschen**, um alle Einträge aus dem Protokoll zu löschen.

Klicken Sie auf **Herunterladen**, um alle Einträge aus dem Protokoll herunterzuladen.

E-Mail-Warnung / Mailserver / Nachrichtenkonfiguration

Die E-Mail-Warnungsfunktion unterstützt die Konfiguration von Mailservern und Nachrichtenschweregraden sowie von bis zu drei E-Mail-Adressen zum Senden dringender und nicht dringender Alarme. Mit der E-Mail-Warnungsfunktion können Sie beim Auftreten bestimmter Systemereignisse Nachrichten an die konfigurierten E-Mail-Adressen senden.

Tipp Verwenden Sie dabei nicht Ihre persönliche E-Mail-Adresse. Andernfalls müssten Sie unnötigerweise Ihre E-Mail-Anmeldeinformationen offenlegen. Verwenden Sie stattdessen ein separates E-Mail Konto. Beachten Sie auch, dass bei vielen E-Mail-Konten standardmäßig eine Kopie aller gesendeten Nachrichten gespeichert wird. Jeder Benutzer, der Zugriff auf dieses E-Mail-Konto hat, kann auf die gesendeten Nachrichten zugreifen. Vergewissern Sie sich, dass die E-Mail-Einstellungen mit Ihrer Datenschutzrichtlinie übereinstimmen.

So konfigurieren Sie das WAP-Gerät zum Senden von E-Mail-Alarmen:

Schritt 1 Wählen Sie **Benachrichtigung > E-Mail-Warnung** aus.

Schritt 2 Konfigurieren Sie im Bereich „Global Configuration“ die folgenden Parameter:

- **Administrativer Modus** — Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die E-Mail-Warnungen zu aktivieren.
- **Von-E-Mail-Adresse**: Geben Sie die E-Mail-Adresse ein, die als Absender der E-Mail angezeigt werden soll. Die Adresse ist eine aus 255 Zeichen bestehende Zeichenfolge, die nur druckbare Zeichen enthält. Standardmäßig ist keine Adresse konfiguriert.
- **Protokollierungsdauer**: Wählen Sie die Häufigkeit in Minuten aus, mit der geplante Nachrichten gesendet werden. Möglich sind Werte im Bereich von 30 bis 1440 Minuten. Die Standardeinstellung beträgt 30 Minuten.
- **Geplanter Nachrichtenschweregrad**: Wählen Sie den Schweregrad in der Dropdownliste aus (**Notfall, Warnung, Kritisch, Fehler** oder **Warnung**), den ein Event mindestens haben muss, um mit der in der Protokollierungsdauer angegebenen Häufigkeit an die konfigurierte E-Mail-Adresse verschickt zu werden. Der Standardschweregrad lautet **Warnung**.
- **Dringender Nachrichtenschweregrad**: Wählen Sie den Schweregrad in der Dropdownliste aus (**Notfall, Warnung, Kritisch, Fehler, Warnung, Hinweis, Info oder Debug**), den ein Event mindestens haben muss, um sofort an die konfigurierte E-Mail-Adresse verschickt zu werden. Der Standardschweregrad lautet **Warnung**.

Schritt 3 Konfigurieren Sie im Bereich „Mailserverkonfiguration" die folgenden Parameter:

- **IPv4-Adresse/Name des Servers**: Geben Sie die IP-Adresse oder den Hostnamen des ausgehenden SMTP-Servers ein. Bei der Serveradresse muss es sich um eine gültige IPv4-Adresse oder einen gültigen Hostnamen handeln. Geben Sie die IPv4-Adresse im Format xxx.xxx.xxx.xxx (192.0.2.10) ein.

  Ein Hostname kann aus mindestens einem Label, d. h. einer Gruppe aus bis zu 63 alphanumerischen Zeichen bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Labels durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.
- **Datenverschlüsselung**: Wählen Sie einen Sicherheitsmodus für ausgehende E-Mail-Warnungen in der Dropdownliste aus (**Offen oder TLSv1**). Mit dem sicheren TLSv1-Protokoll können Sie Abhören und Manipulationen während der Kommunikation über das öffentliche Netzwerk verhindern.
- **Port**: Geben Sie die SMTP-Portnummer ein, die für ausgehende E-Mails verwendet werden soll. Möglich ist eine gültige Portnummer im Bereich 0 bis 65535. Der Standardwert lautet 465.
- **Benutzername**: Geben Sie den Benutzernamen für das E-Mail-Konto ein, das zum Senden dieser E-Mails verwendet werden soll. Normalerweise (jedoch nicht immer) entspricht der Benutzername der vollständigen E-Mail-Adresse einschließlich der Domäne (beispielsweise Name@beispiel.com). Das angegebene Konto wird als E-Mail-Adresse des Absenders verwendet. Der Name kann aus 1 bis 64 alphanumerischen Zeichen bestehen.
- **Password**: Geben Sie das Kennwort für das E-Mail-Konto ein, das zum Senden dieser E-Mails verwendet werden soll. Das Kennwort kann 1 bis 64 Zeichen umfassen.

Schritt 4 Konfigurieren Sie E-Mail-Adressen und Betreffzeile im Bereich „Nachrichtenkonfiguration“:

- **An E-Mail-Adresse 1/2/3**: Geben Sie maximal drei Adressen ein, die E-Mail-Alarme empfangen sollen. Alle E-Mail-Adressen müssen gültig sein.

- **E-Mail-Betreff**: Geben Sie den Text für die Betreffzeile der E-Mail ein. Dabei kann es sich um eine alphanumerische Zeichenfolge aus maximal 255 Zeichen handeln.

Schritt 5 Klicken Sie auf **Speichern**.

Beispiele für E-Mail-Alarme

Im folgenden Beispiel wird gezeigt, wie Sie die Parameter für „Mailserverkonfiguration“ ausfüllen:

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommends the following settings: Data Encryption: TLSv1
SMTP Server: smtp.live.com
SMTP Port: 587
Username: Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password: Your Windows Live account password

Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password
```

Im folgenden Beispiel sehen Sie ein Beispielformat einer allgemeinen Protokoll-E-Mail gezeigt.

```
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          Priority > Process 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
```

User Accounts

Im WAP-Gerät ist standardmäßig ein Verwaltungsbenutzer konfiguriert.

- Benutzername: **cisco**
- Kennwort: **cisco**

Auf der Seite „Benutzerkonten“ können Sie bis zu vier zusätzliche Benutzer konfigurieren und Benutzerkennwörter ändern.

Hinzufügen eines Benutzers

Konfigurieren Sie die folgenden Einstellungen, um einen neuen Benutzer hinzuzufügen:

Schritt 1 Wählen Sie **Systemkonfiguration > Benutzerkonten** aus.

In der Benutzerkontentabelle werden die zurzeit konfigurierten Benutzer angezeigt. Der Benutzer „cisco“ ist im System mit Lese- und Schreibberechtigungen vorkonfiguriert.

Alle anderen Benutzer können Lesezugriff, nicht jedoch Lese- und Schreibzugriff erhalten.

Schritt 2 Klicken Sie auf □, um eine neue Zeile hinzuzufügen.

Schritt 3 Aktivieren Sie das Kontrollkästchen für den neuen Benutzer und geben Sie einen Namen für den Benutzer ein.

Schritt 4 Geben Sie ein neues Passwort mit 0 bis 127 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld „Neues Passwort bestätigen“ ein.

Unter „Kennwortsicherheitsmessung“ wird die Kennwortstärke angezeigt:

- **Rot**: Das Kennwort erfüllt nicht die Mindestsicherheitsanforderungen.
- **Orange**: Das Kennwort erfüllt die Mindestsicherheitsanforderungen, die Kennwortstärke ist jedoch niedrig.
- **Grün**: Kennwort ist stark.

Schritt 5 Klicken Sie auf **Speichern**.

Hinweis Um einen Benutzer zu löschen, wählen Sie den Benutzernamen aus, und klicken Sie auf **Löschen**. Um einen vorhandenen Benutzer zu bearbeiten, wählen Sie den Benutzernamen aus und klicken Sie auf **Bearbeiten**. Klicken Sie anschließend auf **Speichern**, um Ihre Konfigurationsänderungen zu speichern.

Ändern eines Benutzerkennworts

So ändern Sie ein Benutzerkennwort:

Schritt 1 Wählen Sie **Systemkonfiguration > Benutzerkonten** aus.

In der Benutzerkontentabelle werden die zurzeit konfigurierten Benutzer angezeigt. Der Benutzer cisco ist im System mit Lese- und Schreibberechtigungen vorkonfiguriert. Sie können das Kennwort für den Benutzer cisco ändern.

Schritt 2 Wählen Sie den zu konfigurierenden Benutzer aus, und klicken Sie auf **Bearbeiten**.

Schritt 3 Geben Sie ein **neues Passwort** mit 0 bis 127 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld **Neues Passwort bestätigen** ein.

Unter „Kennwortsicherheitsmessung“ wird die Kennwortstärke angezeigt:

- **Rot**: Das Kennwort erfüllt nicht die Mindestsicherheitsanforderungen.

- **Orange**: Das Kennwort erfüllt die Mindestsicherheitsanforderungen, die Kennwortstärke ist jedoch niedrig.
- **Grün**: Kennwort ist stark.

Schritt 4 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Wenn Sie das Kennwort ändern, müssen Sie sich erneut beim System anmelden.

Management

Auf der Seite „Systemeinstellungen“ können Sie Informationen konfigurieren, die das WAP-Gerät im Netzwerk identifizieren.

So konfigurieren Sie die Systemeinstellungen:

Schritt 1 Wählen Sie **Systemkonfiguration > Management** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **Hostname**: Geben Sie den Hostnamen für das WAP-Gerät ein. Standardmäßig ist dieser Name der vollqualifizierte Domänenname (FQDN) des Knotens. Der Standardhostname setzt sich aus dem Wort „wap“ und den sechs letzten Hexadezimalstellen der MAC-Adresse des WAP-Geräts zusammen. Der Hostname darf nur Buchstaben, Ziffern und Bindestriche enthalten. Der Hostname darf nicht mit einen Bindestrich beginnen oder enden. Sonstige Symbole, Satzzeichen oder Leerzeichen sind nicht zulässig. Der Hostname kann aus 1 bis 63 Zeichen bestehen.
- **Systemkontakt**: Geben Sie eine Kontaktperson für das WAP-Gerät ein. Der Systemkontakt kann aus 0 bis 255 Zeichen bestehen und Leerzeichen und Sonderzeichen enthalten.
- **Systemstandort**: Geben Sie den physischen Standort des WAP-Geräts ein. Der Systemstandort kann aus 0 bis 255 Zeichen bestehen und Leerzeichen und Sonderzeichen enthalten.

Schritt 3 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Sitzungs-/Verbindungseinstellungen/HTTP/HTTPS-Service konfigurieren

Auf der Seite „HTTP/HTTPS Service“ können Sie die webbasierten Management-Verbindungen aktivieren und konfigurieren. Wenn Sie HTTPS für sichere Verwaltungssitzungen verwenden, können Sie auf dieser Seite außerdem die erforderlichen SSL-Zertifikate verwalten.

So konfigurieren Sie HTTP- und HTTP-Dienste:

Schritt 1 Wählen Sie **Systemkonfiguration >Management** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter im Bereich „Globale Einstellungen“:

- **Maximale Sitzungen**: Geben Sie Anzahl der Websitzungen inklusive HTTP und HTTPS ein, die gleichzeitig verwendet werden können.

Wenn sich Benutzer beim Konfigurationsdienstprogramm für das WAP-Gerät anmelden, wird eine Sitzung erstellt. Diese Sitzung bleibt aktiv, bis sich die Benutzer abmelden oder das Sitzungs-Timeout eintritt. Möglich sind Werte im Bereich von 1 bis 10 Sitzungen. Die Standardeinstellung ist 5. Wenn die maximale Sitzungsanzahl erreicht ist, wird dem nächsten Benutzer, der sich beim Konfigurationsdienstprogramm anzumelden versucht, eine Fehlermeldung bezüglich des Sitzungslimits angezeigt.

- **Sitzungs-Timeout**: Geben Sie an, für wie viele Minuten ein inaktiver Benutzer angemeldet bleiben soll. Wenn das konfigurierte Timeout erreicht ist, werden die Benutzer automatisch abgemeldet. Möglich sind Werte im Bereich von 2 bis 60 Minuten. Die Standardeinstellung beträgt 10 Minuten.

Schritt 3 Konfigurieren Sie HTTP- und HTTP-Dienste:

- **HTTP-Dienst**: Aktivieren bzw. deaktivieren Sie den Zugriff per HTTP. Der HTTP-Zugriff ist standardmäßig deaktiviert. Wenn Sie diese Option deaktivieren, werden alle aktuellen über dieses Protokoll hergestellten Verbindungen getrennt.
  - **HTTP-Port**: Geben Sie die logische Portnummer für HTTP-Verbindungen ein (von 1025 bis 65535). Die Standard-Portnummer für HTTP-Verbindungen ist die allgemein bekannte IANA-Portnummer 80.
  - **HTTP an HTTPS umleiten**: Leitet Verwaltungszugriffsversuche über HTTP am HTTP-Port an den HTTPS-Port um. Dieses Feld ist nur verfügbar, wenn der HTTP-Zugriff deaktiviert ist.
- **HTTPS-Dienst**: Aktivieren bzw. deaktivieren Sie den sicheren Zugriff per HTTPS. Standardmäßig ist der HTTPS-Zugriff aktiviert. Wenn Sie diese Option deaktivieren, werden alle aktuellen über dieses Protokoll hergestellten Verbindungen getrennt.
  - **HTTPS-Port**: Geben Sie die logische Portnummer für HTTPS-Verbindungen ein (von 1025 bis 65535). Die Standard-Portnummer für HTTPS-Verbindungen ist die allgemein bekannte IANA-Portnummer 443.
- **Management-ACL-Modus**: In diesem Modus ist der Zugriff über das Web und über SNMP auf die angegebenen IP-Hosts beschränkt. Wenn diese Funktion deaktiviert ist, können alle Benutzer über einen beliebigen Netzwerkclient auf das Konfigurationsdienstprogramm zugreifen, indem sie den richtigen Benutzernamen und das richtige Kennwort für das WAP-Gerät angeben.

  Hinweis Überprüfen Sie die IP-Adressen bei der Eingabe. Wenn Sie eine IP-Adresse eingeben, die nicht Ihrem administrativen Computer entspricht, können Sie nicht mehr auf die Konfigurationsschnittstelle zugreifen. Es wird dringend empfohlen, für den administrativen Computer eine statische IP-Adresse zu vergeben, damit die Adresse immer gleich bleibt.

Schritt 4 Klicken Sie auf **Speichern**.

Status der SSL-Zertifikatdatei

Für die Verwendung von HTTPS-Diensten benötigt das WAP-Gerät ein gültiges SSL-Zertifikat. Sie können vom WAP-Gerät ein Zertifikat generieren lassen oder das Zertifikat aus dem Netzwerk oder von einem TFTP-Server herunterladen.

Klicken Sie im Bereich „SSL-Zertifikat generieren“ auf **SSL-Einstellungen** und dann auf **Generieren**, um das Zertifikat für das WAP-Gerät zu generieren. Dies sollte geschehen, nachdem das WAP-Gerät eine IP-Adresse bezogen hat, um sicherzustellen, dass der allgemeine Name für das Zertifikat mit der IP-Adresse des WAP-Geräts übereinstimmt. Beim Generieren eines neuen SSL-Zertifikats wird der sichere Webserver

neu gestartet. Die sichere Verbindung ist erst möglich, wenn das neue Zertifikat vom Browser akzeptiert wurde.

Im Bereich „Status der SSL-Zertifikatdatei“ wird das aktuelle Zertifikat auf dem WAP-Gerät angezeigt. Die folgenden Informationen werden angezeigt:

- Zertifikatdatei vorhanden
- Ablaufdatum der Zertifikatdatei
- Allgemeiner Name des Zertifikatausstellers

Wenn auf dem WAP-Gerät ein SSL-Zertifikat (mit der Erweiterung „.pem“) vorhanden ist, können Sie das Zertifikat als Backup auf den Computer herunterladen. Wählen Sie im Bereich **SSL-Zertifikat herunterladen (von Gerät auf PC)** die Option **HTTP/HTTPS** oder **TFTP** als Downloadmethode aus und klicken Sie auf **Übertragen**.

- Wenn Sie **HTTP/HTTPS** auswählen, werden Sie aufgefordert, den Download zu bestätigen und dann zu dem gewünschten Speicherort im Netzwerk zu navigieren.
- Wenn Sie TFTP auswählen, müssen Sie den gewünschten Dateinamen für die heruntergeladene Datei und die IPv4-Adresse des TFTP-Servers eingeben, von dem Sie die Datei herunterladen möchten.

Außerdem können Sie eine Zertifikatdatei (mit der Erweiterung ".pem") vom Computer in das WAP-Gerät hochladen. Wählen Sie im Bereich **SSL-Zertifikat herunterladen (von PC auf Gerät)** die Option **HTTP/HTTPS** oder **TFTP** als Uploadmethode aus und klicken Sie auf **Übertragen**.

- Wenn Sie HTTP/HTTPS auswählen, wechseln Sie zum Netzwerkspeicherort, wählen Sie die Datei aus, und klicken Sie auf **Übertragen**.
- Wenn Sie TFTP auswählen, geben Sie den Dateinamen und die IPv4-Adresse des TFTP-Servers ein, und klicken Sie auf **Übertragen**. Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? aszxaa, * sowie zwei oder mehr aufeinanderfolgende Punkte.

Nach dem erfolgreichen Upload wird eine Bestätigung angezeigt.

SNMP-/SNMPv2c-Einstellungen

Mit SNMP wird ein Standard für das Aufzeichnen, Speichern und gemeinsame Nutzen von Informationen zu Netzwerkgeräten definiert. SNMP erleichtert die Netzwerkverwaltung, Fehlerbehebung und Wartung. Das WAP-Gerät unterstützt SNMP und kann als ein mit SNMP verwaltetes Gerät dienen, das nahtlos in Netzwerkverwaltungssysteme integriert werden kann.

Aktivieren Sie auf der Seite mit den SNMP-/SNMPv2c-Einstellungen SNMP, und konfigurieren Sie die grundlegenden Protokolleinstellungen.

So konfigurieren Sie allgemeine SNMP-Einstellungen:

Schritt 1 Wählen Sie **Management > SNMP-Einstellungen**.

Schritt 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um SNMP zu aktivieren.

Schritt 3 Geben Sie den UDP-Port für den SNMP-Datenverkehr ein. Die Standardeinstellung ist 161. Sie können diese Funktion jedoch so konfigurieren, dass der Agent auf Anfragen von einem anderen Port reagiert. Gültig sind Werte im Bereich von 1025 bis 65535.

Schritt 4 Konfigurieren Sie im Bereich mit den SNMPv2c-Einstellungen die folgenden SNMPv2-Einstellungen:

- **Schreibgeschützte Community**: Geben Sie einen schreibgeschützten Community-Name für den SNMPv2-Zugriff ein. Gültig sind Werte mit 1 bis 256 alphanumerischen Zeichen und Sonderzeichen.

  Der Community-Name dient als einfache Authentifizierungsfunktion zum Beschränken der Geräte im Netzwerk, die beim SNMP-Agent Daten anfordern können. Der Name dient als Kennwort, und die Anfrage gilt als authentisch, wenn der Absender das Kennwort kennt.

- **Lesen/Schreiben-Community**: Geben Sie einen Namen für eine Lesen/Schreiben-Community ein, der für Anfragen nach SNMP-Sätze verwendet wird. Der gültige Bereich liegt zwischen 1 und 256 und kann alphanumerische Zeichen sowie Sonderzeichen enthalten. Das Festlegen eines Community-Namens ist mit dem Festlegen eines Kennworts vergleichbar. Es werden nur Anfragen von Computern akzeptiert, die sich mithilfe dieses Community-Namens identifizieren.

- **Management-Station**: Bestimmt, welche Stationen über SNMP auf das WAP-Gerät zugreifen können. Wählen Sie eine dieser Optionen:

  - **Alle**: Alle Stationen können über SNMP auf das WAP-Gerät zugreifen.
  - **Benutzerdefiniert**: Der Satz von benutzerdefinierten SNMP-Anforderungen, die zulässig sind.

- **NMS IPv4-Adresse/Name**: Geben Sie die IPv4-IP-Adresse, den DNS-Hostnamen oder das Subnetz des Netzwerkverwaltungssystems (NMS) ein.

  Ein DNS-Hostname kann aus einem oder mehreren Labels, d. h. einer Gruppe aus bis zu 63 alphanumerischen Zeichen, bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Labels durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.

  Wie bei Community-Namen bietet diese Einstellung eine gewisse Sicherheit für die SNMP-Einstellungen. Der SNMP-Agent akzeptiert nur Anfragen von den hier angegebenen IP-Adressen, Hostnamen oder Subnetzen.

  Zum Angeben eines Subnetzes geben Sie mindestens einen Adressbereich eines Subnetzes im Format Adresse/Maskenlänge ein, wobei die Adresse eine IP-Adresse und die Maskenlänge die Anzahl der Maskenbits ist. Beide Formate Adresse/Maske und Adresse/Maskenlänge werden unterstützt. Wenn Sie beispielsweise den Bereich „192.168.1.0/24“ eingeben, entspricht dies einem Subnetz mit der Adresse 192.168.1.0 und der Subnetzmaske 255.255.255.0.

- **NMS IPv6-Adresse/-Name**: Die IPv6-Adresse, der DNS-Hostname oder das Subnetz der Geräte, die GET- und SET-Anfragen an die verwalteten Geräte ausführen können. Geben Sie die IPv6-Adresse im Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) ein.

Hinweis Ein Hostname kann aus mindestens einem Label, d. h. einer Gruppe aus bis zu 63 alphanumerischen Zeichen bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Labels durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.

Schritt 5 Konfigurieren Sie im Bereich mit den SNMPv2c-Trap-Einstellungen die folgenden SNMPv2-Trap-Einstellungen:

- **Trap-Community**: Geben Sie einen globalen Community-String ein, der mit SNMP-Traps verbunden ist. Vom Gerät gesendete Traps stellen diese Zeichenfolge als Community-Namen bereit. Der gültige Bereich liegt zwischen 1 und 60 und kann alphanumerische Zeichen sowie Sonderzeichen enthalten.

- **Trap-Ziel-Tabelle**: Geben Sie eine Liste mit bis zu drei IP-Adressen oder Hostnamen ein, die SNMP-Traps empfangen sollen. Aktivieren Sie das Kästchen und wählen Sie einen Host-IP-Adressentyp (IPv4 oder IPv6), bevor Sie den Hostnamen/IP-Adresse hinzufügen.

Ein Beispiel für einen DNS-Hostnamen ist snmptraps.foo.com. Da die SNMP-Traps nach dem Zufallsprinzip vom SNMP-Agent gesendet werden, müssen Sie angeben, wohin genau die Traps gesendet werden sollen. Möglich sind maximal drei DNS-Hostnamen. Stellen Sie sicher, dass Sie das Kontrollkästchen **Aktiviert** auswählen und den geeigneten Host-IP-Adressentyp auswählen.

Schritt 6 Klicken Sie auf **Speichern**.

SNMPv3-Ansichten

Eine SNMP-MIB-Ansicht ist eine Gruppe von Ansichtsunterstrukturen in der MIB-Hierarchie. Eine Ansichtsunterstruktur wird identifiziert durch die Kombination aus einem OID-Unterstrukturwert (Object Identifier, Objekt-ID) mit einem Bitfolgen-Maskenwert. Jede MIB-Ansicht wird durch zwei Gruppen von Ansichtsunterstrukturen definiert, die in der MIB-Ansicht ein- oder ausgeschlossen sind. Sie können MIB-Ansichten erstellen, um den OID-Bereich zu steuern, auf den SNMPv3-Benutzer zugreifen können.

Der WAP Gerät unterstützt maximal 16 Ansichten.

Dieser Abschnitt fasst die wichtigsten Richtlinien für die Konfiguration der SNMPv3-Ansicht zusammen. Lesen Sie alle Hinweise, bevor Sie fortfahren.

Hinweis Im System wird standardmäßig die MIB-Ansicht „all“ erstellt. Diese Ansicht enthält alle vom System unterstützten Verwaltungsobjekte.

Hinweis Standardmäßig werden im WAP-Gerät die SNMPv3-Ansichten „view-all“ und „view-none“ erstellt. Diese Ansichten können Sie nicht löschen oder ändern.

Gehen Sie wie folgt vor, um eine SNMP-Ansicht hinzuzufügen und zu konfigurieren:

Schritt 1 Wählen Sie **Management** > **SNMPv3**

Schritt 2 Klicken Sie auf □, um eine neue Zeile in der Tabelle **SNMPv3-Ansichten** zu erstellen, oder aktivieren Sie das Kontrollkästchen vorhandener Ansichten. Klicken Sie dann auf **Bearbeiten**.

- **Ansichtsname**: Geben Sie einen Namen ein, um die MIB-Ansicht zu bezeichnen. Ansichtsnamen können bis zu 32 alphanumerische Zeichen enthalten.
- **Typ**: Wählen Sie aus, ob die Ansichtsunterstruktur oder die Gruppe der Unterstrukturen in der MIB-Ansicht ein- oder ausgeschlossen sein soll.
- **OID**: Geben Sie eine OID-Zeichenfolge für die Unterstruktur ein, die in der Ansicht ein- oder ausgeschlossen sein soll. Die Systemunterstruktur beispielsweise geben Sie mit der OID-Zeichenfolge .1.3.6.1.2.1.1 an.
- **Maske**: Geben Sie eine OID-Maske ein. Die Maske besteht aus 47 Zeichen. Das Format der OID-Maske lautet xx.xx.xx (.)... oder xx:xx:xx.... (:) und besteht aus 16 Oktetten. Jedes Oktett besteht aus zwei Hexadezimalzeichen, die durch einen Punkt (.) oder einen Doppelpunkt (:) getrennt sind. In diesem Feld sind nur Hexadezimalzeichen zulässig. Der Wert für die OID-Maske FA.80 beispielsweise lautet 11111010.10000000.

Mit einer Gruppenmaske können Sie eine Gruppe von Ansichtsunterstrukturen definieren. Die Gruppenmaske gibt an, welche Unter-IDs der zugeordneten OID-Gruppenzeichenfolge für die Definition der Gruppe von Bedeutung sind. Mithilfe einer Gruppe von Ansichtsunterstrukturen können Sie den Zugriff auf eine Zeile in einer Tabelle effizient steuern.

Schritt 3 Klicken Sie auf **Speichern**.

Hinweis Zum Entfernen einer Ansicht wählen Sie die Ansicht in der Liste aus und klicken auf **Löschen**.

SNMPv3-Gruppen

Mithilfe der SNMPv3-Gruppen können Sie Benutzer nach unterschiedlichen Autorisierungen und Zugriffsberechtigungen gruppieren. Jede Gruppe ist einer von drei Sicherheitsstufen zugeordnet:

- noAuthNoPriv
- authNoPriv
- authPriv

Den Zugriff auf MIBs (Managementinformationsbasen, Management Information Bases) für die einzelnen Gruppen steuern Sie, indem Sie einer Gruppe getrennte Ansichten für Lese- oder Schreibzugriff zuordnen.

Das WAP-Gerät verfügt standardmäßig über zwei Gruppen:

- **RO**: Eine nur über Lesezugriff verfügende Gruppe mit Authentifizierung und Datenverschlüsselung. Benutzer in dieser Gruppe verwenden den SHA-Schlüssel oder ein Kennwort für die Authentifizierung und einen DES- oder AES128-Schlüssel für die Verschlüsselung. Die SHA-, DES- und AES128-Schlüssel oder -Kennwörter müssen definiert werden. Standardmäßig verfügen Benutzer in dieser Gruppe über Lesezugriff auf die MIB-Standardansicht „all“.
- **RW**: Eine über Lese- und Schreibzugriff verfügende Gruppe mit Authentifizierung und Datenverschlüsselung. Benutzer in dieser Gruppe verwenden den SHA-Schlüssel oder ein Kennwort für die Authentifizierung und einen DES-Schlüssel oder AES128 für die Verschlüsselung. Die SHA-, DES- und AES128-Schlüssel oder -Kennwörter müssen definiert werden. Standardmäßig verfügen Benutzer in dieser Gruppe über Lese- und Schreibzugriff auf die MIB-Standardansicht „all“.

Hinweis Die Standardgruppen „RO“ und „RW“ können nicht gelöscht werden. Das WAP-Gerät unterstützt maximal acht Gruppen.

Gehen Sie wie folgt vor, um die SNMP-Gruppe hinzuzufügen und zu konfigurieren:

Schritt 1 Wählen Sie **Management > SNMPv3**.

Schritt 2 Klicken Sie auf □, um der Tabelle mit den SNMPv3-Gruppen eine neue Zeile hinzuzufügen.

Schritt 3 Aktivieren Sie das Kontrollkästchen für die neue Gruppe und konfigurieren Sie die folgenden Parameter:

- **Gruppenname**: Geben Sie den Namen der Gruppe ein. Die Standardgruppennamen lauten „RO“ und „RW“. Gruppennamen können bis zu 32 alphanumerische Zeichen enthalten.

- **Sicherheitsstufe**: Wählen Sie aus den folgenden Optionen eine Sicherheitsstufe für die Gruppe:
  - **noAuthNoPriv**: Keine Authentifizierung und keine Datenverschlüsselung (keine Sicherheit).
  - **authNoPriv**: Authentifizierung, jedoch keine Datenverschlüsselung. Benutzer dieser Sicherheitsstufe senden SNMP-Nachrichten mit einem SHA-Schlüssel bzw. -Kennwort für die Authentifizierung, jedoch keinen DES-Schlüssel bzw. keinen AES128-Schlüssel für die Verschlüsselung.
  - **authPriv**: Authentifizierung und Datenverschlüsselung. Benutzer dieser Sicherheitsstufe senden den SHA-Schlüssel oder das Kennwort für die Authentifizierung und einen DES- oder AES128-Schlüssel für die Verschlüsselung. Für Gruppen, bei denen Authentifizierung und/oder Verschlüsselung erforderlich ist, müssen Sie die SHA-, DES- und AES128-Schlüssel bzw. -Kennwörter auf der Seite „SNMP Users“ definieren.
- **Schreibansichten**: Wählen Sie aus einer der folgenden Optionen den Schreibzugriff für die MIBs der Gruppe:
  - **view-all:**: Die Gruppe kann MIBs erstellen, ändern und löschen.
  - **view-none:**: Die Gruppe kann MIBs nicht erstellen, ändern oder löschen.
- **Leseansichten**: Wählen Sie aus einer der folgenden Optionen den Lesezugriff für die MIBs der Gruppe:
  - **view-all:**: Die Gruppe kann alle MIBs anzeigen und lesen.
  - **view-none:**: Die Gruppe kann MIBs nicht anzeigen oder lesen.

Schritt 4 Klicken Sie auf **Speichern**, um die Gruppe zur Liste der SNMPv3-Gruppen hinzuzufügen.

Hinweis Zum Löschen einer Gruppe wählen Sie die Gruppe in der Liste aus und klicken auf **Löschen**. Zum Bearbeiten einer Gruppe wählen Sie die Gruppe in der Liste aus und klicken auf **Bearbeiten**.

SNMPv3-Benutzer

Auf der Seite „SNMP Users“ können Sie Benutzer definieren, den einzelnen Benutzern Sicherheitsstufen zuordnen und Sicherheitsschlüssel pro Benutzer konfigurieren.

Jeder Benutzer wird (über die vordefinierten oder benutzerdefinierten Gruppen) einer SNMPv3-Gruppe zugeordnet und optional für Authentifizierung und Verschlüsselung konfiguriert. Für die Authentifizierung wird nur der Typ SHA unterstützt. Für die Verschlüsselung werden nur die Typen DES und AES128 unterstützt. Es gibt auf dem WAP-Gerät keine SNMPv3-Standardbenutzer. Sie können bis zu acht Benutzer hinzufügen.

Gehen Sie wie folgt vor, um SNMP-Benutzer hinzuzufügen:

Schritt 1 Wählen Sie **Management > SNMPv3**.

Schritt 2 Klicken Sie auf □, um der Tabelle mit den SNMPv3-Benutzern eine neue Zeile hinzuzufügen.

Schritt 3 Aktivieren Sie das Kästchen in der neuen Zeile und konfigurieren Sie die folgenden Parameter:

- **Benutzername**: Geben Sie einen Namen ein, der den SNMPv3-Benutzer identifiziert. Benutzernamen können bis zu 32 alphanumerische Zeichen enthalten.

- **Gruppe**: Geben Sie den Namen der Gruppe ein, der der Benutzer zugeordnet ist. Die Standardgruppen lauten RW und RO. Auf der Seite „SNMP Groups“ können Sie zusätzliche Gruppen definieren.
- **Authentifizierungstyp**: Wählen Sie aus den folgenden Optionen den Authentifizierungstyp für die SNMPv3-Anfragen des Benutzers:
  - **SHA**: Für SNMP-Anfragen des Benutzers ist SHA-Authentifizierung erforderlich.
  - **Kein** : Für SNMPv3-Anfragen des Benutzers ist keine Authentifizierung erforderlich.
- **Authentifizierungskennwort**: Wenn Sie den Authentifizierungstyp SHA angegeben haben, geben Sie die Passphrase ein, mit der der SNMP-Agent vom Benutzer gesendete Anfragen authentifizieren kann. Die Passphrase muss zwischen 8 und 32 Zeichen lang sein.
- **Verschlüsselungstyp**: Wählen Sie aus den folgenden Optionen den Verschlüsselungs-/Datenschutztyp aus, der auf SNMP-Anfragen des Benutzers angewendet werden soll:
  - **DES**: Verwendet für SNMPv3-Anfragen des Benutzers die DES-Verschlüsselung.
  - **AES128**: Verwendet für SNMPv3-Anfragen des Benutzers die AES128-Verschlüsselung.
  - **Kein**: Für SNMPv3-Anfragen des Benutzers ist kein Datenschutz erforderlich.
- **Verschlüsselungskennwort**: Wenn Sie als Verschlüsselungstyp DES oder AES128 angegeben haben, geben Sie die Passphrase ein, die zum Verschlüsseln der SNMP-Anfragen verwendet werden soll. Die Passphrase muss zwischen 8 und 32 Zeichen lang sein.

Schritt 4 Klicken Sie auf **Speichern**. Der Benutzer wird der Liste „SNMPv3-Benutzer“ hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Zum Entfernen eines Benutzers wählen Sie den Benutzer in der Liste aus, und klicken Sie auf **Löschen**. Zum Bearbeiten eines Benutzers wählen Sie den Benutzer in der Liste aus und klicken auf **Bearbeiten**.

SNMPv3-Ziele

Die SNMPv3-Ziele senden SNMP-Benachrichtigungen als Inform-Nachrichten an den SNMP-Manager. Für SNMPv3-Ziele werden nur die Inform-Nachrichten gesendet, und keine Traps. Für die SNMP-Versionen 1 und 2 werden Traps gesendet. Jedes Ziel wird durch eine IP-Zieladresse, einen UDP-Port und einen SNMPv3-Benutzernamen definiert.

Hinweis Sie müssen die SNMPv3-Benutzer-Konfiguration abschließen (siehe Seite SNMPv3-Benutzer), bevor Sie die SNMPv3-Ziele konfigurieren.

Das WAP Gerät unterstützt maximal acht Ziele.

Gehen Sie wie folgt vor, um SNMP-Ziele hinzuzufügen:

Schritt 1 Wählen Sie **Management> SNMPv3-Ziele**.

Schritt 2 Klicken Sie auf □, um der Tabelle eine neue Zeile hinzuzufügen.

Schritt 3 Aktivieren Sie das Kästchen in der neuen Zeile und konfigurieren Sie die folgenden Parameter:

- **IP-Adresse**: Geben Sie die IPv4- oder IPv6-Adresse des Remote-SNMP-Managers ein, der das Ziel empfangen soll.
- **UDP-Port**: Geben Sie den UDP-Port ein, der zum Senden von SNMPv3-Zielen verwendet werden soll.
- **Benutzer**: Geben Sie den Namen des SNMP-Benutzers ein, den Sie dem Ziel zuordnen möchten. Informationen zur Konfiguration von SNMP-Benutzern finden Sie auf der Seite SNMPv3-Benutzer, auf Seite 32.

Schritt 4 Klicken Sie auf **Speichern**. Der Benutzer wird der Liste „SNMPv3-Ziele“ hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Zum Entfernen eines SNMP-Ziels wählen Sie den Benutzer in der Liste aus und klicken auf **Löschen**. Zum Bearbeiten eines SNMP-Ziels wählen Sie den Benutzer in der Liste aus und klicken auf **Bearbeiten**.

Security

In diesem Abschnitt wird beschrieben, wie Sie die Sicherheitseinstellungen auf dem WAP-Gerät konfigurieren.

RADIUS-Server

Für verschiedene Funktionen ist eine Kommunikation mit einem RADIUS-Authentifizierungsserver erforderlich. Wenn Sie beispielsweise VAPs (Virtual Access Points) auf dem AP konfigurieren, können Sie Sicherheitsmethoden konfigurieren, um den WLAN-Zugriff zu kontrollieren. Weitere Informationen finden Sie unter Funk. Die „WPA Enterprise“-Sicherheitsmethode verwendet einen externen RADIUS-Server, um Clients zu authentifizieren. Die Funktion zum Filtern von MAC-Adressen, bei der Client-Zugriff auf eine Liste beschränkt wird, kann auch so konfiguriert werden, das für die Zugriffskontrolle ein RADIUS-Server verwendet wird. Die Funktion „Captive Portal“ verwendet ebenfalls RADIUS zur Authentifizierung von Clients.

Sie können die Seite „Radius-Server“ verwenden, um die RADIUS-Server zu konfigurieren, die von diesen Funktionen verwendet werden. Sie können bis zu vier global verfügbare IPv4- oder IPv6-RADIUS-Server verwenden. Sie müssen jedoch auswählen, ob der RADIUS-Client hinsichtlich der globalen Server im IPv4- oder IPv6-Modus ausgeführt wird. Einer der Server tritt immer als der primäre aus, während die anderen als Backup-Server fungieren.

Hinweis Neben der Verwendung der globalen RADIUS-Server, können Sie auch jeden VAP so konfigurieren, dass eine spezielle Reihe von RADIUS-Servern verwendet wird. Siehe Netzwerke.

Konfigurieren globaler RADIUS-Server

Schritt 1 Wählen Sie **Sicherheit** > **RADIUS-Server** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter:

- **Server-IP-Adresstyp**: Wählen Sie die IP-Version aus, die der RADIUS-Server verwendet. Sie können zwischen den Adresstypen umschalten, um globale RADIUS-Adresseinstellungen für IPv4 und IPv6 zu konfigurieren. Das WAP-Gerät verbindet sich jedoch nur mit RADIUS-Servern mit dem in diesem Feld ausgewählten Adresstyp.
- **Server-IP-Adresse 1 oder Server-IPv6-Adresse 1**: Geben Sie die Adresse des primären globalen RADIUS-Servers ein. Wenn sich der erste WLAN-Client gegenüber dem WAP-Gerät zu authentifizieren versucht, sendet das Gerät eine Authentifizierungsanfrage an den primären Server. Wenn der primäre Server auf die Authentifizierungsanfrage antwortet, verwendet das WAP-Gerät diesen RADIUS-Server weiterhin als primären Server und Authentifizierungsanfragen werden an die festgelegte Adresse gesendet.
- **Server-IP-Adresse 2 oder Server-IPv6-Adresse 2**: Geben Sie die Adressen für die IPv4- oder IPv6-RADIUS-Backupserver ein. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird der konfigurierte Backup-Server ausprobiert.
- **Schlüssel 1**: Geben Sie den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät für die Authentifizierung beim primären RADIUS-Server verwendet. Sie können zwischen 1 und 64 alphanumerische Zeichen sowie Sonderzeichen verwenden. Beim Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden, und der Schlüssel muss dem auf dem RADIUS-Server konfigurierten Schlüssel entsprechen. Der eingegebene Text wird mit Sternchen maskiert.
- **Schlüssel 2**: Geben Sie den RADIUS-Schlüssel für die konfigurierten RADIUS-Backupserver ein. Der Server mit der Server-IP (IPv6)-Adresse 2 verwendet Schlüssel 2.
- **RADIUS-Abrechnung aktivieren**: Aktiviert Nachverfolgung und Messung der Ressourcen, die ein bestimmter Benutzer verbraucht hat, wie beispielsweise Systemzeit, die Menge der übertragenen und empfangenen Daten und so weiter. Wenn Sie die RADIUS-Prüfung aktivieren, wird sie für den primären RADIUS-Server und alle Backup-Server aktiviert.

Schritt 3 Klicken Sie auf **Speichern**.

802.1x Supplicant

Die IEEE 802.1X-Authentifizierung ermöglicht es dem WAP-Gerät, Zugriff auf ein gesichertes kabelgebundenes Netzwerk zu erhalten. Sie können das WAP-Gerät als 802.1X-Supplicant (Client) im kabelgebundenen Netzwerk aktivieren. Sie können einen Benutzernamen und ein Passwort mit dem MD5-Algorithmus verschlüsseln und konfigurieren, mit denen sich das WAP-Gerät per 802.1X authentifizieren kann.

In Netzwerken mit IEEE-802.1X-Port-basierter Netzwerkzugriffskontrolle erhalten Supplicant erst dann Zugriff auf das Netzwerk, wenn der 802.1X-Authenticator den Zugriff erlaubt. Wenn Ihr Netzwerk 802.1X verwendet, müssen Sie 802.1X-Authentifizierungsinformationen auf dem WAP-Gerät konfigurieren, damit es diese dem Authenticator bereitstellen kann.

Führen Sie die folgenden Schritte aus, um einen 802.1X-Supplicant zu konfigurieren:

Schritt 1 Klicken Sie auf **Sicherheit > 802.1X-Supplicant**.

Schritt 2 Aktivieren Sie das Kontrollkästchen **Aktivieren** im Bereich „802.1X-Supplicant“, um den administrativen Modus zu aktivieren.

Schritt 3 Konfigurieren Sie den Betriebsstatus und die Basiseinstellungen für 802.1x:

- **EAP-Methode**: Wählen Sie den Algorithmus für die Verschlüsselung von Authentifizierungsbenutzernamen und -Passwörtern aus. Folgende Optionen sind verfügbar:
  - **MD5**: Eine in RFC 3748 definierte Hash-Funktion, die grundlegende Sicherheit bereitstellt.
  - **PEAP**: Protected Extensible Authentication Protocol, das ein höheres Maß an Sicherheit bereitstellt als MD5, indem dieses innerhalb eines TLS-Tunnels eingekapselt wird.
  - **TLS**: Transport Layer Security, wie in RFC 5216 definiert. Ein offener Standard der ein hohes Maß an Sicherheit bietet.
- **Benutzername**: Geben Sie den Benutzernamen ein.
- **Passwort**: Geben Sie das Passwort ein.

Schritt 4 Im Bereich „Zertifikatsdatei-Upload“ können Sie eine Zertifikatsdatei auf das WAP-Gerät hochladen:

a) Wählen Sie entweder **HTTP** oder **TFTP** als Übertragungsmethode aus.
b) Wenn Sie HTTP ausgewählt haben, klicken Sie auf **Durchsuchen**, um die Datei auszuwählen Unter Sitzungs-/Verbindungseinstellungen/HTTP/HTTPS-Service konfigurieren finden Sie weitere Informationen zum Konfigurieren der HTTP-Servereinstellungen.
c) Wenn Sie **TFTP** ausgewählt haben, geben Sie den Dateinamen und die IPv4-Adresse des TFTP-Servers ein.
d) Klicken Sie auf **Hochladen**. Es wird ein Bestätigungsfenster angezeigt, gefolgt von einem Fortschrittsbalken, der den Status des Uploads angibt.

Schritt 5 Klicken Sie auf **Speichern**.

Rogue-AP-Erkennung

Ein Rogue-AP ist ein Access Point, der ohne explizite Autorisierung eines Systemadministrators in einem sicheren Netzwerk installiert wurde. Rogue-Access Points stellen ein Sicherheitsrisiko dar, da beliebige Personen mit Zugang zum Standort unwissentlich oder in böswilliger Absicht ein kostengünstiges WAP-Gerät installieren können, das unbefugten Personen den Zugriff auf das Netzwerk ermöglichen kann.

Das WAP-Gerät führt einen RF-Scan für alle Kanäle aus, um alle APs in der Nähe des Netzwerks zu erkennen. Erkannte Rogue-APs werden auf der Seite "Rogue AP Detection" angezeigt. Wenn ein als Rogue-AP aufgeführter AP legitim ist, können Sie diesen zur Liste der bekannten APs hinzufügen.

Hinweis "Detected Rogue AP List" und "Trusted AP List" enthalten Informationen. Der AP hat keine Kontrolle über die APs in der Liste und kann auf die beim RF-Scan erkannten APs keine Sicherheitsrichtlinien anwenden.

Wenn die Rogue-AP-Erkennung aktiviert ist, wechselt das Funkmodul regelmäßig den Betriebskanal, um andere Kanäle im gleichen Band zu suchen.

Anzeigen der Rogue-AP-Liste

Damit die Rogue-AP-Erkennung funktioniert, muss das drahtlose Funknetz aktiviert sein. Sie müssen zunächst die Funkschnittstelle aktivieren, bevor Sie die Rogue-AP-Erkennung für die Funkschnittstelle aktivieren.

So aktivieren Sie das Funkmodul zum Erfassen von Informationen zu Rogue-APs:

Schritt 1 Wählen Sie **Sicherheit > Rogue-AP-Erkennung** aus.

Schritt 2 Wählen Sie die Option **Aktivieren** aus, um die AP-Erkennung für Funkmodul 1 und Funkmodul 2 zu aktivieren.

Schritt 3 Klicken Sie auf **Speichern**.

In der Liste der erkannten Rogue-APs werden alle erkannten Rogue-APs angezeigt. In der Liste der vertrauenswürdigen APs werden alle vertrauenswürdigen APs angezeigt. Die folgenden Einstellungen werden für jede der Listen mit Rogue-APs angezeigt:

- **MAC-Adresse**: Die MAC-Adresse des Rogue-APs.
- **Beacon-Intervall**: Zeigt das vom Rogue-AP verwendete Beacon-Intervall an. Beacon-Frames werden in regelmäßigen Intervallen von einem AP gesendet, um das Vorhandensein des WLANs anzukündigen. Das Standardverhalten sieht vor, dass alle 100 Millisekunden ein Beacon-Frame gesendet wird (oder zehn pro Sekunde). Das Beacon-Intervall legen Sie auf der Seite Funk, auf Seite 41 fest.
- **Typ**: Der Typ des Geräts: Folgende Optionen sind verfügbar:
  - **AP**: Ein Rogue-AP-Gerät, das das IEEE 802.11 Wireless Networking Framework im Infrastrukturmodus verwendet.
  - **Ad hoc**: Eine Rogue-Station, die im Ad-hoc-Modus ausgeführt wird. Beim Ad-hoc-Modus handelt es sich um ein IEEE 802.11 Wireless Networking Framework, das auch als Peer-to-Peer-Modus oder IBSS (Independent Basic Service Set) bezeichnet wird.
- **SSID**: Die SSID (Service Set Identifier) für das WAP-Gerät.
- **Datenschutz**: Gibt an, ob Sicherheit für das Rogue-Gerät festgelegt ist. Folgende Optionen sind verfügbar:
  - **Aus**: Der Sicherheitsmodus ist deaktiviert (keine Sicherheit).
  - **Ein**: Der Sicherheitsmodus ist aktiviert.
- **WPA**: Gibt an, ob WPA-Sicherheit für den Rogue-AP aktiviert oder deaktiviert ist.
- **Band**: Der auf dem Rogue-AP verwendete IEEE 802.11-Modus, z. B. IEEE 802.11a, IEEE 802.11b oder IEEE 802.11g.

  Die angezeigte Zahl gibt den Modus an:
  - „2,4“ steht für den Modus IEEE 802.11b, 802.11g oder 802.11n (oder eine Kombination dieser Modi).
  - „5“ steht für den Modus IEEE 802.11a oder 802.11n (oder beide Modi).
- **Kanal**: Der Kanal, über den der Rogue-AP zurzeit sendet.
- **Rate**: Die Rate (in Megabit pro Sekunde), mit der der Rogue-AP zurzeit sendet. Bei der aktuellen Rate handelt es sich immer um eine der unter den unterstützten Raten angezeigten Raten.
- **Signal**: Die Stärke des von dem Rogue-AP ausgehenden Funksignals. Wenn Sie den Mauszeiger über die Balken bewegen, wird eine Zahl angezeigt, die die Stärke in Dezibel (dB) angibt.
- **Beacons**: Die Gesamtanzahl der Beacons, die seit der Erkennung des Rogue-APs von diesem empfangen wurden.

- **Letztes Beacon**: Datum und Uhrzeit des Zeitpunkts, zu dem der letzte Beacon vom Rogue-AP empfangen wurde.
- **Raten**: Unterstützte Ratensätze und Basisratensätze (angekündigte Ratensätze) für den Rogue-AP. Raten werden in Megabit pro Sekunde (MBit/s) angezeigt. Es werden alle unterstützten Raten aufgeführt, wobei die Basisraten fett angezeigt werden. Die Ratensätze konfigurieren Sie auf der Seite Funk, auf Seite 41.

Schritt 4 Aktivieren Sie die AP-Liste, und klicken Sie dann auf **In Liste vertrauenswürdiger APs verschieben**, um den AP in die **Liste vertrauenswürdiger APs** zu verschieben. Wenn der AP in der **Liste vertrauenswürdiger APs** vorhanden ist, klicken Sie auf die **Liste erkannter Rogue-APs**, um den AP in die **Liste erkannter Rogue-APs** zu verschieben.

Schritt 5 Klicken Sie auf **Aktualisieren**, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

Speichern der Liste vertrauenswürdiger APs

So erstellen Sie eine "Trusted AP List" und speichern diese in einer Datei:

Schritt 1 Wählen Sie **Sicherheit** aus, und klicken Sie auf **Rogue-AP-Liste anzeigen ...** im Bereich **Rogue-AP-Erkennung**. Die Seite **Rogue-AP-Erkennung** wird angezeigt.

Schritt 2 Klicken Sie in der **Liste erkannter Rogue-APs** neben den Ihnen bekannten APs auf **In Liste vertrauenswürdiger APs verschieben**. Die vertrauenswürdigen APs werden in die Liste vertrauenswürdiger APs verschoben.

Schritt 3 Klicken Sie im Bereich „Liste vertrauenswürdiger APs herunterladen/sichern“ auf **Sichern (AP auf PC)**.

Schritt 4 Klicken Sie auf **Speichern**.

Die Liste enthält die MAC-Adressen aller APs, die zu "Known AP List" hinzugefügt wurden. Der Dateiname lautet standardmäßig „Rogue2.cfg“. Sie können die Datei in einem Texteditor oder Webbrowser öffnen und den Inhalt anzeigen.

Importieren einer Liste vertrauenswürdiger APs

Sie können eine Liste mit bekannten APs aus einer gespeicherten Liste importieren. Die Liste kann von einem anderen AP abgerufen oder aus einer Textdatei erstellt werden. Wenn die MAC-Adresse eines APs in "Trusted AP List" enthalten ist, wird der AP nicht als Rogue-AP erkannt.

So importieren Sie eine AP-Liste aus einer Datei:

Schritt 1 Wählen Sie **Sicherheit > Rogue-AP-Erkennung** aus.

Schritt 2 Klicken Sie im Bereich „Liste vertrauenswürdiger APs herunterladen/sichern“ auf **Herunterladen (PC auf AP)**.

Schritt 3 Klicken Sie im Feld Quelldateiname auf **Durchsuchen**, um die Datei für den Import auszuwählen.

Bei der importierten Datei muss es sich um eine reine Textdatei mit der Erweiterung „.txt“ oder „.cfg“ handeln. Bei den Einträgen in der Datei handelt es sich um MAC-Adressen im Hexadezimalformat mit durch Doppelpunkte getrennten Oktetten, beispielsweise 00:11:22:33:44:55. Sie müssen die Einträge durch ein einzelnes Leerzeichen trennen. Damit die Datei vom AP akzeptiert wird, darf sie nur MAC-Adressen enthalten.

Schritt 4 Wählen Sie im Feld „Ziel für die Dateiverwaltung“ aus, ob die vorhandene Liste der vertrauenswürdigen APs ersetzt werden soll oder ob die Einträge in der importierten Datei zur Liste der vertrauenswürdigen APs hinzugefügt werden sollen. Folgende Optionen sind verfügbar:

- **Ersetzen**: Die Liste wird importiert, und der Inhalt der Liste der bekannten APs wird ersetzt.
- **Zusammenführen**: Die Liste wird importiert, und die APs aus der importierten Datei werden zur aktuellen Liste der bekannten APs hinzugefügt.

Schritt 5 Klicken Sie auf **Speichern**.

Nach Abschluss des Imports wird der Bildschirm aktualisiert, und die MAC-Adressen der APs aus der importierten Datei werden in "Known AP List" angezeigt.

Kennwortkomplexität konfigurieren

Auf der Seite „Kennwortkomplexität“ können Sie die Komplexitätsanforderungen für die Kennwörter festlegen, mit denen auf das Konfigurationshilfsprogramm zugegriffen wird. Durch komplexe Passwörter wird die Sicherheit erhöht.

Führen Sie die folgenden Schritte aus, um die Anforderungen für die Kennwortkomplexität zu konfigurieren:

Schritt 1 Wählen Sie **Sicherheit > Kennwortkomplexität konfigurieren** aus.

Schritt 2 Klicken Sie auf **Aktivieren**, um die Kennwortkomplexität zu aktivieren.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **Mindestanzahl der Passwort-Zeichenklassen**: Geben Sie die Mindestanzahl der Zeichenklassen ein, die im Passwort vertreten sein müssen. Die vier möglichen Zeichenklassen sind Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen auf einer Standardtastatur.
- **Passwort unterscheidet sich vom aktuellen**: Mit dieser Option müssen Benutzer ein anderes Passwort eingeben, wenn ihr aktuelles abläuft. Wenn diese Funktion deaktiviert ist, können die Benutzer dasselbe Passwort eingeben, wenn es abläuft.
- **Maximale Passwortlänge**: Die maximale Zeichenanzahl des Passworts liegt zwischen 64 und 127. Die Standardeinstellung ist 64.
- **Minimale Passwortlänge**: Die minimale Zeichenanzahl des Passworts liegt zwischen 0 und 32. Die Standardeinstellung ist 8.
- **Passwortablauf-Support**: Mit dieser Option laufen Passwörter nach einer festgelegten Zeit ab.
- **Passwortablaufzeit**: Geben Sie die Anzahl der Tage ein, nach der ein neu erstelltes Passwort abläuft (1 bis 365). Die Standardeinstellung ist 180 Tage.

Schritt 4 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Nach Ablauf der **Passwortablaufzeit** werden Sie aufgefordert, die Seite Kennwort ändern zu besuchen.

WPA-PSK-Komplexität konfigurieren

Wenn Sie die VAPs auf dem WAP-Gerät konfigurieren, können Sie eine Methode zur sicheren Authentifizierung von Clients auswählen. Wenn Sie das WPA Personal-Protokoll (auch bekannt als WPA-Pre-Shared-Key oder WPA-PSK) als Sicherheitsmethode auswählen, können Sie auf der Seite „WPA-PSK-Komplexität“ die Komplexitätsanforderungen für den beim Authentifizierungsprozess verwendeten Schlüssel konfigurieren. Komplexere Schlüssel bieten erhöhte Sicherheit.

So konfigurieren Sie die WPA-PSK-Komplexität:

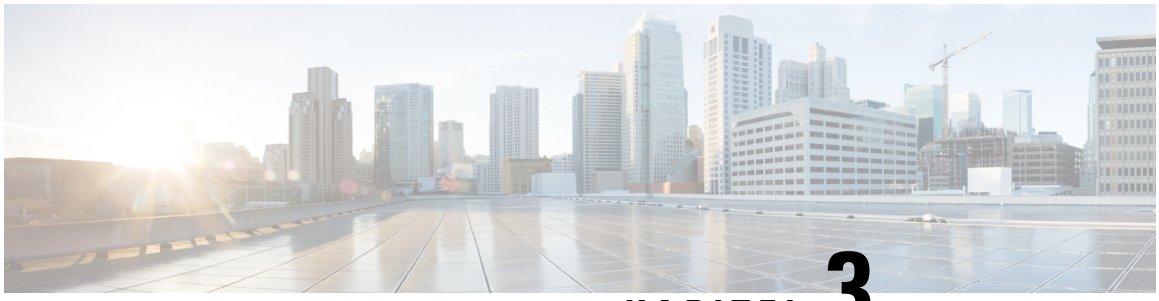
Schritt 1 Wählen Sie **Sicherheit > WPA-PSK-Komplexität konfigurieren** aus.

Schritt 2 Klicken Sie auf **Aktivieren**, damit das WAP-Gerät die WPA-PSK-Schlüssel anhand der konfigurierten Kriterien überprüfen kann. Wenn diese Option deaktiviert ist, werden die konfigurierten Einstellungen nicht verwendet. Die WPA-PSK-Komplexität ist standardmäßig deaktiviert.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **Minimale WPA-PSK-Zeichenklasse**: Wählen Sie die Mindestanzahl der Zeichenklassen aus, die die Zeichenkette enthalten muss. Die vier möglichen Zeichenklassen sind Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen auf einer Standardtastatur. Drei ist die Standardeinstellung.
- **WPA-PSK unterscheidet sich vom aktuellen Wert**: Klicken Sie auf **Aktivieren**, damit Benutzer nach Ablauf des aktuellen Schlüssels einen neuen Schlüssel konfigurieren können. Wenn diese Option deaktiviert ist, können die Benutzer den alten oder vorherigen Schlüssel weiterhin verwenden, nachdem ihr aktueller abgelaufen ist.
- **Maximale WPA-PSK-Länge**: Geben Sie einen Wert für die Schlüssellänge ein. Die maximale Schlüssellänge mit einer Zeichenanzahl von 32 bis 63. Die Standardeinstellung ist 63.
- **Minimale WPA-PSK-Länge**: Geben Sie einen Wert für die Schlüssellänge ein. Die minimale Schlüssellänge mit einer Zeichenanzahl von 8 bis 16. Die Standardeinstellung ist 8.

Schritt 4 Klicken Sie auf **Speichern**.



KAPITEL 3

Wireless

In diesem Kapitel wird beschrieben, wie Sie die WLAN-Funkeigenschaften konfigurieren. Das Kapitel enthält die folgenden Themen:

Funk

Das Funkmodul ist der physische Teil von WAP, der ein Wireless-Netzwerk erstellt. Die WAP-Funkeinstellungen steuern das Verhalten des Funkmoduls und legen fest, welche Arten von Wireless-Signalen das WAP-Gerät sendet.

So konfigurieren Sie die Wireless-Funkeinstellungen:

Schritt 1 Wählen Sie **Wireless > Funk** aus.

Schritt 2 Wählen Sie den Arbeitsmodus aus:

- **Funkmodul 1 (5 G)** — Unterstützt 5 G-Funk mit 4x4 MIMO-Modus.
- **Funkmodul 2 (2,4 G)** — Unterstützt 2,4 G-Funk mit 3x3 MIMO-Modus.

Schritt 3 Wählen Sie im Bereich **Funkeinstellung pro Schnittstelle** die Funkschnittstelle aus, für die die Konfigurationsparameter gelten sollen.

Schritt 4 Konfigurieren Sie im Bereich **Basiseinstellungen** die folgenden Parameter für die ausgewählte Funkschnittstelle:

Hinweis Bestimmte Funkmodi dürfen möglicherweise aufgrund lokaler Bestimmungen nicht verwendet werden. Nicht alle Modi sind in allen Ländern verfügbar.

- **Funk** — Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Funkschnittstelle zu aktivieren.
- **Wireless-Netzwerkmodus**: IEEE 802.11-Standard und Frequenz, die das Funkmodul verwendet. Der Standardwert für „Modus“ ist „802.11b/g/n“ für Funkmodul 2 und „802.11a/n/ac“ für Funkmodul 1. Wählen Sie für jedes Funkmodul einen der verfügbaren Modi aus.

Funkmodul 2 (2,4 G) unterstützt die folgenden Funkmodi:

- **802.11b/g**: 802.11b- und 802.11g-Clients können sich mit dem WAP-Gerät verbinden.
- **802.11b/g/n (Standard)**: 802.11b-, 802.11g- und 802.11n-Clients mit 2,4-GHz-Frequenz können sich mit dem WAP-Gerät verbinden.
- **2,4 GHz 802.11n**: 802.11n-Clients mit 2,4-GHz-Frequenz können sich mit dem WAP-Gerät verbinden.

Funkmodul 1 (5 G) unterstützt die folgenden Funkmodi:

- **802.11a**: 802.11a-Clients können sich mit dem WAP-Gerät verbinden.
- **802.11a/n/ac**: 802.11a-Clients, 802.11n- und 802.11ac-Clients mit 5-GHz-Frequenz können sich mit dem WAP-Gerät verbinden.
- **802.11n/ac** 802.11n- und 802.11ac-Clients mit 5-GHz-Frequenz können sich mit dem WAP-Gerät verbinden.

- **Frequenzband (nur 802.11n- und 802.11ac-Modi)**: Die 802.11n-Spezifizierung erlaubt neben dem älteren 20-MHz-Band, das in anderen Modi verfügbar ist, ein koexistierendes 20/40-MHz-Band. Das 20/40-MHz-Band ermöglicht höhere Datenraten, jedoch bleiben weniger Bänder für andere 2,4-GHz- und 5-GHz-Geräte übrig.

  Die 802.11ac-Spezifizierung erlaubt neben den 20-MHz- und 40-MHz-Bändern ein 80-MHz-breites Band.

  Legen Sie das Feld auf 20 MHz fest, um die Verwendung der Bandauswahl auf ein 20-MHz-Band zu beschränken. Legen Sie für den 802.11ac-Modus das Feld auf 40 MHz fest, um zu verhindern, dass der Funk eine Bandauswahl von 80 MHz verwendet.

- **Primärer Kanal: (Nur 802.11n-Modi mit 20/40-MHz-Bandbreite)**: Ein 40-MHz-Kanal kann als Kombination aus zwei zusammenhängenden 20-MHz-Kanälen im Frequenzbereich betrachtet werden. Diese beiden 20-MHz-Kanäle werden häufig als primärer und sekundärer Kanal bezeichnet. Der primäre Kanal wird für 802.11n-Clients verwendet, die nur eine Kanalbandbreite von 20 MHz unterstützen, sowie für ältere Clients.

  Wählen Sie eine dieser Optionen:

  - **Oben**: Legt den primären Kanal als oberen 20-MHz-Kanal im 40-MHz-Band fest.
  - **Unten**: Legt den primären Kanal als unteren 20-MHz-Kanal im 40-MHz-Band fest. Die Standardauswahl ist „Unten“.

- **Kanal**: Der Teil des Funkspektrums, den das Funkmodul für Übertragung und Empfang verwendet.

  Der Bereich der verfügbaren Kanäle wird durch den Modus der Funkschnittstelle und die Ländercode-Einstellung bestimmt. Wenn Sie die automatische Kanaleinstellung auswählen, sucht das WAP-Gerät verfügbare Kanäle und wählt einen Kanal aus, auf dem der geringste Datenverkehr erkannt wird.

  Jeder Modus bietet eine Reihe von Kanälen, abhängig davon, wie das Spektrum von nationalen und transnationalen Behörden wie beispielsweise der Federal Communications Commission (FCC) oder der International Telecommunication Union (ITU-R) lizenziert wird.

- **Planungsmodul** — Wählen Sie das Profil für die Funkschnittstelle aus der Liste aus.

Schritt 5 Konfigurieren Sie im Bereich **Erweiterte Einstellungen** die folgenden Parameter:

- **DFS-Support**: Dieses Feld ist nur verfügbar, wenn der ausgewählte Funkmodus mit der 5 GHz-Frequenz betrieben wird.

Für Funkmodule im 5 GHz-Frequenzband werden, wenn DFS Support aktiviert ist und die Regulierungsdomäne eine Radarerkennung im Kanal erfordert, die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) von 802.11h aktiviert.

DFS ist ein Mechanismus, mit dem WLAN-Geräte dasselbe Spektrum wie Radarsysteme nutzen können, aber den Betrieb in gleichen Kanälen im 5 GHz-Frequenzband vermeiden. Die DFS-Anforderungen sind abhängig von der Regulierungsdomäne, welche von der Einstellung für den Ländercode des Access Point bestimmt wird.

Bei Verwendung des 802.11h-WLAN-Modus sind einige wichtige Punkte des IEEE 802.11h-Standards zu beachten:

- 802.11h kann nur im 5 GHz-Band verwendet werden. Für das 2,4-GHz-Band ist er nicht erforderlich.
- Wenn Sie das Gerät in einer 802.11h-fähigen Domäne betreiben, versucht der AP, den zugewiesenen Kanal zu verwenden. Wenn der Kanal durch eine vorherige Radarerkennung blockiert ist oder der AP ein Radarsignal im Kanal erkennt, wird automatisch ein anderer Kanal ausgewählt.
- Wenn 802.11h aktiviert ist, ist der AP aufgrund der Radarsuche erst nach frühestens 60 Sekunden im 5-GHz-Band betriebsbereit.
- Wenn 802.11h verwendet wird, ist das Einrichten von WDS-Verbindungen möglicherweise schwierig. Dies ist darauf zurückzuführen, dass sich möglicherweise die Betriebskanäle der beiden an der WDS-Verbindung beteiligten APs abhängig von der Kanalauslastung und von Radarinterferenzen ändern. WDS kann nur verwendet werden, wenn Sie beide APs im gleichen Kanal betreiben. Weitere Informationen zu WDS finden Sie unter WDS Bridge.

- **Kurzes Schutzintervall unterstützt**: Dieses Feld ist nur verfügbar, wenn der ausgewählte Funkmodus 802.11n umfasst. Das Schutzintervall ist die Stillstandszeit zwischen OFDM-Symbolen in Nanosekunden. Das Guard Interval verhindert Interferenzen zwischen Symbolen (Inter-Symbol Interference, ISI) und zwischen Trägern (Inter-Carrier Interference, ICI). Im 802.11n-Modus kann dieses Schutzintervall von den für a und g definierten 800 Nanosekunden auf 400 Nanosekunden reduziert werden. Durch die Reduzierung des Schutzintervalls kann der Datendurchsatz um 10 Prozent gesteigert werden. Das kurze Guard Interval muss auch von dem Client unterstützt werden, mit dem das WAP-Gerät kommuniziert.

  Wählen Sie eine dieser Optionen:

  - **Ja**: Das WAP-Gerät überträgt Daten mit einem 400-Nanosekunden-Schutzintervall, wenn es mit Clients kommuniziert, die das kurze Schutzintervall ebenfalls unterstützen. Dies ist die Standardeinstellung.
  - **Nein**: Das WAP-Gerät überträgt Daten mit einem 800-Nanosekunden-Schutzintervall.

- **Schutz**: Die Schutzfunktion enthält Regeln, um sicherzustellen, dass 802.11-Übertragungen keine Interferenzen mit älteren Stationen oder Anwendungen verursachen. Der Schutz ist standardmäßig aktiviert ("Auto"). Der aktivierte Schutz wird wirksam, wenn sich ältere Geräte in der Reichweite des WAP-Geräts befinden.

  Sie können den Schutz deaktivieren („Off“). In diesem Fall können sich 802.11n-Übertragungen auf ältere Clients oder WAP-Geräte innerhalb der Reichweite auswirken. Schutz ist auch im Modus 802.11b/g verfügbar. Wenn der Schutz in diesem Modus aktiviert ist, werden 802.11b-Clients und WAP-Geräte vor 802.11g-Übertragungen geschützt.

  Hinweis Diese Einstellung hat keine Auswirkungen auf die Möglichkeit, den Client dem WAP-Gerät zuzuordnen.

- **Beacon-Intervall**: Das Intervall zwischen der Übertragung von Beacon-Frames. Das WAP-Gerät sendet diese Frames in regelmäßigen Intervallen, um das Vorhandensein des WLANs anzukündigen. Das Standardverhalten

sieht vor, dass alle 100 Millisekunden ein Beacon-Frame gesendet wird (oder zehn pro Sekunde). Geben Sie eine Ganzzahl von 20 bis 2.000 Millisekunden ein. Der Standardwert liegt bei 100 Millisekunden.

- **DTIM-Zeitraum**: Der DTIM-Zeitraum (Delivery Traffic Information Map). Geben Sie eine Ganzzahl zwischen 1 und 255 Beacons ein. Der Standardwert beträgt zwei Beacons.

  Die DTIM-Nachricht ist als Element in manchen Beacon-Frames enthalten. Aus der Nachricht geht hervor, für welche Clientstationen, die sich zurzeit im Energiesparmodus befinden, Daten im WAP-Gerät zwischengespeichert sind und auf den Abruf warten.

  Der DTIM-Zeitraum legt fest, wie oft die Clients, für die das WAP-Gerät zuständig ist, überprüfen sollen, ob abrufbereite zwischengespeicherte Daten vorhanden sind.

  Der Zeitraum wird in Beacons gemessen. Wenn Sie den Wert beispielsweise auf „1“ festlegen, überprüfen die Clients bei jedem Beacon, ob im WAP-Gerät zwischengespeicherte Daten vorhanden sind. Wenn Sie den Wert auf „10“ festlegen, führen die Clients die Überprüfung bei jedem zehnten Beacon aus.

- **Fragmentierungsschwelle**: Die Schwelle für Framegrößen in Byte. Gültig sind gerade Ganzzahlen zwischen 256 und 2346. Die Standardeinstellung ist 2346.

  Die Fragmentierungsschwelle ist eine Möglichkeit, die Größe der über das Netzwerk gesendeten Pakete (Frames) zu begrenzen. Wenn ein Paket die festgelegte Fragmentierungsschwelle überschreitet, wird die Fragmentierung aktiviert, und das Paket wird in Form mehrerer 802.11-Frames gesendet.

  Wenn das zu sendende Paket die Schwelle nicht überschreitet, wird keine Fragmentierung verwendet. Wenn Sie die Schwelle auf den höchsten Wert (den Standardwert 2.346 Byte) festlegen, deaktivieren Sie die Fragmentierung damit effektiv.

  Die Fragmentierung ist standardmäßig deaktiviert. Verwenden Sie die Fragmentierung nur, wenn Sie vermuten, dass Funkinterferenzen vorliegen. Die auf die einzelnen Fragmente angewendeten zusätzlichen Header erhöhen den Aufwand im Netzwerk und können den Durchsatz deutlich verringern.

- **RTS-Schwelle**: Der Wert für den RTS-Schwellenwert. Der Bereich der gültigen Ganzzahlen liegt zwischen 0 und 65535. Der Standardwert lautet 65535.

  Die RTS-Schwelle gibt die Anzahl der Oktette in einem MPDU-Frame an, unter der kein RTS/CTS-Handshake ausgeführt wird.

  Änderungen am RTS-Schwellenwert können hilfreich sein, um den Datenfluss durch das WAP-Gerät zu steuern. Wenn Sie einen niedrigeren Schwellenwert angeben, werden RTS-Pakete häufiger gesendet. Dabei wird mehr Bandbreite verbraucht und der Durchsatz des Pakets verringert. Durch das Senden einer größeren Anzahl von RTS-Paketen kann sich das Netzwerk jedoch schneller von Interferenzen oder Kollisionen erholen, die in einem ausgelasteten Netzwerk oder in einem Netzwerk mit elektromagnetischen Interferenzen auftreten können.

- **Maximal zugeordnete Clients**: Die maximale Anzahl der Stationen, die gleichzeitig auf das WAP-Gerät zugreifen dürfen. Sie können eine Ganzzahl zwischen 0 und 200 eingeben. Der Standardwert lautet 200.

- **Übertragungsleistung**: Ein Prozentwert für die Leistungsstufe der Übertragung für das WAP-Gerät.

  Der Standardwert „100 Prozent“ kann kostengünstiger sein als ein niedrigerer Prozentanteil, da das WAP-Gerät dadurch über den maximalen Broadcast-Bereich verfügt und weniger Access Points benötigt werden.

  Wenn Sie die Kapazität des Netzwerks erhöhen möchten, platzieren Sie die WAP-Geräte näher beieinander, und verringern Sie den Wert für die Sendeleistung. Mit dieser Einstellung können Sie Überschneidungen und Interferenzen zwischen Access Points reduzieren. Eine niedrigere Einstellung für die Sendeleistung kann auch die Sicherheit des Netzwerks erhöhen, da bei schwächeren Funksignalen die Wahrscheinlichkeit geringer ist, dass sie über den physischen Netzwerkstandort hinaus abgegeben werden.

Bei bestimmten Kombinationen aus Kanalbereich und Ländercode ergibt sich eine relativ niedrige maximale Sendeleistung. Wenn Sie versuchen, die Übertragungsleistung auf die unteren Bereich einzustellen (beispielsweise 25 Prozent oder 12 Prozent), kommt es möglicherweise nicht zum erwarteten Leistungsabfall, da bestimmte Leistungsverstärker über Mindestanforderungen bei der Übertragungsleistung verfügen.

- **Frame-Burst-Unterstützung**: Die Frame-Burst-Unterstützung verbessert im Allgemeinen die Funkleistung im Downstream.
- **Airtime-Fairness-Modus**: Die Airtime-Fairness-Funktion (ATF) wurde implementiert, um zu verhindern, dass schnelle Datenübertragungen durch langsamere Datenübertragungen ausgebremst werden.
- **Maximum Utilization Threshold**: Geben Sie den Prozentanteil der Nutzung der Netzwerkbandbreite für das Funkmodul ein, die zulässig ist, bis das WAP-Gerät keine neuen Clientzuordnungen mehr zulässt. Gültig sind Ganzzahlen von 0 bis 100 Prozent. Der Standardwert lautet „0 Prozent“. Ist dieser Wert auf 0 eingestellt, werden alle neuen Zuordnungen, unabhängig von ihrer Nutzungsrate, zugelassen.
- **Feste Multicast-Rate**: Die Übertragungsrate für Broadcast- und Multicast-Pakete in MBit/s. Diese Einstellung kann in Umgebungen hilfreich sein, in denen Multicast-Video-Streaming per Funk verwendet wird, sofern die WLAN-Clients die konfigurierte Rate unterstützen.

  Ist **Automatisch** ausgewählt, wählt das WAP-Gerät die beste Rate für die zugeordneten Clients aus. Der Bereich der gültigen Werte hängt vom konfigurierten Funkmodus ab.
- **Ältere Ratensätze**: Raten werden in Megabits pro Sekunde ausgedrückt.

  Unter „Unterstützte Ratensätze“ werden die vom WAP-Gerät unterstützten Raten angegeben. Sie können mehrere Raten aktivieren. Das WAP-Gerät wählt anhand bestimmter Faktoren wie Fehlerraten und der Entfernung der Clientstationen zum WAP-Gerät automatisch die effizienteste Rate aus.

  Unter „Einfache Ratensätze“ werden Raten angegeben, die das WAP-Gerät im Netzwerk ankündigt, um Verbindungen mit anderen Access Points und Clientstationen im Netzwerk aufzubauen. Im Allgemeinen ist es effizienter, ein WAP-Gerät eine Teilmenge der unterstützten Ratensätze senden zu lassen.
- **Broadcast-/Multicast-Ratenbegrenzung**: Durch Ratenbegrenzungen für Multicast und Broadcast können Sie die allgemeine Netzwerkleistung verbessern, da die Anzahl der im Netzwerk übertragenen Pakete begrenzt wird.

  Diese Funktion ist standardmäßig deaktiviert. Die folgenden Felder werden erst aktiviert, wenn Sie diese Funktion aktivieren:

  - **Ratenbegrenzung**: Die Ratenbegrenzung für Multicast- und Broadcast-Verkehr. Die Grenze sollte höher als 1 sein, aber unter 50 Paketen pro Sekunde liegen. Verkehr unterhalb dieser Ratenbegrenzung ist immer konform und wird an das entsprechende Ziel gesendet. Die standardmäßige und maximale Ratengrenze liegt bei 50 Paketen pro Sekunde.
  - **Ratenbegrenzungs-Burst**: Die in Byte gemessene Verkehrsmenge, die auch bei Überschreitung der definierten maximalen Rate als temporärer Burst durchgeleitet wird. Die Burst-Einstellung für die Standardratenbegrenzung und die maximale Ratenbegrenzung entspricht 75 Paketen pro Sekunde.
- **Spektrumanalyse-Modus**: Der Status des Spektrumanalyse-Modus kann die folgenden Werte haben:
  - **Dedizierte Spektrumanalyse**: Im dedizierten Modus wird das Funkmodul während mehr als 10 Prozent der Zeit für die Spektrumanalyse verwendet, sodass Clientverbindungen zwar möglich sind, aber nicht garantiert werden.
  - **Hybrid-Spektrumanalyse**: Im Hybridmodus werden Clientverbindungen zwar garantiert, aber Leistungsabfälle sind zu erwarten.

- **3+1-Spektrumanalyse**: Im 3+1-Modus verbinden sich die Clients mit 3x3-Ketten, und die Spektrumanalyse wird in einer 1x1-Kette durchgeführt.
- **Deaktiviert**: Die Standardeinstellung ist „Deaktiviert“.

- **VHT-Funktionen**: Diese Funktion aktiviert/deaktiviert Broadcom-spezifische Erweiterungen in VHT für Broadcom-zu-Broadcom-Verbindungen. Die VHT-Funktion ermöglicht Support für 256QAM-VHT-Raten, die nicht im 802.11ac-Entwurf spezifiziert wurden. Bei allen Raten handelt es sich um den VHT-LDPC-Modus: MCS 9 Nss 1 20 MHz, MCS 9 Nss 2 20 MHz, MCS 6 Nss 3 80 MHz. Die VHT-Funktion wird für 802.11 ac PHY unterstützt.

Schritt 6 Klicken Sie auf **TSPEC konfigurieren** und konfigurieren Sie die folgenden Parameter:

- **TSPEC-Verletzungsintervall**: Geben Sie in dieses Feld das Zeitintervall in Sekunden ein, in dem das WAP-Gerät zugeordnete Clients meldet, die die obligatorischen Verfahren für die Zugangskontrolle nicht einhalten. Die Berichterstattung erfolgt über das Systemprotokoll und über SNMP-Traps. Geben Sie einen Zeitraum zwischen 0 und 900 Sekunden ein. Der Standardwert beträgt 300 Sekunden.
- **TSPEC-Modus**: Regelt den allgemeinen TSPEC-Modus für das WAP-Gerät. Standardmäßig ist der TSPEC-Modus deaktiviert. Folgende Optionen sind verfügbar:
  - **An**: Das WAP-Gerät behandelt TSPEC-Anfragen gemäß den TSPEC-Einstellungen, die Sie auf der Seite „Funk“ konfigurieren.
  - **Aus**: Das WAP-Gerät ignoriert TSPEC-Anfragen von Clientstationen.
- **TSPEC-Modus für Sprach-ACM**: Regelt die obligatorische Zugangskontrolle (ACM) für die Zugriffskategorie „Sprachdaten“. Standardmäßig ist der TSPEC Voice ACM-Modus deaktiviert. Folgende Optionen sind verfügbar:
  - **Ein**: Eine Station muss vor dem Senden oder Empfangen eines Sprachverkehrsstroms eine TSPEC-Anfrage für Bandbreite an das WAP-Gerät senden. Wenn die TSPEC zugelassen wurde, antwortet das WAP-Gerät mit dem Ergebnis der Anfrage, das die zugewiesene mittlere Zeit enthält.
  - **Aus**: Eine Station kann Daten mit Sprachpriorität senden und empfangen, ohne dass eine zugelassene TSPEC erforderlich ist. Das WAP-Gerät ignoriert TSPEC-Sprachanfragen von Clientstationen.
- **TSPEC-Begrenzung für Sprach-ACM**: Die obere Begrenzung für die Verkehrsmenge, die das WAP-Gerät über das Funkmedium zu senden versucht, wobei für den Zugriff eine Sprachzugriffskategorie verwendet wird. Die Standardbegrenzung entspricht 20 Prozent des Gesamtverkehrs.
- **TSPEC-Modus für Video-ACM**: Regelt die obligatorische Zugangskontrolle für die Zugriffskategorie „Video“. Standardmäßig ist der TSPEC Video ACM-Modus deaktiviert. Folgende Optionen sind verfügbar:
  - **An**: Eine Station muss vor dem Senden oder Empfangen eines Videoverkehrsstroms eine TSPEC-Anfrage für Bandbreite an das WAP-Gerät senden. Wenn die TSPEC zugelassen wurde, antwortet das WAP-Gerät mit dem Ergebnis der Anfrage, das die zugewiesene mittlere Zeit enthält.
  - **Aus**: Eine Station kann Verkehr mit Videopriorität senden und empfangen, ohne dass eine zugelassene TSPEC erforderlich ist. Das WAP-Gerät ignoriert TSPEC-Videoanfragen von Clientstationen.
- **TSPEC-Begrenzung für Video-ACM**: Die obere Begrenzung für die Verkehrsmenge, die das WAP-Gerät über das Funkmedium zu senden versucht, wobei für den Zugriff eine Videozugriffskategorie verwendet wird. Die Standardbegrenzung entspricht 15 Prozent des Gesamtverkehrs.

- **TSPEC-Inaktivitätstimeout für AP**: Gibt an, wie lange ein WAP-Gerät Zeit hat, eine Downlink-Verkehrsspezifikation als im Leerlauf zu erkennen, bevor diese gelöscht wird. Gültig sind Ganzzahlen im Bereich von 0 bis 120 Sekunden. Der Standardwert lautet 30 Sekunden.
- **TSPEC-Inaktivitätstimeout für Station**: Gibt an, wie lange ein WAP-Gerät Zeit hat, eine Uplink-Verkehrsspezifikation als im Leerlauf zu erkennen, bevor diese gelöscht wird. Gültig sind Ganzzahlen im Bereich von 0 bis 120 Sekunden. Der Standardwert lautet 30 Sekunden.
- **TSPEC-Modus für älteren Verkehr in WMM-Warteschlangen**: Aktiviert oder deaktiviert die Mischung von älterem Verkehr in Warteschlangen im ACM-Betrieb. Standardmäßig ist dieser Modus deaktiviert.

Schritt 7 Klicken Sie auf **OK** und dann auf **Speichern**.

Netzwerke

Durch virtuelle Access Points (VAPs) wird das WLAN in mehrere Broadcast-Domänen segmentiert, die das WLAN-Äquivalent von Ethernet-VLANs darstellen. VAPs simulieren mehrere Access Points in einem physischen WAP-Gerät. Dieses Cisco WAP-Gerät unterstützt bis zu vier VAPs.

Mit Ausnahme von VAP0 können die einzelnen VAPs unabhängig voneinander aktiviert oder deaktiviert sein. VAP0 ist die physische Funkschnittstelle und bleibt aktiviert, solange das Funkmodul aktiviert ist. Um VAP0 zu deaktivieren, müssen Sie das Funkmodul selbst deaktivieren.

Die einzelnen VAPs werden durch eine vom Benutzer konfigurierte SSID (Service Set Identifier) identifiziert. Mehrere VAPs können nicht den gleichen SSID-Namen haben. SSID-Broadcasts können für die einzelnen VAPs unabhängig voneinander aktiviert oder deaktiviert sein. Standardmäßig sind SSID-Broadcasts aktiviert.

SSID-Benennungskonventionen

Die Standard-SSID für VAP0 lautet **ciscosb**. Jeder zusätzlich erstellte VAP hat einen leeren SSID-Namen. Sie können die SSIDs aller VAPs mit anderen Werten konfigurieren. Die SSID kann ein beliebiger alphanumerischer Wert aus 2 bis 32 Zeichen sein, bei dem zwischen Groß- und Kleinschreibung unterschieden wird.

Die folgenden Zeichen sind zulässig:

- ASCII 0x20 bis 0x7E.
- Nach- oder vorangestellte Leerzeichen (ASCII 0x20) sind nicht zulässig.

Hinweis Das heißt, Leerzeichen sind in der SSID zulässig, jedoch nicht als erstes oder letztes Zeichen. Der Punkt "." (ASCII 0x2E) ist ebenfalls zulässig.

VLAN-IDs

Jeder VAP ist einem VLAN zugeordnet, das durch eine VLAN-ID (VID) identifiziert wird. Eine VID kann ein beliebiger Wert zwischen 1 und 4094 (einschließlich) sein. Das Cisco WAP-Gerät unterstützt neun aktive VLANs (acht für WLAN plus ein Management-VLAN).

Die dem Konfigurationsdienstprogramm für das WAP-Gerät zugewiesene VID lautet "1" und entspricht außerdem der Standard-VID ohne Tag. Wenn die Verwaltungs-VID mit der einem VAP zugewiesenen VID

übereinstimmt, können die dem jeweiligen VAP zugeordneten WLAN-Clients das WAP-Gerät verwalten. Bei Bedarf können Sie eine Zugangskontrollliste (Access Control List, ACL) erstellen, um die Verwaltung über WLAN-Clients zu deaktivieren.

Konfigurieren von VAPs

So konfigurieren Sie VAPs:

Schritt 1 Wählen Sie **Wireless > Netzwerke** aus.

Schritt 2 Klicken Sie im Feld „Funk“ auf die Funkschnittstelle (**Funkmodul 1** oder **Funkmodul 2**), zu der die VAP-Konfigurationsparameter zugeordnet werden sollen.

Schritt 3 Wenn VAP0 der einzige im System konfigurierte VAP ist und Sie einen VAP hinzufügen möchten, klicken Sie auf □. Überprüfen Sie anschließend den VAP.

Schritt 4 Konfigurieren Sie Folgendes:

- **VLAN-ID**: Die VLAN-ID des VLANs, das dem VAP zugeordnet werden soll.

  Die eingegebene VLAN-ID muss im Netzwerk richtig konfiguriert sein. Wenn der VAP WLAN-Clients zu einem VLAN mit ungültiger Konfiguration zuordnet, können Netzwerkprobleme auftreten.

  Wenn ein WLAN-Client über diesen VAP eine Verbindung mit dem WAP-Gerät herstellt, markiert das WAP-Gerät den gesamten Datenverkehr vom WLAN-Client mit der konfigurierten VLAN-ID, es sei denn, Sie geben die VLAN-ID ein oder weisen einen WLAN-Client mithilfe eines RADIUS-Servers zu einem VLAN zu. Für die VLAN-ID sind Werte im Bereich von 1 bis 4094 gültig.

  Wenn Sie die VLAN-ID in eine andere ID als die aktuelle Verwaltungs-VLAN-ID ändern, können dem jeweiligen VAP zugeordnete WLAN-Clients das Gerät nicht verwalten. Sie können die Konfiguration der VLAN-IDs ohne Tag und die Verwaltungs-VLAN-IDs auf der Seite „LAN“ überprüfen. Weitere Informationen finden Sie unter IPv4-Konfiguration, auf Seite 11.

- **SSID-Name**: Geben Sie den Namen für das WLAN ein. Bei der SSID handelt es sich um eine alphanumerische Zeichenfolge mit bis zu 32 Zeichen. Wählen Sie für jeden VAP eine eindeutige SSID aus.

  Wenn Sie als WLAN-Client mit dem WAP-Gerät verbunden sind, das Sie verwalten, geht beim Zurücksetzen der SSID die Konnektivität mit dem WAP-Gerät verloren. Nach dem Speichern der neuen Einstellung müssen Sie sich erneut mit der neuen SSID verbinden.

- **SSID-Übertragung**: Aktiviert und deaktiviert den SSID-Broadcast.

  Geben Sie an, ob das WAP-Gerät die SSID in seinen Beacon-Frames senden darf. Der Parameter "Broadcast SSID" ist standardmäßig aktiviert. Wenn der VAP seine SSID nicht sendet, wird der Netzwerkname auf Clientstationen nicht in der Liste der verfügbaren Netzwerke angezeigt. Stattdessen müssen Sie den genauen Netzwerknamen manuell in das Dienstprogramm für WLAN-Verbindungen auf dem Client eingeben, damit die Verbindung hergestellt werden kann.

  Das Deaktivieren des SSID-Broadcasts reicht aus, um zu verhindern, dass Clients versehentlich eine Verbindung mit Ihrem Netzwerk herstellen. Sie können dadurch jedoch selbst die einfachsten Versuche eines Hackers, eine Verbindung herzustellen oder unverschlüsselten Verkehr zu überwachen, nicht verhindern. Die Unterdrückung des SSID-Broadcasts bietet nur rudimentären Schutz in einem anderweitig ungeschützten Netzwerk (beispielsweise einem Gastnetzwerk), in dem der Schwerpunkt darauf liegt, Clients das Herstellen einer Verbindung zu erleichtern, und in dem keine vertraulichen Informationen verfügbar sind.

WMF: Wireless Multicast Forwarding bietet eine effiziente Möglichkeit, den Multicast-Datenverkehr auf dem WLAN-Gerät weiterzuleiten und die Multicast-Übertragungsprobleme im WLAN zu beheben, indem es wiederholten Unicast oder Multicast für die Frames verwendet.

- **Sicherheit**: Wählen Sie den Authentifizierungstyp für den Zugriff auf den VAP aus. Folgende Optionen sind verfügbar:
  - Kein
  - Static WEP
  - WPA Personal
  - WPA Enterprise

Wenn Sie einen anderen Sicherheitsmodus als „Kein“ auswählen, werden zusätzliche Felder angezeigt. Weitere Informationen zum Konfigurieren von WLAN-Sicherheitseinstellungen finden Sie unter Konfigurieren von Sicherheitseinstellungen.

Es wird empfohlen, den Authentifizierungstyp „WPA Personal“ oder „WPA Enterprise“ zu verwenden, da diese mehr Schutz bieten.

Hinweis „Static WEP“ kann für WLAN-Computer oder Geräte verwendet werden, die „WPA Personal“ und „WPA Enterprise“ nicht unterstützen. Konfigurieren Sie das Funkmodul im 802.11a- oder 802.11b/g-Modus, um die Sicherheit mit „Static WEP“ zu konfigurieren. Im 802.11n-Modus kann nur der statische Sicherheitsmodus verwendet werden.

- **Clientfilter**: Gibt an, ob die Stationen, die auf diesen VAP zugreifen können, auf eine konfigurierte globale Liste von MAC-Adressen beschränkt sind. Sie können unter den folgenden Typen von Clientfiltern wählen:
  - **Deaktiviert**: Verwendet keinen Clientfilter.
  - **Lokal**: Die auf der Seite „Clientfilter“ konfigurierte MAC-Authentifizierungsliste wird verwendet.
  - **RADIUS**: Die MAC-Authentifizierungsliste auf einem externen RADIUS-Server wird verwendet.
- **Kanalisolierung**: Aktivieren Sie diese Option, um Kanalisolierung zu verwenden.

  Wenn diese Option deaktiviert ist, können WLAN-Clients normal miteinander kommunizieren, indem sie Daten durch das WAP-Gerät senden.

  Wenn die Option aktiviert ist, blockiert das WAP-Gerät die Kommunikation zwischen WLAN-Clients im gleichen VAP. Das WAP-Gerät lässt dennoch Datenverkehr zwischen den WLAN-Clients und kabelgebundenen Geräten im Netzwerk über eine WDS-Verbindung sowie zu anderen WLAN-Clients in einem anderen VAP zu. Verbindungen zwischen WLAN-Clients sind nicht zulässig.
- **Band Steering**: Ermöglicht Band Steering, wenn beide Funkmodule aktiv sind. Diese Option verwendet das 5-GHz-Band, indem Clients mit Dual-Band-Unterstützung vom 2,4-GHz-Band auf das 5-GHz-Band umgeleitet werden.
  - Diese Option wird pro VAP konfiguriert und muss in beiden Funkmodulen aktiviert werden.
  - Diese Option sollte nicht auf VAPs mit zeitkritischem Sprach- oder Videodatenverkehr verwendet werden.
  - Die n-Bandbreite des Funkmoduls wird nicht berücksichtigt. Die Clients werden zum entsprechenden Funkmodul weitergeleitet, selbst wenn das 5-GHz-Funkmodul die 20-MHz-Bandbreite verwendet.

- **Planungsmodul**: Wählen Sie ein Planungsmodulprofil aus der Liste aus. VAP0 kann nicht zu einem Planungsmodulprofil zugeordnet werden.
- **Gastzugangsinstanz**: Ordnen Sie eine CP-Instanz zu einem VAP zu. Die Einstellungen für zugeordnete CP-Instanzen gelten für Benutzer, die sich gegenüber dem VAP zu authentifizieren versuchen. Wählen Sie für jeden VAP, dem Sie eine Instanz zuordnen möchten, den Instanznamen aus.

Hinweis Ein VAP kann auf der Seite **Zugriffskontrolle** > **Gastzugang** zu einer Gastzugangsinstanz zugeordnet werden. Konfigurieren Sie dazu zunächst eine **Gastzugangsinstanz**.

Schritt 5 Klicken Sie auf **Speichern**.

Vorsicht Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. In diesem Fall werden die Verbindungen des WAP-Geräts möglicherweise unterbrochen. Zu diesem Zeitpunkt sollten Sie die Einstellungen auf dem WAP-Gerät ändern.

Hinweis Zum Löschen eines VAPs wählen Sie den VAP aus, und klicken Sie auf **Löschen**. Um einen VAP zu bearbeiten, wählen Sie den VAP aus, und klicken Sie auf **Bearbeiten**. Klicken Sie anschließend auf **Speichern**, um Ihre Änderungen zu speichern.

Konfigurieren von Sicherheitseinstellungen

Dieser Abschnitt beschreibt die Sicherheitseinstellungen, die Sie auf der Seite „Netzwerke“ für das WAP-Gerät konfigurieren können. Sie haben drei Sicherheitseinstellungen zur Auswahl: „Kein“, „WPA-Personal“ und „WPA-Enterprise“.

Kein

Wenn Sie den Sicherheitsmodus **Kein** auswählen, werden keine zusätzlichen Sicherheitseinstellungen für das Gerät benötigt. In diesem Modus werden die zum und vom WAP-Gerät übertragenen Daten nicht verschlüsselt. Dieser Sicherheitsmodus kann bei der anfänglichen Netzwerkkonfiguration oder bei der Problembehandlung hilfreich sein. Für die reguläre Verwendung im internen Netzwerk wird der Modus jedoch nicht empfohlen, da er nicht sicher ist.

Static WEP

WEP (Wired Equivalent Privacy) ist ein Datenverschlüsselungsprotokoll für 802.11-WLANs. Alle WLAN-Stationen und Access Points im Netzwerk sind mit einem statischen 64-Bit-Schlüssel (geheimer 40-Bit-Schlüssel plus 24-Bit-Initialisierungsvektor (IV)) oder einem gemeinsamen 128-Bit-Schlüssel (geheimer 104-Bit-Schlüssel plus 24-Bit-IV) für die Datenverschlüsselung konfiguriert.

"Static WEP" ist nicht der sicherste verfügbare Modus, bietet jedoch mehr Schutz als "None" (unverschlüsselt), da Außenstehende den unverschlüsselten WLAN-Verkehr nicht einfach abfangen können.

WEP verschlüsselt die im WLAN übertragenen Daten auf der Grundlage eines statischen Schlüssels. Der Verschlüsselungsalgorithmus ist eine Stream-Verschlüsselung mit dem Namen RC4.

Sie konfigurieren "Static WEP" mit den folgenden Parametern:

- **Übertragungsschlüsselindex**: Geben Sie eine Liste der Schlüsselindizes ein. Zur Verfügung stehen die Schlüsselindizes 1 bis 4. Die Standardeinstellung ist 1. Aus dem „Transferschlüsselindex" geht hervor, welchen WEP-Schlüssel das WAP-Gerät zum Verschlüsseln der übertragenen Daten verwendet.

- **Schlüssellänge**: Wählen Sie 64 Bit oder 128 Bit als Schlüssellänge aus.
- **Schlüsseltyp**: Wählen Sie entweder ASCII oder Hex als Schlüsseltyp aus.
- **WEP-Schlüssel** – Sie können bis zu vier WEP-Schlüssel angeben. Geben Sie in die einzelnen Textfelder eine Zeichenfolge für den jeweiligen Schlüssel ein. Welche Schlüssel Sie eingeben, hängt vom ausgewählten Schlüsseltyp ab:
  - **ASCII**: Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen wie @ und #.
  - **Hex**: Die Ziffern 0 bis 9 und die Buchstaben A bis F.
- Verwenden Sie für die einzelnen Schlüssel die gleiche Anzahl von Zeichen wie im Feld **Benötigte Zeichen**. Dabei handelt es sich um die RC4-WEP-Schlüssel, die auch auf den Stationen hinterlegt sind, die das WAP-Gerät verwenden. Sie müssen alle Clientstationen für die Verwendung eines dieser WEP-Schlüssel in der Position konfigurieren, die Sie auch für das WAP-Gerät angegeben haben.
- **802.1X-Authentifizierung**: Der Authentifizierungsalgorithmus definiert die Methode, mit der ermittelt wird, ob eine Clientstation einem WAP-Gerät zugeordnet werden darf, wenn der Sicherheitsmodus „Static WEP“ ausgewählt ist.
- Geben Sie den gewünschten Authentifizierungsalgorithmus an, indem Sie eine der folgenden Optionen auswählen:
  - In einem offenen System kann jede Clientstation dem WAP-Gerät zugeordnet werden. Dabei spielt es keine Rolle, ob die Clientstation über den richtigen WEP-Schlüssel verfügt. Dieser Algorithmus wird auch im unverschlüsselten Modus und in den Modi IEEE 802.1X und WPA verwendet. Wenn der Authentifizierungsalgorithmus "Open System" festgelegt ist, kann jeder Client dem WAP-Gerät zugeordnet werden.

Hinweis Durch die Zuordnung einer Clientstation ist jedoch nicht sichergestellt, dass die Clientstation Daten mit einem WAP-Gerät austauschen kann. Damit eine Station erfolgreich auf Daten vom WAP-Gerät zugreifen, diese Daten entschlüsseln und lesbare Daten an das WAP-Gerät senden kann, muss die Station über den richtigen WEP-Schlüssel verfügen.

  - Gemeinsamer Schlüssel: In diesem Modus benötigt die Clientstation den richtigen WEP-Schlüssel, damit sie dem WAP-Gerät zugeordnet werden kann. Wenn der Authentifizierungsalgorithmus „Gemeinsamer Schlüssel“ festgelegt ist, kann eine Station mit einem falschen WEP-Schlüssel nicht mit dem WAP-Gerät verbunden werden.
  - Offenes System und Gemeinsamer Schlüssel. Wenn Sie beide Authentifizierungsalgorithmen auswählen, benötigen Clientstationen, die für die Verwendung von WEP im Pre-Shared-Key-Modus konfiguriert sind, für die Zuordnung zum WAP-Gerät einen gültigen WEP-Schlüssel. Außerdem können Clientstationen, die für die Verwendung von WEP als offenes System konfiguriert sind (der Modus für gemeinsame Schlüssel ist nicht aktiviert) auch dann dem WAP-Gerät zugeordnet werden, wenn sie nicht über den richtigen WEP-Schlüssel verfügen.

Regeln für Static WEP

Wenn Sie „Static WEP“ verwenden, gelten die folgenden Regeln:

- Die WLAN-Sicherheit aller Clientstationen muss auf WEP festgelegt sein, und alle Clients benötigen zum Decodieren der Übertragungen vom AP zur Station einen der im WAP angegebenen WEP-Schlüssel.
- Das WAP-Gerät benötigt zum Dekodieren der Übertragungen von Stationen alle Schlüssel, die von Clients für Übertragungen von der Station zum AP verwendet werden.
- Der gleiche Schlüssel muss sich in allen Knoten (AP und Clients) an der gleichen Position befinden. Wenn beispielsweise für das WAP-Gerät der Schlüssel „abc123“ als WEP-Schlüssel 3 definiert ist, muss die gleiche Zeichenfolge für die Clientstationen als WEP-Schlüssel 3 definiert sein.
- Die Clientstationen können für die Übertragung von Daten an den Access Point verschiedene Schlüssel verwenden. (Alternativ können alle den gleichen Schlüssel verwenden. Dies ist jedoch weniger sicher, da in diesem Fall eine Station die von einer anderen Station gesendeten Daten entschlüsseln kann.)
- In manchen WLAN-Clientanwendungen können Sie mehrere WEP-Schlüssel konfigurieren, einen Übertragungsschlüsselindex für Clientstationen definieren, und anschließend für die Stationen festlegen, dass die übertragenen Daten mit verschiedenen Schlüsseln verschlüsselt werden. Dadurch stellen Sie sicher, dass benachbarte Access Points nicht die Übertragungen anderer Access Points dekodieren können.
- Sie können nicht 64-Bit- und 128-Bit-WEP-Schlüssel für den Access Point und die zugehörigen Clientstationen mischen.

WPA Personal

WPA Personal ist ein IEEE 802.11i-Standard der Wi-Fi Alliance und umfasst AES-CCMP- und TKIP-Verschlüsselung. WPA-Personal verwendet anstelle von IEEE 802.1X einen vorher vereinbarten Schlüssel (Pre-Shared Key, PSK), und wie beim Sicherheitsmodus Enterprise WPA wird EAP verwendet. Der PSK wird nur für die anfängliche Überprüfung der Anmeldeinformationen verwendet. WPA Personal wird auch als WPA-PSK bezeichnet.

Dieser Sicherheitsmodus ist abwärtskompatibel mit WLAN-Clients, die den ursprünglichen WPA-Modus unterstützen.

Konfigurieren Sie Folgendes für den WPA-Personal-Modus:

- **WPA-Versionen**: Die Typen der zu unterstützenden Clientstationen:
  - **WPA-TKIP**: Im Netzwerk befinden sich Clientstationen, die nur den ursprünglichen WPA-Modus und das TKIP-Sicherheitsprotokoll unterstützen. Die Auswahl von WPA-TKIP allein für den Access Point ist laut den aktuellen Anforderungen der WiFi Alliance nicht zulässig.
  - **WPA2-AES**: Alle Clientstationen im Netzwerk unterstützen WPA2 und das AES-CCMP-Verschlüsselungs-/Sicherheitsprotokoll. Diese Option bietet die höchste Sicherheit gemäß dem IEEE 802.11i-Standard. Laut den aktuellen Anforderungen der WiFi Alliance muss der AP diesen Modus immer unterstützen.

    Wenn im Netzwerk eine Mischung aus Clients vorhanden ist, also einige Clients mit Unterstützung für WPA2 und andere nur mit Unterstützung für den ursprünglichen WPA-Modus, aktivieren Sie beide Optionen. Auf diese Weise können WPA- und WPA2-Clientstationen zugeordnet und authentifiziert werden, während für Clients mit entsprechender Unterstützung der robustere WPA2-Modus verwendet wird. Bei dieser WPA-Konfiguration wird ein Teil der Sicherheit durch bessere Interoperabilität ersetzt.

    Für die Zuordnung zum WAP-Gerät benötigen WPA-Clients einen der folgenden Schlüssel:

    - Einen gültigen TKIP-Schlüssel

- Einen gültigen AES-CCMP-Schlüssel

- **PMF (Protection Management Frame, Schutzverwaltungsframe)**: Bietet Sicherheit für die unverschlüsselten 802.11-Management-Frames. Bei aktiviertem Sicherheitsmodus ist die PMF-Option auf „Kein PMF“ festgelegt und nicht editierbar (ausgeblendet oder ausgegraut). Im Sicherheitsmodus WPA2-xxx ist PMF standardmäßig auf „Fähig“ festgelegt und kann bearbeitet werden. Hierzu können die folgenden drei Kontrollkästchenwerte konfiguriert werden.
  - **Nicht erforderlich**
  - **Fähig**
  - **Erforderlich**

Hinweis Die WiFi Alliance hat festgelegt, dass PMF aktiviert und als „Fähig“ (Standard) konfiguriert werden sollte. Sie können diese Option deaktivieren, wenn auf inkompatiblen WLAN-Clients Stabilitäts- oder Verbindungsprobleme auftreten.

- **Schlüssel**: Der gemeinsame geheime Schlüssel für WPA-Personal-Sicherheit. Geben Sie eine Zeichenfolge mit mindestens 8 bis maximal 63 Zeichen ein. Zulässig sind Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen wie @ und #.
- **Schlüssel als Klartext anzeigen**: Wenn diese Option aktiviert ist, wird der eingegebene Text angezeigt. Wenn die Option deaktiviert ist, wird der Text bei der Eingabe nicht maskiert.
- **Schlüsselsicherheitsmessung**: Das WAP-Gerät überprüft den Schlüssel anhand von Komplexitätskriterien wie beispielsweise der Anzahl der verwendeten Zeichentypen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen) und der Länge der Zeichenfolge. Wenn die WPA-PSK-Funktion für die Komplexitätsüberprüfung aktiviert ist, werden nur Schlüssel akzeptiert, die den Mindestkriterien entsprechen. Weitere Informationen zum Konfigurieren der Komplexitätsüberprüfung finden Sie unter WPA-PSK-Komplexität konfigurieren, auf Seite 40.
- **Aktualisierungsrate für Broadcast-Schlüssel**: Das Intervall, in dem der Broadcast-Schlüssel (Gruppenschlüssel) für diesem VAP zugeordnete Clients aktualisiert wird. Der Standardwert lautet 86400 Sekunden. Gültig sind Werte im Bereich von 0 bis 86400 Sekunden. Der Wert "0" bedeutet, dass der Broadcast-Schlüssel nicht aktualisiert wird.

WPA Enterprise

WPA Enterprise mit RADIUS ist eine Implementierung des IEEE 802.11i-Standards der Wi-Fi Alliance und umfasst CCMP-Verschlüsselung (AES) und TKIP-Verschlüsselung. Im Enterprise-Modus müssen Benutzer mit einem RADIUS-Server authentifiziert werden.

Dieser Sicherheitsmodus ist abwärtskompatibel mit WLAN-Clients, die den ursprünglichen WPA-Modus unterstützen.

Der dynamische VLAN-Modus ist standardmäßig aktiviert, damit der RADIUS-Authentifizierungsserver entscheiden kann, welches VLAN für die Stationen verwendet wird.

Sie konfigurieren "WPA Enterprise" mit den folgenden Parametern:

- **WPA-Versionen**: Wählen Sie die Typen der zu unterstützenden Clientstationen aus. Folgende Optionen sind verfügbar:
  - **WPA-TKIP**: Im Netzwerk befinden sich Clientstationen mit Unterstützung für den ursprünglichen WPA-Modus und das TKIP-Sicherheitsprotokoll. Die Auswahl von WPA-TKIP allein für den Access Point ist laut den aktuellen Anforderungen der WiFi Alliance nicht zulässig.
  - **WPA2-AES**: Alle Clientstationen im Netzwerk unterstützen die WPA2-Version und das AES-CCMP-Verschlüsselungs-/Sicherheitsprotokoll. Diese Option bietet die höchste Sicherheit gemäß dem IEEE 802.11i-Standard. Laut den aktuellen Anforderungen der WiFi Alliance muss der AP diesen Modus immer unterstützen.

- **Vorauthentifizierung aktivieren**: Wenn Sie unter „WPA-Versionen“ nur „WPA2“ oder „WPA und WPA2“ auswählen, können Sie die Vorauthentifizierung für WPA2-Clients aktivieren.

  Aktivieren Sie diese Option, wenn WPA2-WLAN-Clients Vorauthentifizierungspakete senden sollen. Die Vorauthentifizierungsinformationen werden von dem zurzeit vom Client verwendeten WAP-Gerät an das WAP-Zielgerät weitergeleitet. Mit dieser Funktion können Sie die Authentifizierung für Roaming-Clients beschleunigen, die sich mit mehreren APs verbinden.

  Diese Option gilt nicht, wenn Sie unter „WPA-Versionen“ die Option „WPA“ ausgewählt haben, da diese Funktion im ursprünglichen WPA-Modus nicht unterstützt wird.

  Clientstationen, die für die Verwendung von WPA-Versionen mit RADIUS konfiguriert sind, müssen über eine der folgenden Adressen und Schlüssel verfügen:
  - Eine gültige TKIP-RADIUS-IP-Adresse und ein RADIUS-Schlüssel
  - Eine gültige CCMP (AES)-RADIUS-IP-Adresse und ein RADIUS-Schlüssel

- **PMF (Protection Management Frame, Schutzverwaltungsframe)**: Bietet Sicherheit für die unverschlüsselten 802.11-Management-Frames. Bei aktiviertem Sicherheitsmodus ist die PMF-Option auf **Kein PMF** festgelegt und nicht editierbar (ausgeblendet oder ausgegraut). Im Sicherheitsmodus **WPA2-xxx** ist PMF standardmäßig auf **Fähig** festgelegt und kann bearbeitet werden. Hierzu können die folgenden drei Kontrollkästchenwerte konfiguriert werden.
  - **Nicht erforderlich**
  - **Fähig**
  - **Erforderlich**

Hinweis Die WiFi Alliance hat festgelegt, dass PMF mit der Standardeinstellung **Fähig** aktiviert werden sollte. Sie können diese Option deaktivieren, wenn auf inkompatiblen WLAN-Clients Stabilitäts- oder Verbindungsprobleme auftreten.

- **Globale RADIUS-Servereinstellungen verwenden**: Standardmäßig verwenden alle VAPs die für das WAP-Gerät definierten globalen RADIUS-Einstellungen. Sie können jedoch für jeden VAP andere RADIUS-Server konfigurieren.

  Aktivieren Sie diese Option, um die globalen RADIUS-Servereinstellungen zu verwenden, oder deaktivieren Sie die Option, um einen separaten RADIUS-Server für den VAP zu verwenden, und geben Sie die IP-Adresse und den Schlüssel des RADIUS-Servers in die entsprechenden Felder ein.

- **Server-IP-Adresstyp**: Die IP-Version, die der RADIUS-Server verwendet. Sie können zwischen den Adresstypen umschalten, um globale RADIUS-Adresseinstellungen für IPv4 und IPv6 zu konfigurieren. Das WAP-Gerät stellt jedoch nur Verbindungen mit den RADIUS-Servern für den in diesem Feld ausgewählten Adresstyp her.
- **Server-IP-Adresse 1 oder Server-IPv6-Adresse 1**: Die Adresse des primären RADIUS-Servers für diesen VAP.
- **Server-IP-Adresse 2 oder Server-IPv6-Adresse 2**: Bis zu drei IPv4- und/oder IPv6-Adressen, die als RADIUS-Backupserver für diesen VAP verwendet werden sollen. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird der Reihe nach jeder konfigurierte Backup-Server ausprobiert.
- **Schlüssel 1**: Der gemeinsame geheime Schlüssel für den globalen RADIUS-Server. Sie können bis zu 63 alphanumerische Standardzeichen und Sonderzeichen verwenden. Beim Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden, und Sie müssen im WAP-Gerät und auf dem RADIUS-Server den gleichen Schlüssel konfigurieren. Der eingegebene Text wird mit Sternchen maskiert, damit andere den RADIUS-Schlüssel bei der Eingabe nicht sehen können.
- **Schlüssel 2**: Der RADIUS-Schlüssel für die konfigurierten RADIUS-Backupserver. Der Server mit der Server-IP (IPv6)-Adresse 2 verwendet Schlüssel 2.
- **RADIUS-Abrechnung aktivieren**: Verfolgt und misst die von einem bestimmten Benutzer verwendeten Ressourcen, beispielsweise Systemzeit, Menge der gesendeten und empfangenen Daten usw. Wenn Sie die RADIUS-Prüfung aktivieren, wird sie für den primären RADIUS-Server und alle Backup-Server aktiviert.
- **Aktiver Server**: Aktiviert die administrative Auswahl des aktiven RADIUS-Servers, anstatt dass das WAP-Gerät der Reihe nach eine Verbindung mit den einzelnen konfigurierten Servern herzustellen versucht und den ersten aktiven Server auswählt.
- **Aktualisierungsrate für Broadcast-Schlüssel**: Das Intervall, in dem der Broadcast-Schlüssel (Gruppenschlüssel) für diesem VAP zugeordnete Clients aktualisiert wird. Der Standardwert beträgt 86400 Sekunden. Gültig sind Werte im Bereich von 0 bis 86400 Sekunden. Der Wert "0" bedeutet, dass der Broadcast-Schlüssel nicht aktualisiert wird.
- **Aktualisierungsrate für Sitzungsschlüssel**: Das Intervall, in dem das WAP-Gerät Sitzungsschüssel (Unicast) für die einzelnen dem VAP zugeordneten Clients aktualisiert Gültig sind Werte im Bereich von 30 bis 86400 Sekunden. Der Wert „0“ bedeutet, dass der Sitzungsschlüssel nicht aktualisiert wird.

Clientfilter

Mit Clientfiltern können Sie den aufgeführten Clientstationen die Authentifizierung beim WAP-Gerät erlauben oder verbieten. Die MAC-Authentifizierung wird auf der Seite Netzwerke, auf Seite 47 konfiguriert. Abhängig von der VAP-Konfiguration verwendet das WAP-Gerät möglicherweise eine auf einem externen RADlUS-Server oder lokal im WAP-Gerät gespeicherte Clientfilterliste.

Konfigurieren einer lokalen Clientfilterliste im WAP-Gerät

Das WAP-Gerät unterstützt nur eine lokale Clientfilterliste. Sie können den Filter so konfigurieren, dass der Zugriff nur den MAC-Adressen in der Liste gewährt oder verweigert wird.

Sie können bis zu 512 Client-Adressen zur Filterliste hinzufügen.

Führen Sie die folgenden Schritte aus, um den Clientfilter zu konfigurieren:

Schritt 1 Wählen Sie **Wireless > Clientfilter** aus.

Schritt 2 Wählen Sie aus, wie das WAP-Gerät die Filterliste verwenden soll:

- **Zulassen (Nur Clients in Liste zulassen)**: Allen nicht in der Stationsliste enthaltenen Stationen wird der Zugriff auf das Netzwerk über das WAP-Gerät verweigert.
- **blockieren (Alle Clients in Liste blockieren)**: Nur den in der Liste enthaltenen Stationen wird der Zugriff auf das Netzwerk über das WAP-Gerät verweigert. Allen anderen Stationen wird der Zugriff gewährt.

Hinweis Die Filtereinstellung gilt gegebenenfalls auch für die auf dem RADIUS-Server gespeicherte Clientfilterliste.

Schritt 3 Geben Sie weitere MAC-Adressen ein, bis die Liste vollständig ist. Klicken Sie auf den Pfeil neben **Associated Clients**, um die Liste der zugeordneten Clients anzuzeigen. Wählen Sie eine der MAC-Adressen, und klicken Sie auf **Hinzufügen**. Der MAC-Adressentabelle wird eine Regel hinzugefügt. Die Liste zugeordneter Clients:

- **MAC-Adresse**: die MAC-Adresse des zugeordneten Wi-Fi-Clients
- **Hostname**: der Hostname des zugeordneten Wi-Fi-Clients
- **IP-Adresse**: die IP-Adresse des zugeordneten Wi-Fi-Clients
- **Netzwerk (SSID)**: die SSID des WAP-Geräts Bei der SSID handelt es sich um eine alphanumerische Zeichenfolge mit bis zu 32 Zeichen, die ein WLAN eindeutig identifiziert. Die SSID wird auch als Netzwerkname bezeichnet.

Schritt 4 Klicken Sie auf **Speichern**.

Konfigurieren der MAC-Authentifizierung auf dem RADIUS-Server

Wenn mindestens ein VAP einen Clientfilter verwendet, müssen Sie die Stationsliste auf dem RADIUS-Server konfigurieren. Das Format für die Liste wird in der folgenden Tabelle beschrieben:

RADIUS-Serverattribut	Beschreibung	Wert
User-Name (1)	MAC-Adresse der Clientstation	Gültige Ethernet-MAC-Adresse
User-Password (2)	Ein festes globales Kennwort, das zum Suchen eines MAC-Clienteintrags verwendet wird	NOPASSWORD

Planungsmodul

Mit dem Planungsmodul für Funkmodule und VAPs können Sie eine Regel mit einem konkreten Zeitintervall konfigurieren, in dem VAPs oder Funkmodule betriebsbereit sind.

Mit dieser Funktion können Sie beispielsweise den Betrieb der VAPs nur während der Arbeitszeit planen, um die Sicherheit zu erhöhen und den Stromverbrauch zu verringern.

Das WAP-Gerät unterstützt bis zu 16 Profile. Nur gültige Regeln werden dem Profil hinzugefügt. Bis zu 16 Regeln werden in einem Planungsprofil gruppiert. Zum gleichen Profil gehörende periodische Zeiteinträge können nicht überlappen.

Planungsmodulprofil-Konfiguration

Sie können bis zu 16 Namen für Planungsmodulprofile erstellen. Standardmäßig werden keine Profile erstellt.

So können Sie den Planungsstatus anzeigen und ein Planungsmodulprofil hinzufügen:

Schritt 1 Wählen Sie **Wireless > Planungsmodul** aus.

Schritt 2 Klicken Sie auf **Aktivieren**, um den administrativen Modus zu aktivieren. Standardmäßig ist die Option deaktiviert.

Im Bereich "Scheduler Operational Status" wird der aktuelle Betriebsstatus des Planungsmoduls angezeigt:

- **Status**: Der Betriebsstatus (aktiviert oder deaktiviert) des Planungsmoduls. Die Standardeinstellung ist „Deaktiviert“.
- **Grund**: Der Grund für den Betriebsstatus des Planungsmoduls. Folgende Werte sind möglich:
  - **Aktiv**: Das Planungsmodul ist administrativ aktiviert.
  - **Administrativer Modus ist deaktiviert**: Der administrative Modus für das Planungsmodul ist deaktiviert.
  - **Systemzeit ist veraltet**: Die Systemzeit ist veraltet.
  - **Verwalteter Modus**: Das Planungsmodul befindet sich im verwalteten Modus.

Schritt 3 Zum Hinzufügen eines Profils geben Sie in das Textfeld Planungsmodulprofil-Konfiguration einen Profilnamen ein, und klicken Sie auf **Hinzufügen**. Der Profilname kann aus bis zu 32 alphanumerischen Zeichen bestehen.

Profilregelkonfiguration

Sie können für ein Profil bis zu 16 Regeln konfigurieren. Jede Regel gibt die Startzeit, die Endzeit und die Wochentage für den Betrieb des Funkmoduls bzw. des VAPs an. Die Regeln sind periodisch und werden wöchentlich wiederholt. Eine gültige Regel muss die folgenden Parameter (Wochentage, Stunde und Minute) für die Start- und Endzeit enthalten. Regeln dürfen nicht im Konflikt miteinander stehen. So können Sie beispielsweise eine Regel für den Start an allen Wochentagen und eine weitere für den Start an allen Tagen des Wochenendes konfigurieren, jedoch nicht eine Regel für den täglichen Start und eine weitere Regel für den Start an Wochenenden.

So konfigurieren Sie eine Profilregel:

Schritt 1 Wählen Sie das Profil in der Liste **Profilnamen auswählen** aus.

Schritt 2 Klicken Sie auf □.

Die neue Regel wird in der **Profilregeltabelle** angezeigt.

Schritt 3 Aktivieren Sie das Kontrollkästchen neben **Profilname** und klicken Sie auf **Bearbeiten**.

Schritt 4 Wählen Sie im Menü **Wochentag** den wiederkehrenden Zeitplan für die Regel aus. Sie können die Regel so konfigurieren, dass sie täglich, an allen Wochentagen, an allen Tagen des Wochenendes (Samstag und Sonntag) oder an einem einzigen Wochentag ausgeführt wird.

Schritt 5 Legen Sie die Start- und Endzeiten fest:

- **Startzeit**: Der Zeitpunkt, zu dem das Funkmodul oder der VAP aktiviert wird. Geben Sie die Uhrzeit im 24-Stundenformat ein (hh:mm). Möglich sind Werte im Bereich <00-23>:<00-59>. Die Standardeinstellung ist 00:00.
- **Endzeit**: Der Zeitpunkt, zu dem das Funkmodul oder der VAP deaktiviert wird. Geben Sie die Uhrzeit im 24-Stundenformat ein (hh:mm). Möglich sind Werte im Bereich <00-23>:<00-59>. Die Standardeinstellung ist 00:00.

Schritt 6 Klicken Sie auf **Speichern**.

Hinweis Ein Planungsmodulprofil wird erst wirksam, wenn es zu einer Funkschnittstelle oder VAP-Schnittstelle zugeordnet ist.

Zum Löschen einer Regel wählen Sie in der Spalte Profilname das Profil aus, und klicken Sie auf **Löschen**.

QoS

Mit den Quality of Service (QoS)-Einstellungen können Sie die Übertragungswarteschlangen für optimierten Durchsatz konfigurieren und die Leistung bei der Verarbeitung von differenziertem WLAN-Datenverkehr verbessern. Bei diesen Daten kann es sich um VoIP, andere Typen von Audiodaten, Video, Streaming-Medien und herkömmliche IP-Daten handeln.

Zum Konfigurieren von QoS auf dem WAP-Gerät legen Sie Parameter für die Übertragungswarteschlangen für verschiedene WLAN-Verkehrstypen fest und geben minimale und maximale Wartezeiten für die Übertragung an.

Die WAP-EDCA-Parameter (Enhanced Distributed Channel Access) wirken sich auf den Datenfluss vom WAP-Gerät zur Clientstation aus. Die EDCA-Parameter für Stationen wirken sich auf den Datenfluss von der Clientstation zum WAP-Gerät aus.

Im Normalbetrieb ist es nicht notwendig, die EDCA-Standardwerte für das WAP-Gerät und die Stationen zu ändern. Änderungen dieser Werte wirken sich auf die bereitgestellte QoS aus.

So können Sie das WAP-Gerät und die EDCA-Parameter konfigurieren:

Schritt 1 Wählen Sie **Wireless > QoS** aus.

Schritt 2 Wählen Sie die Funkschnittstelle aus (**Funkmodul 1 oder Funkmodul 2**).

Schritt 3 Wählen Sie eine der folgenden Optionen aus der EDCA-Dropdownliste aus:

- **WFA-Standards**: Füllt die EDCA-Parameter für das WAP-Gerät und die Stationen mit Standardwerten der WiFi Alliance aus, die sich für allgemeine gemischte Daten am besten eignen.
- **Optimiert für Sprache**: Füllt die EDCA-Parameter für das WAP-Gerät und die Stationen mit optimierten Werten für Sprachdaten aus.

- **Benutzerdefiniert**: Ermöglicht die Auswahl benutzerdefinierter EDCA-Parameter.

Diese vier Warteschlangen werden für verschiedene Datentypen definiert, die vom WAP zu Stationen übertragen werden. Wenn Sie eine benutzerdefinierte Vorlage auswählen, können Sie die Parameter zum Definieren der Warteschlangen konfigurieren. Anderenfalls sind die Parameter auf für die Auswahl geeignete vordefinierte Werte festgelegt. Es handelt sich um die folgenden vier Warteschlangen:

- **Daten 0 (Sprache)**: Warteschlange mit hoher Priorität und minimaler Verzögerung. Zeitkritische Daten wie beispielsweise VoIP und Streaming-Medien werden automatisch an diese Warteschlange gesendet.
- **Daten 1 (Video)**: Warteschlange mit hoher Priorität und minimaler Verzögerung. Zeitkritische Videodaten werden automatisch an diese Warteschlange gesendet.
- **Daten 2 (Beste Leistung)**: Warteschlange mit mittlerer Priorität, mittlerem Durchsatz und mittlerer Verzögerung. Die meisten herkömmlichen IP-Daten werden an diese Warteschlange gesendet.
- **Daten 3 (Hintergrund)**: Warteschlange mit der niedrigsten Priorität und hohem Durchsatz. Massendaten, für die maximaler Durchsatz erforderlich ist und die nicht zeitkritisch sind (beispielsweise FTP-Daten), werden an diese Warteschlange gesendet.

Schritt 4 Markieren Sie das Kontrollkästchen **Aktivieren**, um Wi-Fi MultiMedia (WMM)-Erweiterungen zu aktivieren.

Wi-Fi MultiMedia (WMM): Dieses Feld ist standardmäßig aktiviert. Wenn WMM aktiviert ist, ist die QoS-Priorisierung und die Koordinierung des Zugriffs auf WLAN-Medien aktiviert. Wenn WMM aktiviert ist, steuern die QoS-Einstellungen für das WAP-Gerät den Downstream-Verkehrsfluss vom WAP-Gerät zur Clientstation (AP-EDCA-Parameter) und den Upstream-Verkehrsfluss von der Station zum AP (EDCA-Stationsparameter).

Durch Deaktivieren von WMM deaktivieren Sie die QoS-Steuerung der EDCA-Stationsparameter für den Upstream-Verkehrsfluss von der Station zum WAP-Gerät. Wenn WMM deaktiviert ist, können Sie dennoch einige Parameter für den Downstream-Verkehrsfluss vom WAP-Gerät zur Clientstation (AP-EDCA-Parameter) festlegen.

Schritt 5 Konfigurieren Sie die folgenden EDCA-Parameter und EDCA-Stationsparameter:

- **Arbitration Inter-Frame Space (AIFS)**: Die Wartezeit für Daten-Frames. Die Wartezeit wird in Positionen gemessen. Gültig sind AIFS-Werte von 1 bis 255.
- **Minimales Konfliktfenster**: Eine Eingabe für den Algorithmus, der die anfängliche zufällige Backoff-Wartezeit (Zeitfenster) für die Wiederholung nach einem Übertragungsfehler bestimmt.

  Dieser Wert stellt die obere Grenze (in Millisekunden) eines Bereichs dar, anhand dessen die anfängliche zufällige Backoff-Wartezeit bestimmt wird. Bei der ersten generierten Zufallszahl handelt es sich um eine Zahl zwischen 0 und der hier angegebenen Zahl. Wenn die erste zufällige Backoff-Wartezeit abläuft, bevor der Daten-Frame gesendet wurde, wird ein Wiederholungszähler erhöht, und der zufällige Backoff-Wert (Zeitfenster) wird verdoppelt. Die Verdoppelung wird fortgesetzt, bis die Größe des zufälligen Backoff-Werts die in "Maximum Contention Window" definierte Zahl erreicht hat.

  Gültige Werte sind 1, 3, 7, 15, 31, 63, 127, 255, 511 oder 1023. Dieser Wert muss höher sein als der Wert für das minimale Konfliktfenster.
- **Maximales Konfliktfenster**: Die obere Grenze (in Millisekunden) für die Verdoppelung des zufälligen Backoff-Werts. Die Verdoppelung wird fortgesetzt, bis der Daten-Frame gesendet wurde oder die in "Maximum Contention Window" angegebene Größe erreicht ist.

  Wenn die Größe von "Maximum Contention Window" erreicht ist, werden die Wiederholungen fortgesetzt, bis die maximale Anzahl der zulässigen Wiederholungen erreicht ist.

Gültige Werte sind 1, 3, 7, 15, 31, 63, 127, 255, 511 oder 1023. Dieser Wert muss höher sein als der Wert für das minimale Konfliktfenster.

- **Maximale Burst-Länge**: Ein EDCA-Parameter für WAPs, der nur für den Verkehrsfluss vom WAP zur Clientstation gilt.

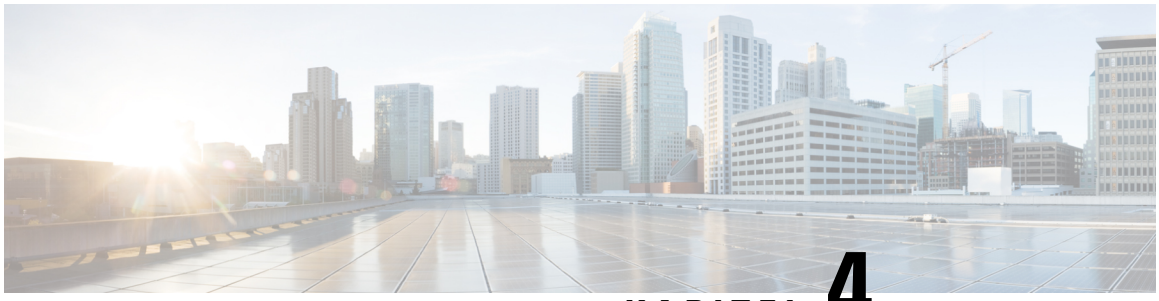
  Der Wert gibt die maximal zulässige Burst-Länge (in Millisekunden) für Paket-Bursts im WLAN an. Bei einem Paket-Burst handelt es sich um eine Sammlung von mehreren Frames, die ohne Header-Informationen übertragen werden. Durch den niedrigeren Aufwand ergeben sich ein höherer Durchsatz und eine bessere Leistung. Gültig sind Werte von 0,0 bis 999.

- **TXOP-Begrenzung (nur Station)**: Der TXOP-Grenzwert ist ein EDCA-Stationsparameter, der nur für den Verkehrsfluss von der Clientstation zum WAP-Gerät gilt. Bei TXOP (Transmission Opportunity) handelt es sich um ein in Millisekunden gemessenes Zeitintervall, in dem eine WME-Clientstation über das Recht verfügt, Übertragungen an das WLAN-Medium (WM) in Richtung des WAP-Geräts zu initiieren. Der Maximalwert für "TXOP Limit" lautet "65535".

Schritt 6 Konfigurieren Sie die folgenden zusätzlichen Einstellungen:

- **Keine Bestätigung**: Wählen Sie **Aktivieren** aus, um anzugeben, dass das WAP-Gerät Frames mit dem Dienstklassenwert „QosNoAck“ nicht bestätigen soll.
- **Ungeplanter automatischer Energiesparmodus (Unscheduled Automatic Power Save Delivery, APSD)**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um APSD zu aktivieren. APSD wird empfohlen, wenn VoIP-Telefone über das WAP-Gerät auf das Netzwerk zugreifen.

Schritt 7 Klicken Sie auf **Speichern**.



KAPITEL 4

WLAN-Bridge

In diesem Kapitel wird beschrieben, wie Sie die WLAN-Bridge-Einstellungen konfigurieren. Das Kapitel enthält die folgenden Themen:

WLAN-Bridge

Mithilfe von WDS (Wireless Distribution System) können Sie mehrere WAP-Geräte verbinden. Mit WDS können die WAP-Geräte drahtlos miteinander kommunizieren. Diese Funktion ermöglicht die nahtlose Verwendung von Roaming-Clients und die Verwaltung mehrerer WLANs. Sie können das WAP-Gerät abhängig von der Anzahl der herzustellenden Verbindungen im Point-to-Point- oder Point-to-Multipoint-Bridge-Modus konfigurieren.

Im Point-to-Point-Modus akzeptiert das WAP-Gerät Client-Zuordnungen und kommuniziert mit WLAN-Clients. Das WAP-Gerät leitet den gesamten für das andere Netzwerk gedachten Verkehr durch den zwischen den Access Points aufgebauten Tunnel. Die Hop-Zählung erhöht sich durch die Bridge nicht. Die Bridge fungiert als einfaches Netzwerkgerät auf der OSI-Schicht 2.

Im Point-to-Multipoint-Bridge-Modus fungiert ein WAP-Gerät als gemeinsame Verbindung zwischen mehreren Access Points. In diesem Modus akzeptiert das zentrale WAP-Gerät Client-Zuordnungen und kommuniziert mit den Clients und anderen Repeatern. Alle anderen Access Points werden nur dem zentralen WAP-Gerät zugeordnet, das die Pakete zu Routing-Zwecken an die entsprechende WLAN-Brücke weiterleitet.

Der WAP-Gerät kann auch als Repeater fungieren. In diesem Modus dient das WAP-Gerät als Verbindung zwischen zwei WAP-Geräten, die möglicherweise zu weit voneinander entfernt sind, um das Funksignal zu empfangen. Wenn das WAP-Gerät als Repeater eingesetzt wird, ist keine Kabelverbindung mit dem LAN erforderlich, und die Signale werden über die WLAN-Verbindung weitergesendet. Sie müssen keine besonderen Einstellungen konfigurieren, um das WAP-Gerät als Repeater zu verwenden, und es gibt keine Einstellungen für den Repeater-Modus. Die WLAN-Clients können mit einem als Repeater betriebenen WAP-Gerät nach wie vor Verbindungen herstellen.

Beachten Sie beim Konfigurieren von WDS im WAP-Gerät die folgenden Richtlinien:

- Alle an einer WDS-Verbindung beteiligten WAP-Geräte von Cisco müssen über die folgenden identischen Einstellungen verfügen:

- Funk
- IEEE 802.11 Mode
- Kanalbandbreite
- Channel (Auto wird nicht empfohlen.)

Wenn Sie Bridging im 802.11n-2,4-GHz-Band verwenden, legen Sie „Kanalbandbreite“ nicht auf den Standardwert „20/40 MHz“, sondern auf „20 MHz“ fest. Im 2,4-GHz-Band mit 20/40 MHz kann die Bandbreite im Betrieb von 40 MHz zu 20 MHz wechseln, wenn im Bereich WAP-Geräte mit 20 MHz erkannt werden. Wenn die Kanalbandbreite abweicht, kann das dazu führen, dass die Verbindung getrennt wird.

- Achten Sie bei Verwendung von WDS darauf, diese Funktion für beide an der WDS-Verbindung beteiligten WAP-Geräte zu konfigurieren.
- Zwischen einem WAP-Gerätepaar ist nur jeweils eine WDS-Verbindung möglich. Das heißt, eine Remote-MAC-Adresse kann auf der Seite "WDS" nur einmal pro WAP-Gerät angezeigt werden.

Konfigurieren einer WDS-Bridge

So konfigurieren Sie eine WDS-Bridge:

Schritt 1 Wählen Sie **WLAN-Bridge** aus.

Schritt 2 Wählen Sie **WDS** als Modus für die WLAN-Bridge aus.

Schritt 3 Klicken Sie auf **Aktivieren**, um einen WDS-Port in den WDS-Einstellungen zu aktivieren.

Schritt 4 Konfigurieren Sie die übrigen Parameter:

- **Funk**: Legt die ID des Funkmoduls fest (Funkmodul 1 (2,4 GHz) oder Funkmodul 2 (5 GHz).
- **Lokale MAC-Adresse**: Die physische oder MAC-Adresse des aktuellen oder lokalen WAP-Geräts, an das die Daten übertragen werden.
- **Remote-MAC-Adresse**: Die MAC-Adresse des WAP-Zielgeräts. Sie finden die MAC-Adresse auf der Seite „Überwachung > Dashboard > WLAN“.
- **Verschlüsselung**: Wählen Sie den Verschlüsselungstyp für die WDS-Verbindung aus (**Kein, Static WEP oder WPA Personal**).

  Wenn Sie keine Sicherheitsprobleme für die WDS-Verbindung befürchten, können Sie auch wahlweise keinen Verschlüsselungstyp festlegen. Wenn Sie Sicherheitsbedenken haben, können Sie zwischen „Static WEP“ und „WPA Personal“ auswählen. Im Modus "WPA Personal" verwendet das WAP-Gerät WPA2-PSK mit CCMP-Verschlüsselung (AES) über die WDS-Verbindung. Weitere Verschlüsselungsoptionen finden Sie unter WPA/PSK für WDS-Verbindungen, auf Seite 63.

Schritt 5 Wiederholen Sie diese Schritte für bis zu vier WDS-Schnittstellen.

Schritt 6 Klicken Sie auf **Speichern**.

Schritt 7 Wiederholen Sie diese Schritte für alle Geräte, die sich mit der Bridge verbinden.

Hinweis Auf der Seite **Überwachung** > **Dashboard** > **WLAN** können Sie überprüfen, ob die Bridge-Verbindung aktiv ist. In der Tabelle „Schnittstellenstatus“ sollte für WDS(x) der Status **Up** angezeigt werden.

WEP für WDS-Verbindungen

Diese zusätzlichen Felder werden angezeigt, wenn Sie den Verschlüsselungstyp WEP auswählen.

- **Schlüssellänge**: Wenn WEP aktiviert ist, geben Sie 64 Bit oder 128 Bit für die Länge des WEP-Schlüssels an.
- **Schlüsseltyp**: Wenn WEP aktiviert ist, wählen Sie entweder **ASCII** oder **Hex** als Schlüsseltyp aus.
- **WEP-Schlüssel**: Wenn Sie **ASCII** ausgewählt haben, geben Sie eine beliebige Kombination aus 0 bis 9, a bis z und A bis Z ein. Wenn Sie **Hex** ausgewählt haben, geben Sie hexadezimale Ziffern ein (eine beliebige Kombination aus 0 bis 9 und a bis f oder A bis F). Dabei handelt es sich um die RC4-Verschlüsselungsschlüssel, die gemeinsam mit den Stationen genutzt werden, die das WAP-Gerät verwenden.

  Beachten Sie, dass die erforderliche Zeichenanzahl rechts neben dem Feld angegeben ist und sich abhängig von der Auswahl in den Feldern Schlüsseltyp und Schlüssellänge ändert.

WPA/PSK für WDS-Verbindungen

Diese zusätzlichen Felder werden angezeigt, wenn Sie den Verschlüsselungstyp WPA/PSK auswählen:

- **WDS-ID**: Geben Sie einen Namen für die neu erstellte WDS-Verbindung ein. Wichtig ist, dass Sie am anderen Ende der WDS-Verbindung die gleiche WDS-ID eingeben. Wenn die WDS-ID nicht bei beiden WAP-Geräten in der WDS-Verbindung gleich ist, können die Geräte nicht kommunizieren und Daten austauschen.

  Die WDS-ID kann eine beliebige Kombination aus alphanumerischen Zeichen sein.
- **Schlüssel**: Geben Sie einen eindeutigen gemeinsamen Schlüssel für die WDS-Bridge ein. Diesen eindeutigen gemeinsamen Schlüssel müssen Sie auch für das WAP-Gerät am andere Ende der WDS-Verbindung eingeben. Wenn der Schlüssel nicht bei beiden WAPs gleich ist, können die Geräte nicht kommunizieren und Daten austauschen.

  Beim WPA-PSK-Schlüssel handelt es sich um eine Zeichenfolge mit mindestens 8 und maximal 63 Zeichen. Zulässig sind Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen wie @ und #.

Work Group Bridge

Mithilfe der Work Group Bridge-Funktion kann das WAP-Gerät die Zugriffsmöglichkeiten in einem Remotenetzwerk erweitern. Im Work Group Bridge-Modus fungiert das WAP-Gerät im WLAN als WLAN-Station (STA). Es kann Verkehr zwischen einem drahtgebundenen Remotenetzwerk oder zugeordneten WLAN-Clients und dem im Work Group Bridge-Modus verbundenen WLAN überbrücken.

Die Work Group Bridge-Funktion ermöglicht die Unterstützung des gleichzeitigen Betriebs im STA-Modus und im AP-Modus. Das WAP-Gerät kann in einem BSS (Basic Service Set) als STA-Gerät und in einem anderen BSS als WAP-Gerät betrieben werden. Wenn der Work Group Bridge-Modus aktiviert ist, unterstützt das WAP-Gerät nur einen BSS für zugeordnete WLAN-Clients und einen anderen BSS, dem das WAP-Gerät als WLAN-Client zugeordnet wird.

Wir empfehlen, dass Sie den Work Group Bridge-Modus nur dann verwenden, wenn die WDS-Bridge-Funktion nicht mit einem Peer-WAP-Gerät betrieben werden kann. WDS ist als bessere Lösung der Work Group Bridge-Lösung vorzuziehen. Verwenden Sie WDS, wenn Sie Cisco WAP150- und WAP361-Geräte überbrücken. Ziehen Sie anderenfalls den Work Group Bridge-Modus in Betracht. Wenn die Work Group Bridge-Funktion aktiviert ist, wird anstelle der VAP-Konfigurationen nur die Work Group Bridge-Konfiguration angewendet.

Hinweis Die WDS-Funktion kann nicht verwendet werden, wenn der Work Group Bridge-Modus für das WAP-Gerät aktiviert ist.

Im Work Group Bridge-Modus wird der vom WAP-Gerät im WAP-Gerätemodus verwaltete BSS als Access Point-Schnittstelle bezeichnet, und die zugeordneten STAs werden als Downstream-STAs bezeichnet. Der vom anderen WAP-Gerät (dem WAP-Gerät, dem das WAP-Gerät als STA zugeordnet wird) verwaltete BSS wird als Infrastrukturclient-Schnittstelle bezeichnet, und das andere WAP-Gerät wird als Upstream-AP bezeichnet.

Die mit der drahtgebundenen Schnittstelle des WAP-Geräts verbundenen Geräte sowie die der Access Point-Schnittstelle des Geräts zugeordneten Downstream-Stationen können auf das über die Infrastrukturclient-Schnittstelle verbundene Netzwerk zugreifen. Damit Pakete überbrückt werden können, muss die VLAN-Konfiguration für die Access Point-Schnittstelle und die drahtgebundene Schnittstelle der der Infrastrukturclient-Schnittstelle entsprechen.

Sie können den Work Group Bridge-Modus zum Erweitern der Reichweite verwenden, um den Zugriff auf Remotenetzwerke oder schwer erreichbare Netzwerke über den BSS zu ermöglichen. Sie können ein einziges Funkmodul für die Weiterleitung von Paketen von zugeordneten STAs an andere WAP-Geräte im gleichen ESS konfigurieren, ohne WDS zu verwenden.

Beachten Sie beim Konfigurieren der **Work Group Bridge** auf dem WAP-Gerät die folgenden Berichte:

- Alle an der Work Group Bridge beteiligten WAP-Geräte müssen über die folgenden identischen Einstellungen verfügen:
  - Funk
  - IEEE 802.11 Mode
  - Kanalbandbreite
  - Channel (Auto wird nicht empfohlen.)

  Weitere Informationen zum Konfigurieren dieser Einstellungen finden Sie unter Funk, auf Seite 41 (Basiseinstellungen).
- Im Work Group Bridge-Modus wird zurzeit nur IPv4-Verkehr unterstützt.
- In einem Single Point Setup wird der Work Group Bridge-Modus nicht unterstützt.

So konfigurieren Sie den Work Group Bridge-Modus:

Schritt 1 Wählen Sie **WLAN-Bridge** aus.

Schritt 2 Klicken Sie auf **WorkGroup**.

Schritt 3 Wählen Sie den WGB-Port aus, für den die Konfigurationsparameter gelten sollen.

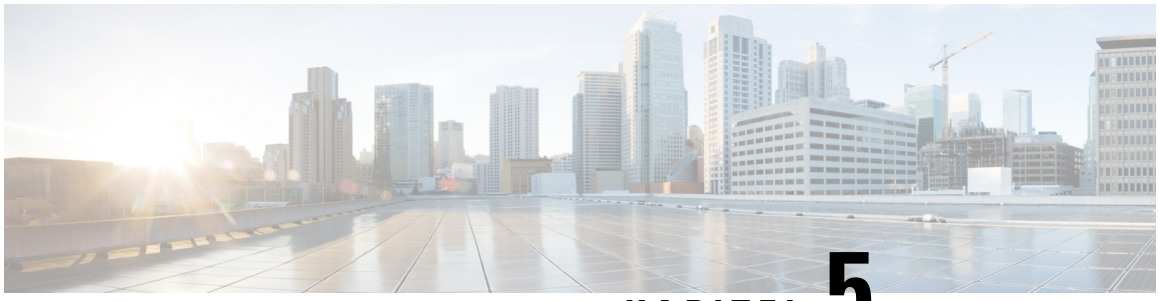
Schritt 4 Klicken Sie auf **Bearbeiten**, um die folgenden Parameter für die Infrastrukturclient-Schnittstelle zu konfigurieren (Uplink/Downlink):

Tabelle 1: Infrastrukturclient-Schnittstelle (Uplink/Downlink):

WGB-Port	Uplink	Downlink
Aktiviert	Aktivieren Sie das Kontrollkästchen, um die Infrastrukturclient-Schnittstelle zu aktivieren.	Aktivieren Sie das Kontrollkästchen, um die Infrastrukturclient-Schnittstelle zu aktivieren.
Funk	Gibt die ID des Funkmoduls an (Funkmodul 1 (2,4 GHz) oder Funkmodul 2 (5 GHz)).	Gibt die ID des Funkmoduls an (Funkmodul 1 (2,4 GHz) oder Funkmodul 2 (5 GHz)).
SSID	Gibt die aktuelle SSID des BSS an. **Hinweis** Unter „SSID Scanning“ befindet sich ein Pfeil neben SSID. Diese Funktion ist standardmäßig deaktiviert und wird nur aktiviert, wenn unter „Rogue-AP-Erkennung“ (ebenfalls standardmäßig deaktiviert) die Option „AP-Erkennung“ aktiviert ist.	Die SSID für die Access Point-Schnittstelle muss nicht mit der für den Infrastrukturclient übereinstimmen.
Verschlüsselung	Der Typ der Sicherheit, die für die Authentifizierung als Clientstation für das Upstream-WAP-Gerät verwendet werden soll. Es kann sich dabei um Folgendes handeln: • **Kein** • **Static WEP** • **WPA Personal** • **WPA Enterprise**	Der Typ der für die Authentifizierung zu verwendenden Sicherheit. Folgende Optionen sind verfügbar: • **Kein** • **WPA Personal** • **Static WEP**
Verbindungsstatus	Gibt an, ob der WAP mit dem Upstream-WAP-Gerät verbunden ist.	Nicht zutreffend (N/A)
VLAN-ID	Das dem BSS zugeordnete VLAN.	Konfigurieren Sie die Access Point-Schnittstelle mit der gleichen VLAN-ID, die an der Infrastrukturclient-Schnittstelle angekündigt wird.

WGB-Port	Uplink	Downlink
Hinweis Die Infrastrukturclient-Schnittstelle wird dem Upstream-WAP-Gerät mit den konfigurierten Anmeldeinformationen zugeordnet. Das WAP-Gerät kann seine IP-Adresse von einem DHCP-Server über die Upstream-Verbindung beziehen. Alternativ können Sie eine statische IP-Adresse zuweisen.		
SSID-Broadcast	Gibt an, ob der Broadcast der SSID verfügbar, aktiviert oder deaktiviert ist.	Wählen Sie dies aus, wenn die Downstream-SSID übertragen werden soll. Standardmäßig sind SSID-Broadcasts aktiviert.
Clientfilter	Nicht zutreffend (N/A)	Wählen Sie eine der folgenden Optionen aus: • Deaktiviert: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist nicht auf die in einer MAC-Adressenliste angegebenen Clients beschränkt. • Local: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist auf die in einer lokal definierten MAC-Adressenliste angegebenen Clients beschränkt. • RADIUS: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist auf die in einer MAC-Adressenliste auf einem RADIUS-Server angegebenen Clients beschränkt.
Hinweis Wenn Sie „Local“ oder „RADIUS“ auswählen, finden Sie unter Clientfilter Anweisungen zum Erstellen der Client-Filterliste.		

Schritt 5 Klicken Sie auf **Speichern**. Die zugeordneten Downstream-Clients verfügen jetzt über Konnektivität mit dem Upstream-Netzwerk.



KAPITEL 5

Schnelle Serverspeicherung

In diesem Kapitel wird beschrieben, wie Sie die Einstellungen für die schnelle Serverspeicherung konfigurieren. Das Kapitel enthält die folgenden Themen:

Schnelle Serverspeicherung

Die schnelle Serverspeicherung, auch bekannt als IEEE 802.11r oder schneller BSS-Übergang, ermöglicht schnelles *Roaming* für Clientgeräte in Umgebungen mit WPA2 Enterprise-Sicherheit, indem sichergestellt wird, dass sich das Clientgerät nicht bei jedem Wechsel des Access Points erneut beim RADIUS-Server authentifizieren muss.

Die schnelle Serverspeicherung ist eine Ergänzung des IEEE 802.11-Standards und ermöglicht permanente Konnektivität für mobile WLAN-Geräte mit schneller, nahtloser und sicherer Übergabe zwischen verwalteten APs. Für optimale Sprachqualität und Netzwerksicherheit muss die tragbare Station in der Lage sein, beim Roaming zwischen APs, die sonstigen Datenverkehr verwalten, einen sicheren Sprachanruf mit niedriger Latenz aufrechtzuerhalten.

Dieses Gerät unterstützt den in 802.11r definierten schnellen BSS-Übergang für die schnelle Übergabe mit WPA2 Enterprise-Sicherheit. Für Sprache über WLAN Enterprise wird nur eine Teilmenge der in 802.11r definierten Funktionen unterstützt. Der schnelle BSS-Übergang reduziert die Latenz beim Roaming.

Dieser Übergang wird pro VAP und pro Funkmodul aktiviert.

Hinweis Bevor Sie den schnellen BSS-Übergang auf einem VAP konfigurieren, müssen Sie sicherstellen, dass auf dem VAP die WPA2-Sicherheit konfiguriert und Vorauthentifizierung sowie MFP deaktiviert sind.

Konfigurieren der schnellen Serverspeicherung

Diese Schritte dienen als allgemeine Beschreibung für das Konfigurieren der schnellen Serverspeicherung:

Schritt 1 Wählen Sie **Schnelle Serverspeicherung > Roaming-Tabelle** aus.

Schritt 2 Klicken Sie auf □, um eine neue Zeile zur Roaming-Tabelle hinzuzufügen.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **Aktivieren**: Diese Option ist standardmäßig aktiviert.
- **BSSID** — Wählen Sie den VAP (**2,4 G VAP 0** oder **5 G VAP 0**) aus, den Sie aktivieren möchten.
- **Mobilitätsdomäne**: Gibt den Bezeichner der Mobilitätsdomäne (Mobility Domain identifier, MDID) des FBT VAP an. Der MDID bezeichnet eine Gruppe von APs in einem ESS, zwischen denen ein STA schnelle BSS-Übergangsdienste verwenden kann. Schnelle BSS-Übergänge sind nur zwischen APs möglich, die denselben MDID haben und sich im gleichen ESS befinden. Schnelle BSS-Übergänge zwischen APs mit unterschiedlichen MDIDs oder in unterschiedlichen ESS sind nicht möglich.
- **FT-Modus**: Mit dem Protokoll für schnelle Übergänge können sich Mobilstationen (MS) mit dem ersten AP in der Domäne (die Gruppe von APs, die das FT-Protokoll unterstützen und über das Distributionssystem (DS) verbunden sind) vollständig authentifizieren und für die nächsten APs in derselben Domäne einen schnelleren Zuordnungsprozess verwenden. Wählen sie eine der folgenden FT-Methoden aus:
  - **Funkgesteuert**: Im funkgesteuerten Modus kommuniziert die Mobilstation über eine direkte 802.11-Verbindung mit dem neuen AP.
  - **Über DS**: In diesem Modus kommuniziert die MS über den alten AP mit dem neuen AP.
- **R0-Schlüsselinhaber**: Gibt den NAS-Bezeichner an, der in der RADIUS-Zugriffsanfrage gesendet werden soll. Der NAS-Bezeichner wird als ID des R0-Schlüsselinhabers verwendet.
- **R1-Schlüsselinhaber**: Gibt die ID des R1-Schlüsselinhabers an, der den Träger von PMK-R1 im Authenticator benennt.
- **Liste der Remoteschlüsselinhaber**: Wählen Sie eine zuvor erstellte Liste der Remoteschlüsselinhaber im Dropdownmenü aus.

Schritt 4 Klicken Sie auf **Speichern**.

Hinweis Um eine Roamingeinstellung zu löschen oder zu bearbeiten, wählen Sie die Einstellung aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Konfigurieren Sie die FBT-Einstellungen, und klicken Sie auf **Speichern**, um die Änderungen zu speichern. Änderungen an bestimmten Einstellungen führen dazu, dass der AP Systemprozesse beendet und neu startet. In diesem Fall werden die Verbindungen der WLAN-Clients vorübergehend unterbrochen. Ändern Sie die AP-Einstellungen nach Möglichkeit, wenn der WLAN-Datenverkehr gering ist.

Konfigurieren von Listenprofilen für Remoteschlüsselinhaber

So können Sie die Listenprofile für R0-Schlüsselinhaber konfigurieren:

Schritt 1 Wählen Sie **Schnelle Serverspeicherung > Listenprofil für Remoteschlüsselinhaber** aus.

Schritt 2 Klicken Sie auf □, um ein neues Profil hinzuzufügen, oder auf **Bearbeiten**, um ein vorhandenes Profil zu bearbeiten. Die Seite **Listenprofile für Remoteschlüsselinhaber** wird geöffnet.

Schritt 3 Geben Sie einen Namen für das Listenprofil für Remoteschlüsselinhaber ein.

Schritt 4 Konfigurieren Sie die folgenden Parameter: Pro VAP können maximal 10 Einträge für R0-Schlüsselinhaber konfiguriert werden.

- **MAC-Adresse**: Geben Sie die VAP MAC-Zieladresse ein, bei der es sich um den R0-Schlüsselinhaber handelt. Die „RRB PULL"-Nachricht wird an diese AP MAC-Adresse gesendet, um den PMKR1-Schlüssel abzurufen. Diese MAC-Adresse muss unter allen VAPs eindeutig sein.
- **NAS-ID**: Die auf dem FBT-fähigen Ziel-VAP konfigurierte NAS-ID.
- **RRB-Schlüssel**: Der Schlüssel, der zum Verschlüsseln von RRM-Protokollnachrichten verwendet wird.

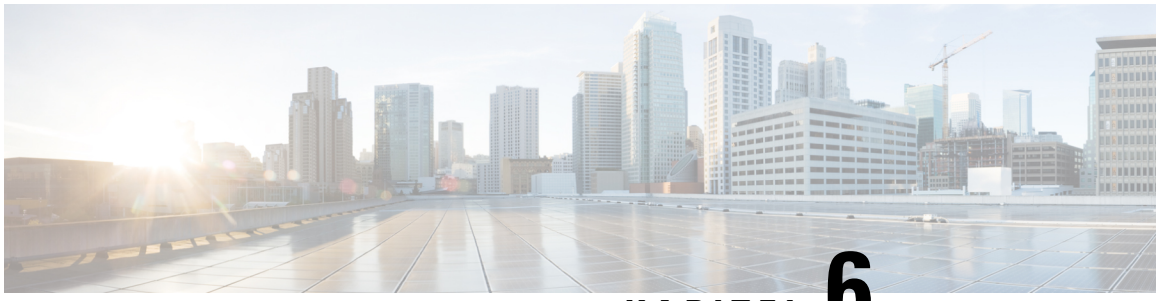
Schritt 5 Wiederholen sie die Schritte 1 bis 4 und konfigurieren Sie anschließend den R1-Schlüsselinhaber in der Liste der R1-Schlüsselinhaber. Pro VAP können maximal 10 Einträge für R1-Schlüsselinhaber konfiguriert werden. Die Daten der Schlüsselinhaber werden pro VAP konfiguriert.

- **MAC-Adresse**: Die VAP MAC-Zieladresse, bei der es sich um den R1-Schlüsselinhaber handelt. Der PMKR1 wird in der „RRB PUSH"-Nachricht an diese AP MAC-Adresse gesendet. Diese MAC-Adresse muss unter allen VAPs eindeutig sein.
- **R1-Schlüsselinhaber**: Die ID des R1-Schlüsselinhabers, der den Träger von PMK-R1 im Authenticator benennt.
- **RRB-Schlüssel**: Der Schlüssel, der zum Verschlüsseln von RRM-Protokollnachrichten verwendet wird.

Hinweis Nachdem Sie die Einstellungen für die Liste der Remoteschlüsselinhaber konfiguriert haben, können Sie auf **Wiederherstellen** klicken, um die alten Einstellungen wiederherzustellen, oder auf **Speichern**, um die Einstellungen zu speichern. Klicken Sie auf **Abbrechen**, um zur Seite vor **Schnelle Serverspeicherung** zurückzukehren.

Klicken Sie auf **Speichern**, nachdem Sie ein Profil kopiert oder gelöscht haben.

Vorsicht Klicken Sie auf **Exportieren** für ausgewählte Profile, um nur diese Profile zu exportieren. Klicken Sie auf **Exportieren**, ohne ein Profil auszuwählen, um alle Profile zu **exportieren**.



KAPITEL 6

Single Point Setup

In diesem Kapitel wird beschrieben, wie Sie Single Point Setup für mehrere WAP-Geräte konfigurieren. Das Kapitel enthält die folgenden Themen:

Single Point Setup – Übersicht

Mit Single Point Setup können Sie WLAN-Dienste für mehrere Geräte zentral verwalten und steuern. Sie erstellen mit Single Point Setup eine einzelne Gruppe oder einen Cluster aus WLAN-Geräten. Wenn die WAP-Geräte in einem Cluster gruppiert sind, können Sie das WLAN als eine einzige Entität anzeigen, bereitstellen, konfigurieren und schützen. Nach der Erstellung eines WLAN-Clusters erleichtert Single Point Setup außerdem die Kanalplanung für alle WLAN-Geräte, sodass Sie im WLAN Funkinterferenzen verringern und die Bandbreite maximieren können.

Bei der Ersteinrichtung des WAP-Geräts können Sie mithilfe des Einrichtungsassistenten Single Point Setup konfigurieren oder einem vorhandenen Single Point Setup beitreten. Wenn Sie den Einrichtungsassistenten nicht verwenden möchten, können Sie das webbasierte Konfigurationsdienstprogramm verwenden.

Verwalten von Single Point Setup für mehrere Access Points

Mit Single Point Setup erstellen Sie einen dynamischen, konfigurationsbasierten Cluster oder eine Gruppe von WAP-Geräten im gleichen Subnetz eines Netzwerks. Ein Cluster unterstützt eine Gruppe von bis zu 16 konfigurierten WAP581-Geräten, jedoch keine anderen Modelle als WAP581 im selben Cluster.

Single Point Setup ermöglicht die Verwaltung mehrerer Cluster im gleichen Subnetz oder Netzwerk, die jedoch als einzelne unabhängige Entitäten verwaltet werden. Die folgende Tabelle enthält die Einschränkungen für Wireless-Services in einem Single Point Setup:

Tabelle 2: Wireless-Service-Einschränkungen in einem Single Point Setup

Gruppentyp/Clustertyp	WAP-Geräte pro Single Point Setup	Anzahl der aktiven Clients pro Single Point Setup	Maximale Anzahl der Clients (aktiv und im Leerlauf)
Cisco WAP581	16	960 für das WAP581 mit zwei Funkmodulen	2048 für das WAP581 mit zwei Funkmodulen

In einem Cluster können Konfigurationsinformationen wie VAP-Einstellungen, QoS-Warteschlangenparameter und Funkparameter verbreitet werden. Wenn Sie Single Point Setup für ein Gerät konfigurieren, werden die Einstellungen des Geräts (manuell festgelegte Einstellungen ebenso wie Standardeinstellungen) an andere dem Cluster beitretende Geräte verbreitet.

Vergewissern Sie sich beim Bilden eines Clusters, dass die folgenden Voraussetzungen oder Bedingungen erfüllt sind:

Schritt 1 Planen Sie den Single Point Setup-Cluster. Die zwei oder mehr WAP-Geräte, die Sie in einem Cluster anordnen möchten, müssen vom gleichen Modell sein. Beispielsweise können Cisco WAP581-Geräte nur mit anderen Cisco WAP581-Geräten geclustert werden.

Hinweis Es wird dringend empfohlen, auf allen WAP-Geräten im Cluster die neueste Firmwareversion auszuführen. Firmwareupgrades werden nicht an alle WAP-Geräte in einem Cluster verbreitet. Sie müssen jedes Gerät einzeln aktualisieren.

Schritt 2 Richten Sie die WAP-Geräte ein, die im gleichen IP-Subnetz in einem Cluster angeordnet werden sollen. Vergewissern Sie sich, dass die Geräte miteinander verbunden sind und dass der Zugriff auf die Geräte über das LAN dieses Switches möglich ist.

Schritt 3 Aktivieren Sie Single Point Setup für alle WAP-Geräte. Weitere Informationen finden Sie unter Access Points.

Schritt 4 Vergewissern Sie sich, dass alle WAP-Geräte auf den gleichen Single Point Setup-Namen verweisen. Weitere Informationen finden Sie unter Access Points.

Single Point Setup-Aushandlung

Wenn ein AP für Single Point Setup aktiviert und konfiguriert ist, beginnt das Gerät, regelmäßig alle zehn Sekunden sein Vorhandensein anzukündigen. Wenn andere WAP-Geräte vorhanden sind, die den Kriterien für den Cluster entsprechen, beginnt die Vermittlung. Dabei wird bestimmt, welches WAP-Gerät die Masterkonfiguration an die übrigen Mitglieder des Clusters verteilt.

Für die Bildung von Single Point Setup-Clustern und die Vermittlung gelten die folgenden Regeln:

- Wenn der Administrator die Konfiguration eines Mitglieds eines vorhandenen Single Point Setup-Clusters aktualisiert, wird die Konfigurationsänderung an alle Mitglieder des Clusters verbreitet, und das konfigurierte WAP-Gerät übernimmt die Steuerung des Clusters.
- Wenn zwei separate Single Point Setup-Cluster einem einzigen Cluster beitreten, erhält der zuletzt geänderte Cluster bei der Konfigurationsvermittlung den Vorrang und überschreibt und aktualisiert die Konfiguration aller WAP-Geräte im Cluster.

- Wenn ein WAP-Gerät im Cluster länger als 60 Sekunden keine Ankündigungen von einem WAP-Gerät erhält (beispielsweise aufgrund eines Konnektivitätsverlusts zwischen dem Gerät und anderen Geräten im Cluster), wird das Gerät aus dem Cluster entfernt.
- Bei einem Konnektivitätsverlust eines WAP-Geräts im Single Point Setup-Modus wird das Gerät nicht sofort aus dem Cluster gelöscht. Wenn die Konnektivität wiederhergestellt wird, das Gerät dem Cluster beitritt, ohne gelöscht worden zu sein, und während des Zeitraums ohne Konnektivität Konfigurationsänderungen an diesem Gerät vorgenommen wurden, werden die Änderungen an die anderen Clustermitglieder verbreitet, sobald die Konnektivität wiederhergestellt ist.
- Wenn bei einem WAP-Gerät in einem Cluster ein Konnektivitätsverlust auftritt, das Gerät gelöscht wird, später wieder dem Cluster beitritt und während des Zeitraums ohne Konnektivität Konfigurationsänderungen an diesem Gerät vorgenommen wurden, werden die Änderungen beim erneuten Beitritt an das Gerät verbreitet. Wenn sowohl am getrennten Gerät als auch am Cluster Konfigurationsänderungen vorgenommen wurden, wird das Gerät mit den meisten Änderungen und dann das Gerät mit der neuesten Änderung ausgewählt, um seine Konfiguration an den Cluster zu verbreiten. (Das heißt, wenn WAP1 mehr Änderungen aufweist, während WAP2 über die neueste Änderung verfügt, wird WAP1 ausgewählt. Wenn beide Geräte gleich viele Änderungen aufweisen und WAP2 die neueste Änderung hat, wird WAP2 ausgewählt.)

Funktionsweise eines aus einem Single Point Setup gelöschten Geräts

Wenn ein WAP-Gerät, das zuvor Mitglied eines Clusters war, vom Cluster getrennt wird, gelten die folgenden Richtlinien:

- Aufgrund des Verlusts der Verbindung mit dem Cluster erhält das WAP-Gerät nicht die neuesten Konfigurationseinstellungen für den Betrieb. Die Trennung führt dazu, dass der nahtlose WLAN-Dienst im Produktionsnetzwerk nicht mehr ordnungsgemäß funktioniert.
- Das WAP-Gerät wird weiter mit den letzten vom Cluster empfangenen WLAN-Parametern betrieben.
- Dem nicht im Cluster enthaltenen WAP-Gerät zugeordnete WLAN-Clients sind ohne Unterbrechung der WLAN-Verbindung weiterhin dem Gerät zugeordnet. Der Verlust der Verbindung mit dem Cluster verhindert also nicht, dass dem WAP-Gerät zugeordnete WLAN-Clients weiterhin auf Netzwerkressourcen zugreifen können.
- Wenn der Verlust der Verbindung mit dem Cluster auf eine physische oder logische Trennung von der LAN-Infrastruktur zurückzuführen ist, sind je nach Art des Fehlers möglicherweise Netzwerkdienste für die WLAN-Clients betroffen.

An Single Point Setup-Access Points verbreitete und nicht verbreitete Konfigurationsparameter

Die folgende Tabelle fasst die Konfigurationen zusammen, die von allen WAP-Geräten im Cluster gemeinsam genutzt und verbreitet werden.

Tabelle 3: Verbreitete und nicht verbreitete Konfigurationsparameter

Allgemeine Konfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
Zugriffssteuerung	Password Complexity

Allgemeine Konfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
Client-QoS	User Accounts
E-Mail-Warnung	QoS
HTTP/HTTP-Service (Ausnahme: Konfiguration mit SSL-Zertifikaten)	Funkeinstellungen inklusive TSpec-Einstellungen (mit Ausnahmen)
Protokolleinstellungen	Rogue-AP-Erkennung
Clientfilter	Planungsmodul
Verwaltungszugangskontrolle	SNMP und SNMPv3
Netzwerke	WPA-PSK-Komplexität
Time Settings	Umbrella
Funkkonfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
WLAN-Modus	
Fragmentation Threshold	
RTS Threshold	
Ratensätze	
Kanal	
Schutz	
Feste Multicast-Rate	
Broadcast or Multicast Rate Limiting	
Frequenzband	
Kurzes Schutzintervall unterstützt	
Funkkonfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden	
Kanal	
Beacon-Intervall	
DTIM-Periode	
Maximum Stations	
Sendeleistung	
Andere Konfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden	
Auslastungsschwellenwert	Port-Einstellungen

Allgemeine Konfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
Bonjour	VLAN und IPv4
IPv6-Adresse	Bridge
IPv6 Tunnel	Paketerfassung

Access Points

Auf der Seite **Access Points** können Sie Single Point Setup für ein WAP-Gerät aktivieren oder deaktivieren, die Cluster-Mitglieder anzeigen und den Standort und den Cluster-Namen eines Mitglieds konfigurieren. Außerdem können Sie auf die IP-Adresse eines Mitglieds klicken, um das Gerät zu konfigurieren und seine Daten anzuzeigen.

Konfigurieren des WAP-Geräts für Single Point Setup

So konfigurieren Sie den Standort und den Namen eines einzelnen Single Point Setup-Cluster-Mitglieds:

Schritt 1 Wählen Sie **Single Point Setup** > **Access Points** aus.

Single Point Setup ist auf dem WAP-Gerät standardmäßig deaktiviert. Wenn die Option deaktiviert ist, wird die Schaltfläche „Single Point Setup aktivieren“ angezeigt.

Schritt 2 Konfigurieren Sie die folgenden Parameter für alle Mitglieder eines Single Point Setup-Clusters:

- **AP-Standort**: Geben Sie eine Beschreibung für den physischen Standort des WAP-Geräts ein, beispielsweise „Rezeption“. Das Feld für den Standort ist optional. Gültig sind Werte mit 1 bis 64 alphanumerischen Zeichen und Sonderzeichen.
- **AP-Priorität**: Geben Sie die Priorität des Clusters für die Wahl des dominanten AP (Cluster-Controller) ein.
- **Clustername für den Beitritt**: Geben Sie den Namen des Clusters ein, dem das WAP-Gerät beitreten soll, beispielsweise „Rezeption_Cluster“. Der Clustername wird nicht an andere WAP-Geräte gesendet. Sie müssen für alle Mitgliedsgeräte den gleichen Namen konfigurieren. Der Clustername muss für jedes im Netzwerk konfigurierte Single Point Setup eindeutig sein. Der Standardwert lautet "ciscosb-cluster". Gültig sind Werte mit 1 bis 64 alphanumerischen Zeichen und Sonderzeichen.

  Eine höhere Nummer gibt an, dass dieser AP mit einer höheren Priorität als dominanter AP bestimmt wird. Bei einem Gleichstandergebnis wird die niedrigste MAC-Adresse dominant. Bereich: 0 bis 255. Der Standardwert ist 0.
- **Clustering-IP-Protokoll**: Wählen Sie die IP-Version aus, die von den WAP-Geräten im Cluster für die Kommunikation mit anderen Mitgliedern des Clusters verwendet wird. Der Standardwert lautet "IPv4".
- Wenn Sie IPv6 auswählen, kann für Single Point Setup die Link Local-Adresse, die automatisch konfigurierte globale IPv6-Adresse und die statisch konfigurierte globale IPv6-Adresse verwendet werden. Stellen Sie bei Verwendung von IPv6 sicher, dass alle WAP-Geräte im Cluster nur Link Local-Adressen oder nur globale Adressen verwenden.

Single Point Setup kann nur für WAP-Geräte verwendet werden, die den gleichen IP-Adressierungstyp verwenden. Die Funktion kann nicht für eine Gruppe von WAP-Geräten verwendet werden, die teilweise IPv4-Adressen und teilweise IPv6-Adressen haben.

Das WAP-Gerät sucht nun nach anderen WAP-Geräten im Subnetz, die mit dem gleichen Cluster-Namen und dem gleichen IP-Protokoll konfiguriert sind. Ein potenzielles Cluster-Mitglied kündigt sein Vorhandensein alle zehn Sekunden an.

Schritt 3 Konfigurieren Sie die Cluster-Management-Adresse:

Cluster-Management-Adresse: Um mit einer einzigen IP auf das Cluster zugreifen zu können. Das Cluster kann mit einer optionalen Cluster-IPv4-Adresse konfiguriert werden. Dies ist Teil der globalen Konfiguration des Clusters im entsprechenden Bereich. Diese Option muss vom Cluster-Administrator statisch konfiguriert werden. Die Management-IP-Adresse des Clusters muss demselben Subnetz wie die Cluster-Management-IP-Adressen des APs angehören. Die Cluster-IP-Adresse wird als sekundäre IP-Adresse für die Management-Schnittstellen des dominanten AP konfiguriert. Die Benutzeroberfläche für den dominanten AP ist unter der Cluster-IP-Adresse erreichbar. Wenn die Cluster-IP-Adresse als sekundäre IP-Adresse auf dem dominanten AP festgelegt ist, werden regelmäßige ARPs im Management-VLAN verschickt, um die Zuordnung zwischen der neuen IP-Adresse und der MAC-Adresse im Subnetz einrichten zu können. Die Konfiguration der Cluster-IP-Adresse wird zwischen allen Cluster-APs geteilt.

Schritt 4 Klicken Sie auf **Speichern**.

Schritt 5 Wiederholen Sie diese Schritte für weitere WAP-Geräte, die Sie Single Point Setup hinzufügen möchten.

Firmwareverwaltung

Cluster bieten eine zentrale Funktion für Cluster-Firmware-Upgrades, mit der alle APs im Cluster über den dominanten AP (Cluster-Controller) aktualisiert werden können. Das Cluster-Firmware-Upgrade kann nur über den dominanten AP durchgeführt werden.

Auf der Seite „Cluster-Firmware-Upgrade“ werden die erkannten WAP-Geräte in einer Tabelle aufgeführt. Die folgenden Informationen werden angezeigt:

- **Standort**: Beschreibung des physischen Standorts des Access Points
- **IP-Adresse**: Die IP-Adresse für den Access Point
- **MAC-Adresse**: Die MAC-Adresse (Media Access Control, Medienzugriffssteuerung) des Access Points. Die Adresse entspricht der MAC-Adresse für die Bridge (br0). Unter dieser Adresse ist das WAP-Gerät extern anderen Netzwerken bekannt.
- **Aktuelle Firmwareversion**: Die aktuell ausgeführte Firmware-Version des Access Points
- **Firmware-Transferstatus**: Zeigt folgende Status zu Firmware-Download und -Validierung im Cluster-Mitglied an: Keine/Gestartet/Heruntergeladen/Erfolgreich/Fehlgeschlagen/Abbruch durch Administrator/Abbruch durch lokalen Benutzer/Dap_resigned.
- **Firmware-Transferfortschrittsbalken**: Zeigt den Fortschritt des Firmware-Downloads an.

So wählen Sie ein Cluster-Mitglied für ein Upgrade aus

1. Wählen Sie im Navigationsbereich die Option **Single Point Setup** > **Firmwareverwaltung** aus.
2. Aktivieren Sie das Kontrollkästchen neben dem AP, der aktualisiert werden soll.

3. Klicken Sie auf **Speichern**.

So rufen Sie den neuesten Status einer Cluster-Firmware-Upgrades ab:

Klicken Sie auf **Aktualisieren**.

So aktualisieren Sie die Firmware eines Cluster-Mitglieds über TFTP:

1. Wählen Sie TFTP als Transfermethode.
2. Geben Sie in das Feld „Quelldateiname“ einen Namen (1 bis 256 Zeichen) für die Image-Datei ein. Der Name muss den Pfad des Verzeichnisses enthalten, in dem sich das hochzuladende Image befindet.

   Wenn Sie beispielsweise das Image „ap_upgrade.tar“ aus dem Verzeichnis „/share/builds/ap“ hochladen möchten, geben Sie Folgendes ein: /share/builds/ap/ap_upgrade.tar

   Bei der angewendeten Firmware-Upgrade-Datei muss es sich um eine TAR-Datei handeln. Versuchen Sie nicht, BIN-Dateien oder Dateien in anderen Formaten für das Upgrade zu verwenden; mit diesen Dateitypen ist kein Upgrade möglich.

   Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * sowie zwei oder mehr aufeinanderfolgende Punkte.
3. Geben Sie die IPv4-Adresse des TFTP-Servers und klicken Sie auf Upgrade starten.

So führen Sie das Upgrade über HTTP durch:

1. Wählen HTTP als Transfermethode.
2. Wenn Sie den Namen und den Pfad der neuen Datei kennen, geben Sie diese Informationen in das Feld „Neues Firmware-Image“ ein.

   Anderenfalls klicken Sie auf die Schaltfläche Durchsuchen und suchen Sie die Firmware-Image-Datei im Netzwerk.

   Bei der angewendeten Firmware-Upgrade-Datei muss es sich um eine TAR-Datei handeln. Versuchen Sie nicht, BIN-Dateien oder Dateien in anderen Formaten für das Upgrade zu verwenden; mit diesen Dateitypen ist kein Upgrade möglich.
3. Klicken Sie auf „Upgrade starten“, um das neue Firmware-Image zu übernehmen.

Hinweis Upgradestatus insgesamt: Zeigt den kombinierten Upgradestatus (Nicht initialisiert/Wird durchgeführt/Abgeschlossen/Fehlgeschlagen/Abbruch durch Administrator/Kein) aller Cluster-Mitglieder an.

Stoppen des Upgrades eines Cluster-Mitglieds über den dominanten AP

Klicken Sie auf „Upgrade stoppen“.

Kanalverwaltung

Auf der Seite „Kanalverwaltung“ können Sie die Kanäle für die WAP-Geräte in einem Single Point Setup-Cluster verwalten.

Wenn die Kanalverwaltung aktiviert ist, weist das WAP-Gerät die von WAP-Geräten in einem Single Point Setup-Cluster verwendeten Funkkanäle automatisch zu. Die automatische Kanalzuweisung reduziert gegenseitige Interferenzen (oder Interferenzen mit anderen WAP-Geräten außerhalb des Clusters). Außerdem wird die WLAN-Bandbreite maximiert, um die effiziente Kommunikation über das WLAN aufrechtzuerhalten.

Die automatische Kanalzuweisung ist standardmäßig deaktiviert. Der Status der Kanalverwaltung (aktiviert oder deaktiviert) wird an die anderen Geräte im Single Point Setup-Cluster verbreitet.

Konfigurieren der erweiterten Einstellungen

Im Bereich „Erweitert“ können Sie den Kanalplan für das Single Point Setup anpassen und planen.

Die Kanäle werden standardmäßig einmal pro Stunde neu zugewiesen, jedoch nur, wenn die Interferenz um mindestens 25 Prozent reduziert werden kann. Die Kanäle werden auch dann neu zugewiesen, wenn das Netzwerk ausgelastet ist.

Die Standardeinstellungen sind für die meisten Szenarien geeignet, in denen Sie die Kanalverwaltung implementieren müssten.

In den erweiterten Einstellungen können Sie die folgenden Optionen ändern:

- **Schwellenwert für Kanalwechsel**: Der Prozentanteil der Interferenzreduzierung, der mindestens erreicht werden muss, damit ein vorgeschlagener Plan angewendet wird. Der Standardwert lautet „75 Prozent“. Wählen Sie einen Wert zwischen 5 und 75 Prozent aus. Mit dieser Einstellung können Sie eine Schwelle für die Effizienzsteigerung bei der Kanalneuzuweisung festlegen, damit es im Netzwerk nicht zu ständigen Unterbrechungen kommt, die nur zu minimalen Effizienzsteigerungen führen.

  Wenn beispielsweise die Kanalinterferenz um 75 Prozent reduziert werden muss, und die vorgeschlagenen Kanalzuweisungen die Interferenz nur um 30 Prozent reduzieren, werden die Kanäle nicht neu zugewiesen. Wenn Sie jedoch die minimale Kanalinterferenzreduzierung auf 25 Prozent festlegen und auf **Speichern** klicken, wird der vorgeschlagene Kanalplan implementiert, und die Kanäle werden nach Bedarf neu zugewiesen.

- **Intervall für Neubewertung der Kanalzuweisungen**: Der Zeitplan für automatische Updates. Sie können zwischen Intervallen im Bereich von 30 Minuten bis sechs Monaten wählen. Standardmäßig ist eine Stunde festgelegt, die Kanalverwendung wird also stündlich neu bewertet, und der resultierende Kanalplan wird angewendet.

  Wenn Sie diese Einstellungen ändern, klicken Sie auf **Speichern**. Die Änderungen werden in der aktiven Konfiguration und in der Startkonfiguration gespeichert.

  Wenn die automatische Kanalzuweisung aktiviert ist, wird auf dieser Seite die Tabelle der Kanalzuweisungen angezeigt.

Kanalzuordnungstabelle

Die Kanalzuordnungstabelle enthält eine nach IP-Adressen sortierte Liste aller WAP-Geräte im Single Point Setup-Cluster.

Die Tabelle enthält die folgenden Details zu den Kanalzuweisungen:

- **AP-Standort**: Der physische Standort des WAP-Geräts.
- **MAC-Adresse**: Die MAC-Adresse des Funkmoduls.
- **IP-Adresse**: Die IP-Adresse des WAP-Geräts.

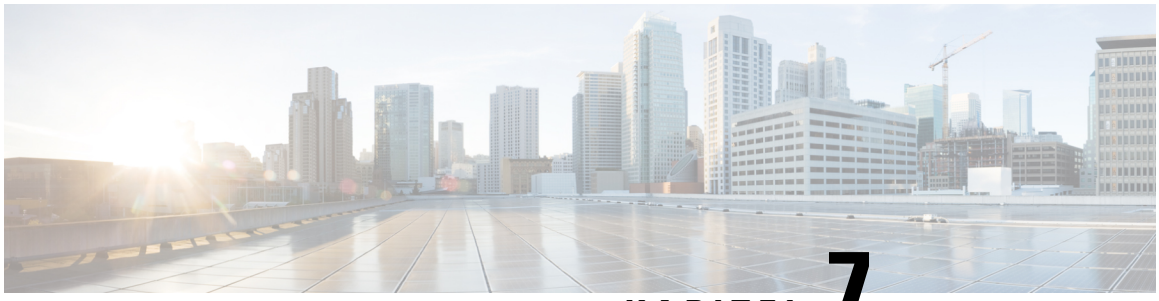
- **Funkband**: Das Band, auf dem das WAP-Gerät sendet.
- **Up/Down**: Zeigt den Status des WLAN-Funkmoduls im WAP-Gerät an. (Manche WAP-Geräte können mehrere WLAN-Funkmodule haben, die jeweils in einer separaten Zeile der Tabelle angezeigt werden.) Der Funkstatus entspricht „Aktiv“ (betriebsbereit) oder „Nicht aktiv“ (nicht betriebsbereit).
- **Aktueller Kanal**: Der Funkkanal, auf dem das WAP-Gerät momentan sendet.
- **Vorgeschlagener Kanal (vor xx Stunden)**: Der vorgeschlagene Funkkanal, dem dieses WAP-Gerät bei der Anwendung des Kanalplans zugewiesen würde.

Wenn automatisierte Kanalverwaltungspläne für ein WAP-Gerät ausgewählt sind, wird das WAP-Gerät im Rahmen der Optimierungsstrategie nicht zu einem anderen Kanal zugewiesen. Stattdessen werden WAP-Geräte mit gesperrten Kanälen als Voraussetzungen für den Plan berücksichtigt.

Klicken Sie auf Speichern, um die Sperreinstellung zu aktualisieren. Für gesperrte Geräte wird in den Tabellen „Aktuelle Kanalzuordnung“ und „Vorgeschlagene Kanalzuordnung“ der gleiche Kanal angezeigt. Gesperrte Geräte behalten die aktuellen Kanäle bei.

Die vorgeschlagenen Kanäle, die den einzelnen WAP-Geräten beim nächsten Update zugewiesen werden sollen. Gesperrte Kanäle werden nicht neu zugewiesen. Bei der Optimierung der Kanalverteilung zwischen den Geräten wird berücksichtigt, dass gesperrte Geräte die aktuellen Kanäle beibehalten müssen. Nicht gesperrte WAP-Geräte können abhängig von den Ergebnissen des Plans zu anderen Kanälen als den bisher verwendeten zugewiesen werden.

Aktualisieren Sie die Seite, um die neue Kanalzuordnungstabelle anzuzeigen.



KAPITEL 7

Zugriffssteuerung

In diesem Abschnitt wird die Konfiguration der ACL- und der Quality of Service (QoS)-Funktion auf dem WAP-Gerät beschrieben. Das Kapitel enthält die folgenden Themen:

ACL

ACLs (Access Control Lists, Zugriffssteuerungslisten) sind eine Sammlung an Zulassungs- und Verweigerungsbedingungen, Regeln genannt, die Sicherheit bieten, indem nicht autorisierte Benutzer blockiert werden und autorisierten Benutzern Zugriff auf bestimmte Ressourcen erlaubt wird. Durch ACLs können unbefugte Zugriffsversuche auf Netzwerkressourcen blockiert werden.

Das WAP-Gerät unterstützt bis zu 50 IPv4-, IPv6- und MAC-ACLs und bis zu 10 Regen pro ACL. Jede ACL unterstützt mehrere Schnittstellen.

IPv4- und IPv6-ACLs

Jede ACL stellt eine Reihe von Regeln dar, die auf beim WAP-Gerät eingehenden Datenverkehr angewendet werden. Jede Regel legt fest, ob die Inhalte eines gegebenen Feldes verwendet werden sollen, um den Zugriff auf das Netzwerk zuzulassen oder zu verweigern. Regeln können auf verschiedenen Kriterien basieren und auf eines oder mehrere Felder innerhalb eines Pakets angewendet werden, darunter die Quell- oder Ziel-IP-Adresse, der Quell- oder Ziel-Port oder das im Paket getragene Protokoll. Die IP-ACLs klassifizieren den Datenverkehr für die Layer 3 und 4.

Hinweis Am Ende jeder erstellten Regel gibt es eine implizite Verweigerung. Um eine allgemeine Verweigerung zu vermeiden, sollten Sie in der ACL eine Zulassungsregel hinzufügen, um Datenverkehr zu erlauben.

MAC-ACLs

MAC-ACLs sind Layer-2-ACLs. Sie können die Regeln zur Untersuchung von Feldern eines Frames konfigurieren, darunter die Quell- und Ziel-MAC-Adresse, die VLAN-ID oder die Serviceklasse. Wenn ein Frame den Anschluss des WAP-Geräts erreicht, untersucht das WAP-Gerät den Frame und gleicht die

ACL-Regeln mit den Inhalten des Frames ab. Wenn eine der Regeln auf den Inhalt angewendet werden kann, wird der Frame entweder zugelassen oder verweigert.

Workflow zur Konfiguration von ACLs

Verwenden Sie die ACL-Regeln, um die ACLs zu konfigurieren, und wenden Sie die Regeln dann auf eine festgelegte Schnittstelle an.

Gehen Sie wie folgt vor, um die ACLs zu konfigurieren:

Schritt 1 Wählen Sie **Zugriffssteuerung > ACL** aus.

Schritt 2 Klicken Sie in der ACL-Tabelle auf □, um eine neue Zeile hinzuzufügen und eine ACL zu erstellen.

Schritt 3 Geben Sie einen Namen für die ACL an.

Schritt 4 Wählen Sie den ACL-Typ aus der Dropdown-Liste aus (**IPv4, IPv6** oder **MAC**).

Schritt 5 Klicken Sie auf □, wählen Sie die Schnittstellen aus, zu denen die ACL zugeordnet werden soll, und klicken Sie auf **OK**. Wenn Sie die zugeordneten Schnittstellen ändern möchten, können Sie auf □ klicken, um die ausgewählten Schnittstellen zu löschen, und anschließend auf □ klicken, um neue Schnittstellen zuzuordnen.

Schritt 6 Klicken Sie auf **Mehr**, um die ACL-Parameter anzuzeigen.

Schritt 7 Konfigurieren Sie als Nächstes die Regeln für die ACL. Für IPv4-ACLs finden Sie weitere Informationen unter Konfiguration von IPv4-ACLs, auf Seite 82. Für IPv6-ACLs finden Sie weitere Informationen unter Konfiguration von IPv6-ACLs, auf Seite 85. Für MAC-ACLs finden Sie weitere Informationen unter Konfiguration von MAC-ACLs, auf Seite 88.

Schritt 8 Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.

Konfiguration von IPv4-ACLs

So konfigurieren Sie eine IPv4-ACL:

Schritt 1 Wählen Sie **Zugriffssteuerung > ACL** aus.

Schritt 2 Klicken Sie auf □, um eine ACL hinzuzufügen.

Schritt 3 Geben Sie im Feld „ACL-Name“ den Namen der ACL ein. Der Name kann bis zu 31 alphanumerische Zeichen und Sonderzeichen ohne Leerzeichen enthalten.

Schritt 4 Wählen Sie **IPv4** aus der Liste der ACL-Typen aus. IPv4-ACLs kontrollieren den Zugriff auf Netzwerkressourcen basierend auf Layer-3- und Layer-4-Kriterien.

Schritt 5 Klicken Sie auf □ und wählen Sie die Schnittstellen aus, auf denen die ACL angewendet werden soll. Klicken Sie auf **OK**. Wenn Sie die zugeordneten Schnittstellen ändern möchten, können Sie auf □ klicken, um die ausgewählte Schnittstelle zu löschen, und anschließend auf □ klicken, um neue Schnittstellen zuzuordnen.

Schritt 6 Klicken Sie auf **Mehr**, um die Konfigurationsparameter anzuzeigen. Klicken Sie auf □, um eine Regel hinzuzufügen, und konfigurieren Sie Folgendes:

Hinweis Wenn keine Regeln hinzugefügt werden, blockiert der DUT standardmäßig sämtlichen Datenverkehr.

- **Regelpriorität**: Wenn eine ACL mehrere Regeln enthält, werden die Regeln in der angegebenen Reihenfolge auf Pakete oder Frames angewendet. Eine niedrigere Nummer bedeutet eine höhere Priorität. Die neue Regel

erhält die niedrigste Priorität unter allen expliziten Regeln. Es existiert immer eine implizite Regel mit der niedrigsten Priorität, die sämtlichen Datenverkehr blockiert.

- **Aktion**: Wählen Sie aus, ob die Aktion **Abgelehnt** oder **Zugelassen** werden soll. Die Standardaktion ist **Ablehnen**.

  Wenn Sie **Zulassen** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr zugelassen, der die Regelkriterien erfüllt. Datenverkehr, der die Kriterien nicht erfüllt, wird abgewiesen.

  Wenn Sie **Verweigern** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr blockiert, der die Regelkriterien erfüllt. Datenverkehr, der nicht die Kriterien erfüllt, wird weitergeleitet, sofern es sich bei dieser Regel nicht um die Abschlussregel handelt. Da am Ende jeder ACL eine implizite „Alle ablehnen"-Regel existiert, wird nicht explizit zugelassener Datenverkehr abgewiesen.

- **Dienst (Protokoll)**: Verwendet eine Layer-3 oder Layer-4-Protokollabgleichbedingung basierend auf dem Wert des Feldes „IP-Protokoll". Wählen Sie eine dieser Optionen:
  - **Sämtlicher Datenverkehr**: Alle Daten, die die Kriterien der Regeln erfüllen, werden zugelassen.
  - **Aus Liste auswählen**: Wählen Sie eines dieser Protokolle: **IP, ICMP, IGMP, TCP** oder **UDP**.
  - **Benutzerdefiniert**: Geben Sie eine standardmäßige, von IANA zugewiesene Protokoll-ID von 0 bis 255 ein. Wählen Sie diese Methode aus, um ein Protokoll zu identifizieren, das nicht in der Auswahlliste aufgeführt ist.

- **IPv4-Quelladresse**: Die IP-Quelladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle IP-Adressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie eine IP-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie eine Platzhaltermaske für die IP-Quelladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits verwendet werden. Dieses Feld ist erforderlich, wenn **IP-Quelladresse** aktiviert ist.

    Eine Platzhaltermaske ist im Wesentlichen eine umgekehrte Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Platzhaltermaske von 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (z. B 192.168.10.0/24) abgleichen möchten, verwenden Sie die Maske 0.0.0.255.

- **Quell-Port**: Schließt einen Quell-Port in die Abgleichbedingung für die Regel ein. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Sämtlicher Datenverkehr**: Alle Daten, die die Kriterien der Regeln erfüllen, werden zugelassen.
  - **Aus Liste wählen**: Wählen Sie das Schlüsselwort aus, das dem Quell-Port zugeordnet ist, der abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Geben Sie die IANA-Port-Nummer ein, die mit dem im Datagramm-Header identifizierten Quell-Port abgeglichen werden soll. Der Port-Bereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports

- 49152 bis 65535: Dynamische und/oder private Ports

- **IPv4-Zieladresse**: Die IP-Zieladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle IP-Adressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie eine IP-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie eine Platzhaltermaske für die IP-Zieladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits verwendet werden. Dieses Feld ist erforderlich, wenn „IP-Quelladresse“ aktiviert ist.

    Eine Platzhaltermaske ist im Wesentlichen eine umgekehrte Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Platzhaltermaske von 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (z. B 192.168.10.0/24) abgleichen möchten, verwenden Sie die Maske 0.0.0.255.

- **Ziel-Port**: Schließt einen Ziel-Port in die Abgleichbedingung für die Regel ein. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Alle**: Alle Ports, die die Kriterien der Regeln erfüllen, werden zugelassen.
  - **Aus Liste wählen**: Wählen Sie das Stichwort aus, das dem abzugleichenden Quell-Port zugeordnet ist: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Geben Sie die IANA-Port-Nummer ein, die mit dem im Datagramm-Header identifizierten Ziel-Port abgeglichen werden soll. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports

- **Servicetyp**: Gleicht die Pakete auf der Grundlage eines speziellen Servicetyps ab.
  - **Alle**: Alle Servicetypen.
  - **Aus Liste auswählen**: Gleicht die Pakete basierend auf deren DSCP-Werten „Assured Forwarding“ (AS), „Class of Service“ (CS) oder „Expedited Forwarding“ (EF) ab.
  - **DSCP**: Gleicht die Pakete basierend auf einem benutzerdefinierten DSCP-Wert ab. Ist die Funktion ausgewählt, geben Sie in diesem Feld einen Wert zwischen 0 und 63 ein.
  - **Vorrang**: Gleicht die Pakete auf der Grundlage ihres IP-Vorrangswerts ab. Ist diese Funktion ausgewählt, geben Sie einen IP-Vorrangswert zwischen 0 und 7 ein.
  - **ToS/Maske**: Geben Sie einen IP-ToS-Maskenwert ein, um die Bit-Positionen im IP-ToS-Bit-Wert zu identifizieren, die für den Abgleich gegen das IP-ToS-Feld in einem Paket verwendet werden.

    Beim IP-ToS-Maskenwert handelt es sich um eine zweistellige Hexadezimalzahl von 00 bis FF, die eine umgekehrte (d. h. Platzhalter-) Maske darstellt. Die nullwertigen Bits in der IP-ToS-Maske bezeichnen die Bit-Positionen im IP-ToS-Bit-Wert, die für den Abgleich gegen das IP-ToS-Feld eines Pakets verwendet

werden. Verwenden Sie zum Beispiel für die Suche nach einem IP-ToS-Wert, bei dem die Bits 7 und 5 festgelegt und Bit 1 frei ist und bei dem Bit 7 am relevantesten ist, einen IP-ToS-Bit-Wert von 0 und eine IP-ToS-Maske von 00.

Schritt 7 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine ACL zu löschen oder zu bearbeiten, wählen Sie die ACL aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Um eine Regel zu löschen oder zu bearbeiten, wählen Sie die Regel im Bereich „Regelkonfiguration“ aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Schritt 8 Klicken Sie auf **Speichern**.

Konfiguration von IPv6-ACLs

So konfigurieren Sie eine IPv6-ACL:

Schritt 1 Wählen Sie **Zugriffssteuerung > ACL** aus.

Schritt 2 Klicken Sie auf □, um eine ACL hinzuzufügen.

Schritt 3 Geben Sie im Feld „ACL-Name“ den Namen der ACL ein.

Schritt 4 Wählen Sie **IPv6** aus der Liste der ACL-Typen aus. IPv4-ACLs kontrollieren den Zugriff auf Netzwerkressourcen basierend auf Layer-3- und Layer-4-Kriterien.

Schritt 5 Klicken Sie auf □ und wählen Sie die Schnittstellen aus, auf denen die ACL angewendet werden soll. Klicken Sie anschließend auf **OK**. Wenn Sie die zugeordneten Schnittstellen ändern möchten, können Sie auf □ klicken, um die ausgewählte Schnittstelle zu löschen, und anschließend auf □ klicken, um neue Schnittstellen zuzuordnen.

Schritt 6 Klicken Sie auf **Mehr**, um die Konfigurationsparameter anzuzeigen. Klicken Sie auf □, um eine Regel hinzuzufügen, und konfigurieren Sie Folgendes:

Hinweis Wenn keine Regeln hinzugefügt werden, blockiert der DUT standardmäßig sämtlichen Datenverkehr.

- **Regelpriorität**: Wenn eine ACL mehrere Regeln enthält, werden die Regeln in der angegebenen Reihenfolge auf Pakete oder Frames angewendet. Eine niedrigere Nummer bedeutet eine höhere Priorität. Die neue Regel erhält die niedrigste Priorität unter allen expliziten Regeln. Klicken Sie auf die Pfeilschaltflächen nach oben oder unten, um die Priorität zu ändern. Es existiert immer eine implizite Regel mit der niedrigsten Priorität, die sämtlichen Datenverkehr blockiert.
- **Aktion**: Wählen Sie aus, ob die Aktion **Abgelehnt** oder **Zugelassen** werden soll. Die Standardaktion ist **Ablehnen**.

  Wenn Sie **Zulassen** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr zugelassen, der die Regelkriterien erfüllt. Datenverkehr, der die Kriterien nicht erfüllt, wird abgewiesen.

  Wenn Sie **Verweigern** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr blockiert, der die Regelkriterien erfüllt. Datenverkehr, der nicht die Kriterien erfüllt, wird weitergeleitet, sofern es sich bei dieser Regel nicht um die Abschlussregel handelt. Da am Ende jeder ACL eine implizite „Alle ablehnen“-Regel existiert, wird nicht explizit zugelassener Datenverkehr abgewiesen.

- **Dienst (Protokoll)**: Verwendet eine Layer-3 oder Layer-4-Protokollabgleichbedingung basierend auf dem Wert des Feldes „IP-Protokoll“. Wählen Sie eine dieser Optionen:
  - **Sämtlicher Datenverkehr**: Alle Daten, die die Kriterien der Regeln erfüllen, werden zugelassen.
  - **Aus Liste auswählen**: Wählen Sie eines dieser Protokolle: **IPv6, ICMPv6, TCP** oder **UDP**.
  - **Benutzerdefiniert**: Geben Sie eine standardmäßige, von IANA zugewiesene Protokoll-ID von 0 bis 255 ein. Wählen Sie diese Methode aus, um ein Protokoll zu identifizieren, das nicht in der Auswahlliste aufgeführt ist.
- **IPv6-Quelladresse**: Die IP-Quelladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle IP-Adressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie eine IP-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie eine Platzhaltermaske für die IP-Quelladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits verwendet werden. Dieses Feld ist erforderlich, wenn **IP-Quelladresse** aktiviert ist.

    Eine Platzhaltermaske ist im Wesentlichen eine umgekehrte Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Platzhaltermaske von 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (z. B 192.168.10.0/24) abgleichen möchten, verwenden Sie die Maske 0.0.0.255.
- **Quell-Port**: Schließt einen Quell-Port in die Abgleichbedingung für die Regel ein. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Beliebig**: Alle Quell-Ports werden zugelassen.
  - **Aus Liste wählen**: Wählen Sie das Schlüsselwort aus, das dem Quell-Port zugeordnet ist, der abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Geben Sie die IANA-Port-Nummer ein, die mit dem im Datagramm-Header identifizierten Quell-Port abgeglichen werden soll. Der Port-Bereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports
- **IPv6-Zieladresse**: Die IP-Zieladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle IP-Adressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie eine IP-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie eine Platzhaltermaske für die IP-Zieladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255

gibt an, dass alle Bits ignoriert werden. Der Platzhalter 0.0.0.0 gibt an, dass alle Bits verwendet werden. Dieses Feld ist erforderlich, wenn „IP-Quelladresse“ aktiviert ist.

Eine Platzhaltermaske ist im Wesentlichen eine umgekehrte Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Platzhaltermaske von 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (z. B 192.168.10.0/24) abgleichen möchten, verwenden Sie die Maske 0.0.0.255.

- **Ziel-Port**: Schließt einen Ziel-Port in die Abgleichbedingung für die Regel ein. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Alle**: Alle Ports, die die Kriterien der Regeln erfüllen, werden zugelassen.
  - **Aus Liste wählen**: Wählen Sie das Stichwort aus, das dem abzugleichenden Quell-Port zugeordnet ist: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Geben Sie die IANA-Port-Nummer ein, die mit dem im Datagramm-Header identifizierten Ziel-Port abgeglichen werden soll. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports

- **Flow-Label**: Eine 20-Bit-Nummer, die für ein IPv6-Paket eindeutig ist.
  - **Beliebig**: Beliebige 20-Bit-Nummern.
  - **DSCP**: Gleicht die Nummer mit einem benutzerdefinierten DSCP-Wert ab.

- **DSCP**: Gleicht die Pakete mit ihrem IP-DSCP-Wert ab.
  - **Beliebig**: Alle DSCP-Werte werden zugelassen.
  - **Aus Liste auswählen**: Wählen Sie eine DSCP-Wert aus der Dropdownliste aus.
  - **Benutzerdefiniert**: Geben Sie einen benutzerdefinierten DSCP-Wert von 0 bis 63 ein.

Schritt 7 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine ACL zu löschen oder zu bearbeiten, wählen Sie die ACL aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Um eine Regel zu löschen oder zu bearbeiten, wählen Sie die Regel im Regelkonfigurationsbereich aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Schritt 8 Klicken Sie auf **Speichern**.

Konfiguration von MAC-ACLs

So konfigurieren Sie eine MAC-ACL:

Schritt 1 Wählen Sie **Zugriffssteuerung > ACL** aus.

Schritt 2 Klicken Sie auf □, um eine MAC-ACL hinzuzufügen.

Schritt 3 Geben Sie im Feld „ACL-Name“ den Namen zur Kennzeichnung der ACL ein.

Schritt 4 Wählen Sie **MAC** als ACL-Typ aus der Liste aus. MAC-ACLs kontrollieren Zugriff auf der Grundlage von Layer-2-Kriterien.

Schritt 5 Klicken Sie auf □, wählen Sie die Schnittstellen aus, zu denen die ACL zugeordnet werden soll, und klicken Sie auf **OK**. Wenn Sie die zugeordneten Schnittstellen ändern möchten, können Sie auf □ klicken, um die ausgewählte Schnittstelle zu löschen, und anschließend auf □ klicken, um neue Schnittstellen zuzuordnen.

Schritt 6 Klicken Sie auf **Mehr**, um die Konfigurationsparameter anzuzeigen. Klicken Sie auf □, um eine Regel hinzuzufügen, und konfigurieren Sie die folgenden Parameter:

- **Regelpriorität**: Wenn eine ACL mehrere Regeln enthält, werden die Regeln in der angegebenen Reihenfolge auf Pakete oder Frames angewendet. Eine niedrigere Nummer bedeutet eine höhere Priorität. Die neue Regel erhält die niedrigste Priorität unter allen expliziten Regeln, und Sie können die Priorität mit den Pfeilen nach oben bzw. nach unten ändern. Es existiert immer eine implizite Regel mit der niedrigsten Priorität, die sämtlichen Datenverkehr blockiert.
- **Aktion**: Wählen Sie aus, ob die Aktion **Abgelehnt** oder **Zugelassen** werden soll. Die Standardaktion ist **Ablehnen**.

  Wenn Sie **Zulassen** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr zugelassen, der die Regelkriterien erfüllt. Datenverkehr, der die Kriterien nicht erfüllt, wird abgewiesen.

  Wenn Sie **Verweigern** wählen, wird durch die Regel sämtlicher an dem WAP-Gerät eingehender Datenverkehr blockiert, der die Regelkriterien erfüllt. Datenverkehr, der nicht die Kriterien erfüllt, wird weitergeleitet, sofern es sich bei dieser Regel nicht um die Abschlussregel handelt. Da am Ende jeder ACL eine implizite „Alle ablehnen“-Regel existiert, wird nicht explizit zugelassener Datenverkehr abgewiesen.
- **Service (ETH-Typ)**: Wählen Sie diese Option aus, um die Abgleichkriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Wählen Sie einen ETH-Typ aus der Dropdownliste aus.
  - Beliebig: Alle Protokolle werden zugelassen.
  - **Aus Liste auswählen**: Wählen Sie einen dieser Protokolltypen aus: **ARP, IPv4, IPv6, IPX, NetBIOS, PPPoE**.
  - **Benutzerdefiniert**: Geben Sie einen Protokollbezeichner ein, mit dem die Pakete abgeglichen werden sollen. Der Wert ist eine vierstellige Hexadezimalzahl im Bereich zwischen 0600 und FFFF.
- **MAC-Quelladresse**: Die MAC-Quelladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle MAC-Quelladressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie die MAC-Quelladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **Adresse/Maske**: Geben Sie die MAC-Quelladresse ein, die festlegt, welche Bits in der Quell-MAC mit einem Ethernet-Frame abgeglichen werden sollen.

Für jede Bitposition in der MAC-Maske gibt eine 0 an, dass das entsprechende Adress-Bit relevant ist. Eine 1 gibt an, dass das Adress-Bit ignoriert wird. Um nur die ersten vier Oktette einer MAC-Adresse zu prüfen, wird beispielsweise die MAC-Maske 00:00:00:00:ff:ff verwendet. Eine MAC-Maske mit 00:00:00:00:00:00 prüft alle Adressbits und wird zum Abgleich einer einzigen MAC-Adresse verwendet.

- **MAC-Zieladresse**: Die MAC-Zieladresse des Pakets muss mit der in den entsprechenden Feldern definierten Adresse übereinstimmen.
  - **Beliebig**: Alle MAC-Zieladressen werden zugelassen.
  - **Einzelne Adresse**: Geben Sie die MAC-Zieladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **Adresse/Maske**: Geben Sie die MAC-Zieladresse ein, um festzulegen, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.
- **VLAN-ID**: Die VLAN-ID, die mit einem Ethernet-Frame verglichen werden soll.
  - **Beliebig**: Alle VLAN-IDs werden zugelassen.
  - **Benutzerdefiniert**: Geben Sie die spezifische VLAN-ID ein, die mit einem Ethernet-Frame verglichen werden soll. Dieses Feld befindet sich im ersten/einzigen 802.1Q VLAN-Tag. Der Port-Bereich liegt zwischen 1 und 4094.
- **Class of Service**: Legt einen Wert für die Class of Service-802.1p-Benutzerpriorität fest.
  - **Beliebig**: Alle Class of Service-Typen werden zugelassen.
  - **Benutzerdefiniert**: Geben Sie eine 802.1p-Benutzerpriorität ein, die mit einem Ethernet-Frame verglichen werden soll. Gültig sind Werte im Bereich von 0 bis 7.

Schritt 7 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine ACL zu löschen oder zu bearbeiten, wählen Sie die ACL aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**. Um eine Regel zu löschen oder zu bearbeiten, wählen Sie die Regel im Bereich **Regelkonfiguration** aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Schritt 8 Klicken Sie auf **Speichern**.

Client-QoS

Die Client-Quality of Service (QoS) dient zur Kontrolle der WLAN-Clients, die mit dem Netzwerk verbunden sind, und zur Verwaltung der verwendeten Bandbreite. Mit der Client-QoS können Sie beispielsweise den HTTP-Datenverkehr oder den Datenverkehr aus einem bestimmten Subnetz mithilfe von Zugriffskontrolllisten (Access Control Lists, ACLs) steuern. Eine ACL ist eine Sammlung von Zulassungs- und Verweigerungsbedingungen, sogenannten Regeln, die Sicherheit bieten, indem nicht autorisierte Benutzer blockiert werden und autorisierten Benutzern Zugriff auf bestimmte Ressourcen gewährt wird. Durch ACLs können unbefugte Zugriffsversuche auf Netzwerkressourcen blockiert werden.

Verkehrsklassen

Die QoS-Funktion unterstützt Differenzierte Dienste (Differentiated Services, DiffServ), mit denen der Datenverkehr in Streams klassifiziert werden kann. Außerdem erhalten die Daten eine bestimmte QoS-Behandlung gemäß eines definierten Verhaltens für Hops.

Herkömmliche IP-basierte Netzwerke sind so konzipiert, dass die Daten nach dem Prinzip der besten Leistung übermittelt werden. „Beste Leistung“ bedeutet, dass die Daten zeitnah im Netzwerk übermittelt werden, auch wenn dies nicht garantiert wird. Bei Überlastungen können Pakete verzögert, sporadisch gesendet oder gelöscht werden. Bei typischen Internetanwendungen wie E-Mail und Dateiübertragungen ist eine geringfügige Verschlechterung des Diensts akzeptabel und in vielen Fällen nicht wahrnehmbar. Bei Anwendungen mit strikten zeitlichen Anforderungen wie beispielsweise Sprach- oder Multimediaanwendungen hat jede Verschlechterung des Diensts unerwünschte Auswirkungen.

Eine DiffServ-Konfiguration beginnt mit dem Definieren von Klassenzuordnungen, in denen der Verkehr nach dem IP-Protokoll und anderen Kriterien klassifiziert wird. Jede Klassenzuordnung kann dann einer Richtlinienzuordnung zugeordnet werden, in der die Behandlung der Verkehrsklasse definiert wird. Klassen mit zeitkritischem Datenverkehr können zu den Richtlinienzuordnungen zugewiesen werden.

Konfigurieren von Ipv4-Verkehrsklassen

So können Sie eine IPv4-Klassenzuordnung hinzufügen und konfigurieren:

Schritt 1 Wählen Sie **Client-QoS > Verkehrsklassen** aus.

Schritt 2 Klicken Sie auf □, um eine Verkehrsklasse hinzuzufügen.

Hinweis Sie können maximal 50 Klassenzuordnungen konfigurieren.

Schritt 3 Geben Sie im Textfeld **Verkehrsklassenname** den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

Schritt 4 Wählen Sie unter **Klassentyp** den Wert **IPv4** in der Liste aus. IPv4-Verkehrsklassen gelten nur für den IPv4-Datenverkehr im WAP-Gerät.

Schritt 5 Konfigurieren Sie Folgendes:

- **Quelladresse**: Die IPv4-Quelladresse des Pakets muss mit der in den entsprechenden Feldern definierten IPv4-Adresse übereinstimmen.
  - **Beliebig**: Beliebige IPv4-Adressen können als Quelladresse verwendet werden.
  - **Einzelne Adresse**: Geben Sie eine IPv4-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie eine Maske für die IPv4-Quelladresse ein. Bei der Maske für DiffServ handelt es sich um eine Netzwerk-Bitmaske im Punkt-Dezimalformat für IP-Adressen. Die Maske gibt an, welche Teile der IP-Zieladresse für den Abgleich mit dem Paketinhalt verwendet werden sollen.

    Die DiffServ-Maske 255.255.255.255 gibt an, dass alle Bits wichtig sind. Die Maske 0.0.0.0 gibt an, dass kein Bit wichtig ist. Für eine ACL-Platzhaltermaske gilt das Gegenteil. Wenn Sie beispielsweise die Kriterien mit einer einzelnen Hostadresse abgleichen möchten, verwenden Sie die Maske 255.255.255.255. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (beispielsweise 192.168.10.0/24) abgleichen möchten, verwenden Sie die Maske 255.255.255.0.

- **Zieladresse**: Die IPv4-Zieladresse des Pakets muss mit der in den entsprechenden Feldern definierten IPv4-Adresse übereinstimmen.
  - **Beliebig**: Beliebige IPv4-Adressen können als Zieladresse verwendet werden.

- **Einzelne Adresse**: Geben Sie eine IPv4-Adresse für dieses Kriterium ein.
- **Adresse/Maske**: Geben Sie eine Platzhaltermaske für die IP-Zieladresse ein.

Schritt 6 Klicken Sie auf **Mehr** und konfigurieren Sie die folgenden Parameter:

- **Protokoll**: Verwendet eine Layer-3 oder Layer-4-Protokollabgleichbedingung, die auf dem Wert des Feldes „IP-Protokoll“ in IPv4-Paketen oder dem Feld „Nächster Header“ in IPv6-Paketen basiert. Wählen Sie das Protokoll aus, das per Stichwort oder Protokoll-ID abgeglichen werden soll.
  - **Sämtlicher Datenverkehr**: Alle Daten aus allen Protokollen werden zugelassen.
  - **Aus Liste auswählen**: Das ausgewählte Protokoll wird abgeglichen: IP, ICMP, IGMP, TCP oder UDP.
  - **Benutzerdefiniert**: Gleicht ein Protokoll ab, dessen Name nicht aufgeführt ist. Geben Sie die Protokoll-ID ein. Die Protokoll-ID ist ein von IANA zugewiesener Standardwert. Möglich sind Zahlen im Bereich 0 bis 255.

  Hinweis Wenn Sie unter **Protokoll** den Wert „Sämtlicher Datenverkehr“ ausgewählt haben, müssen Sie die Felder **Quelladresse** und **Zieladresse** ausfüllen.

- **Quell-Port**: Schließt einen Quell-Port in die Abgleichbedingung für die Regel ein. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Beliebig**: Jeder beliebige Port wird als Quellport akzeptiert.
  - **Aus Liste wählen**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Gleicht die Quellportnummer im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports

- **Ziel-Port**: Schließt einen Ziel-Port in die Abgleichbedingung für die Regel ein. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Beliebig**: Jeder beliebige Port wird als Zielport akzeptiert.
  - **Aus Liste wählen**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Gleicht die Quellportnummer im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports

- **Servicetyp**: Gibt den Servicetyp an, der für den Abgleich von Paketen mit Klassenkriterien verwendet werden soll.
  - **Alle**: Alle Servicetypen können als Abgleichkriterium verwendet werden.
  - **IP-DSCP aus Liste auswählen**: Wählen Sie einen DSCP-Wert (Differentiated Services Code Point), der als Übereinstimmungskriterium verwendet werden soll:
  - **IP-DSCP mit Wert abgleichen**: Geben Sie einen benutzerdefinierten DSCP-Wert von 0 bis 63 ein.
  - **Priorisierung von IP-Verkehr**: Gleicht den Wert für Priorisierung von IP-Verkehr eines Pakets mit dem in diesem Feld definierten Wert für Priorisierung von IP-Verkehr ab. Für „Priorisierung von IP-Verkehr“ sind Werte im Bereich von 0 bis 7 möglich.
  - **IP-TOS-Bits**: Verwendet die Type of Service-Bits des Pakets im IP-Header als Übereinstimmungskriterium. Für IP TOS Bits sind Werte im Bereich von 00 bis FF möglich. Die höherwertigen drei Bits stellen den IP-Vorrangwert dar. Die höherwertigen drei Bits stellen den IP-DSCP-Wert dar.
  - **IP-ToS-Maske**: Geben Sie einen IP-ToS-Maskenwert ein, um die Bit-Positionen im IP-ToS-Bit-Wert zu identifizieren, die für den Abgleich gegen das IP-ToS-Feld in einem Paket verwendet werden.

    Der Wert der IP-ToS-Bits ist eine zweistellige Hexadezimalzahl zwischen 00 und FF. Die nicht-nullwertigen Bits in der IP-ToS-Maske bezeichnen die Bit-Positionen im IP-ToS-Bit-Wert, die für den Abgleich gegen das IP-ToS-Feld eines Pakets verwendet werden.

Schritt 7 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine Klassenzuordnung zu löschen oder zu bearbeiten, wählen Sie den Namen der Klassenzuordnung in der Liste aus und klicken Sie auf **Löschen**. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Schritt 8 Klicken Sie auf **Speichern**.

Konfigurieren von IPv6-Verkehrsklassen

So fügen Sie eine IPv6-Klassenzuordnung hinzu und konfigurieren sie:

Schritt 1 Wählen Sie **Client-QoS > Verkehrsklassen** aus.

Schritt 2 Klicken Sie auf □, um eine Verkehrsklasse hinzuzufügen.

Hinweis Sie können maximal 50 Klassenzuordnungen konfigurieren.

Schritt 3 Geben Sie im Textfeld **Verkehrsklassenname** den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

Schritt 4 Wählen Sie **IPv6** als Verkehrsklassen-Typ aus der Liste aus. Die IPv6-Verkehrsklassen gelten nur für den IPv6-Datenverkehr im WAP-Gerät.

Schritt 5 Konfigurieren Sie Folgendes:

- **Quelladresse**: Die IPv6-Quelladresse des Pakets muss mit der in den entsprechenden Feldern definierten IPv6-Adresse übereinstimmen.

- **Beliebig**: Beliebige IPv6-Adressen können als Quelladresse verwendet werden.
- **Einzelne Adresse**: Geben Sie eine IPv6-Adresse für dieses Kriterium ein.
- **Adresse/Maske**: Geben Sie die Präfixlänge der IPv6-Quelladresse ein.

- **Zieladresse**: Die IPv4-Zieladresse des Pakets muss mit der in den entsprechenden Feldern definierten IPv4-Adresse übereinstimmen.
  - **Beliebig**: Beliebige IPv6-Adressen können als Zieladresse verwendet werden.
  - **Einzelne Adresse**: Geben Sie eine IPv6-Adresse für dieses Kriterium ein.
  - **Adresse/Maske**: Geben Sie die IPv6-Zieladresse und die Präfixlänge der IPv6-Zieladresse ein.

Schritt 6 Klicken Sie auf **Mehr** und konfigurieren Sie die folgenden Parameter:

- **Protokoll**: Verwendet eine Layer-3 oder Layer-4-Protokollabgleichbedingung, die auf dem Wert des Feldes „IP-Protokoll“ in IPv4-Paketen oder dem Feld „Nächster Header“ in IPv6-Paketen basiert. Wählen Sie das Protokoll aus, das per Stichwort oder Protokoll-ID abgeglichen werden soll.
  - **Sämtlicher Datenverkehr**: Alle Daten aus allen Protokollen werden zugelassen.
  - **Aus Liste auswählen**: Das ausgewählte Protokoll wird abgeglichen: IP, ICMP, IGMP, TCP oder UDP.
  - **Benutzerdefiniert**: Gleicht ein Protokoll ab, dessen Name nicht aufgeführt ist. Geben Sie die Protokoll-ID ein. Die Protokoll-ID ist ein von IANA zugewiesener Standardwert. Möglich sind Zahlen im Bereich 0 bis 255.

- **Quell-Port**: Schließt einen Quell-Port in die Abgleichbedingung für die Regel ein. Der Quell-Port wird im Datagramm-Header identifiziert.

  Hinweis Wenn Sie unter **Protokoll** den Wert „Sämtlicher Datenverkehr“ ausgewählt haben, müssen Sie die Felder **Quelladresse** und **Zieladresse** ausfüllen.

  - **Beliebig**: Jeder beliebige Port wird als Quellport akzeptiert.
  - **Aus Liste wählen**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Benutzerdefiniert**: Gleicht die Quellportnummer im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
    - 0 bis 1023: Bekannte Ports
    - 1024 bis 49151: Registrierte Ports
    - 49152 bis 65535: Dynamische und/oder private Ports

- **Ziel-Port**: Schließt einen Ziel-Port in die Abgleichbedingung für die Regel ein. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - Beliebig: Jeder beliebige Port wird als Zielport akzeptiert.
  - **Aus Liste wählen**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.

- **Benutzerdefiniert**: Gleicht die Quellportnummer im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Der Portbereich liegt zwischen 0 und 65535 und umfasst drei verschiedene Arten von Ports:
  - 0 bis 1023: Bekannte Ports
  - 1024 bis 49151: Registrierte Ports
  - 49152 bis 65535: Dynamische und/oder private Ports

- **IPv6-Flow-Label**: Das Flow-Label wird von Knoten verwendet, um Pakete in einem Datenfluss zu markieren.
  - **Beliebig**: Eine beliebige 20-Bit-Nummer, die für ein IPv6-Paket eindeutig ist.
  - **Benutzerdefiniert**: Geben Sie eine für ein IPv6-Paket eindeutige 20-Bit-Zahl ein. Dieser Wert wird von Endgeräten verwendet, um die QoS-Verarbeitung in Routern zu kennzeichnen (Bereich 0 bis FFFFF).

- **Servicetyp**: Gibt den Servicetyp an, der für den Abgleich von Paketen mit Klassenkriterien verwendet werden soll.
  - **Alle**: Alle Servicetypen können als Abgleichkriterium verwendet werden.
  - **IP-DSCP aus Liste auswählen**: Wählen Sie einen DSCP-Wert (Differentiated Services Code Point), der als Übereinstimmungskriterium verwendet werden soll:
  - **IP-DSCP mit Wert abgleichen**: Geben Sie einen benutzerdefinierten DSCP-Wert von 0 bis 63 ein.

Schritt 7 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine Klassenzuordnung zu löschen oder zu bearbeiten, wählen Sie den Namen der Klassenzuordnung in der Liste aus und klicken Sie auf **Löschen**. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Schritt 8 Klicken Sie auf **Speichern**.

Konfigurieren von MAC-Verkehrsklassen

So können Sie eine MAC-Klassenzuordnung hinzufügen und konfigurieren:

Schritt 1 Wählen Sie **Client-QoS > Verkehrsklassen** aus.

Schritt 2 Klicken Sie auf □, um eine Verkehrsklasse hinzuzufügen.

Hinweis Sie können maximal 50 Klassenzuordnungen konfigurieren.

Schritt 3 Geben Sie im Textfeld Verkehrsklassenname den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

Schritt 4 Wählen Sie aus der Liste der Klassenzuordnungstypen **MAC** als Klassenzuordnungstyp aus. Die MAC-Klasse gilt für Layer 2-Kriterien.

Schritt 5 **Quell-Adresse**: Schließt eine MAC-Quelladresse in die Übereinstimmungsbedingungen für die Regel ein.

- **Beliebig**: Beliebige MAC-Adressen können als Quelladresse verwendet werden.
- **Einzelne Adresse**: Geben Sie die MAC-Quelladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
- **Adresse/Maske**: Geben Sie die MAC-Quelladressmaske ein, die festlegt, welche Bits in der Ziel-MAC mit einem Ethernet-Frame abgeglichen werden sollen.

  Für jede Bitposition in der MAC-Maske gibt eine 1 an, dass das entsprechende Adress-Bit relevant ist. Eine 0 gibt an, dass das Adress-Bit ignoriert wird. Um nur die ersten vier Oktette einer MAC-Adresse zu prüfen, wird beispielsweise die MAC-Maske ff:ff:ff:ff:00:00 verwendet. Die MAC-Maske ff:ff:ff:ff:ff:ff prüft alle Adressbits und wird zum Abgleich einer einzigen MAC-Adresse verwendet.

Schritt 6 **Ziel-Adresse**: Schließt eine MAC-Zieladresse in die Übereinstimmungsbedingung für die Regel ein.

- **Beliebig**: Beliebige MAC-Adressen können als Zieladresse verwendet werden.
- **Einzelne Adresse**: Geben Sie die MAC-Zieladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
- **Adresse/Maske**: Geben Sie die MAC-Zieladressmaske ein, um anzugeben, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.

Schritt 7 Klicken Sie auf **Mehr** und konfigurieren Sie die folgenden Parameter:

- **Protokoll**: Vergleicht die Übereinstimmungskriterien mit dem Wert im Header eines Ethernet-Frames. Wählen Sie ein Ethernettyp-Schlüsselwort aus, oder geben Sie einen Ethernettyp-Wert ein, um die Übereinstimmungskriterien anzugeben.
  - **Sämtlicher Datenverkehr**: Alle Daten aus allen Protokollen werden zugelassen.
  - **Aus Liste auswählen**: Gleicht den Ethertype im Datagramm-Header mit den ausgewählten Protokolltypen ab: Apple Talk, ARP, IPv4, IPv6, IPX, NETBIOS, PPPoE.
  - **Benutzerdefiniert**: Gleicht den Ethernettyp im Datagramm-Header mit einer angegebenen benutzerdefinierten Protokoll-ID ab. Der Wert ist eine vierstellige Hexadezimalzahl im Bereich zwischen 0600 und FFFF.

  Hinweis Wenn Sie unter **Protokoll** den Wert „Sämtlicher Datenverkehr“ ausgewählt haben, müssen Sie die Felder **Quelladresse** und **Zieladresse** ausfüllen.

- **Class of Service**: Legt einen Wert für die Class of Service-802.1p-Benutzerpriorität fest.
  - **Beliebig**: Alle Class of Service-Typen werden zugelassen.
  - **Benutzerdefiniert**: Geben Sie eine 802.1p-Benutzerpriorität ein, die mit einem Ethernet-Frame verglichen werden soll. Gültig sind Werte im Bereich von 0 bis 7.
- **VLAN-ID**: Die VLAN-ID, die mit einem Ethernet-Frame verglichen werden soll.
  - **Beliebig**: Alle VLAN-IDs werden zugelassen.
  - **Benutzerdefiniert**: Geben Sie die spezifische VLAN-ID ein, die mit einem Ethernet-Frame verglichen werden soll. Dieses Feld befindet sich im ersten/einzigen 802.1Q VLAN-Tag. Der Port-Bereich liegt zwischen 1 und 4094.

Schritt 8 Klicken Sie auf **OK**. Die Änderungen werden in der Startkonfiguration gespeichert.

Hinweis Um eine Klassenzuordnung zu löschen oder zu bearbeiten, wählen Sie die Klassenzuordnung in der Liste aus und klicken Sie auf **Löschen**. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Schritt 9 Klicken Sie auf **Speichern**.

QoS-Richtlinie

Pakete werden anhand definierter Kriterien klassifiziert und verarbeitet. Die Klassifizierungskriterien werden anhand einer Klasse auf der Seite „Klassenzuordnung“ definiert. Die Verarbeitung definieren Sie anhand der Attribute einer Richtlinie auf der Seite „Richtlinienzuordnung“. Richtlinienattribute werden pro Klasseninstanz definiert und bestimmen, auf welche Weise der den Klassenkriterien entsprechende Verkehr behandelt wird.

Das WAP-Gerät kann bis zu 50 Richtlinien und bis zu 10 Klassen pro Richtlinie enthalten.

So können Sie eine Richtlinienzuordnung hinzufügen und konfigurieren:

Schritt 1 Wählen Sie **Client-QoS > QoS-Richtlinie** aus.

Schritt 2 Klicken Sie auf □, um eine QoS-Richtlinie hinzuzufügen: Geben Sie im Feld „Name der QoS-Richtlinie“ einen Namen für die QoS-Richtlinie ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

Schritt 3 Sie können eine zuvor erstellte zugeordnete Datenverkehrsklasse auswählen.

Schritt 4 Konfigurieren Sie im Bereich „Definition der QoS-Richtlinie“ die folgenden Parameter für die Richtlinienzuordnung:

- **Vereinbarte Rate**: Die vereinbarte Bitrate in KBit/s, der der Verkehr entsprechen muss. Möglich sind Werte im Bereich von 1 bis 1000000 KBit/s.
- **Vereinbarter Burst**: Die vereinbarte Burst-Größe in Byte, der der Verkehr entsprechen muss. Möglich sind Werte im Bereich von 1 bis 1600000 KBit/s.
- **Aktion**: Wählen Sie eine der folgenden Optionen aus:
  - **Senden**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom weitergeleitet werden sollen, wenn das Kriterium der Datenverkehrsklasse erfüllt ist.
  - **Löschen**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom gelöscht werden sollen, wenn das Kriterium der Datenverkehrsklasse erfüllt ist.
- **Datenverkehr neu markieren**: Markiert alle Pakete für den zugeordneten Verkehrsstrom mit dem angegebenen Class of Service-Wert aus dem Prioritätsfeld des 802.1p-Headers. Wenn der Header nicht bereits im Paket enthalten ist, wird er eingefügt. Der CoS-Wert ist eine Ganzzahl von 0 bis 7.
  - **COS neu markieren**: Der Netzwerkdatenverkehr kann in mehrere Prioritätsstufen oder Classes of Service partitioniert werden. Die CoS-Werte reichen von 0 bis 7, wobei 0 die niedrigste und 7 die höchste Priorität darstellt.
  - **DSCP neu markieren**: Gibt ein bestimmtes Verhalten für Hops (per-hop behavior, PHB) an, das auf Basis der angegebenen QoS auf ein Paket angewendet wird. Wählen Sie einen Wert aus der Dropdownliste aus.

- **IP-Priorisierung neu markieren**: Markiert alle Pakete für den zugeordneten Verkehrsstrom mit dem angegebenen Wert für den IP-Vorrang. Der Wert für den IP-Vorrang ist eine Ganzzahl von 0 bis 7.

Schritt 5 Klicken Sie auf **Richtlinienattribut hinzufügen**. Sie können die andere Klassenzuordnung hinzufügen, aber für diese Richtlinie gilt eine Obergrenze von 10 Klassenzuordnungen.

Schritt 6 Klicken Sie auf **Speichern**.

Hinweis Um eine QoS-Richtlinie zu löschen oder zu bearbeiten, wählen Sie die QoS-Richtlinie in der Liste aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

QoS-Zuordnung

Die Seite „QoS-Zuordnung“ bietet zusätzliche Kontrolle über bestimmte QoS-Aspekte der Wireless- und Ethernet-Schnittstelle.

Neben der Steuerung der allgemeinen Verkehrskategorien können Sie mit QoS die Abstimmung verschiedener Mikrodatenflüsse auf einzelne Clients über den QoS-Richtliniennamen konfigurieren. Mit dem QoS-Richtliniennamen können Sie eine allgemeine Definition für ein- und ausgehende Mikrodatenflüsse und für Behandlungsmerkmale festlegen, die bei der Authentifizierung im Netzwerk auf die einzelnen WLAN-Clients angewendet werden können.

So konfigurieren Sie die Parameter für die QoS-Zuordnung:

Schritt 1 Wählen Sie **Client-QoS** > **QoS-Zuordnung** aus.

Schritt 2 Klicken Sie auf □, um eine QoS-Zuordnung hinzuzufügen.

Schritt 3 Wählen Sie in der Dropdownliste **QoS-Richtlinienname** einen Namen für die QoS-Richtlinie aus.

Schritt 4 Konfigurieren Sie Folgendes:

- **Ratenlimit (vom AP zum Client)**: Die maximal zulässige Übertragungsrate vom WAP-Gerät zum Client in Bit pro Sekunde (Bit/s). Gültig sind Werte zwischen 0 und 1733 Mbps.
- **Ratenlimit (vom Client zum AP)**: Die maximal zulässige Übertragungsrate vom Client zum WAP-Gerät in Bit pro Sekunde (Bit/s). Gültig sind Werte zwischen 0 und 1733 Mbps.

Schritt 5 Klicken Sie auf **Speichern**.

Hinweis Eine Schnittstelle kann entweder mit einer QoS-Richtlinie oder mit einer ACL gebunden werden, jedoch nicht mit beidem.

Gastzugang

Sie können die CP-Standardinstanz auf dem WAP-Gerät konfigurieren. Die CP-Instanz besteht aus einem definierten Satz von Instanzparametern. Die Instanz kann zu einem oder mehreren VAPs zugeordnet werden.

Wenn Sie sich mit einem WLAN-Client mit einem VAP verbinden und eine beliebige URL aufrufen, werden Sie auf die Seite „Gebietsschema für das Webportal“ weitergeleitet, die Sie auf der Seite „Zugangskontrolle/Gastzugriff“ konfigurieren können.

Das Gebietsschema für das Webportal definiert den Anzeigestil der umgeleiteten GUI-Seite, und die Gastgruppe definiert den Benutzernamen und das Passwort des Benutzers.

So können Sie die Gastzugangsinstanz konfigurieren:

Schritt 1 Bearbeiten Sie **Gebietsschematabelle für das Webportal**, um den Anzeigestil der umgeleiteten GUI-Seite festzulegen. Klicken Sie auf die Registerkarte **Vorschau**, um eine Vorschau anzuzeigen.

Schritt 2 Bearbeiten Sie die **Gastgruppentabelle**, klicken Sie auf den Link „Wert“ neben **Gastbenutzer insgesamt**, um einen Benutzer hinzuzufügen, und klicken Sie auf **Speichern**.

Schritt 3 Konfigurieren Sie die **Gastzugangsinstanz-Tabelle**, und wählen Sie die **Gastgruppe** und das **Gebietsschema für das Webportal** aus, die Sie in den vorherigen Schritten konfiguriert haben.

Schritt 4 Unter **Wireless-** > **Netzwerke** können Sie den VAP-Gastzugang zuordnen und die Gastzugangsinstanz konfigurieren.

Gastzugangsinstanz-Tabelle

Schritt 1 Wählen Sie **Gastzugang** > **Gaszugangsinstanz-Tabelle** aus.

Schritt 2 Geben Sie im Feld **Name der Gastzugangsinstanz** einen Namen für die CP-Instanz ein. Der Name kann bis zu 32 alphanumerische Zeichen enthalten.

Schritt 3 Daraufhin wird der Bereich „Captive Portal-Instanzparameter“ mit zusätzlichen Optionen erneut angezeigt. Konfigurieren Sie die folgenden Parameter:

- **Protokoll**: Geben Sie HTTP oder HTTPS als das Protokoll an, das die CP-Instanz während des Überprüfungsvorgangs verwenden soll.
  - **HTTP**: Bei der Überprüfung wird keine Verschlüsselung verwendet.
  - **HTTPS**: Verwendet Secure Sockets Layer (SSL). Dabei ist für die Verschlüsselung ein Zertifikat erforderlich. Das Zertifikat wird den Benutzern beim Herstellen der Verbindung angezeigt.
- **Authentifizierungsmethode**: Wählen Sie das Authentifizierungsverfahren aus, das CP zum Überprüfen von Clients verwendet: Folgende Optionen sind verfügbar:
  - **Lokale Datenbank**: Das WAP-Gerät verwendet zum Authentifizieren von Benutzern eine lokale Datenbank. Konfigurieren Sie die folgenden Felder, wenn Sie eine lokale Datenbank verwenden.
    - **Name der Gastgruppe**: Geben Sie einen Namen für die Gastgruppe ein.
    - **Zeitlimit bei Inaktivität**: Geben Sie ein Zeitlimit in Minuten für die Inaktivität ein.
    - **Maximale Uploadbandbreite**: Die maximale Upload-Geschwindigkeit in Megabit pro Sekunde, mit der ein Client bei Verwendung des Captive Portals Daten senden kann. Diese Einstellung begrenzt die Bandbreite, mit der Daten an das Netzwerk gesendet werden. Möglich sind Werte im Bereich von 0 bis 1733 Mbps. Die Standardeinstellung ist 0.
    - **Maximale Downloadbandbreite**: Die maximale Download-Geschwindigkeit in Megabit pro Sekunde, mit der ein Client bei Verwendung des Captive Portals Daten empfangen kann. Diese

Einstellung begrenzt die Bandbreite, mit der Daten vom Netzwerk empfangen werden. Möglich sind Werte im Bereich von 0 bis 1733 Mbps. Die Standardeinstellung ist 0.

- **Gastbenutzer insgesamt**: Die Anzahl aller Gastbenutzer

- **RADIUS-Authentifizierung**: Das WAP-Gerät verwendet zum Authentifizieren von Benutzern eine Datenbank auf einem Remote-RADIUS-Server. Konfigurieren Sie die folgenden Felder, wenn Sie die RADIUS-Authentifizierung verwenden.
  - **Radius-IP-Netzwerk**: Wählen Sie das Radius-IP-Netzwerk in der Dropdownliste aus (**IPv4 oder IPv6**).
  - **RADIUS global**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die globale RADIUS-Option zu aktivieren. Wenn die CP-Funktion andere RADIUS-Server verwenden soll, deaktivieren Sie das Feld und konfigurieren Sie die Server in den Feldern auf dieser Seite.
  - **RADIUS-Abrechnung**: Aktivieren Sie **Aktivieren**, um von einem bestimmten Benutzer verwendete Ressourcen zu verfolgen und zu messen, beispielsweise die Systemzeit und die Menge der gesendeten und empfangenen Daten.

    Wenn Sie die RADIUS-Abrechnung aktivieren, wird die Funktion für den primären RADIUS-Server, alle Backup-Server sowie alle konfigurierten Server aktiviert.
  - **Server-IP-Adresse 1 oder Server-IPv6-Adresse1**: Geben Sie die IPv4- oder IPv6-Adresse des primären RADIUS-Servers für diesen VAP ein. Geben Sie die IPv4-Adresse im Format xxx.xxx.xxx.xxx (192.0.2.10) ein. Geben Sie die IPv6-Adresse im Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) ein.

    Wenn sich der erste WLAN-Client bei einem VAP zu authentifizieren versucht, sendet das WAP-Gerät eine Authentifizierungsanfrage an den primären Server. Wenn der primäre Server auf die Authentifizierungsanfrage antwortet, verwendet das WAP-Gerät diesen RADIUS-Server weiterhin als primären Server, und Authentifizierungsanfragen werden an die angegebene Adresse gesendet.

    Server-IP-Adresse 2 oder Server-IPv6-Adresse 2 : Geben Sie bis zu drei IPv4- oder IPv6-Adressen für RADIUS-Backup-Server ein. Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird der Reihe nach jeder konfigurierte Backup-Server ausprobiert.
  - **Schlüssel 1**: Geben Sie den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät für die Authentifizierung beim primären RADIUS-Server verwendet. Sie können bis zu 63 alphanumerische Standardzeichen und Sonderzeichen verwenden. Beim Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden, und der Schlüssel muss dem auf dem RADIUS-Server konfigurierten Schlüssel entsprechen. Der eingegebene Text wird mit Sternchen maskiert.

    Schlüssel 2: Geben Sie den RADIUS-Schlüssel für die konfigurierten RADIUS-Backupserver ein. Der Server mit der IP-Adresse 1 verwendet Schlüssel 1, IP-Adresse 2 verwendet Schlüssel 2 und so weiter.

- **Keine Authentifizierung**: Die Benutzer müssen nicht anhand einer Datenbank authentifiziert werden.
- **Anmeldedaten von Dritten** – Das WAP-Gerät nutzt Anmeldedaten aus Social Media, um Benutzer zu authentifizieren. Konfigurieren Sie Folgendes, wenn Sie die Einstellung „Authentifizierung mit anderen Anmeldedaten“ nutzen.
  - **Akzeptierte Anmeldedaten** – Wählen Sie Facebook, Google oder beides, um sie für die Authentifizierung der Anmeldedaten zu verwenden.

- **Geschlossene Plattform** – Diese Standardkonfiguration wird automatisch festgelegt, wenn **Akzeptierte Anmeldedaten** ausgewählt wird.

Hinweis Cisco integriert Datenschutz, Privatsphäre und Sicherheitsanforderungen in Produktdesign und Entwicklungsmethoden von der Ideenfindung bis zur Produkteinführung. Weitere Informationen finden Sie unter: *https://www.cisco.com/c/en/us/about/trust-center/gdpr.html*.

- **Active Directory-Service** – Das WAP-Gerät nutzt eine Datenbank auf einem Remote-ADS-Server, um Benutzer zu authentifizieren. Konfigurieren Sie Folgendes, wenn Sie die Einstellung „Authentifizierung durch ADS“ nutzen.
  - **Active Directory-Server** – Fügen Sie einen neuen ADS-Server hinzu, indem Sie auf das Symbol klicken. Sie können bis zu 3 Server hinzufügen. Verwenden Sie den **Pfeil**, um Server zu verschieben und priorisieren. Wählen Sie den **Papierkorb** aus, um die Konfiguration zu löschen. Verwenden Sie die Funktion Test, um zu prüfen, ob der ADS-Server gültig ist.

- **Gastgruppe**: Wenn Sie die Authentifizierungsmethode „Lokale Datenbank“ oder „RADIUS-Authentifizierung“ verwenden, wählen Sie eine zuvor erstellte Gastgruppe aus. Alle zu der Gruppe gehörenden Benutzer können über dieses Portal auf das Netzwerk zugreifen.
- **Weiterleitungs-URL**: Geben Sie die URL ein, um die URL-Weiterleitung zu aktivieren (inklusive „http://“). Möglich sind Werte im Bereich von 0 bis 256 Zeichen.
- **Sitzungstimeout**: Geben Sie die Zeit in Sekunden ein, während der die CP-Sitzung gültig ist. Wenn dieser Timer abläuft, wird die Authentifizierung des Clients aufgehoben. Möglich sind Werte im Bereich von 0 bis 1440 Minuten. Der Standardwert lautet "0".
- **Webportal-Gebietsschema**: Wählen Sie ein zuvor erstelltes Gebietsschema für das Webportal aus der Dropdownliste aus.

Schritt 4 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Gastgruppentabelle

Auf dem Gerät wird jeder lokale Benutzer zu einer Benutzergruppe zugewiesen, und die Gruppe wird zu einer CP-Instanz zugewiesen. Die Gruppe erleichtert das Verwalten der Zuordnung von Benutzern zu CP-Instanzen.

Die integrierte Benutzergruppe „Standard“ kann nicht gelöscht werden.

So konfigurieren Sie einen lokalen Benutzer:

Schritt 1 Wählen Sie **Gastzugriff > Gastgruppentabelle** aus.

Schritt 2 Konfigurieren Sie die folgenden Parameter im Bereich „Gastgruppeneinstellungen“:

- **Gastgruppenname**: Geben Sie einen Namen für die neue Gastgruppe ein. Der Standardname für Gastgruppen lautet **Default**.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **Zeitlimit bei Inaktivität**: Gibt an, wie lange ein Benutzer in der Liste der authentifizierten CP-Clients bleibt, nachdem die Zuordnung zum WAP-Gerät aufgehoben wurde. Wenn der in diesem Feld angegebene Zeitraum verstreicht, bevor der Client sich erneut zu authentifizieren versucht, wird der Clienteintrag aus der Liste der authentifizierten Clients entfernt. Möglich sind Werte im Bereich von 0 bis 1440 Minuten. Der Standardwert lautet "60". Der hier konfigurierte Timeout-Wert hat Vorrang vor dem für die CP-Instanz konfigurierten Wert, es sei denn, der Benutzerwert ist auf 0 festgelegt Wenn der Wert auf 0 festgelegt ist, wird der für die CP-Instanz konfigurierte Timeout-Wert verwendet.
- **Maximale Uploadbandbreite**: Die maximale Upload-Geschwindigkeit in Megabit pro Sekunde, mit der ein Client bei Verwendung des Captive Portals Daten senden kann. Diese Einstellung begrenzt die Bandbreite, mit der Daten an das Netzwerk gesendet werden. Möglich sind Werte im Bereich von 0 bis 1.733 MBit/s. Die Standardeinstellung ist 0.
- **Maximale Downloadbandbreite**: Die maximale Download-Geschwindigkeit in Megabit pro Sekunde, mit der ein Client bei Verwendung des Captive Portals Daten empfangen kann. Diese Einstellung begrenzt die Bandbreite, mit der Daten vom Netzwerk empfangen werden. Möglich sind Werte im Bereich von 0 bis 1.733 MBit/s. Die Standardeinstellung ist 0.
- **Gastbenutzer insgesamt**: Zeigt die Gesamtzahl aller Gastbenutzer an. Klicken Sie auf den Link „Wert“ neben **Gastbenutzer insgesamt**, um die Seite **Gastbenutzerkonto** zu öffnen.

Schritt 4 Klicken Sie auf **Speichern**.

Gastbenutzerkonto

So konfigurieren Sie ein Gastbenutzerkonto:

Schritt 1 Wählen Sie **Gastzugriff > Gastgruppentabelle** aus.

Schritt 2 Klicken Sie auf den Link „Nummer“ neben **Gastbenutzer insgesamt**, um die **Gastbenutzerkonto-Tabelle** auf der Seite **Gastbenutzerkonto** zu öffnen.

Schritt 3 Klicken Sie auf □, um einen Benutzer hinzuzufügen:

Schritt 4 **Gastbenutzername**: Geben Sie den Namen des neuen Gastbenutzers ein. Der Name kann bis zu 32 alphanumerische Zeichen enthalten.

Schritt 5 **Gastbenutzerpasswort**: Geben Sie das Passwort ein. Das Passwort kann 8 bis 64 alphanumerische Zeichen sowie Sonderzeichen enthalten.

Schritt 6 Klicken Sie auf **Speichern**.

Hinweis Klicken Sie auf **Zurück**, um die Seite **Gastzugang** anzuzeigen.

Um einen Gastbenutzer zu löschen oder zu bearbeiten, wählen Sie den Benutzer aus und klicken Sie auf **Löschen** oder auf **Bearbeiten**.

Anpassung des Webportals

Nachdem die CP-Instanz einem VAP zugeordnet wurde, müssen Sie ein Gebietsschema erstellen und dieses der CP-Instanz zuordnen. Wenn der Benutzer auf einen VAP zugreift, der einer CP-Instanz zugeordnet ist, wird eine Authentifizierungsseite angezeigt.

Auf der Seite „Anpassung des Webportals“ können Sie eindeutige Seiten für verschiedene Gebietsschemas im Netzwerk erstellen und den Text und die Bilder auf den Seiten anpassen.

Schritt 1 Wählen Sie **Gastzugang** > **Gebietsschematabelle für das Webportal**.

Schritt 2 Klicken Sie in dieser Tabelle auf **hinzufügen**, um auf die Seite **Captive Portal-Anpassung** zuzugreifen. Um das Gebietsschema zu ändern, markieren sie die Zeile, und klicken Sie auf **Bearbeiten**, oder klicken Sie auf **Löschen**, um es zu löschen.

Sie können bis zu drei verschiedene Authentifizierungsseiten mit verschiedenen Gebietsschemas im Netzwerk erstellen.

Schritt 3 Konfigurieren Sie im Bereich **Gebietsschemaparameter für das Captive Portal-Web** die folgenden Einstellungen:

- **Gebietsschemaname für das Webportal**: Geben Sie einen Gebietsschemanamen für das Web ein, der der Seite zugeordnet werden soll. Der Name kann aus 1 bis 32 alphanumerischen Zeichen bestehen.

Schritt 4 Der Bereich „Gebietsschemaparameter für das Captive Portal-Web“ zeigt die zusätzlichen Optionen für die Änderung des Gebietsschemas an. Der Gastzugangs-Instanzname kann nicht bearbeitet werden. Die Felder, die Sie bearbeiten können, sind mit Standardwerten gefüllt. Konfigurieren Sie die folgenden Parameter:

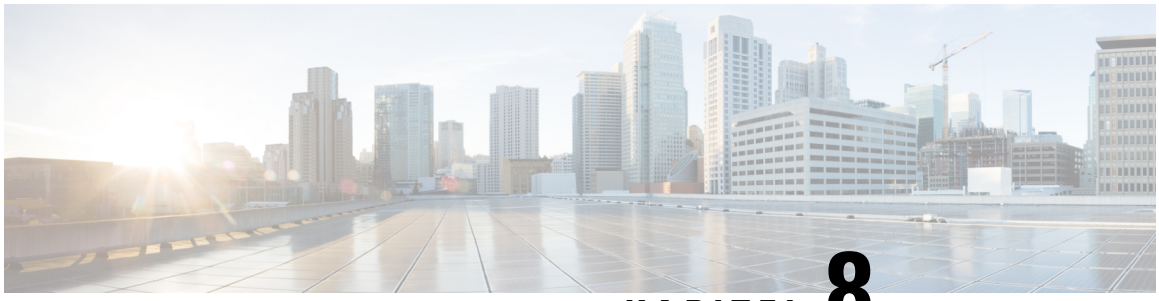
- **Gastzugangs-Instanzname**: Zeigt den Namen der Gastzugangsinstanz an.
- **Hintergrundbild**: Klicken Sie auf **Durchsuchen**, um das Bild auszuwählen. Sie können auf **Hochladen** klicken, um die Bilder für CP-Instanzen hochzuladen.
- **Logo-Bild** : Klicken Sie auf **Durchsuchen**, um das Logo-Bild auszuwählen. Sie können auf **Hochladen** klicken, um die Logo-Bilder hochzuladen.
- **Vordergrundfarbe**: Geben Sie den HTML-Code für die Vordergrundfarbe im sechsstelligen Hexadezimalformat ein. Sie können 1 bis 32 Zeichen eingeben. Der Standardwert lautet „#FFFFFF“.
- **Hintergrundfarbe**: Geben Sie den HTML-Code für die Hintergrundfarbe im sechsstelligen Hexadezimalformat ein. Sie können 1 bis 32 Zeichen eingeben. Der Standardwert lautet „#FFFFFF“.
- **Trennlinienfarbe**: Geben Sie den HTML-Code für die Farbe der dicken horizontalen Linie, die die Seitenüberschrift vom Hauptbereich trennt, im sechsstelligen Hexadezimalformat ein. Sie können 1 bis 32 Zeichen eingeben. Der Standardwert lautet „#FFFFFF“.
- **Kontobild**: Klicken Sie auf **Durchsuchen**, um das Bild auszuwählen. Sie können auf **Hochladen** klicken, um die Kontobilder hochzuladen.
- **Schriftarten**: Wählen Sie eine Schriftart aus der Dropdown-Liste aus. Diese Schriftart wird auf den gesamten angezeigten Text angewendet.
- **Kontobezeichnung**: Geben Sie einen Benutzernamen ein. Sie können 1 bis 32 Zeichen eingeben.
- **Benutzernamenbezeichnung**: Das Label des Textfelds für den Benutzernamen. Sie können 1 bis 32 Zeichen eingeben.

- **Kennwortbezeichnung**: Das Label des Textfelds für das Benutzerkennwort. Sie können 1 bis 64 Zeichen eingeben.
- **Schaltflächenbezeichnung**: Das Label der Schaltfläche, auf die Benutzer klicken, um den Benutzernamen und das Kennwort zur Authentifizierung zu übermitteln. Sie können 2 bis 32 Zeichen eingeben. Der Standardwert lautet „Verbinden“.
- **Browsertitelbezeichnung**: Der Text, der in der Titelleiste des Browsers angezeigt werden soll. Sie können 1 bis 128 Zeichen eingeben. Der Standardwert lautet „Captive Portal“.
- **Portaltitelbezeichnung** : Der Text, der im Seiten-Header rechts neben dem Logo angezeigt wird. Sie können 1 bis 128 Zeichen eingeben. Der Standardwert lautet „Welcome to the Wireless Network“.
- **Kontotippsbezeichnung**: Der Text, der im Textkörper der Seite unter den Textfeldern für Benutzername und Kennwort angezeigt wird. Sie können 1 bis 256 Zeichen eingeben. Der Standardwert lautet „To start using this service, enter your credentials and click the connect button“.
- **Nutzungsrichtlinie akzeptieren**: Der Text, der im Feld „Nutzungsrichtlinie akzeptieren“ angezeigt wird. Sie können 1 bis 4096 Zeichen eingeben. Der Standardwert lautet „Nutzungsrichtlinien akzeptieren“.
- **Akzeptierungsbezeichnung**: Der Text, mit dem Benutzer angewiesen werden, durch Aktivieren des Kontrollkästchens zu bestätigen, dass sie die Richtlinien für die Nutzung gelesen haben und akzeptieren. Sie können 1 bis 128 Zeichen eingeben.
- **Text bei Nicht-Akzeptieren**: Der Text, der in einem Popupfenster angezeigt wird, wenn Benutzer Anmeldeinformationen übermitteln, ohne das Kontrollkästchen „Nutzungsrichtlinie akzeptieren“ zu aktivieren. Sie können 1 bis 128 Zeichen eingeben.
- **Bezeichnung für „In Bearbeitung“**: Der Text, der während des Authentifizierungsvorgangs angezeigt wird. Sie können 1 bis 128 Zeichen eingeben.
- **Bezeichnung bei ungültigen Anmeldeinformationen**: Der Text, der angezeigt wird, wenn die Authentifizierung eines Benutzers fehlschlägt. Sie können 1 bis 128 Zeichen eingeben.
- **Bezeichnung bei erfolgreicher Verbindungsherstellung**: Der Text, der angezeigt wird, wenn der Client beim VAP authentifiziert wurde. Sie können 1 bis 128 Zeichen eingeben.
- **Begrüßungsbezeichnung**: Der Text, der angezeigt wird, wenn der Client eine Verbindung mit dem Netzwerk hergestellt hat. Sie können 1 bis 256 Zeichen eingeben.
- **Wiederherstellen**: Löscht das aktuelle Gebietsschema.

Schritt 5 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Schritt 6 Klicken Sie auf **Vorschau**, um die aktualisierte Seite anzuzeigen.

Sie können auf **Vorschau** klicken, um den Text und die Bilder anzuzeigen, die bereits in der Startkonfiguration gespeichert sind. Wenn Sie eine Änderung vornehmen, klicken Sie auf **Speichern**, bevor Sie auf **Vorschau** klicken, um die Änderungen anzuzeigen.



KAPITEL 8

Umbrella

In diesem Kapitel wird beschrieben, wie der Dienst **Cisco Umbrella** konfiguriert wird. Das Kapitel enthält die folgenden Themen:

Cisco Umbrella

Cisco Umbrella ist eine Cloud-Sicherheitsplattform, welche die erste Verteidigungslinie gegen Bedrohungen im Internet bildet. Die Lösung fungiert als Gateway zwischen dem Internet und Ihren Systemen und Daten, um Malware, Botnets und Phishing-Versuche über diverse Ports, Protokolle oder Anwendungen zu blockieren.

Mithilfe eines Umbrella-Kontos fängt diese Integration DNS-Abfragen transparent ab und leitet sie an Umbrella weiter. Dieses Gerät wird im Umbrella-Dashboard als Netzwerkgerät für die Anwendung von Richtlinien und die Anzeige von Berichten angezeigt.

Schritt 1 Aktivieren Sie das Kontrollkästchen, um die Umbrella-Funktion zu aktivieren.

Schritt 2 Geben Sie den geheimen Schlüssel und den API-Schlüssel, den Sie von der **Umbrella**-Website erhalten, im entsprechenden Feld ein.

Hinweis Melden Sie sich bei Ihrem Cisco Umbrella-Konto an und wechseln Sie zum Dashboard: Gehen Sie zu **Verwaltung > Plattform-API-Schlüssel**, um einen Namen hinzuzufügen und einen geheimen Schlüssel und zugehörige Informationen zu erstellen.

Schritt 3 Geben Sie im Feld **Zu umgehende lokale Domänen (optional)** einen vertrauenswürdigen Domänennamen ein, dann werden die Pakete ohne Umweg über Umbrella ihr Ziel erreichen.

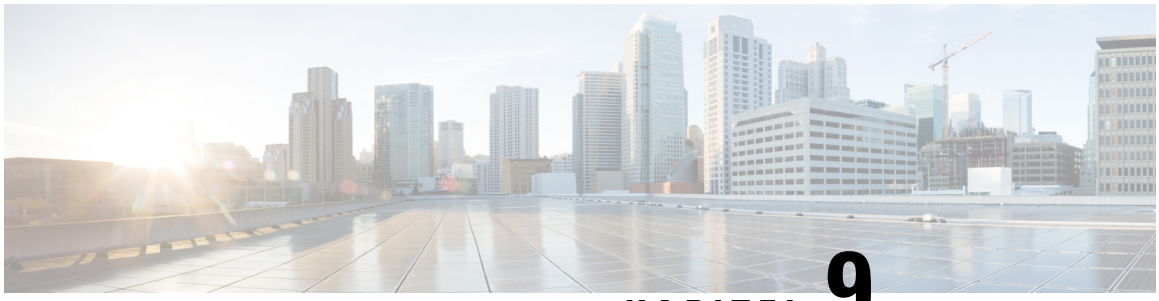
Hinweis Dies ist für alle Intranet-Domänen und Split-DNS-Domänen erforderlich

Schritt 4 Geben Sie im Feld **Geräte-Tag (optional)** einen Tag-Namen ein, um das Gerät zu kennzeichnen.

Schritt 5 Aktivieren Sie das Kontrollkästchen, um die DNS-Verschlüsselung zu aktivieren.

Hinweis DNSCrypt wird verwendet, um die Kommunikation zwischen einem DNS-Client und einem verschleierten DNS-Resolver zu sichern. Damit werden verschiedene Arten von DNS-Angriffen und Snooping verhindert. Diese Funktion ist standardmäßig aktiviert.

Schritt 6 Klicken Sie auf **Speichern**, um diese Konfigurationen anzuwenden. Der Status der Registration wird im Feld Registrationsstatus angezeigt.



KAPITEL 9

Überwachen

In diesem Kapitel wird beschrieben, wie Sie Status und Statistiken für das WAP-Gerät anzeigen. Das Kapitel enthält die folgenden Themen:

Dashboard

Im Dashboard wird der Durchsatzstatus zusammen mit einfachen Schritten für die Konfiguration oder Überwachung Ihres Netzwerkgeräts angezeigt. Diese Seite wird alle 30 Sekunden aktualisiert.

Verbundene Clients

Die Gesamtanzahl der Clients, die momentan zum WAP-Gerät zugeordnet sind. Klicken Sie auf das Feld, um zur Seite „Clients“ zu gelangen.

Internet/LAN/Wireless

Die runden Symbole oben rechts auf der Seite zeigen den Status der Internet-, LAN- und Wireless-Verbindungen an.

Internet

- **Roter Kreis**: Keine Internetverbindung.
- **Grüner Kreis**: Internetverbindung ist vorhanden.

LAN

- **Roter Kreis**: Keine Kabelverbindung.
- **Grüner Kreis**: Kabelverbindung ist vorhanden.

Klicken Sie auf den Link **LAN**, um die Seite **LAN-Status** zu öffnen.

Wireless

- **Roter Kreis**: Alle Funkmodule sind deaktiviert.
- **Grüner Kreis**: Mindestens ein Funkmodul ist einsatzbereit. Ein oder zwei Funkmodule sind aktiviert.

Klicken Sie auf den Link **Wireless**, um Seite **Wireless-Status** zu öffnen.

Durchsatz des 2,4-GHz-Funkmoduls

Dieses Liniendiagramm zeigt den Durchsatz des 2,4-GHz-Funkmoduls an und wird alle 30 Sekunden aktualisiert.

- **Upload**: Durchsatz der letzten 30 Sekunden an gesendeten Daten.
- **Download**: Durchsatz der letzten 30 Sekunden an empfangenen Daten.

Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

Durchsatz des 5-GHz-Funkmoduls

Dieses Liniendiagramm zeigt den Durchsatz des 5-GHz-Funkmoduls an und wird alle 30 Sekunden aktualisiert.

- **Upload**: Durchsatz der letzten 30 Sekunden an gesendeten Daten.
- **Download**: Durchsatz der letzten 30 Sekunden an empfangenen Daten.

Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

Top-Clients

Dieses Balkendiagramm zeigt die 5 Clientgeräte mit dem höchsten Datenverkehr an.

- **Upload**: Durchsatz der letzten 30 Sekunden an gesendeten Daten.
- **Download**: Durchsatz der letzten 30 Sekunden an empfangenen Daten.

Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

SSID-Auslastung

Dieses Balkendiagramm zeigt die 5 SSIDs mit dem höchsten Datenverkehr an.

- Datenverkehr: Die Gesamtzahl der empfangenen und gesendeten Bytes.

Netzwerkverwendung

Dieses Liniendiagramm zeigt den Ethernet-Durchsatz an.

- **Upload**: Durchsatz der letzten 30 Sekunden an gesendeten Daten.
- **Download**: Durchsatz der letzten 30 Sekunden an empfangenen Daten.

Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

Schnellzugang

Zur Vereinfachung der Gerätekonfiguration finden Sie auf der Seite **Erste Schritte** Links zum Ausführen allgemeiner Aufgaben. Weitere Details finden Sie unter QuickStart-Konfiguration, auf Seite 8.

LAN-Status

Klicken Sie auf den LAN-Kreis, um die folgenden Konfigurations- und Statuseinstellungen für die LAN-Schnittstelle anzuzeigen.

- **MAC-Adresse**: Die MAC-Adresse des WAP-Geräts.

- **IP-Adresse**: Die IP-Adresse des WAP-Geräts.
- **Subnetzmaske**: Die Subnetzmaske des WAP-Geräts.
- **Standardgateway**: Das Standardgateway des WAP-Geräts.
- **DNS-Server 1**: Die vom WAP-Gerät verwendete IP-Adresse von DNS-Server 1.
- **DNS-Server 2**: Die vom WAP-Gerät verwendete IP-Adresse von DNS-Server 2.
- **IPv6-Adresse**: Die IPv6-Adresse des WAP-Geräts.
- **Automatisch konfigurierte globale IPv6-Adressen**: Die automatisch konfigurierten globalen IPv6-Adressen.
- **IPv6-Link Local-Adresse**: Die IPv6-Link Local-Adresse des WAP-Geräts.
- **IPv6-Standardgateway**: Das IPv6-Standardgateway des WAP-Geräts.
- **IPv6-DNS-1**: Die IPv6-Adresse von IPv6-DNS-Server 1, die vom WAP-Gerät verwendet wird.
- **IPv6-DNS-2**: Die IPv6-Adresse von IPv6-DNS-Server 2, die vom WAP-Gerät verwendet wird.

Hinweis Diese Einstellungen gelten für die interne Schnittstelle. Klicken Sie auf **Bearbeiten**, um diese Einstellungen zu ändern. Sie werden auf die Seite **LAN** weitergeleitet.

Sie können auf **Aktualisieren** klicken, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

Klicken Sie auf **Zurück**, um zur Seite **Dashboard** zurückzukehren.

WLAN-Status

Klicken Sie auf den WLAN-Kreis, um die WLAN-Funkschnittstellen zu konfigurieren:

- **WLAN-Funk**: Der WLAN-Funkmodus ist für die Funkschnittstelle aktiviert oder deaktiviert.
- **MAC-Adresse**: Die MAC-Adresse, die der Funkschnittstelle zugeordnet ist.
- **Modus**: Der 802.11-Modus (a/b/g/n/ac), den die Funkschnittstelle verwendet.
- **Kanal**: Der von der Funkschnittstelle verwendete Kanal.
- **Betriebsbandbreite**: Die Betriebsbandbreite, die von der Funkschnittstelle verwendet wird.

Klicken Sie auf **Bearbeiten**, um diese Einstellungen zu ändern. Sie werden auf die Seite **Funk** weitergeleitet.

Sie können auf **Aktualisieren** klicken, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

Klicken Sie auf **Zurück**, um zur Seite **Dashboard** zurückzukehren.

Schnittstellenstatus

Die Tabelle „Schnittstellenstatus“ enthält Statusinformationen für die einzelnen VAPs (Virtual Access Points) und WDS-Schnittstellen (Wireless Distribution System):

- **Netzwerkschnittstelle**: Die WLAN-Schnittstelle des WAP-Geräts.
- **Name (SSID)**: Der Name der WLAN-Schnittstelle.
- **Status**: Der Verwaltungsstatus des VAP (in Betrieb oder außer Betrieb).
- **MAC-Adresse**: Die MAC-Adresse der Funkschnittstelle.
- **VLAN-ID**: Die VLAN-ID der Funkschnittstelle.
- **Profil**: Der Name eines beliebigen zugeordneten Planungsmodulprofils.
- **Status**: Der aktuelle Status (aktiv oder inaktiv). Aus dem Status geht hervor, ob der VAP Daten mit einem Client austauscht.

Verkehrsstatistik

Auf der Seite „Verkehrsstatistik“ werden Sende- und Empfangsstatistiken für die Ethernet-Schnittstelle, die VAPs (Virtual Access Points) und sämtliche WDS-Schnittstellen in Echtzeit angezeigt. Alle Sende- und Empfangsstatistiken geben die Gesamtmengen seit dem letzten Start des WAP-Geräts wieder. Wenn Sie das WAP-Gerät neu starten, geben diese Zahlen die insgesamt gesendeten und empfangenen Mengen seit dem Neustart an.

Wählen Sie **Überwachung** > **Dashboard** > **Schnellzugriff** > **Verkehrsstatistik** aus, um die Verkehrsstatistiken anzuzeigen.

Die folgenden Informationen werden angezeigt:

- **Schnittstelle**: Die Namen der Ethernet-Schnittstelle und der einzelnen VAP- und WDS-Schnittstellen. Im Anschluss an die einzelnen VAP-Schnittstellen folgt jeweils die SSID in Klammern.
- **Pakete gesamt**: Die Gesamtanzahl der vom WAP-Gerät gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) Pakete.
- **Bytes gesamt**: Die Gesamtanzahl der vom WAP-Gerät gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) Bytes.
- **Gelöschte Pakete gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät gelöschten gesendeten (in der Tabelle „Senden“) oder empfangenen Pakete (in der Tabelle „Empfangen“).
- **Gelöschte Bytes gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät gelöschten gesendeten (in der Tabelle „Senden“) oder empfangenen Bytes (in der Tabelle „Empfangen“).
- **Fehler**: Die Gesamtanzahl der Fehler beim Senden und Empfangen von Daten auf diesem WAP-Gerät.

Hinweis Klicken Sie auf **Aktualisieren**, um die aktuellen Informationen anzuzeigen.

Single Point Setup

Auf dieser Seite werden die Clustermitglieder und der Datenverkehr auf den WAP-Geräten angezeigt, die momentan im Cluster enthalten sind.

APs mit dem höchsten Datenverkehr

Dieses Balkendiagramm zeigt die 5 WAP-Geräte mit dem höchsten Datenverkehr an.

- **Upload**: Durchsatz der übertragenen Daten.
- **Download**: Durchsatz der empfangenen Daten.

Hinweis Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

APs mit den meisten Clientverbindungen

Listet die APs nach der Anzahl der Clientverbindungen auf. Dieses Balkendiagramm zeigt die 5 WAP-Geräte mit den meisten Verbindungen an.

Kanalzuordnungstabelle

Die Kanalzuordnungstabelle enthält eine nach IP-Adressen sortierte Liste aller WAP-Geräte im Single Point Setup-Cluster.

Die Tabelle enthält die folgenden Details zu den aktuellen Kanalzuweisungen.

- **AP-Standort**: Der physische Standort des WAP-Geräts.
- **WLAN-Kanal**: Der Funkkanal, auf dem das WAP-Gerät momentan sendet.
- **IP-Adresse**: Die IP-Adresse des WAP-Geräts.
- **Datenverkehr (Up / Down)**: Die Gesamtzahl der gesendeten (Up) und empfangenen (Down) Bytes auf dem Clientgerät.
- **Clientverbindungen (2,4 G / 5 G)**: Die Anzahl der Clients, die sich mit dem WAP-Gerät verbinden.

Clients

Clients

Auf der Seite „Clients“ werden die zum Gerät zugeordneten Clientstationen angezeigt.

Gesamtzahl zugeordnete Clients: Die Gesamtanzahl der Clients, die momentan zum WAP-Gerät zugeordnet sind.

Client-Übersicht

Zeigt die Client-Übersicht nach aktuellem 802.11-Clienttyp auf dem Gerät an.

Durchschnittliche Bandbreite

Zeigt die durchschnittliche Clientbandbreite in Mbit/s an.

- **Upload**: Durchsatz der letzten 30 Sekunden an gesendeten Daten.

- **Download**: Durchsatz der letzten 30 Sekunden an empfangenen Daten.

Hinweis Klicken Sie auf **Upload** oder **Download**, um Daten auszublenden.

Clients mit niedrigstem Signal-Rausch-Verhältnis (SNR)

Listet die 5 Geräte mit dem niedrigsten SNR auf.

Clients mit niedrigster Geschwindigkeit

Listet die 5 Geräte mit der niedrigsten Geschwindigkeit auf.

Assoziierten Clients

- **Client-Details**: Der Hostname und die Mac-Adresse des zugeordneten Wi-Fi-Clients.
- **IP-Adresse**: die IP-Adresse des zugeordneten Wi-Fi-Clients.
- **Netzwerk (SSID)**: Die SSID (Service Set Identifier) für das WAP-Gerät. Bei der SSID handelt es sich um eine alphanumerische Zeichenfolge mit bis zu 32 Zeichen, die ein WLAN eindeutig identifiziert. Die SSID wird auch als Netzwerkname bezeichnet.
- **Modus**: Der auf dem Client verwendete IEEE 802.11-Modus, z. B. IEEE 802.11a, IEEE 802.11b oder IEEE 802.11g.
- **Datenrate**: Die aktuelle Datenübertragungsrate.
- **Kanal**: Der Kanal, über den der Client aktuell verbunden ist. Der Kanal definiert den Teil des Funkspektrums, den das Funkmodul zum Senden und Empfangen verwendet. Auf der Seite „Funk“ können Sie den Kanal festlegen.
- **Datenverkehr (Up / Down)**: Die Gesamtzahl der gesendeten (Up) und empfangenen (Down) Bytes auf dem Clientgerät.
- **SNR (db)**: Zeigt die SNR-Stärke in Dezibel (dB) an.
- **Durchsatzmessung**: Der Durchsatz bzw. die Datenrate der letzten 30 Sekunden.

Hinweis Sie können die Clients nach Client-Details, Netzwerk (SSID) und anderen Kriterien ordnen.

Sie können die Clients nach Client-Details, Netzwerk (SSID) und anderen Kriterien filtern.

Single Point Setup-Clients

- **Client-Details**: Die MAC-Adresse des zugeordneten WLAN-Clients.IPv4-Adresse: Die IP-Adresse des WAP-Geräts.
- **IP-Adresse**: Die IP-Adresse des WAP-Geräts.

- **Netzwerk (SSID)**: Die SSID (Service Set Identifier) für das WAP-Gerät. Bei der SSID handelt es sich um eine alphanumerische Zeichenfolge mit bis zu 32 Zeichen, die ein WLAN eindeutig identifiziert. Die SSID wird auch als Netzwerkname bezeichnet.
- **Modus**: Der auf dem Client verwendete IEEE 802.11-Modus, z. B. IEEE 802.11a, IEEE 802.11b oder IEEE 802.11g.
- **Datenrate**: Die aktuelle Übertragungsrate.
- **AP-Standort**: Der physische Standort des WAP-Geräts.
- **Kanal**: Der Kanal, über den sich der Client aktuell verbindet. Der Kanal definiert den Teil des Funkspektrums, den das Funkmodul zum Senden und Empfangen verwendet. Auf der Seite „Funk“ können Sie den Kanal festlegen.
- **Datenverkehr (Up / Down)**: Die Gesamtzahl der gesendeten (Up) und empfangenen (Down) Bytes auf dem Clientgerät.
- **SNR (db)**: Zeigt die SNR-Stärke in Dezibel (dB) an.
- **Durchsatzmessung**: Der Durchsatz bzw. die Datenrate der letzten 30 Sekunden.

Hinweis Sie können die Clients nach Client-Details, Netzwerk (SSID) und anderen Kriterien ordnen und filtern.

Gäste

Die Seite „Gäste“ enthält zwei Tabellen. Die Tabelle „Authentifizierte Clients“ enthält Informationen zu Clients, die in einer Captive Portal-Instanz authentifiziert wurden. Die Tabelle „Clients mit fehlgeschlagener Authentifizierung“ enthält Informationen zu Clients, die erfolglos versucht haben, sich im Captive Portal zu authentifizieren.

Wählen Sie **Überwachung > Gäste** aus, um eine Liste der Clients anzuzeigen, deren Authentifizierung fehlgeschlagen ist.

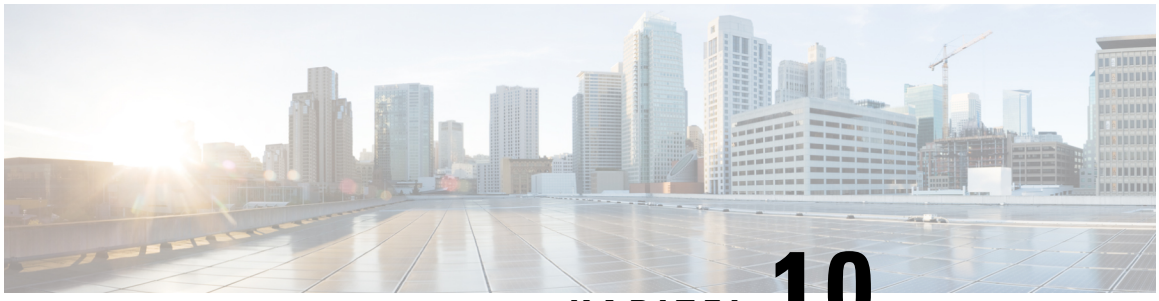
Die folgenden Informationen werden angezeigt:

- **MAC**: Die MAC-Adresse des Clients.
- **IP-Adresse**: Die IP-Adresse des Clients.
- **Benutzername**: Der CP-Benutzername des Clients.
- **Protokoll**: Das Protokoll, das der Benutzer zum Herstellen der Verbindung verwendet hat (HTTP oder HTTPS).
- **Verifizierung**: Die Methode, die für die Authentifizierung des Benutzers in Captive Portal verwendet wurde. Einer der folgenden Werte ist möglich:
  - **Gast**: Der Benutzer muss nicht anhand einer Datenbank authentifiziert werden.
  - **Lokal**: Das WAP-Gerät verwendet zum Authentifizieren von Benutzern eine lokale Datenbank.
  - **RADIUS**: Das WAP-Gerät verwendet zum Authentifizieren von Benutzern eine Datenbank auf einem Remote-RADIUS-Server.

- **VAP-/Funk-ID**: Der VAP und das Funkmodul, die dem Benutzer zugeordnet sind.
- **Captive Portal-ID**: Die ID der Captive Portal-Instanz, der der Benutzer zugeordnet ist.
- **Timeout**: Die verbleibende Zeit in Sekunden, während der die CP-Sitzung gültig ist. Wenn dieser Timer abläuft, wird die Authentifizierung des Clients aufgehoben.
- **Löschungstimeout**: Die verbleibende Zeit in Sekunden, während der der Clienteintrag gültig ist. Der Timer startet, wenn die Zuordnung zwischen Client und CP aufgehoben wird. Wenn dieser Timer abläuft, wird die Authentifizierung des Clients aufgehoben.
- **Up/Down (MP)**: Die Anzahl der Bytes, die zwischen WAP-Gerät und Benutzerstation gesendet und empfangen wurden.
- **Fehlerzeit**: Der Zeitpunkt, zu dem der Authentifizierungsfehler aufgetreten ist. Aus dem enthaltenen Zeitstempel geht der Zeitpunkt des Fehlers hervor.

Klicken Sie auf „Exportieren“, um die aktuelle Authentifizierungs-/Fehlermeldung für den Client hochzuladen.

Hinweis Wählen Sie zunächst den authentifizierten bzw. fehlgeschlagenen Client aus, den Sie exportieren möchten, und klicken Sie anschließend auf **Exportieren**.



KAPITEL 10

Administration

In diesem Kapitel wird beschrieben, wie Sie die Administrationseinstellungen konfigurieren und Diagnosefunktionen ausführen können. Das Kapitel enthält die folgenden Themen:

Firmware

Das WAP-Gerät enthält zwei Firmware-Images. Ein Image ist aktiv, das andere ist inaktiv. Wenn das aktive Image beim Start nicht geladen werden kann, wird das inaktive Image geladen und als aktives Image festgelegt. Sie können auch das aktive Image und das inaktive Image tauschen.

Wenn neue Versionen der Firmware für Ihr WAP-Gerät verfügbar sind, können Sie die Firmware aktualisieren, um neue Funktionen und Verbesserungen zu erhalten. Der WAP-Gerät verwendet einen TFTP- oder HTTP/HTTPS-Client für Firmwareupgrades.

Wenn Sie neue Firmware hochgeladen und das System neu gestartet haben, wird die neue Firmware als primäres Image festgelegt. Wenn beim Upgrade ein Fehler auftritt, wird die ursprüngliche Firmware weiter als primäres Image verwendet.

Hinweis Beim Aktualisieren der Firmware werden die vorhandenen Konfigurationsinformationen für das WAP-Gerät beibehalten.

Austauschen des Firmware-Images

So tauschen Sie das auf dem WAP Gerät ausgeführte Firmware-Image aus:

Schritt 1 Wählen Sie **Administration > Firmware** aus.

Die Produkt-ID (PID-VID) sowie die aktive und die inaktive Firmwareversionen werden angezeigt.

Schritt 2 Klicken Sie auf **Images austauschen**.

Daraufhin wird ein Dialogfeld angezeigt, in dem der Wechsel des Firmware-Images und der anschließende Neustart bestätigt wird.

Schritt 3 Klicken Sie auf **OK**, um fortzufahren.

Der Vorgang kann mehrere Minuten dauern. In dieser Zeit ist das WAP-Gerät nicht verfügbar. Schalten Sie das WAP-Gerät während des Image-Wechsels nicht aus. Nach Abschluss des Image-Wechsels wird das WAP-Gerät neu gestartet. Das WAP-Gerät nimmt den Normalbetrieb wieder auf. Dabei werden die gleichen Konfigurationseinstellungen wie vor dem Upgrade verwendet.

HTTP/HTTPS-Aktualisierung

So führen Sie ein Upgrade per HTTP/HTTPS durch:

Schritt 1 Wählen Sie **HTTP/HTTPS** als Übertragungsmethode aus.

Schritt 2 Klicken Sie auf die Schaltfläche **Durchsuchen** und suchen Sie die Firmware-Image-Datei in Ihrem Netzwerk.

Bei der angewendeten Firmware-Upgrade-Datei muss es sich um eine TAR-Datei handeln. Versuchen Sie nicht, BIN-Dateien oder Dateien in anderen Formaten für das Upgrade zu verwenden; mit diesen Dateitypen ist kein Upgrade möglich.

Schritt 3 Klicken Sie auf **"Upgrade"**, um das neue Firmware-Image zu übernehmen.

Das Hochladen der neuen Firmware kann mehrere Minuten dauern. Aktualisieren oder verlassen Sie die Seite nicht, während die neue Firmware hochgeladen wird. Andernfalls wird der Firmwareupload abgebrochen. Nach Abschluss des Vorgangs wird das WAP-Gerät neu gestartet und setzt den Normalbetrieb fort.

Schritt 4 Vergewissern Sie sich, dass das Firmware-Upgrade erfolgreich abgeschlossen wurde, indem Sie sich beim webbasierten Konfigurationshilfsprogramm anmelden und auf der Seite „Firmware-Upgrade“ die aktive Firmwareversion überprüfen.

TFTP-Aktualisierung

So aktualisieren Sie die Firmware auf dem WAP-Gerät über TFTP:

Schritt 1 Wählen Sie **TFTP** als Übertragungsmethode aus.

Schritt 2 Geben Sie in das Feld „Quelldateiname“ einen Namen (1 bis 256 Zeichen) für die Image-Datei ein. Der Name muss den Pfad des Verzeichnisses enthalten, in dem sich das hochzuladende Image befindet.

Wenn Sie beispielsweise das Image „ap_upgrade.tar“ aus dem Verzeichnis „/share/builds/ap“ hochladen möchten, geben Sie Folgendes ein: /share/builds/ap/ap_upgrade.tar

Bei der angewendeten Firmware-Upgrade-Datei muss es sich um eine TAR-Datei handeln. Versuchen Sie nicht, BIN-Dateien oder Dateien in anderen Formaten für das Upgrade zu verwenden; mit diesen Dateitypen ist kein Upgrade möglich.

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * sowie zwei oder mehr aufeinanderfolgende Punkte.

Schritt 3 Geben Sie die IPv4-Adresse des TFTP-Servers ein, und klicken Sie auf **Upgrade**.

Das Hochladen der neuen Firmware kann mehrere Minuten dauern. Aktualisieren oder verlassen Sie die Seite nicht, während die neue Firmware hochgeladen wird. Andernfalls wird der Firmwareupload abgebrochen. Nach Abschluss des Vorgangs wird das WAP-Gerät neu gestartet und setzt den Normalbetrieb fort.

Schritt 4 Vergewissern Sie sich, dass das Firmware-Upgrade erfolgreich abgeschlossen wurde, indem Sie sich beim Konfigurationshilfsprogramm anmelden und auf der Seite für das Firmware-Upgrade die aktive Firmwareversion anzeigen.

Konfigurationsdateien

Die Konfigurationsdateien für das WAP-Gerät liegen im XML-Format vor und enthalten alle Informationen zu den Einstellungen des WAP-Geräts. Sie können die Konfigurationsdateien auf einem Netzwerk-Host oder einem TFTP-Server sichern (hochladen), um den Inhalt manuell zu bearbeiten oder Sicherungen zu erstellen. Nachdem Sie eine gesicherte Konfigurationsdatei bearbeitet haben, können Sie die Datei auf das WAP-Gerät herunterladen, um die Konfiguration zu ändern. Auf dem WAP-Gerät sind die folgenden Konfigurationsdateien gespeichert:

- **Startkonfiguration**: Die im Flash-Speicher abgelegte Konfigurationsdatei.
- **Backup-Konfiguration**: Eine zusätzliche Konfigurationsdatei, die als Backup im WAP-Gerät gespeichert ist.
- **Spiegelkonfiguration**: Wenn die Startkonfiguration mindestens 24 Stunden lang nicht geändert wurde, wird sie automatisch als Spiegelkonfigurationsdatei gespeichert. Die Spiegelkonfigurationsdatei ist eine Momentaufnahme einer ehemaligen Startkonfiguration. Die Spiegelkonfiguration bleibt beim Zurücksetzen auf die Werkseinstellungen erhalten und kann daher zum Wiederherstellen einer Systemkonfiguration nach dem Zurücksetzen auf die Werkseinstellungen verwendet werden. Dazu kopieren Sie die Spiegelkonfiguration in die Startkonfiguration.

Hinweis Sie können diese Dateien nicht nur herunterladen und in ein anderes System hochladen, sondern auch in andere Dateitypen auf dem WAP-Gerät kopieren.

Konfigurationsdateien sichern

So sichern Sie die Konfigurationsdatei auf einem Netzwerk-Host oder TFTP-Server (bzw. laden sie hoch):

Schritt 1 Wählen Sie **Administration > Konfigurationsdateien > Download/Backup** aus.

Schritt 2 Wählen Sie **TFTP** oder **HTTP/HTTPS** als Übertragungsmethode aus.

Schritt 3 Wählen Sie **Backup (Access Point zu PC)** aus, um die Konfigurationsdaten auf dem PC zu sichern.

Schritt 4 Geben Sie für eine TFTP-Sicherung den Zieldateinamen mit der Erweiterung „.xml“ ein. Geben Sie dabei auch den Pfad an, unter dem Sie die Datei auf dem Server speichern möchten. Geben Sie dann die IPv4-Adresse des TFTP-Servers ein.

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * sowie zwei oder mehr aufeinanderfolgende Punkte.

Schritt 5 Bei einer TFTP-Sicherung geben Sie die IPv4-Adresse des TFTP-Servers ein.

Schritt 6 Wählen Sie die Konfigurationsdatei aus, die Sie sichern möchten:

- **Startkonfiguration**: Der beim letzten Start des WAP-Geräts verwendete Konfigurationsdateityp. Diese Datei enthält keine angewendeten Konfigurationsänderungen, die noch nicht im WAP-Gerät gespeichert sind.
- **Backup-Konfiguration**: Der im WAP-Gerät gespeicherte Backup-Konfigurationsdateityp.
- **Spiegelkonfiguration**: Wenn die Startkonfiguration mindestens 24 Stunden lang nicht geändert wurde, wird sie automatisch als Spiegelkonfigurationsdatei gespeichert. Die Spiegelkonfiguration ist eine Momentaufnahme einer ehemaligen Startkonfiguration. Die Spiegelkonfiguration bleibt beim Zurücksetzen auf die Werkseinstellungen erhalten und kann daher zum Wiederherstellen einer Systemkonfiguration nach dem Zurücksetzen auf die Werkseinstellungen verwendet werden. Dazu kopieren Sie die Spiegelkonfiguration in die Startkonfiguration.

Schritt 7 Klicken Sie auf **"Speichern"**, um mit der Sicherung zu starten. Bei HTTP/HTTPS-Sicherungen wird ein Fenster angezeigt, in dem Sie zum gewünschten Speicherort für die Datei navigieren können.

Herunterladen von Konfigurationsdateien

Sie können eine Datei auf das WAP-Gerät herunterladen, um die Konfiguration zu aktualisieren oder um eine zuvor gesicherte Konfiguration auf dem WAP-Gerät wiederherzustellen.

So laden Sie eine Konfigurationsdatei auf das WAP-Gerät herunter:

Schritt 1 Wählen Sie **Administration > Konfigurationsdateien > Download/Backup** aus.

Schritt 2 Wählen Sie **TFTP** oder **HTTP/HTTPS** als Übertragungsmethode aus.

Schritt 3 Wählen Sie **Download (PC zu Access Point)** aus, um die Konfigurationsdaten auf dem PC zu sichern.

Schritt 4 Geben Sie für eine TFTP-Sicherung den Zieldateinamen mit der Erweiterung „.xml“ ein. Geben Sie dabei auch den Pfad an, unter dem Sie die Datei auf dem Server speichern möchten. Geben Sie dann die IPv4-Adresse des TFTP-Servers ein.

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * sowie zwei oder mehr aufeinanderfolgende Punkte.

Schritt 5 Wählen Sie **Startkonfiguration** oder **Backup-Konfiguration** aus, um die Datei durch die heruntergeladene Datei zu ersetzen.

Wenn die Startkonfigurationsdatei mit der heruntergeladenen Datei überschrieben und die Gültigkeit der Datei erfolgreich überprüft wurde, wird die heruntergeladene Konfiguration beim nächsten Neustart des WAP-Geräts wirksam.

Schritt 6 Klicken Sie auf **Speichern**, um das Upgrade bzw. die Sicherung zu starten. Bei HTTP/HTTPS-Downloads wird ein Fenster angezeigt, in dem Sie die herunterzuladende Datei auswählen können.

Vorsicht Die Stromversorgung des WAP-Geräts darf beim Herunterladen der Konfigurationsdatei nicht unterbrochen werden. Wenn beim Herunterladen der Konfigurationsdatei der Strom ausfällt, geht die Datei verloren, und Sie müssen den Vorgang neu starten.

Kopieren von Konfigurationsdateien

Sie können Dateien innerhalb des Dateisystems auf dem WAP-Gerät kopieren. Sie können beispielsweise die Backup-Konfigurationsdatei in die Startkonfigurationsdatei kopieren, damit sie beim nächsten Start des WAP-Geräts verwendet wird.

So kopieren Sie eine Datei in einen anderen Dateityp:

Schritt 1 Wählen Sie **Administration > Konfigurationsdateien > Kopieren** aus.

Schritt 2 Wählen Sie im Feld „Kopieren von“ einen der folgenden Quelldateitypen für den Kopiervorgang aus:

- **Startkonfiguration**: Die beim Systemstart verwendete Konfigurationsdatei.
- **Backup-Konfiguration**: Die auf dem WAP-Gerät gespeicherte Backup-Konfigurationsdatei.
- **Spiegelkonfiguration**: Wenn die Startkonfiguration mindestens 24 Stunden lang nicht geändert wurde, wird sie automatisch als Spiegelkonfigurationsdatei gespeichert. Die Spiegelkonfiguration ist eine Momentaufnahme einer ehemaligen Startkonfiguration. Die Spiegelkonfiguration bleibt beim Zurücksetzen auf die Werkseinstellungen erhalten und kann daher zum Wiederherstellen einer Systemkonfiguration nach dem Zurücksetzen auf die Werkseinstellungen verwendet werden. Dazu kopieren Sie die Spiegelkonfiguration in die Startkonfiguration.

Schritt 3 Wählen Sie im Feld „Ziel“ den Dateityp aus, den Sie durch die kopierte Datei ersetzen möchten.

Schritt 4 Klicken Sie auf **Speichern**, um den Kopiervorgang zu starten.

Löschen von Konfigurationsdateien

Sie können die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei löschen. Wenn Sie die Startkonfigurationsdatei löschen, wird die Backup-Konfigurationsdatei beim nächsten Neustart des WAP-Geräts aktiv.

So löschen Sie die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei:

Schritt 1 Wählen Sie **Administration > Konfigurationsdateien > Löschen** aus.

Schritt 2 Wählen Sie **Startkonfiguration** oder **Backup-Konfiguration** aus.

Schritt 3 Klicken Sie auf **Dateien löschen**.

Schritt 4 Klicken Sie auf **OK**.

Neustart

Auf der Seite „Neustart“ können Sie das WAP-Gerät neu starten oder auf die Werkseinstellungen zurücksetzen. Gehen Sie wie folgt vor, um das WAP-Gerät zurückzusetzen:

Schritt 1 Wählen Sie **Administration > Neustart** aus.

Schritt 2 Klicken Sie auf **Werkseinstellungen wiederherstellen**, um das WAP-Gerät mit der Standard-Konfigurationsdatei neu zu starten. Alle angepassten Einstellungen gehen verloren.

Schritt 3 Klicken Sie auf **Neu starten**. Es wird ein Fenster angezeigt, in dem Sie den Neustart bestätigen oder abbrechen können.

Schritt 4 Klicken Sie auf **OK**, um das Gerät neu zu starten.

Neustart planen

Führen Sie die folgenden Schritte aus, um einen Neustart auf dem WAP-Gerät zu planen:

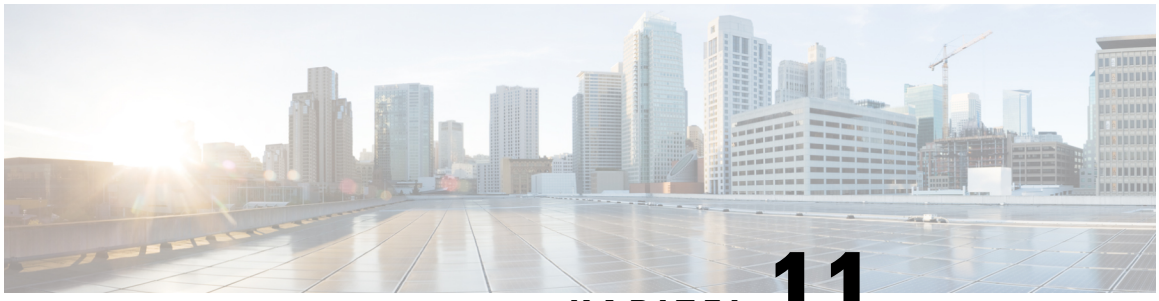
Schritt 1 Klicken Sie auf das Kontrollkästchen **Neustart planen**, um die Funktion zum Planen von Neustarts zu aktivieren.

Schritt 2 Sie können einen Neustart auf zwei Arten planen.

- **Datum**: Legen Sie das Datum und die Uhrzeit fest, zu denen das Gerät neu gestartet werden soll.
- **In**: Legen Sie die Zeit für den Neustart so fest, dass der Neustart nach dem Aktivieren der Funktion durchgeführt wird.

Hinweis Mit der Option **In** ist der Plan für den Neustart nach dem Neustart weiterhin aktiv.

Schritt 3 Klicken Sie auf **Speichern**.



KAPITEL 11

Problembehandlung

In diesem Kapitel wird beschrieben, wie Sie die Paketerfassung auf mehreren WAP-Geräten für die Fehlersuche konfigurieren. Das Kapitel enthält die folgenden Themen:

Spektruminformationen

Die Seite „Spektruminformationen“ zeigt den Status der Spektrumanalysator-Funktion an und stellt den Link zum Anzeigen der Spektrumdaten bereit. Die folgende Seite enthält ausführlichere Informationen über den Spektrumanalysator.

Spektrumanalysemodus aktivieren: Der Spektrumanlaysemodus ist entweder „Dedizierte Spektrumanalyse“ oder „Hybrid-Spektrumanalyse“ oder „3+1-Spektrumanalyse“.

Schritt 1 Wählen Sie **Problembehandlung** > **Spektruminformationen**

Schritt 2 Wählen Sie die Funkschnittstelle aus, und klicken Sie dann auf die Schaltfläche **Festlegen**, um die Spektruminformationen zu starten.

Schritt 3 Klicken Sie auf **Spektrumdaten anzeigen**, um die Details zur **Kanalqualität** und zur **Nutzung des Nicht-WLAN-Kanals** anzuzeigen.

Spektrumdaten anzeigen: Hiermit wird der Spektrum-Viewer gestartet, wenn als Scanmodus „Dedizierte Spektrumanalyse“ oder „Hybrid-Spektrumanalyse“ oder „3+1-Spektrumanalyse“ ausgewählt ist, der Funkstatus auf „Ein“ eingestellt ist und nur über eine IPv4-Adresse auf die Webseite zugegriffen wird.

Schritt 4 Klicken Sie auf **Stoppen**, um den Status „Spektrumanalyse-Modus“ zu deaktivieren.

Paketerfassung

Mit der WLAN-Paketerfassung können Sie vom WAP-Gerät empfangene und gesendete Pakete erfassen und speichern. Sie können die erfassten Pakete mit einem Analyseprogramm für Netzwerkprotokolle analysieren, um Fehler zu beheben oder die Leistung zu optimieren.

Es gibt zwei Methoden für die Paketerfassung:

- **Lokale Erfassungsmethode**: Die erfassten Pakete werden in einer Datei auf dem WAP-Gerät gespeichert. Die Datei kann vom WAP-Gerät an einen TFTP-Server übertragen werden. Die Datei liegt im PCAP-Format vor und kann mit Wireshark untersucht werden. Klicken Sie auf **Datei auf diesem Gerät speichern**, um die lokale Erfassungsmethode auszuwählen.
- **Remote-Erfassungsmethode**: Die erfassten Pakete werden in Echtzeit an einen externen Computer weitergeleitet, auf dem Wireshark läuft. Klicken Sie auf **Streaming auf einen Remote-Host**, um die Remote-Erfassungsmethode auszuwählen.

  Erfasste Pakete könnten in Echtzeit an CloudShark, einer webbasierten Seite für die Paketentschlüsselung und -analyse, weitergeleitet werden. Sie ist der Wireshark-UI für Paketanalysen sehr ähnlich. Sie können **Auf CloudShark streamen** anklicken, um die Remoteerfassungsmethode auszuwählen.

Die folgenden Pakettypen können im WAP-Gerät erfasst werden:

- Auf den Funkschnittstellen empfangene und gesendete 802.11-Pakete. Auf den Funkschnittstellen erfasste Pakete enthalten den 802.11-Header.
- Auf der Ethernet-Schnittstelle empfangene und gesendete 802.3-Pakete.
- Auf den internen logischen Schnittstellen wie beispielsweise VAPs und WDS-Schnittstellen empfangene und gesendete 802.3-Pakete.

Auf der Seite „Paketerfassung“ können Sie die Parameter für die Paketerfassung konfigurieren, eine lokale oder Remotepaketerfassung starten, den aktuellen Status der Paketerfassung abrufen und eine Paketerfassungsdatei herunterladen.

Lokale Paketerfassung

So initiieren Sie eine lokale Paketerfassung:

Schritt 1 Wählen Sie **Problembehandlung > Paketerfassung** aus.

Schritt 2 Stellen Sie sicher, dass unter „Paketerfassungsmethode“ die Option **Datei auf diesem Gerät speichern** ausgewählt ist.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

- **Schnittstelle**: Geben Sie einen Erfassungsschnittstellentyp für die Paketerfassung ein:
  - **Ethernet**: 802.3-Datenverkehr auf dem Ethernet-Port.
  - **Funkmodul 1/Funkmodul 2**: 802.11-Datenverkehr auf der Funkschnittstelle.
- **Dauer**: Geben Sie die Dauer der Erfassung in Sekunden ein. Möglich sind Werte im Bereich von 10 bis 3600. Die Standardeinstellung ist 60.
- **Maximale Dateigröße**: Geben Sie die maximal zulässige Größe für die Erfassungsdatei in Kilobyte (KB) ein. Möglich sind Werte im Bereich von 64 bis 4096. Die Standardeinstellung ist 1024.

Schritt 4 Es gibt zwei Methoden für die Paketerfassung:

- **Sämtlicher WLAN-Datenverkehr**: Erfasst alle WLAN-Pakete.

- **Datenverkehr von/zu diesem AP**: Erfasst die von diesem AP gesendeten oder empfangenen Pakete.

Schritt 5 Klicken Sie auf **Filter aktivieren**. Sie haben drei Kontrollkästchen zur Auswahl (**Beacons ignorieren, Nach Client filtern, Nach SSID filtern**).

- **Beacons ignorieren**: Aktiviert oder deaktiviert die Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder gesendet wurden.
- **Nach Client filtern**: Gibt die MAC-Adresse für den WLAN-Clientfilter an. Der Clientfilter ist nur aktiv, wenn eine Erfassung an einer 802.11-Schnittstelle ausgeführt wird.
- **Nach SSID filtern**: Wählen Sie einen SSID-Namen für die Paketerfassung aus.

Schritt 6 Klicken Sie auf **Einstellungen speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Schritt 7 Klicken Sie auf **Erfassung starten** und anschließend auf **Aktualisieren**, um den **Paketerfassungsstatus** abzurufen, der die folgenden Daten enthält:

a) **Aktueller Erfassungsstatus**
b) **Paketerfassungszeit**
c) **Größe der Paketerfassungsdatei**

Im Modus „Paketdateierfassung“ werden erfasste Pakete im RAM-Dateisystem des WAP-Geräts gespeichert. Bei der Aktivierung wird die Paketerfassung fortgesetzt, bis eines der folgenden Ereignisse eintritt:

- Die konfigurierte Dauer für die Erfassung ist erreicht.
- Die maximale Größe der Erfassungsdatei ist erreicht.
- Der Administrator beendet die Erfassung.

Remotepaketerfassung

Mit der Funktion für die Remoteerfassung können Sie einen Remote-Port als Ziel für Paketerfassungen angeben. Diese Funktion wird in Verbindung mit dem Wireshark-Netzwerkanalysetool für Windows verwendet. Im WAP-Gerät wird ein Paketerfassungsserver ausgeführt, der die erfassten Pakete über eine TCP-Verbindung an das Wireshark-Tool sendet. Wireshark ist ein kostenloses Open Source-Tool, das Sie unter https://www.wireshark.org/ herunterladen können.

Den erfassten Verkehr können Sie mit einem Microsoft Windows-Computer, auf dem das Wireshark-Tool ausgeführt wird, anzeigen, protokollieren und analysieren. Die Remotepaketerfassung ist eine Standardfunktion des Wireshark-Tools für Windows. Die Linux-Version kann nicht für das WAP-Gerät verwendet werden.

Im Remoteerfassungsmodus werden die erfassten Daten nicht lokal im Dateisystem des WAP-Geräts gespeichert.

Wenn zwischen dem Wireshark-Computer und dem WAP-Gerät eine Firewall installiert ist, muss der Verkehr für diese Ports die Firewall passieren können. Außerdem muss die Firewall so konfiguriert sein, dass auf dem Wireshark-Computer eine TCP-Verbindung mit dem WAP-Gerät initiiert werden kann.

Auf Remotehost streamen

So initiieren Sie auf einem WAP-Gerät eine Remoteerfassung mit der Option „Auf Remotehost streamen“:

Schritt 1 Wählen Sie **Problembehandlung > Paketerfassung** aus.

Schritt 2 Klicken Sie unter **Paketerfassungsmethode** auf das Optionsfeld **Streaming auf einen Remote-Host**.

Schritt 3 Wählen Sie im Feld „Remoterfassungsport“ den Standardport 2002 aus, oder geben Sie ggf. die gewünschte Portnummer für die Verbindung zwischen Wireshark und dem WAP-Gerät ein. Möglich sind Ports im Bereich von 1025 bis 65530.

Schritt 4 Es gibt zwei Methoden für die Paketerfassung:

- **Sämtlicher WLAN-Datenverkehr**: Erfasst alle übertragenen WLAN-Pakete.
- **Datenverkehr von/zu diesem AP**: Erfasst die von diesem AP gesendeten oder empfangenen Pakete.

Schritt 5 Aktivieren Sie anschließend die Option **Filter aktivieren**. Wählen Sie anschließen unter den folgenden Optionen:

- **Beacons ignorieren**: Aktiviert oder deaktiviert die Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder gesendet wurden.
- **Nach Client filtern**: Gibt die MAC-Adresse für den WLAN-Clientfilter an. Der Clientfilter ist nur aktiv, wenn eine Erfassung an einer 802.11-Schnittstelle ausgeführt wird.
- **Nach SSID filtern**: Wählen Sie einen SSID-Namen für die Paketerfassung aus.

Schritt 6 Wenn Sie die Einstellungen zur späteren Verwendung speichern möchten, klicken Sie auf **Speichern**. Die Auswahl von „Remote“ als Paketerfassungsmethode wird jedoch nicht gespeichert.

Schritt 7 Klicken Sie auf **Erfassung starten**, um die Erfassung zu starten. Klicken Sie auf **Erfassung stoppen**, um die Erfassung zu beenden.

Auf CloudShark streamen

Um auf einem WAP-Gerät eine Remoteerfassung mit der Option **Auf CloudShark streamen** zu initiieren, gehen Sie wie folgt vor:

Schritt 1 Wählen Sie **Fehlerbehebung > Paketerfassung** aus.

Schritt 2 Zur Auswahl der **Paketerfassungsmethode** klicken Sie auf die Optionsschaltfläche **Auf CloudShark streamen**.

Schritt 3 Konfigurieren Sie die folgenden Parameter:

a) Schnittstelle – Geben Sie für die Paketerfassung einen Erfassungsschnittstellentyp ein.
b) Ethernet – 802.3-Datenverkehr am Ethernet-Port
c) Funkmodul 1 (5 GHz)/Funkmodul 2 (2,4 GHz) – 802.11-Datenverkehr auf der Funkschnittstelle
d) Erfassungsdauer – Geben Sie Die Dauer der Erfassung in Sekunden ein. Von CloudShark gibt es keine Einschränkung der Dauer. Die Standardeinstellung ist 60.
e) Max. Dateigröße – Geben Sie die maximal zulässige Größe für die Erfassungsdatei in Kilobyte (kB) ein. Eine Größenbeschränkung gibt es hier nicht. Die Standardeinstellung ist 1024.

Hinweis Für CloudShark gibt es zwei gültige Kontotypen: privat und geschäftlich. Die maximale Größe für ununterbrochene Uploads auf das private Konto beträgt 25 MB, auf das geschäftliche Konto 150 MB. CloudShark kürzt übergroße Teile auf Basis des Kontotyps.

f) CloudShark-URL – Geben Sie den Hostnamen von CloudShark ein. Die standardmäßige URL lautet: https://www.cloudshark.org

g) API-Schlüssel von CloudShark – Geben Sie den gültigen API-Token ein, den Sie für CloudShark registriert haben.

Schritt 4 Die Kommunikation mit CloudShark erfolgt über HTTPS. Wenn Sie ein selbstsigniertes SSL-Zertifikat verwenden möchten, wählen Sie die Option Ja und klicken auf **Zertifikat hochladen**, um das von Ihnen signierte Zertifikat hochzuladen.

Schritt 5 Geben Sie im Feld „Filterausdruck“ die Protokolle ein, die Sie erfassen möchten. Nur diese Pakete werden nach dem Filtern an CloudShark übertragen.

Schritt 6 Für die Paketerfassung gibt es zwei Methoden:

a) **Sämtlicher WLAN-Verkehr** – Erfassen Sie alle Wireless-Pakete.

b) **Datenverkehr an/von diesem AP** – Erfassen Sie das Paket, das vom AP gesendet oder empfangen wurde.

Schritt 7 Klicken Sie auf **Filter aktivieren**. Die folgenden drei Optionen stehen zur Verfügung:

a) **Beacons ignorieren** – Aktiviert oder deaktiviert die Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder gesendet wurden.

b) **Nach Client filtern** – Gibt die MAC-Adresse für den WLAN-Clientfilter an.

Hinweis Der Clientfilter ist nur aktiv, wenn eine Erfassung an einer 802.11-Schnittstelle ausgeführt wird.

c) **Nach SSID filtern** – Wählt einen SSID-Namen für die Paketerfassung aus.

Schritt 8 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Schritt 9 Klicken Sie auf **Erfassung starten**. Im Paketerfassungsmodus werden die erfassten Pakete in Echtzeit an CloudShark übertragen. Bei der Aktivierung wird die Paketerfassung fortgesetzt, bis eines der folgenden Ereignisse eintritt:

a) Die Erfassungszeit erreicht den konfigurierten Wert.

b) Die Erfassungsdatei erreicht die maximale Größe.

c) Der Administrator beendet die Erfassung.

Wireshark

Laden Sie Wireshark zuerst herunter, und installieren Sie es auf Ihrem Computer. Sie können Wireshark von https://www.wireshark.org/ herunterladen.

Gehen Sie wie folgt vor, um das Wireshark-Netzwerkanalysetool für Microsoft Windows zu initiieren:

Schritt 1 Initiieren Sie auf dem Ihrem Computer das Wireshark-Tool.

Schritt 2 Klicken Sie im Menü auf **Erfassung > Optionen**. Daraufhin wird ein Popup-Fenster angezeigt.

Schritt 3 Wählen Sie im Feld „Schnittstelle“ die Option **Remote**. Daraufhin wird ein Popup-Fenster angezeigt.

Schritt 4 Geben Sie im Feld „Host“ die IP-Adresse des WAP-Geräts ein.

Schritt 5 Geben Sie im Feld „Port“ die Portnummer des WAP-Geräts ein. Geben Sie beispielsweise „2002“ ein, wenn Sie den Standardport verwenden, oder geben Sie, wenn Sie nicht den Standardport verwenden, die Portnummer ein.

Schritt 6 Klicken Sie auf **OK**.

Schritt 7 Wählen Sie die Schnittstelle aus, an der Sie die Pakete erfassen möchten. Das Wireshark-Popup-Fenster enthält neben der IP-Adresse ein Dropdown-Menü, in dem Sie die Schnittstellen auswählen können. Folgende Schnittstellen sind möglich:

Linux bridge interface in the wap device

```
--rpcap://[192.168.1.220]:2002/brtrunk
```

Wired LAN interface

```
-- rpcap://[192.168.1.220]:2002/eth0
```

VAP0 traffic on radio 1

```
-- rpcap://[192.168.1.220]:2002/wlan0
```

802.11 traffic

```
-- rpcap://[192.168.1.220]:2002/radio1
```

At WAP361, VAP1 ~ VAP7 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
```

At WAP150, VAP1 ~ VAP3 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3
```

Sie können bis zu vier Schnittstellen im WAP-Gerät gleichzeitig verfolgen. Sie müssen jedoch für jede Schnittstelle eine separate Wireshark-Sitzung starten. Um weitere Remote-Erfassungssitzungen zu initiieren, wiederholen Sie die Wireshark-Konfigurationsschritte. Auf dem WAP-Gerät ist keine Konfiguration erforderlich.

Hinweis Das System verwendet vier fortlaufende Portnummern, beginnend mit dem konfigurierten Port für die Remotepaketerfassungssitzungen. Vergewissern Sie sich, dass vier fortlaufende Portnummern verfügbar sind. Wenn Sie nicht den Standardport verwenden, sollten Sie eine höhere Portnummer als 1024 verwenden.

Wenn Sie den Verkehr an der Funkschnittstelle erfassen, können Sie die Beacon-Erfassung deaktivieren. Andere 802.11-Control Frames werden dennoch an Wireshark gesendet. Sie können einen Anzeigefilter einrichten, um nur Folgendes anzuzeigen:

- Daten-Frames in der Verfolgung
- Verkehr für bestimmte BSSIDs (Basic Service Set IDs)
- Verkehr zwischen zwei Clients

Beispiele für hilfreiche Anzeigefilter:

- Ausschließen von Beacons und ACK-, RTS- bzw. CTS-Frames:

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

- Nur Daten-Frames:

  wlan.fc.type == 2

- Verkehr für eine bestimmte BSSID:

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

- Gesamter Verkehr zu und von einem bestimmten Client:

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

Im Remoteerfassungsmodus wird der Verkehr über eine der Netzwerkschnittstellen an den Computer gesendet, auf dem Wireshark ausgeführt wird. Abhängig vom Speicherort des Wireshark-Tools kann der Verkehr über eine Ethernet-Schnittstelle oder über eines der Funkmodule gesendet werden. Das WAP-Gerät installiert automatisch einen Erfassungsfilter zum Herausfiltern aller an die Wireshark-Anwendung gerichteten Pakete, um eine

Verkehrs-Flood aufgrund der Paketverfolgung zu verhindern. Wenn beispielsweise für Wireshark der IP-Port 58000 konfiguriert ist, wird automatisch der folgende Erfassungsfilter im WAP-Gerät installiert:

not port range 58000-58004

Aufgrund von Leistungs- und Sicherheitsproblemen wird der Paketerfassungsmodus nicht im NVRAM auf dem WAP-Gerät gespeichert. Wenn das WAP-Gerät zurückgesetzt wird, wird der Erfassungsmodus deaktiviert. Sie müssen ihn dann wieder aktivieren, um mit der Erfassung des Datenverkehrs fortfahren zu können. Die Paketerfassungsparameter (mit Ausnahme des Modus) werden im NVRAM gespeichert.

Das Aktivieren der Paketerfassungsfunktion kann zu einem Sicherheitsproblem führen: Nicht autorisierte Clients können möglicherweise eine Verbindung mit dem WAP-Gerät herstellen und Benutzerdaten verfolgen. Außerdem wird die Leistung des WAP-Geräts durch die Paketerfassung beeinträchtigt. Zu dieser Beeinträchtigung kommt es in geringerem Ausmaß auch dann, wenn keine Wireshark-Sitzung aktiv ist. Sie können die Leistungsbeeinträchtigung für das WAP-Gerät während der Verkehrserfassung minimieren, indem Sie Erfassungsfilter installieren, um den an das Wireshark-Tool gesendeten Verkehr zu begrenzen. Bei der Erfassung von 802.11-Verkehr handelt es sich bei einem großen Teil der erfassten Frames oft um Beacons (die in der Regel alle 100 ms von allen APs gesendet werden). Wireshark unterstützt zwar einen Anzeigefilter für Beacon-Frames, jedoch keinen Erfassungsfilter, mit dem Sie die Weiterleitung erfasster Beacon-Pakete an das Wireshark-Tool verhindern können. Deaktivieren Sie den Beacon-Erfassungsmodus, um die Leistungsbeeinträchtigung durch die Erfassung der 802.11-Beacons zu verringern.

Paketerfassungsdatei herunterladen

Sie können eine Erfassungsdatei über TFTP auf einen konfigurierten TFTP-Server oder über HTTP/HTTPS auf einen Computer herunterladen. Beim Auslösen des Befehls zum Herunterladen einer Paketerfassungsdatei wird die Erfassung automatisch beendet.

Da sich die Erfassungsdatei im RAM-Dateisystem befindet, wird sie beim Zurücksetzen des WAP-Geräts gelöscht.

So laden Sie eine Paketerfassungsdatei über TFTP herunter:

Schritt 1 Klicken Sie auf **Auf TFTP-Server herunterladen**.

Schritt 2 Geben Sie in das Feld die IPv4-Adresse des TFTP-Servers ein.

Schritt 3 Geben Sie den TFTP-Server-Dateiname, um eine vom Standard abweichende Datei herunterzuladen. Standardmäßig werden die erfassten Pakete im WAP-Gerät in der Datei "/tmp/apcapture.pcap" gespeichert.

Schritt 4 Klicken Sie auf **Herunterladen**.

Verwenden von HTTP

So laden Sie eine Paketerfassungsdatei über HTTP herunter:

Schritt 1 Klicken Sie auf **Auf dieses Gerät herunterladen**. Eine Pop-up-Meldung zur Bestätigung wird angezeigt.

Schritt 2 Klicken Sie auf **OK**. In einem Pop-up-Dialogfeld können Sie einen Netzwerkspeicherort zum Speichern der Datei auswählen.

Supportinformationen

Auf der Seite mit den Supportinformationen wird der Status der CPU und des RAM angezeigt.

Gehen Sie wie folgt vor, um die CPU-/RAM-Aktivität aufzuzeichnen und anzuzeigen:

Schritt 1 Wählen Sie **Problembehandlung > Supportinformationen** aus.

Schritt 2 Klicken Sie auf **CPU**: Das Gerät zum Aufzeichnen und Anzeigen der CPU-Aktivität. Um die Aufzeichnung zu stoppen, klicken Sie erneut auf **CPU**.

Schritt 3 Klicken Sie auf **RAM**: Das Gerät zum Aufzeichnen und Anzeigen der RAM-Aktivität. Um die Aufzeichnung zu stoppen, klicken Sie erneut auf **RAM**.

Im Diagramm wird der CPU-/RAM-Status wie folgt angezeigt:

- Eine blaue Linie stellt die CPU-Aktivität dar.
- Eine rote Linie stellt die RAM-Aktivität dar.
- Das erste Liniendiagramm aktualisiert die Daten jede Sekunde. Es zeigt die CPU-/RAM-Aktivität im Zeitraum von 60 Sekunden an.
- Das zweite Liniendiagramm aktualisiert die Daten all fünf Sekunden. Es zeigt die CPU-/RAM-Aktivität im Zeitraum von fünf Minuten an.

Schritt 4 Klicken Sie auf **Speichern**.

CPU/RAM-Daten herunterladen

Auf der Seite „Supportinformationen“ können Sie die CPU/RAM-Aktivität für den ausgewählten Zeitraum herunterladen. Anschließend können Sie die Textdatei Mitarbeitern des technisches Supports als Unterstützung bei der Fehlerbehebung zur Verfügung stellen. Gehen Sie wie folgt vor, um die CPU/RAM-Daten herunterzuladen:

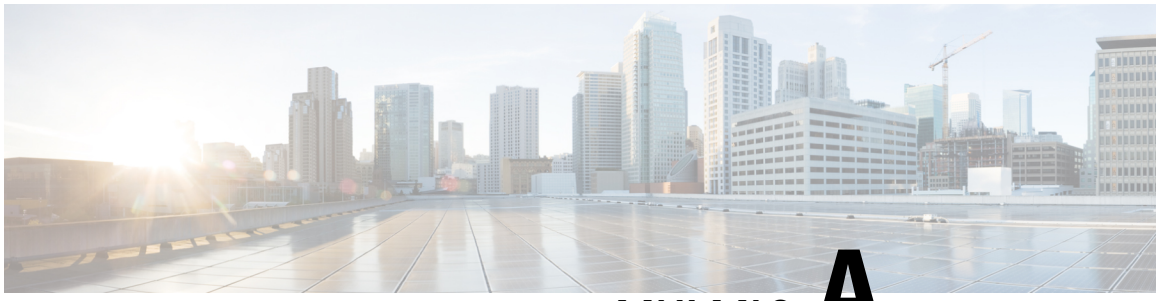
Schritt 1 Wählen Sie **Problembehandlung > Supportinformationen** aus.

Schritt 2 Klicken Sie im Bereich „Daten herunterladen“ auf **Aktivieren**, um den Download zu aktivieren.

Schritt 3 Wählen Sie den Zeitraum aus, für den Sie die Daten herunterladen möchten: **Heute, Letzte 7 Tage, Letzte 30 Tage, Alles, Benutzerdefiniert**.

Schritt 4 Füllen Sie die Felder **Von** und **Bis** im Format jjjj-mm-tt aus, und geben Sie die Uhrzeit im Format hh:mm:ss an.

Schritt 5 Klicken Sie auf **Herunterladen**, um die Datei für die aktuellen Systemeinstellungen zu generieren. Nach einer kurzen Pause wird ein Fenster angezeigt, in dem Sie die Datei auf dem Computer speichern können.



ANHANG A

Ursachencodes für Deauthentifizierungsnachrichten

Dieser Anhang enthält die folgenden Abschnitte:

Ursachencodes für Deauthentifizierungsnachrichten

Bei der Deauthentifizierung eines Clients gegenüber dem WAP-Gerät wird eine Nachricht an das Systemprotokoll gesendet. Die Nachricht enthält einen Ursachencode, mit dessen Hilfe Sie möglicherweise leichter ermitteln können, warum ein Client deauthentifiziert wurde. Sie können Protokollnachrichten anzeigen, wenn Sie auf **Systemkonfiguration** > **Benachrichtigung** > **Systemprotokoll anzeigen** klicken.

Weitere Informationen finden Sie unter Tabelle mit Ursachencodes für Deauthentifizierungen, auf Seite 129.

Tabelle mit Ursachencodes für Deauthentifizierungen

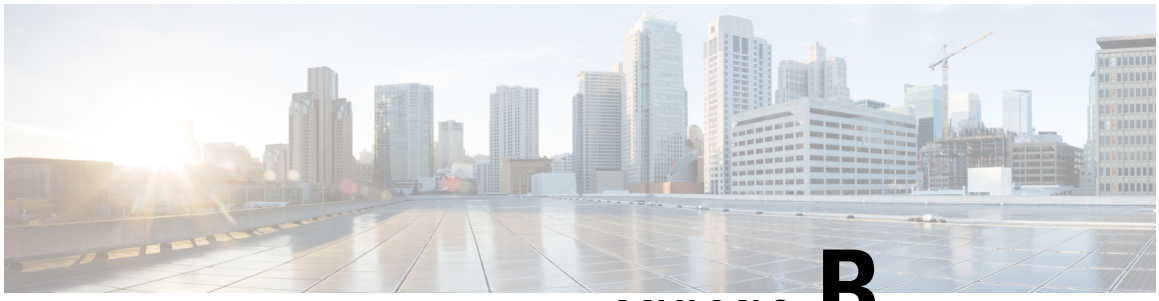
In der folgenden Tabelle werden die Ursachencodes für Deauthentifizierungen beschrieben.

Tabelle 4: Tabelle mit Ursachencodes für Deauthentifizierungen

Ursachencode	Bedeutung
0	Reserviert
1	Nicht angegebene Ursache
2	Die vorherige Authentifizierung ist nicht mehr gültig.
3	Der Client wurde deauthentifiziert, da die sendende Station (STA) den IBSS (Independent Basic Service Set) oder ESS verlassen hat oder verlässt.
4	Die Zuordnung wurde aufgrund von Inaktivität aufgehoben.
5	Die Zuordnung wurde aufgehoben, da das WAP-Gerät nicht alle zurzeit zugeordneten STAs verarbeiten kann.

Ursachencodes für Deauthentifizierungsnachrichten

Ursachencode	Bedeutung
6	Es wurde ein Klasse-2-Frame von einer nicht authentifizierten STA empfangen.
7	Es wurde ein Klasse-3-Frame von einer nicht zugeordneten STA empfangen.
8	Die Zuordnung wurde aufgehoben, da die sendende STA den BSS (Basic Service Set) verlassen hat oder verlässt.
9	Die STA, die die (erneute) Zuordnung anfordert, ist gegenüber der antwortenden STA nicht authentifiziert.
10	Die Zuordnung wurde aufgehoben, da die Informationen im Power Capability-Element nicht akzeptabel sind.
11	Die Zuordnung wurde aufgehoben, da die Informationen im Supported Channels-Element nicht akzeptabel sind.
12	Reserviert
13	Ungültiges Element, das heißt ein in diesem Standard definiertes Element, dessen Inhalt nicht den Angaben in Clause 8 entspricht.
14	Fehler im Nachrichtenintegritätscode (Message Integrity Code, MIC)
15	Timeout beim Vier-Wege-Handshake
16	Timeout beim Gruppenschlüssel-Handshake
17	Ein Element im Vier-Wege-Handshake stimmt nicht mit der (erneuten) Zuordnungsanfrage, der Anfrageantwort oder dem Beacon-Frame überein.
18	Ungültige Gruppenverschlüsselung
19	Ungültige paarweise Verschlüsselung
20	Ungültiges AKMP
21	Nicht unterstützte RSNE-Version
22	Ungültige RSNE-Funktionen
23	IEEE 802.1x-Authentifizierung fehlgeschlagen
24	Verschlüsselungssuite aufgrund der Sicherheitsrichtlinien abgelehnt



ANHANG B

Weitere Informationen

Der Abschnitt enthält die folgenden Themen:

Weitere Informationen

Support

Cisco Support Community	http://www.cisco.com/go/smallbizsupport
Cisco Support und Ressourcen	http://www.cisco.com/go/smallbizhelp
Telefonsupport-Kontakte	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
Cisco Firmware-Downloads	http://www.cisco.com/go/smallbizfirmware Wählen Sie einen Link aus, um die Firmware für Ihr Cisco-Produkt herunterzuladen. Es ist keine Anmeldung erforderlich.
Cisco Open Source-Anfragen	Um ein Exemplar des Quellcodes zu erhalten, zu dem Sie im Rahmen der entsprechenden kostenlosen/Open Source-Lizenz(en) (beispielsweise GNU Lesser/General Public License) berechtigt sind, senden Sie eine Anfrage an: external-opensource-requests@cisco.com. Geben Sie in Ihrer Anfrage bitte den Namen und die Version des Cisco Produkts sowie die 18-stellige Referenznummer an (zum Beispiel: 7XEEX17D99-3X49X08 1), die Sie in der Open Source-Dokumentation des Produkts finden.
Cisco WAP581 – Administratorhandbuch	http://www.cisco.com/go/500_wap_resources
Cisco Netzteile	http://www.cisco.com/go/wap_accessories

Weitere Informationen